Vorblatt

1. Problem:

Die fortschreitende Nutzung von Informations- und Kommunikationstechnologien stellt die moderne globale Gesellschaft vor große Herausforderungen. Aus diesem Grund ist es erforderlich, bestehende internationale Rechtsinstrumente zu ergänzen bzw. wirksamer zu gestalten.

2. Ziel:

Mit der Ratifikation des Übereinkommens des Europarats über Computerkriminalität, welches Österreich am 23. November 2001 in Budapest unterzeichnet hat, soll die Bedeutung der konsequenten strafrechtlichen Verfolgung krimineller Handlungen im Bereich der Computerkriminalität unterstrichen werden.

3. Inhalt, Problemlösung:

Das Übereinkommen enthält einerseits materielle Straftatbestände, welche von den Unterzeichnerstaaten ins nationale Recht umzusetzen sind, andererseits umfangreiche strafprozessuale Vorschriften, die der Durchsetzung des Strafanspruchs dienen sollen. Die strafbaren Tatbestände des Übereinkommens umfassen zum Beispiel den unbefugten Zugang zu einem Computersystem (sog. „Hacking“), die Fälschung von Computerdaten sowie bestimmte Handlungen in Zusammenhang mit Kinderpornographie und Urheberrechtsverstöße. Zur Verfolgung von Verstößen gegen das Übereinkommen und anderer mittels eines Computersystems begangener Verstöße sind spezielle Befugnisse der zuständigen Behörden (u.a. umgehende Sicherung gespeicherter Computerdaten, Durchsuchung und Beschlagnahme gespeicherter Computerdaten, Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit) vorgesehen. Mit der Schaffung von harmonisierten Regelungen im Bereich der internationalen Zusammenarbeit soll insbesondere der Auslieferungs- und Rechtshilfeverkehr im Hinblick auf das Erfordernis der beiderseitigen Strafbarkeit erleichtert werden.

4. Alternativen:

Keine.

5. Auswirkungen des Regelungsvorhabens:

5.1 Finanzielle Auswirkungen:

Grundsätzlich ist festzuhalten, dass Maßnahmen mit finanziellen Implikationen nur nach Maßgabe der zur Verfügung stehenden Mittel erfolgen können. Allfällige entstehende durch die im ER - Übereinkommen angeführten Maßnahmen hervorgerufene Mehrkosten werden im jeweiligen Ressortbudget bedeckt

5.2 Wirtschaftspolitische Auswirkungen:

5.2.1 Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Eine effiziente Strafverfolgung im Bereich der Computerkriminalität trägt dazu bei, den Wirtschaftsstandort Österreich zu stärken.

5.2.2 Auswirkungen auf die Verwaltungskosten für Bürger/innen und für Unternehmen:

Keine.

5.3 Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit:

Das Regelungsvorhaben ist nicht klimarelevant.

5.4. Auswirkungen in konsumentenpolitischer sowie sozialer Hinsicht

Eine erfolgreiche Bekämpfung der Computerkriminalität trägt dazu bei, KonsumentInnen vor kriminellen Handlungen (z. B. im Rahmen der Bekämpfung des sog. „Hacking“, der Fälschung von Computerdaten, bestimmter Handlungen in Zusammenhang mit Kinderpornographie und Urheberrechtsverstöße) zu schützen.

5.5 Geschlechtsspezifische Auswirkungen:

Keine.

6. Verhältnis zu Rechtsvorschriften der Europäischen Union:

Die vorgesehenen Regelungen stehen mit dem Recht der Europäischen Union (EU) in Einklang. Unbeschadet des Ziels und Zwecks dieses Übereinkommens und seiner uneingeschränkten Anwendung gegenüber anderen Vertragsparteien wenden Vertragsparteien, die Mitglieder der Europäischen Union sind, in ihren Beziehungen untereinander die Vorschriften der Gemeinschaft und der Europäischen Union

an, soweit es für die betreffende Frage Vorschriften der Gemeinschaft oder der Europäischen Union gibt und diese auf den konkreten Fall anwendbar sind (Art. 43 Abs. 3 des Übereinkommens). Aufbauend auf dem Europaratsübereinkommen verabschiedete der Rat der Europäischen Union am 24. Februar 2005 den Rahmenbeschluss des Rates 2005/222/JI über Angriffe auf Informationssysteme (ABl. L Nr. 69 vom 16. März 2005 S. 67). Am 30. September 2010 brachte die Europäische Kommission einen Vorschlag für eine Richtlinie des Europäischen Parlamentes und des Rates über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates ein. Beim JI-Rat am 9./10. Juni 2011 wurde im Rat eine Allgemeine Ausrichtung zu dieser Richtlinie erzielt. Da das Europaratsübereinkommen über Computerkriminalität auch eine Verpflichtung zur Kriminalisierung verschiedener Verhaltensweisen im Zusammenhang mit Kinderpornographie und Computern bzw. Internet enthält (vgl. Art. 9), sei an dieser Stelle auch auf den Rahmenbeschluss 2004/68/JI des Rates vom 22. Dezember 2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie (ABl. L Nr. 13 vom 20. Jänner 2004 S. 44) verwiesen. Dieser Rahmenbeschluss wird durch die Richtlinie des Europäischen Parlamentes und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornographie und zur Aufhebung des Rahmenbeschlusses 2004/68/JI des Rates ersetzt, welche in Erster Lesung vom Europäischen Parlament (EP) am 27. Oktober 2011 und vom Rat am 15. November 2011 angenommen wurde.

7. Besonderheiten des Normerzeugungsverfahrens:

Sonderkundmachung gemäß Art. 49 Abs. 2 B-VG

Erläuterungen

Allgemeiner Teil

Das Übereinkommen über Computerkriminalität wurde im Rahmen des Europarates ausgearbeitet und gemäß dem Beschluss der Bundesregierung vom 13. November 2001 (vgl. Pkt. 26 des Beschl. Prot. Nr. 76) und der entsprechenden Ermächtigung durch den Bundespräsidenten am 23. November 2001 im Rahmen der internationalen Konferenz über Computerkriminalität in Budapest (22./23. November 2001) von Österreich unterzeichnet. Österreich hat anlässlich der Unterzeichnung keinen Vorbehalt angebracht.

Das Übereinkommen über Computerkriminalität ist das erste völkerrechtliche Instrument auf dem Gebiet der Computerkriminalität. Das Übereinkommen dient als Leitlinie für jeden Staat, der eine umfassende nationale Gesetzgebung gegen Computerkriminalität ausarbeiten möchte und bietet einen Rahmen für die internationale Zusammenarbeit zwischen den Vertragsstaaten des Übereinkommens.

Das Übereinkommen steht in Einklang mit der Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (Europäische Menschenrechtskonvention; BGBl. Nr. 210/1958). So werden zum Beispiel das Recht auf freie Meinungsäußerung und das Recht auf Privatleben gewahrt.

Das Übereinkommen sieht einerseits materielle Straftatbestände vor, die von den Unterzeichnerstaaten ins nationale Recht umzusetzen sind, andererseits ins nationale Recht umzusetzende umfangreiche strafprozessuale Vorschriften, die der Durchsetzung des Strafanspruchs dienen sollen. Die strafbaren Tatbestände des Übereinkommens umfassen zum Beispiel den unbefugten Zugang zu einem Computersystem (sog. „Hacking“), die Fälschung von Computerdaten, bestimmte Handlungen in Zusammenhang mit Kinderpornographie und Urheberrechtsverstöße. Zur Verfolgung von Verstößen gegen das Übereinkommen und anderer mittels eines Computersystems begangener Verstöße sind spezielle Befugnisse der zuständigen Behörden (u.a. umgehende Sicherung gespeicherter Computerdaten, Durchsuchung und Beschlagnahme gespeicherter Computerdaten, Erhebung von Verkehrs- und Inhaltsdaten in Echtzeit) vorgesehen. Mit der Schaffung von harmonisierten Regelungen im Bereich der internationalen Zusammenarbeit soll insbesondere der Auslieferungs- und Rechtshilfeverkehr im Hinblick auf das Erfordernis der beiderseitigen Strafbarkeit erleichtert werden.

Das Übereinkommen steht unter der Voraussetzung, dass eine Einladung durch das Ministerkomitee des Europarats ausgesprochen wird, auch Staaten offen, die nicht Mitgliedstaaten des Europarats sind. Das Übereinkommen trat objektiv am 1. Juli 2004 in Kraft.

Laut derzeitigem Stand haben 32 Staaten das Übereinkommen ratifiziert und weitere 15 Staaten unterzeichnet.

Österreich hat die wesentlichen Bestimmungen des Übereinkommens bereits umgesetzt. Trotz vergangener Reformbemühungen müssen jedoch im Hinblick auf das Übereinkommen vereinzelte Bestimmungen noch umgesetzt werden. So befindet sich das gemäß Artikel 35 des Übereinkommens genannte „24/7-Netzwerk“ in Österreich derzeit im Aufbau.

Das Übereinkommen hat gesetzändernden bzw. gesetzesergänzenden Inhalt und bedarf daher der Genehmigung des Nationalrats gemäß Artikel 50 Abs. 1 Z 1 B-VG. Es hat nicht politischen Charakter. Es ist – mit Ausnahme der Bestimmungen in Art. 1 bis 22 und Art. 35 bis 48 – nicht erforderlich, eine allfällige unmittelbare Anwendung des Abkommens im innerstaatlichen Rechtsbereich auszuschließen, hinsichtlich Art. 1 bis 22 und 35 bis 48 ist jedoch ein Beschluss gemäß Art. 50 Abs. 2 Z 3 B-VG, dass dieser Staatsvertrag durch Erlassung von Gesetzen zu erfüllen ist, erforderlich. Da durch das Übereinkommen keine Angelegenheiten des selbstständigen Wirkungsbereiches der Länder geregelt werden, bedarf es keiner Zustimmung des Bundesrates gemäß Artikel 50 Abs. 2 Z 2 B-VG.

Besonderer Teil

Zur Präambel

Die Präambel nennt den Schutz der Gesellschaft vor Computerkriminalität, u.a. durch die Annahme geeigneter Rechtsvorschriften und die Förderung der internationalen Zusammenarbeit, als Ziel der Konvention. Sie verweist auf bestehende Übereinkommen des Europarates über die Zusammenarbeit auf strafrechtlichem Gebiet und auf Empfehlungen zur zwischenstaatlichen Verbrechensbekämpfung und Telekommunikationsüberwachung.

KAPITEL I - Begriffsbestimmungen

Zu Art. 1:

Dieser Artikel enthält mehrere für das Übereinkommen bedeutende Definitionen, unter anderem die Begriffe „Computersystem“, „Computerdaten“, „Diensteanbieter“ und „Verkehrsdaten“.

Nach Art. 1 lit. a wird unter einem Computersystem eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen umschrieben, die einzeln oder zu mehreren auf der Grundlage eines Programms automatische Datenverarbeitung durchführen. Damit übereinstimmend wird der Begriff „Computersystem“ in § 74 Abs. 1 Z 8 StGB sowohl als einzelne als auch verbundene Vorrichtungen definiert, welche der automationsunterstützten Datenverarbeitung dienen.

Nach Art. 1 lit. b werden unter „Computerdaten“ jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann, definiert. Zwar verwendet das Strafgesetzbuch nicht explizit den Begriff der Computerdaten, jedoch enthält § 74 Abs. 2 StGB einen sehr weiten Datenbegriff, der sämtliche in Art. 1 lit. b erwähnte Daten, einschließlich Computerprogramme, erfasst.

Unter „Diensteanbieter“ nach Art. 1 lit. c wird jede öffentliche oder private Stelle, die es NutzerInnen ihres Dienstes ermöglicht, mit Hilfe eines Computersystems zu kommunizieren (sublit. i), oder jede andere Stelle verstanden, die für einen solchen Kommunikationsdienst oder für seine NutzerInnen Computerdaten verarbeitet oder speichert (sublit. ii). Eine gesetzliche Verankerung des Begriffs „Diensteanbieters“ findet sich sowohl in § 2 Z 1 Zugangskontrollgesetz und in § 3 Z 2 E-Commerce-Gesetz (ECG). Das Telekommunikationsgesetz (TKG 2003) verwendet den Begriff „Anbieter“ in § 92 Abs. 3 Z 1 TKG 2003. Diese verwendeten Definitionen entsprechen auch jener des Übereinkommens.

Art. 1 lit. d definiert „Verkehrsdaten“ als alle Computerdaten im Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht. Als „Verkehrsdaten“ gelten gemäß § 92 Abs. 3 Z 4 TKG 2003 jene Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zweck der Fakturierung dieses Vorgangs verarbeitet werden. Als „Verkehrsdaten“ werden insbesondere die aktive und passive Nummer des Teilnehmers/der Teilnehmerin, die Art des Endgeräts, der Tarifcode, die Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, die Art, das Datum, der Zeitpunkt und die Dauer der Verbindung oder sonstigen Nutzung, die übermittelte Datenmenge, die Leitwege, das verwendete Protokoll, das Netz, von dem die Nachricht ausgeht oder an das sie gesendet wird, das Format der Nachricht, sowie andere Zahlungsinformationen, wie Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen verstanden (vgl. EBRV 128 BlgNR XXII. GP, Seite 18).

KAPITEL II – Innerstaatlich zu treffende Maßnahmen

Zu Art. 2:

Der erste Abschnitt des Übereinkommens umfasst Regelungsbereiche des materiellen Strafrechts. Die Art. 2 bis 6 stehen unter dem Titel „Straftaten gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Computerdaten und -systemen“.

Die innerstaatliche Umsetzung des Art. 2 („Illegal access“) erfolgte durch die Einführung des § 118a StGB. § 118a StGB und erfasst jene Handlungen, die man herkömmlich als das

sog. „Hacking“ bezeichnet und stellt sohin den unerlaubten Zugang zu einem Computersystem oder zu einem Teil eines solchen unter Strafe. Art. 2 des Übereinkommens sieht auch die Möglichkeit vor, den Tatbestand einzuschränken. Es ist möglich, eine Strafbarkeit nur dann eintreten zu lassen, wenn der unerlaubte Zugriff durch Überwindung von Sicherheitssystemen erfolgt, oder wenn der Täter/die Täterin mit dem erweiterten Vorsatz oder in anderer unredlicher Absicht handelt, Computerdaten zu erhalten. Schließlich kann die Strafbarkeit auch auf vernetzte Computersysteme eingeschränkt werden. Von dieser Möglichkeit machte Österreich Gebrauch, und es wird nicht jeder widerrechtliche Zugriff auf ein Computersystem schlechthin mit Strafe bedroht. Nur derjenige/diejenige erfüllt den objektiven Tatbestand gemäß § 118a StGB, der sich den Zugriff auf ein System (oder Teile davon) dadurch verschafft, dass er spezifische Sicherheitsvorkehrungen im Computersystem verletzt. Zum anderen verlangt die subjektive Tatseite einen erweiterten Vorsatz in Form der Absichtlichkeit, der sich auf Datenspionage und auf eine gewinnbringende oder schädigende Verwendung der auszuspionierenden Daten beziehen muss.

Zu Art. 3:

Die innerstaatliche Umsetzung des Art. 3 („Illegal Interception“) erfolgte durch §§ 119 und 119a StGB. Mit Art. 3 soll eine widerrechtliche Überwachung nicht öffentlicher Übertragungen von Computerdaten zu und von Computersystemen oder innerhalb eines solchen Systems unter Strafe gestellt werden (einschließlich des Abfangens von elektromagnetischen Abstrahlungen aus einem Computersystem, das Träger solcher Computerdaten ist).

Da Art. 3 im Wesentlichen über eine (bloße) Telekommunikation iSd § 119 StGB hinausgeht, nämlich das Auffangen der elektromagnetischen Abstrahlung eines Computersystems ebenfalls mit umfasst, wurde eine entsprechende Erweiterung in § 119a StGB vorgesehen. Art. 3 sieht ebenfalls eine Strafbarkeitseinschränkungsmöglichkeit vor, nämlich auf Fälle, die mit „dishonest intent“ begangen wurden, oder Straftaten die in Bezug auf miteinander verbundene Computersysteme begangen wurden. Von dieser Einschränkungsmöglichkeit wurde dahingehend Gebrauch gemacht, dass sich nach §§ 119 und 119a StGB nur derjenige/diejenige strafbar macht, der/die in der Absicht handelt, sich oder einem anderen Unbefugten Kenntnis zu verschaffen.

Zu Art. 4:

Art. 4 („Data Interference“) wird innerstaatlich durch § 126a StGB umgesetzt. Nach Art. 4 soll das unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten unter Strafe gestellt werden. Von der Möglichkeit, dass nur ein solches Verhalten unter Strafe zu stellen ist, wenn die strafbare Handlung zu einem schweren Schaden führt, wurde nicht Gebrauch gemacht, sodass eine Strafbarkeit auch dann eintritt, wenn kein schwerer Schaden verursacht wird.

Zu Art. 5:

Die innerstaatliche Umsetzung dieses Artikels („System interference“) erfolgte durch § 126b StGB, soweit die Tat nicht bereits ohnehin nach § 126a StGB strafbar ist (Subsidiaritätsklausel). Gemäß dieser Subsidiaritätsklausel zu Gunsten der Bestimmung des § 126a StGB sollen nur die Fälle der „reinen“ Eingabe bzw. des „reinen“ Übermittelns erfasst werden, ohne dass es zu einer Datenbeschädigung kommt. Der Tatbestand des § 126b StGB ist sohin dann erfüllt, wenn durch Eingeben oder Übermitteln von Daten eine schwere Störung der Funktionsfähigkeit eines Computersystems herbeigeführt wird.

Zu Art. 6:

Als Vorbereitungsdelikt zu den Art. 2 bis 5 des Übereinkommens verlangt Art. 6 die Einführung eines Straftatbestandes, der die Produktion, den Verkauf, das Beschaffen zwecks Gebrauchs, die Einfuhr, die Verbreitung und das anderweitige Verfügbarmachen (Art. 6 lit. a) sowie den Besitz (Art. 6 lit. b) bestimmter Vorrichtungen, mit denen eines der in Art. 2 bis 5 genannten Delikte begangen werden kann, entsprechend erfasst. Diese Umsetzungsverpflichtung wird durch § 126c StGB bzw. auch durch § 10 Zugangskontrollgesetz erfüllt.

Die Tathandlung des § 126c StGB besteht im Herstellen, Einführen, Vertreiben, Veräußern, sonst Zugänglichmachen, sich Verschaffen oder Besitzen eines Computerprogramms, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a StGB), einer Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB), eines missbräuchlichen Abfangens von Daten (§ 119a StGB), einer Datenbeschädigung (§ 126a StGB), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a StGB) geschaffen oder adaptiert worden ist, oder einer

vergleichbaren solchen Vorrichtung oder eines Computerpasswortes, eines Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder eines Teiles davon ermöglichen.

§ 126c StGB tritt gegenüber der spezielleren Norm des Eingriffs in das Recht auf Zugangskontrolle nach § 10 Zugangskontrollgesetz zurück, wenn die Handlung auf ein gewerbsmäßiges Vertreiben, Verkaufen, Vermieten, Verpachten (Abs. 1 leg. cit.), Herstellen, Einführen, Erwerben oder Innehaben (Abs. 2 leg. cit.) der dort genannten Umgehungsvorrichtungen abstellt.

Zu Art. 7:

Die Art. 7 und 8 stehen unter dem Titel „Computerbezogene Straftaten". Die Umsetzung des Art. 7 („Computer-related Forgery") machte es notwendig, die Fälschung von Computerdaten, als Gegenstück zur herkömmlichen Urkundenfälschung, in einem eigenen Paragraphen, nämlich § 225a StGB vorzusehen. In Entsprechung des Übereinkommens lehnt sich die Formulierung des Tatbestandes des § 225a StGB an jener des § 223 StGB an. Strafbar nach § 225a StGB ist die Herstellung von falschen Daten oder die Verfälschung von echten Daten durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten.

Nach dem Übereinkommen steht es den Vertragsparteien offen, die strafrechtliche Erfassung derartiger Handlungsweisen erst in Verbindung mit einer betrügerischen oder ähnlichen Absicht eintreten zu lassen. Von dieser Möglichkeit wurde insoweit Gebrauch gemacht, als der Täter/die Täterin mit einem sog. Gebrauchsvorsatz handeln muss, d.h. er muss mit dem erweiterten Vorsatz handeln, dass diese Daten im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden. Im Zusammenhang mit der Neuregelung des § 225a StGB wurde auch der Tatbestand des schweren Betruges erweitert, indem nunmehr auch falsche oder verfälschte Daten die Qualifikation eintreten lassen sollen (vgl. § 147 Abs. 1 Z 1 StGB).

Zu Art. 8:

Die Begehungsweisen in Art. 8 („Computer-related fraud") waren bereits größtenteils durch § 148a StGB erfasst, sodass dieser Artikel keinen unmittelbaren Umsetzungsbedarf auslöste. Lediglich im Bereich der aufgelisteten Tathandlungen wurde zur Klarstellung der bestehende Katalog um die Begehungsweise der „Unterdrückung" von Daten erweitert.

Zu Art. 9:

Die Umsetzung des Art. 9 („Offences related to child pornography") erfolgte durch eine entsprechende Novellierung des § 207a StGB. Nach Art. 9 Abs. 1 soll das Herstellen von Kinderpornographie zum Zweck ihrer Verbreitung (lit. a), das Anbieten oder Verfügbarmachen (lit. b), das Verbreiten oder Übermitteln (lit. c), das Beschaffen für sich selbst oder einem anderen (lit. d), sowie der Besitz in einem Computersystem oder auf einem Computerdatenträger (lit. e) unter Strafe gestellt werden. Dies wird durch § 207a Abs. 1 und 3 StGB umgesetzt. Die Umsetzung geht sogar etwas weiter, weil eine Verbreitung über ein Computersystem nicht zum Tatbild gehört, sondern mit § 207a StGB generell sämtliche Verbreitungsformen (somit auch über ein Computersystem) erfasst werden.

Art. 9 Abs. 2 umreißt, was unter „Kinderpornographie" zu verstehen ist, weshalb in § 207a Abs. 4 StGB ebenfalls eine Legaldefinition aufgenommen wurde, die den Vorgaben des Übereinkommens entspricht.

Art. 9 Abs. 3 sieht auch (optional) eine Herabsetzung des „Schutzalters" auf 16 Jahre vor, wovon aber Österreich keinen Gebrauch machte (wobei weiter gehende Vorgaben im EU- aber auch im VN-Bereich das gar nicht (mehr) zuließen).

Nach Art. 9 Abs. 4 kann vorbehalten werden, Abs. 1 lit. d und e sowie Abs. 2 lit. b und c ganz oder teilweise nicht anzuwenden. Teilweise wird durch § 207a Abs. 5 Z 2 StGB (iVm § 207a Abs. 4 Z 4 StGB) hinsichtlich der „Altersanscheinspornographie" eine Ausnahme statuiert, nämlich dass derjenige/diejenige nicht tatbildlich handelt, der DarstellerInnen so „manipuliert" oder wenn sie so gewählt wurden, dass sie aussehen, als ob sie unter der maßgeblichen Altersgrenze liegen würden, in Wahrheit diese Altersgrenze jedoch sehr wohl überschreiten. Dies entspricht Art. 9 Abs. 4 in Bezug auf Art. 9 Abs. 2 lit. b, wonach die virtuelle Pornographie auch gänzlich von einer Strafbarkeit ausgenommen werden kann. (Auch hier gibt es weiter gehende Vorgaben aus dem EU- und VN-Bereich.)

Die Regierungsvorlage zur Strafgesetznovelle 2011 mit welcher ein neuer Straftatbestand zu „Grooming": (§ 208a StGB: als Straftat einzustufende on- und offline-Kontakte mit Unmündigen) vorgeschlagen wird, wurde am 8. November 2011 im Ministerrat beschlossen und dem Nationalrat zur verfassungsmäßigen Behandlung vorgelegt.

Art. 10:

Art. 10 verpflichtet zur strafrechtlichen Verfolgung bestimmter Verletzungen des Urheberrechts (Abs. 1) und verwandter Schutzrechte (Abs. 2). Vorbild dieser Bestimmungen ist die Bestimmung in Art. 61 des Abkommens über handelsbezogene Aspekte der Rechte des geistigen Eigentums (Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPS), Anhang 1C zum WTO-Abkommen, BGBl 1995/1. Es sind nur jene Verletzungshandlungen zu kriminalisieren, die in gewerbsmäßigem Umfang („on a commercial scale") und vorsätzlich begangen wurden, wobei Art. 10 – wie Art. 61 TRIPS-Abkommen – die innere Tatseite in der englischen Fassung mit „willfully" umschreibt, also eher „absichtlich", während diese in allen anderen Kriminalisierungsbestimmungen – Art. 2 bis 9 – „intentionally" lautet, also vorsätzlich; diese Abweichung kommt in der deutschen Fassung nicht zum Ausdruck, wo durchgängig der Begriff „vorsätzlich" verwendet wird.

Art. 10 ist insofern enger als Art. 61 des TRIPS-Abkommens, als – entsprechend dem Anwendungsbereich des Übereinkommens – nur jene Verhaltensweisen unter Strafe zu stellen sind, die mittels eines Computersystems begangen wurden.

Diese Einschränkung ist allerdings für Österreich nicht von Bedeutung: Nach § 91 des Urheberrechtsgesetzes wird derjenige bestraft, der Urheberrechte – und verwandte Schutzrechte: § 91 verweist auf den gesamten § 86 Abs. 1, also auch auf § 86 Abs. 1 Z 2 bis 6 – verletzt, ohne dass der Tatbestand bestimmte Tatmodalitäten, wie etwa die Begehung mittels eines Computersystems, vorsieht. Nach § 91 Abs. 1 Satz 2 des Urheberrechtsgesetzes sind bestimmte Verletzungen (Vervielfältigung, Festhalten eines Vortrages oder einer Aufführung zum Eigengebrauch) nicht strafbar; die Strafbarkeitsschwelle liegt daher unterhalb der Schwelle der Gewerbsmäßigkeit (diese stellt vielmehr nach Abs. 2 eine Qualifikation dar).

Die Anforderungen des Art. 10 werden daher im österreichischen Recht mehr als erfüllt, sodass auch vom Vorbehalt des gänzlichen Ausschluss der Strafbarkeit nach Abs. 3 kein Gebrauch gemacht werden muss.

Im Unionsrecht gibt es bisher keine Verpflichtungen zur Kriminalisierung von Verletzungen von Immaterialgüterrechten; zwar hat die Kommission bereits mehrfach diesbezügliche Vorschläge vorgelegt, diese sind aber vom Gesetzgeber nicht angenommen worden (vgl. Zeder, Europastrafrecht aktuell – Strafrechtlicher Schutz von Immaterialgüterrechten in Sicht, JSt. 2011, 22).

Zu Art. 11:

Art. 11 Abs. 1 erfasst sowohl die Bestimmungs- als auch die BeitragstäterInnenschaft, in Form der Beihilfe und Anstiftung zur Begehung einer nach den Art. 2 bis 10 umschriebenen Straftat. Diese TäterInnenformen sind innerstaatlich durch § 12 StGB abgedeckt.

Art. 11 Abs. 2 erfasst die Strafbarkeit des Versuchs dergestalt, dass die Begehung einer nach Art. 3 bis 5 sowie 7, 8 und 9 Abs. 1 lit. a und c umschriebenen Straftaten ebenfalls unter Strafe zu stellen ist. Dieser Vorgabe wird durch § 15 StGB entsprochen. Von dem in Art. 11 Abs. 3 vorgesehenen gänzlichen oder teilweisen Ausschluss der Versuchsstrafbarkeit wurde in der Umsetzung kein Gebrauch gemacht, die ohnehin primär für Mitgliedstaaten gedacht ist; in denen es – anders als in Österreich – keine generelle Strafbarkeit des Versuches gibt.

Zu Art. 12:

Die strafrechtliche Verantwortlichkeit juristischer Personen ist in Österreich durch das Verbandsverantwortlichkeitsgesetz (VbVG, BGBl. I Nr. 151/2005) gewährleistet. Durch das VbVG ist sichergestellt, dass ein Verband dann strafrechtlich verantwortlich ist, wenn einerseits an der Straftat ein Entscheidungsträger/eine Entscheidungsträgerin in irgendeiner Form beteiligt ist (§ 3 Abs. 2 VbVG) oder andererseits infolge einer mangelnden Kontrolle oder Aufsicht ein Mitarbeiter/eine Mitarbeiterin eine strafbare Handlung begeht (§ 3 Abs. 3 VbVG). In beiden Fällen müssen die in § 3 Abs. 1 VbVG genannten Fälle, nämlich Tatbegehung zu Gunsten des Verbandes oder Verletzung von Pflichten des Verbandes durch die Tat gegeben sein. Dies entspricht auch der Diktion von Art. 12 des Übereinkommens. In Entsprechung des Art. 12 Abs. 4 sieht das VbVG auch vor, dass von einer Verantwortlichkeit des Verbandes die strafrechtliche Verantwortung der handelnden natürlichen Person unberührt bleibt.

Nach Art. 12 Abs. 3 bleibt es den Vertragsstaaten überlassen, welche Sanktionen (straf-, zivil- oder verwaltungsrechtlicher Art) zur Anwendung gelangen sollen; durch das VbVG hat sich Österreich zu der Einführung von strafrechtlichen Sanktionen (Verbandsgeldbuße) bekannt.

Zu Art. 13:

Art. 13 Abs. 1 sieht vor, dass die in Art. 2 bis 11 umschriebenen Straftaten durch wirksame, verhältnismäßige und abschreckende Sanktionen, einschließlich Freiheitsentziehung, bedroht werden

müssen. In Entsprechung dieser Verpflichtung sehen § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem), § 119 StGB (Verletzung des Telekommunikationsgeheimnisses), § 119a (Missbräuchliches Abfangen von Daten), die Grundstrafdrohung des § 126a Abs. 1 StGB (Datenbeschädigung), § 126c StGB (Störung der Funktionsfähigkeit eines Computersystems), § 126c Abs. 1 StGB (Missbrauch von Computerprogrammen oder Zugangsdaten) sowie der Grundtatbestand des § 148a Abs. 1 StGB (Betrügerischer Datenverarbeitungsmissbrauch) jeweils einen Strafrahmen von Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen vor.

Die Qualifikation des § 126a Abs. 2 und § 148a Abs. 2 StGB sehen einen entsprechend höheren Strafrahmen vor: § 126a Abs. 2 StGB sieht Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bis zu 360 Tagessätzen vor, wenn der Schaden 3.000 Euro übersteigt und eine Freiheitsstrafe von sechs Monaten bis zu fünf Jahren, wenn der Schaden 50.000 Euro übersteigt. § 148a Abs. 2 StGB sieht ebenfalls eine Freiheitsstrafe von bis zu drei Jahren vor, wenn der Schaden 3.000 Euro übersteigt oder die Tat gewerbsmäßig begangen wurde bzw. - wenn der Schaden 50.000 Euro übersteigt - eine Freiheitsstrafe von einem bis zu zehn Jahren.

Datenfälschung nach § 225a StGB ist – in Anlehnung an die Urkundenfälschung nach § 223 StGB – mit Freiheitsstrafe bis zu einem Jahr bedroht. Pornographische Darstellung Minderjähriger ist nach § 207a Abs. 1 StGB bereits im Grundtatbestand mit Freiheitsstrafe bis zu drei Jahren strafbar, die Qualifikationen des § 207a Abs. 2 sehen noch höhere Strafrahmen vor. § 207a Abs. 3 StGB sieht für das Verschaffen oder den Besitz einer pornographischen Darstellung einer mündigen minderjährigen Person eine Freiheitsstrafe von bis zu einem Jahr vor; der Strafrahmen erhöht sich auf Freiheitsstrafe bis zu zwei Jahren, wenn die Darstellung eine unmündige Person zeigt.

Für Versuch, Beihilfe und Anstiftung iSd Art. 11 gelten nach österreichischem Recht zufolge §§ 12, 15 StGB die gleichen Strafrahmen wie für den unmittelbaren Täter/die unmittelbare Täterin bzw. wie für das vollendete Delikt.

Die in Art. 13 Abs. 2 enthaltene Verpflichtung, wirksame, verhältnismäßige und abschreckende strafrechtliche Sanktionen auch für juristische Personen vorzusehen, wird mit dem Verbandsverantwortlichkeitsgesetz (VbVG) umgesetzt; dieses ermöglicht Geldbußen nach einem Tagessatzsystem (§§ 4-f VbVG). Die Höhe des Tagessatzes richtet sich nach der Ertragslage des Verbandes und ist mit 10.000 Euro begrenzt; die Anzahl der Tagessätze richtet sich nach der Freiheitsstrafdrohung des betreffenden Delikts (vgl. § 4 Abs. 3 VbVG).

Zu Art. 14:

Art. 14 umschreibt den Geltungsbereich der verfahrensrechtlichen Bestimmungen dieses Übereinkommens. Demnach müssen auch die erforderlichen Maßnahmen ergriffen werden, damit die danach vorgesehenen Befugnisse und Verfahren bei Ermittlungen oder Verfahren wegen in diesem Übereinkommen umschriebenen Straftatbeständen (Art. 2 bis 11) sowie anderer mittels eines Computersystems begangener Straftaten angewendet werden können, ebenso bei der Erhebung von in elektronischer Form vorhandenem Beweismaterial. Diesen Verpflichtungen wird Österreich durch die Strafprozessordnung (StPO) hinreichend gerecht, wobei die StPO für Computerstraftaten grundsätzlich keine Besonderheiten vorsieht. Auch was die Art des Beweismaterials anlangt, gibt die StPO keine Vorgaben, sodass auch Beweismittel in elektronischer Form ebenfalls zulässig sind.

Von den in Abs. 3 umschriebenen Vorbehaltsmöglichkeiten hat Österreich keinen Gebrauch gemacht.

Zu Art. 15:

Art. 15 umschreibt ganz allgemein die einzuhaltenden Verfahrensgarantien. Nach Abs. 1 ist sicherzustellen, dass das innerstaatliche Recht einen angemessenen Schutz der Menschenrechte, welche in der EMRK verbrieft sind, einzuhalten hat. Auch Verpflichtungen nach dem Internationalen Pakt der Vereinten Nationen von 1966 über bürgerliche und politische Rechte und anderen anwendbaren völkerrechtlichen Übereinkünften auf dem Gebiet der Menschenrechte sind einzuhalten. Insbesondere muss dazu auch der Grundsatz der Verhältnismäßigkeit gehören. Die StPO bekennt sich zu einem umfassenden Grundrechtsschutz; speziell was den Grundsatz der Verhältnismäßigkeit anlangt, wurde in § 5 StPO auch eine einfachgesetzliche Ausgestaltung festgeschrieben.

Nach Abs. 2 sollen die einzuhaltenden Bedingungen und Garantien unter anderem eine gerichtliche oder sonstige unabhängige Kontrolle, eine Begründung der Anwendung sowie die Begrenzung des Umfanges und der Dauer der Befugnis oder des Verfahrens enthalten. Dieser Verpflichtung wird insbesondere durch die Bestimmungen der §§ 101 ff StPO entsprochen. Nach § 105 Abs. 1 StPO hat das Gericht über die Bewilligung von bestimmten Zwangsmitteln zu entscheiden und hat für die Durchführung auch eine bestimmte Frist vorzugeben. Eine Anordnung hat auch einen bestimmten Inhalt sowie eine Begründung zu enthalten, die näher in § 102 StPO festgelegt sind. Auch was den gerichtlichen Rechtsschutz

anbelangt, wurden durch das mit 1. Jänner 2008 in Kraft getretene Strafprozessreformgesetz (BGBl. I Nr. 19/2004) die Garantien erweitert. Nach § 106 StPO steht im Ermittlungsverfahren jeder Person das Recht zu, einen Einspruch an das Gericht zu erheben, wenn diese behauptet, durch die Staatsanwaltschaft in einem subjektiven Recht verletzt worden zu sein.

Nach Abs. 3 sollen auch Auswirkungen der nach diesem Übereinkommen vorgesehenen Befugnisse und Verfahren auf die Rechte, Verantwortlichkeiten und berechtigten Interessen dritter Personen berücksichtigt werden. Berechtigte Interessen dritter Personen werden durch die StPO hinreichend gewahrt, sei es dass beispielsweise einer Sicherstellung widersprochen werden kann (§ 112 StPO), sei es, dass die angemessenen und ortsüblichen Kosten einer Sicherstellung jenen Personen, die nicht selbst der Tat beschuldigt sind, zu ersetzen sind (§ 111 Abs. 3 StPO); ebenso werden die Kosten für die Mitwirkung eines Anbieters (§ 92 Abs. 3 Z 1 TKG 2003) an der Auskunftserteilung über Daten einer Nachrichtenübermittlung sowie der Überwachung von Nachrichten nach den Bestimmungen der Überwachungskostenverordnung (BGBl. II Nr. 322/2004) ersetzt.

Zu Art. 16:

Die Art. 16 und Art. 17 betreffen die umgehende Sicherung von bereits existierenden und aktuell noch gespeicherten Daten. Es soll sichergestellt werden, dass bereits gespeicherte Daten in ihrer derzeitigen Form unverändert belassen werden („data preservation"). Der Zugriff und die Verwendung dieser Daten können weiterhin möglich bleiben, sofern die Daten nicht verändert werden.

Durch Art. 16 Abs.1 soll sichergestellt werden, dass die zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zur Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht. Nach Art. 16 Abs. 1 kann das Ziel der umgehenden Sicherung von Daten entweder durch eine an eine bestimmte Person gerichtete Anordnung (erste Alternative) oder in ähnlicher Weise (zweite Alternative) bewirkt werden. Österreich wählt die zweite Alternative, indem die Sicherstellung nach den §§ 110 ff StPO erfolgt. Diese Vorgangsweise steht mit dem Übereinkommen im Einklang. Nach §§ 110 ff StPO ist die Gefahr eines Datenverlusts oder einer Datenveränderung nicht Voraussetzung für eine Sicherstellung. Grundsätzlich ist die Sicherstellung auf Anordnung der Staatsanwaltschaft durchzuführen (§ 110 Abs. 2 StPO); bei Gefahr in Verzug (allfälliger unmittelbar drohender Datenverlust) kann die Kriminalpolizei nach § 99 Abs. 2 StPO auch ohne eine solche Anordnung vorgehen, wobei jedoch unverzüglich um Genehmigung anzufragen ist. Was die „bloße" Sicherstellung von Verkehrsdaten anlangt, so müssen diese zuerst ermittelt werden, damit diese sichergestellt werden können. Dies wird in den §§ 134ff StPO geregelt, und es kann an dieser Stelle auf die Ausführungen zu den Artikeln 17 und 20 verwiesen werden. Jedenfalls sehen das TKG 2003 sowie § 138 Abs. 2 StPO für Diensteanbieter eine Mitwirkungsverpflichtung vor.

Werden Personen nach der ersten Alternative des Art. 16 Abs. 1 im Wege einer Anordnung aufgefordert, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden, sicherzustellen, so ist gemäß Art. 16 Abs. 2 zu gewährleisten, dass diese Daten solange wie notwendig - längstens aber neunzig Tage - gesichert und erhalten werden, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken. Da sich Art. 16 Abs. 2 nur auf die erste Alternative des Art. 16 Abs. 1 (Anordnung an eine bestimmte Person) bezieht, Österreich hingegen die zweite Alternative (Bewirkung in ähnlicher Weise) wählt, ist Art. 16 Abs. 2 für Österreich ohne Belang.

Nach Art. 16 Abs. 3 sind die sichergestellten Daten vertraulich zu behandeln. Zumal die Sicherstellung zunächst von der Kriminalpolizei durchzuführen ist und diese auch bis zur Berichterstattung über die Sicherstellung die Daten zu verwahren hat, während danach für die Verwahrung die Staatsanwaltschaft zuständig ist (§ 114 Abs. 1 StPO), gelangen diese Daten nur an Personen, die dem Amtsgeheimnis unterliegen, sodass für eine hinreichende Vertraulichkeit gesorgt wird; gleiches gilt auch für einen allfälligen beauftragten (externen) Verwahrer. Für Diensteanbieter ergibt sich die Verpflichtung zur vertraulichen Behandlung aus § 138 Abs. 3 StPO.

Zu Art. 17:

Nach Art. 17 Abs. 1 ist in Bezug auf Verkehrsdaten (die nach Art. 16 zu sichern sind) sicherzustellen, dass die umgehende Sicherung von Verkehrsdaten unabhängig davon möglich ist, ob ein oder mehrere Diensteanbieter an der Übermittlung dieser Kommunikation beteiligt waren (lit. a), und dass Verkehrsdaten in einem solchen Umfang umgehend an die zuständige Behörde der Vertragspartei oder an eine von dieser Behörde bezeichnete Person weitergegeben werden, sodass die Vertragspartei die Diensteanbieter und den Weg feststellen kann, auf dem die Kommunikation übermittelt wurde (lit. b).

Die in Art. 17 umschriebenen Verpflichtungen sind einerseits im TKG 2003 sowie in der StPO festgelegt. Nach § 94 Abs. 1 TKG 2003 ist der Diensteanbieter verpflichtet, alle Einrichtungen bereitzustellen, die zur Überwachung von Nachrichten sowie zur Auskunft über Daten einer Nachrichtenübermittlung einschließlich der Auskunft über Vorratsdaten nach den Bestimmungen der StPO erforderlich sind. Diese Verpflichtung ist davon unabhängig, wie viele Diensteanbieter an der Kommunikation beteiligt waren oder sind. Nach § 94 Abs. 4 TKG 2003 hat die Übermittlung von Verkehrsdaten, Standortdaten und Stammdaten, welche die Verarbeitung von Verkehrsdaten erfordern, einschließlich der Übermittlung von Vorratsdaten, nach den Bestimmungen der StPO sowie des SPG, unter Verwendung einer Übertragungstechnologie, welche die Identifikation und Authentifizierung von Sender und Empfänger sowie die Datenintegrität sicherstellt, zu erfolgen. Die Daten sind unter Verwendung einer technisch anspruchsvollen Verschlüsselungstechnologie als "Comma-Separated Value (CSV)" - Dateiformat zu übermitteln. Auch § 138 Abs. 2 StPO statuiert eine entsprechende Mitwirkungsverpflichtung der Anbieter.

Zu Art. 18:

Nach Art. 18 Abs. 1 muss sichergestellt werden, dass Personen bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen haben (lit. a) und dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Stammdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat (lit. b). Bei der Herausgabeanordnung nach Art. 18 handelt es sich gegenüber anderen Instrumenten (Durchsuchung, Beschlagnahme) um die flexiblere und weniger eingriffsintensive Maßnahme.

Der Verpflichtung zur Vorlage von Computerdaten nach Art. 18 Abs. 1 lit. a wird durch § 111 Abs. 2 StPO entsprochen. Was die Vorlage von Stammdaten durch Diensteanbieter anlangt, ergibt sich diese Verpflichtung aus § 90 Abs. 7 TKG 2003 iVm § 76a Abs. 1 StPO (BGBl. I Nr. 33/11) sowie 99 Abs. 5 Z 2 TKG 2003 iVm § 76a Abs. 2 StPO (BGBl I Nr. 33/11). Demnach sind Anbieter von Kommunikationsdiensten auf Ersuchen der kriminalpolizeilichen Behörden, der Staatsanwaltschaften und der Gerichte verpflichtet, Auskunft über Stammdaten eines Teilnehmers zu erteilen.

Art. 18 Abs. 3 umschreibt, was unter Stammdaten (Bestandsdaten) zu verstehen ist. Demnach fallen darunter alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über TeilnehmerInnen seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten. Durch diese Daten müssen die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dauer des Dienstes (lit. a), die Identität des Teilnehmers/der Teilnehmerin, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummern sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen (lit. b), sowie andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen (lit. c), festgestellt werden können.

Was innerstaatlich unter Stammdaten zu verstehen ist, umschreibt § 92 Abs. 3 Z 3 TKG 2003. Demnach sind Stammdaten alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen den BenutzerInnen und den Anbietern oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Dazu zählen der Name (Familienname und Vorname bei natürlichen Personen, Name bzw. Bezeichnung bei juristischen Personen), der akademische Grad bei natürlichen Personen, sowie die Anschrift (Wohnadresse bei natürlichen Personen, Sitz bzw. Rechnungsadresse bei juristischen Personen). Sowohl das Übereinkommen als auch das TKG gehen vom selben Verständnis der Stammdaten aus. Die in Art. 16 Abs. 3 lit. c angesprochenen anderen Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, beziehen sich auf solche Informationen, die aufgrund der Rechtsbeziehung zwischen den Anbietern und den TeilnehmerInnen sich erschließen und bezieht sich im Wesentlichen nur auf Kommunikationsanlagen, die nicht mobil sind.

Zu Art. 19:

Art. 19 sieht Regelungen für die Durchsuchung und Beschlagnahme von gespeicherten Computerdaten vor. Nach Abs. 1 müssen die Strafverfolgungsbehörden ermächtigt werden, ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten (lit. a) und einen Computerdatenträger, auf dem Computerdaten gespeichert sein können (lit. b), zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen. Art. 19 Abs. 1 ist durch die §§ 119 bis 122 StPO umgesetzt. Diese Bestimmungen der StPO ermöglichen für den Fall, dass der Betroffene seiner Verpflichtung zur Herausgabe nach § 111 Abs. 2 StPO nicht nachkommt, die Durchsuchung von Orten und Gegenständen, um auf die Computerdaten bzw. auf ein bestimmtes Computersystem zugreifen zu können. Ebenso kann auf die in

Art. 19 Abs. 2 geforderte Ausdehnung der Ermittlungen auf andere Computer bzw. Computersysteme rasch reagiert werden, indem die Anordnung der Sicherstellung entsprechend erweitert wird bzw. bei einer Anordnung auf Durchsuchung von Orten und Gegenständen kann durch die eingerichteten Journaldienste bei den Staatsanwaltschaften und Gerichten entsprechend schnell reagiert werden. Bei Gefahr in Verzug kann die Kriminalpolizei auch ohne eine gerichtlich bewilligte Anordnung eine Durchsuchung von Orten und Gegenständen vorläufig vornehmen (vgl. § 120 Abs. 1 StPO).

Nach Art. 19 Abs. 3 muss den Strafverfolgungsbehörden ermöglicht werden, dass sie ein Computersystem oder einen Teil davon oder einen Computerdatenträger beschlagnahmen oder in ähnlicher Weise sicherstellen können (lit. a), eine Kopie dieser Computerdaten anfertigen und zurückbehalten können (lit. b), die Unversehrtheit der einschlägigen gespeicherten Computerdaten erhalten können (lit. c), und diese Computerdaten in dem Computersystem unzugänglich machen oder sie daraus entfernen können (lit. d). Dieser Verpflichtung wird durch die Bestimmungen der Sicherstellung (§§ 110 ff StPO) sowie der Beschlagnahme (§ 115 StPO) entsprochen. Die Bestimmungen der Sicherstellung umfassen auch, wie von der lit. d gefordert, die Unzugänglichmachung bzw. die Entfernung von Computerdaten.

Hinsichtlich der in Art. 19 Abs. 4 umschriebenen Mitwirkungspflicht kann auf die Ausführungen zu Art. 16 verwiesen werden. Einer Verweigerung der Mitwirkungsverpflichtung kann durch Anwendung von Zwang oder durch eine Ersatzvornahme nach § 93 Abs. 2 StPO begegnet werden.

Zu Art. 20:

Art. 20 sieht Regelungen über die Erhebung (Ermittlung) von Verkehrsdaten in Echtzeit vor. Nach Abs. 1 müssen die zuständigen Behörden ermächtigt werden, Verkehrsdaten in Echtzeit zu erheben oder aufzuzeichnen (lit. a) und einen Diensteanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu verpflichten, solche Verkehrsdaten durch Anwendung technischer Mittel in Echtzeit zu erheben oder aufzuzeichnen (sublit. i) oder bei der Erhebung oder Aufzeichnung solcher Verkehrsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen (sublit. ii). Diese Verpflichtung wird durch die §§ 134 Z 2, 135 Abs. 2 StPO umgesetzt. Nach § 137 Abs. 3 StPO kann sich eine Anordnung sowohl auf einen vergangenen als auch auf einen zukünftigen Zeitraum erstrecken, sodass die hier geforderte Ermittlung in Echtzeit möglich ist.

Die in Art. 20 Abs. 3 angesprochene Verpflichtung, dass Anbieter verpflichtet sind, die aufgrund ihrer Befugnis erlangten Informationen vertraulich zu behandeln, wird durch § 138 Abs. 3 StPO erfüllt. Nach dieser Bestimmung müssen die Anbieter die mit einer Anordnung verbundenen Tatsachen und Vorgänge gegenüber Dritten geheim halten.

Zu Art. 21:

Entsprechend dem Art. 20 muss durch Art. 21 sichergestellt werden, dass auch die Erhebung von Inhaltsdaten in Echtzeit möglich sein soll. Dies wird durch die §§ 134 Z 3, 135 Abs. 3 StPO ermöglicht. Auf die Ausführungen zu Art. 20 kann verweisen werden.

Zu Art. 22:

Artikel 22 normiert die Anknüpfungspunkte für die inländische Gerichtsbarkeit. Nach Abs. 1 muss die Gerichtsbarkeit hinsichtlich der Tatbestände der Art. 2 bis 11 dann vorliegen, wenn die Straftat in ihrem Hoheitsgebiet (lit. a), an Bord eines Schiffes, das die Flagge dieser Vertragspartei führt (lit. b), an Bord eines Luftfahrzeugs, das nach dem Recht dieser Vertragspartei eingetragen ist (lit. c), oder von einem ihrer Staatsangehörigen, wenn die Straftat nach dem am Tatort geltenden Recht strafbar ist oder die Straftat außerhalb des Hoheitsbereichs irgendeines Staates (lit. d), begangen wird. Diese Verpflichtung wird durch die Bestimmungen der §§ 62, 63 und 65 StGB erfüllt.

Von der in Art. 22 Abs. 2 vorgesehenen Vorbehaltsmöglichkeit, nämlich die in Abs. 1 lit. 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, wurde kein Gebrauch gemacht.

Art. 22 Abs. 3 ist gemeinsam mit Art. 22 Abs. 1 lit. d sowie Art. 24 Abs. 1 und 6 zu lesen. Wiewohl Art. 22 Abs. 3 nicht explizit auf das Erfordernis der gegenseitigen Strafbarkeit abstellt, ist aber dennoch davon auszugehen, dass eine solche auch in den Fällen des Abs. 3 vorliegen muss, weil nur das Vorliegen einer strafbaren Handlung ein Auslieferungsersuchen rechtfertigen kann. Insoweit ist Abs. 3 als durch § 65 StGB umgesetzt zu betrachten.

KAPITEL III – Internationale Zusammenarbeit

Zu Art. 23:

Diese Bestimmung statuiert die Verpflichtung zur weitestgehenden Zusammenarbeit der Vertragsparteien im Zusammenhang mit Ermittlungen sowie strafgerichtlichen Verfahren in Bezug auf die unter das Übereinkommen fallenden Straftaten sowie bei der Erhebung von Beweisen in elektronischer Form im Einklang mit bestehenden völkerrechtlichen Verträgen über die internationale Zusammenarbeit sowie den innerstaatlichen Rechtsvorschriften auf diesem Gebiet.

Zu Art. 24:

Abs. 1 dieses Artikels normiert die Auslieferungsfähigkeit der in Art. 2 bis 11 angeführten Straftaten, sofern diese nach dem Recht der beteiligten Vertragsparteien mit einer Mindesthöchststrafe im Ausmaß von 1 Jahr bedroht sind (lit. a). In lit. b wird klargestellt, dass für den Fall, dass nach einem zwischen den Vertragsparteien anwendbaren bi- oder multilateralen Vertrag oder auf der Grundlage der Gegenseitigkeit ein geringerer Schwellenwert besteht, dieser maßgebend ist.

Nach Abs. 2 gelten die erwähnten Straftaten als in jeden zwischen den Vertragsparteien bestehenden Auslieferungsvertrag einbezogene, der Auslieferung unterliegende Straftaten. Bei neu abzuschließenden Verträgen dieser Art besteht die Verpflichtung, die Straftaten, auf die das gegenständliche Übereinkommen Anwendung findet, als auslieferungsfähig aufzunehmen.

Abs. 3 ermöglicht es Vertragsstaaten, die – anders als Österreich – nach innerstaatlichem Recht ohne Bestehen eines Vertrages nicht zu einer Auslieferung in der Lage sind, das vorliegende Übereinkommen als ausreichende Grundlage für die Auslieferung anzusehen.

Die in diesem Übereinkommen vorgesehenen Straftaten (Art. 2 bis 10) sind von Staaten, die – wie Österreich – auch ohne Bestehen eines Vertrages zur Auslieferung in der Lage sind, nach Abs. 4 als der Auslieferung unterliegende Straftaten anzusehen; dies ist in Österreich nach § 11 Abs. 1 ARHG gewährleistet.

In Abs. 5 wird klargestellt, dass sich die Auslieferung einschließlich der Ablehnungsgründe nach dem Recht der ersuchten Vertragspartei bzw. den in anwendbaren Auslieferungsverträgen vorgesehenen Bedingungen richtet.

Abs. 6 verankert das Prinzip „aut dedere aut judicare“: ein Vertragsstaat, auf dessen Hoheitsgebiet sich ein Verdächtiger aufhält, hat, sofern er diesen ausschließlich aufgrund von dessen Staatsangehörigkeit oder deswegen ablehnt, weil ihm nach seiner Auffassung selbst Gerichtsbarkeit zukommt, den Fall unverzüglich den zuständigen Behörden zum Zweck der Strafverfolgung zu unterbreiten, was durch die Bestimmung des § 65 Abs. 1 Z 1 StGB gewährleistet wird, und die ersuchte Vertragspartei vom Ergebnis des eingeleiteten Verfahrens zu verständigen.

Nach Abs. 7 haben die Vertragsparteien dem Generalsekretär des Europarats jene Behörden mitzuteilen, die in Ermangelung eines Vertrages für die Stellung und Entgegennahme von Auslieferungsersuchen bzw. Ersuchen um Verhängung der vorläufigen Auslieferungshaft zuständig sind. Die zuständige österreichische Behörde ist das Bundesministerium für Justiz, Abteilung IV.4.

Zu Art. 25:

Die Bestimmung enthält allgemeine Regeln zur Rechtshilfe.

Abs. 1 sieht eine weitgehende Rechtshilfeverpflichtung der Vertragsparteien im Zusammenhang mit Ermittlungen sowie strafgerichtlichen Verfahren in Bezug auf die unter das Übereinkommen fallenden Straftaten sowie für die Erhebung von Beweisen in elektronischer Form vor.

Abs. 2 verpflichtet die Vertragsparteien allgemein zur Setzung der erforderlichen legislativen oder sonstigen Maßnahmen zwecks Erfüllung der in Art. 27 bis 35 im Einzelnen enthaltenen Formen der Rechtshilfe. Dazu ist zunächst festzuhalten, dass die die Zusammenarbeit betreffenden Bestimmungen des Übereinkommens mit dessen Ratifikation für Österreich unmittelbar anwendbar sind (self executing). Soweit Rechtshilfe durch bestimmte Ermittlungsmaßnahmen begehrt wird, ist nach § 9 Abs. 1 ARHG die StPO anzuwenden. Da die im Übereinkommen vorgesehenen Ermittlungsmaßnahmen auf der Grundlage der geltenden Bestimmungen der StPO möglich sind, besteht daher auch insofern für den Bereich der Rechtshilfe kein Umsetzungsbedarf.

Nach Abs. 3 können Rechtshilfeersuchen und die mit diesen im Zusammenhang stehenden Mitteilungen in dringenden Fällen durch schnelle Kommunikationsmittel (z. B. Telefax oder e-mail) übermittelt und beantwortet werden. Über entsprechendes Ersuchen der ersuchten Vertragspartei ist das Ersuchen bzw. die sonstige Mitteilung in der Folge auf den Postweg nachzureichen.

In Abs. 4 wird klargestellt, dass sich die Rechtshilfeleistung einschließlich der Ablehnungsgründe grundsätzlich nach dem Recht der ersuchten Vertragspartei bzw. den in anwendbaren

Rechtshilfeverträgen vorgesehenen Bedingungen richtet. Dabei darf die Rechtshilfeleistung nicht alleine mit der Begründung abgelehnt werden, dass sich das Ersuchen auf eine fiskalische Straftat bezieht.

Sofern eine Vertragspartei die Rechtshilfeleistung vom Vorliegen der beiderseitigen Strafbarkeit abhängig macht, was für Österreich aufgrund des österreichischen Vorbehalts zu Art. 1 Abs. 1 des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen vom 20.4.1959, BGBl. Nr. 41/1969, bzw. nach Art. 51 Abs. 1 Z 1 ARHG der Fall ist, so ist diese Bedingung nach Abs. 5 dann erfüllt, wenn die dem Ersuchen zugrunde liegende Straftat unabhängig von deren Bezeichnung nach ihrem Recht eine Straftat darstellt.

Zu Art. 26:

Diese Bestimmung regelt die Informationsübermittlung ohne Ersuchen nach Maßgabe des nationalen Rechts. Diese kommt nach österreichischem Recht auf der Grundlage des § 59a ARHG in Betracht.

Zu Art. 27:

Dieser Artikel regelt das Verfahren für die Rechtshilfeleistung in Ermangelung anwendbarer bi- oder multilateraler Rechtshilfeverträge oder mangels Reziprozität sowie für den Fall, dass dies zwischen den Vertragsparteien vereinbart wurde (Abs. 1).

Nach Abs. 2 haben die Vertragsparteien eine oder mehrere zentrale Behörden zur Übermittlung und Entgegennahme von Rechtshilfeersuchen namhaft zu machen. In Österreich ist die zuständige Zentralbehörde das Bundesministerium für Justiz, Abteilung IV.4.

Sofern die ersuchende Vertragspartei um Einhaltung eines bestimmten Verfahrens bei der Erledigung des Rechtshilfeersuchens ersucht, ist diesem Ersuchen nach Abs. 3 zu entsprechen, sofern eine derartige Vorgangsweise nicht mit dem Recht der ersuchten Vertragspartei unvereinbar ist.

Abs. 4 führt als weitere Ablehnungsgründe (neben jenem der mangelnden beiderseitigen Strafbarkeit; s. Art. 25 Abs. 5) den Umstand an, dass die dem Ersuchen zugrunde liegende Straftat eine politische oder eine mit einer solchen zusammenhängende Straftat darstellt (lit. a), sowie dass die Erledigung des Ersuchens nach Ansicht der ersuchten Vertragspartei geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung oder andere wesentliche Interessen zu beeinträchtigen (sog. ordre public-Klausel) (lit. b).

Nach Abs. 5 besteht die Möglichkeit des Aufschubs der Erledigung des Ersuchens, wenn diese laufende Ermittlungen oder Verfahren der ersuchten Vertragspartei beeinträchtigen könnte.

Abs. 6 statuiert die Verpflichtung der ersuchten Vertragspartei, vor Ablehnung oder Aufschub der Erledigung des Ersuchens zu prüfen, ob diesem zum Teil oder unter bestimmten Bedingungen entsprochen werden kann.

Nach Abs. 7 sind die Ablehnung und der Aufschub der Erledigung eines Rechtshilfeersuchens ebenso zu begründen wie die Unmöglichkeit oder voraussichtliche erhebliche Verzögerung von dessen Erledigung.

Abs. 8 enthält Regelungen zur vertraulichen Behandlung des Ersuchens. Diesbezüglich wird auf die Erläuterungen zu Art. 16 Abs. 3 verwiesen.

Abs. 9 sieht die Möglichkeit vor, Rechthilfeersuchen und mit diesen im Zusammenhang stehende Mitteilungen in dringenden Fällen im unmittelbaren Behördenverkehr (unter gleichzeitiger Übermittlung einer Kopie an die Zentralbehörde der ersuchten Vertragspartei) sowie im Interpol-Weg zu übermitteln. Der unmittelbare Behördenverkehr ist darüber hinaus für die Übermittlung von Rechtshilfeersuchen zulässig, deren Erledigung keine Zwangsmaßnahmen erfordert. Lit. e enthält zwar eine Vorbehaltsmöglichkeit, von der aber Österreich keinen Gebrauch machen wird.

Zu Art. 28:

Abs. 1 dieses Artikels stellt klar, dass die enthaltenen Regelungen nur in Ermangelung anwendbarer bi- oder multilateraler Rechtshilfeverträge oder mangels Reziprozität sowie für den Fall Anwendung finden, dass dies zwischen den Vertragsparteien vereinbart wurde.

Nach Abs. 2 kann die ersuchte Vertragspartei die Übermittlung der erbetenen Informationen oder Beweismittel davon abhängig machen, dass diese von der ersuchenden Vertragspartei vertraulich behandelt (lit. a) bzw. nicht für andere als das dem Rechtshilfeersuchen zugrunde liegende Verfahren verwendet werden (lit. b; Spezialität).

Wenn die ersuchende Vertragspartei diesen Bedingungen nicht entsprechen kann, so hat sie die ersuchte Vertragspartei von diesem Umstand in Kenntnis zu setzen. Diese entscheidet in der Folge, ob dem Rechtshilfeersuchen ungeachtet dessen entsprochen werden kann (Abs. 3).

Zu Art. 29:

Dieser Artikel enthält Bestimmungen über die zwischenstaatliche Zusammenarbeit durch jene vorläufige Maßnahme, die für die innerstaatliche Ebene in Art. 16 vorgesehen ist, nämlich die umgehende Sicherung von Computerdaten, die mittels eines Computersystems, das sich im Hoheitsgebiet eines anderen Staates befindet, gespeichert sind. Um eine solche Sicherung kann ein Staat einen anderen Staat vor Stellung eines Rechtshilfeersuchens um Durchsuchung und Beschlagnahme ersuchen (Abs. 1).

Abs. 2 regelt den erforderlichen Inhalt eines Ersuchens um vorläufige Datensicherung.

Abs. 3 sieht zunächst vor, dass sich die Erledigung des Ersuchens nach dem nationalen Recht der ersuchten Vertragspartei richtet. Es ist daher auch aus dem Blickwinkel der zwischenstaatlichen Zusammenarbeit mit dem Übereinkommen vereinbar, dass Österreich eine umgehende Sicherung von Computerdaten nicht durch eine an eine bestimmte Person gerichtete Anordnung, sondern nur durch Sicherstellung nach § 110 StPO erfolgt (vgl. Erläuterungen zu Art. 16).

Weiters bestimmt Abs. 3, dass das Vorliegen der beiderseitigen Strafbarkeit grundsätzlich keine Voraussetzung für die Zulässigkeit einer einstweiligen Datensicherung sein darf. Diesbezüglich besteht jedoch nach Abs. 4 eine Vorbehaltsmöglichkeit. Danach kann eine Vertragspartei, die die Erledigung von Rechtshilfeersuchen um Durchsuchung und Beschlagnahme vom Vorliegen der beiderseitigen Strafbarkeit abhängig macht, die einstweilige Sicherung der Daten verweigern, wenn Grund zu der Annahme besteht, dass zum Zeitpunkt der Datenweitergabe keine beiderseitige Strafbarkeit vorliegen wird, es sei denn, es handelt sich um eines der in Art. 2 bis 11 des Übereinkommens angeführten Delikte. Österreich bringt dazu einen Vorbehalt ein.

Darüber hinaus kann die Erledigung eines Ersuchens um einstweilige Datensicherung nur aus den in Art. 27 Abs. 4 angeführten Gründen (politische Straftat, ordre public) abgelehnt werden (Abs. 5).

In Abs. 6 ist eine Konsultation zwischen den Vertragsparteien (u.a.) vorgesehen, wenn nach Ansicht der ersuchten Vertragspartei durch die (begehrte) Sicherung die Verfügbarkeit der Daten nicht gewährleistet scheint; diese Bestimmung wird für Österreich ohne Relevanz sein, da die Sicherung ohnehin immer durch Sicherstellung nach § 110 StPO erfolgt.

Eine einstweilige Datensicherung hat nach Abs. 7 für mindestens 60 Tage zu erfolgen, um der ersuchenden Vertragspartei die Möglichkeit der Stellung eines förmlichen Rechtshilfeersuchens um Durchsuchung und Beschlagnahme zu geben. Nach Einlangen eines solchen Ersuchens ist die Datensicherung bis zur Entscheidung über das Ersuchen fortzusetzen.

Zu Art. 30:

Art. 30 enthält Bestimmungen über die zwischenstaatliche Zusammenarbeit parallel zu den für die innerstaatliche Ebene in Art. 17 vorgesehenen Sonderbestimmungen betreffend die umgehende Sicherung und Weitergabe von Verkehrsdaten: Wenn sich bei Entsprechung eines Ersuchens nach Art. 29, das auf die vorläufige Sicherung von Verkehrsdaten gerichtet ist, herausstellt, dass ein Serviceprovider in einem weiteren Staat an der Übermittlung der Kommunikation, auf die sich das Ersuchen bezieht, beteiligt war, so hat die ersuchte Vertragspartei die zur Feststellung des betreffenden Serviceproviders und des Kommunikationswegs erforderliche Anzahl von Verkehrsdaten an die ersuchende Vertragspartei zu übermitteln (Abs. 1).

Von der Weitergabe der gesicherten Verkehrsdaten kann nach Abs. 2 nur aus den in Art. 29 Abs. 4 angeführten Gründen (politische Straftat, ordre public) abgesehen werden.

Zu Art. 31:

Diese Bestimmung regelt die Rechtshilfe beim Zugriff auf gespeicherte Computerdaten durch Durchsuchung und Beschlagnahme derselben und stellt daher das zwischenstaatliche Gegenstück zu Art. 19 dar.

Zu diesem Zweck ist die Übermittlung eines förmlichen Rechtshilfeersuchens erforderlich, dessen Erledigung sich nach den zwischen den beteiligten Vertragsparteien anwendbaren bi- und multilateralen Verträgen über die Rechtshilfe in Strafsachen, in Ermangelung derselben nach dem in Art. 25 vorgesehenen Verfahren richtet (Abs. 2).

Abs. 3 sieht dabei die Verpflichtung zur umgehenden Erledigung des Ersuchens vor, wenn die Gefahr besteht, dass relevante Computerdaten verloren gehen oder verändert werden (lit. a) oder dies in den anwendbaren völkerrechtlichen Übereinkünften vorgesehen ist (lit. b).

Zu Art. 32:

Dieser Artikel regelt den grenzüberschreitenden Zugriff auf gespeicherte Computerdaten ohne Zustimmung der anderen Vertragspartei, wobei diese nur in folgenden Fällen zulässig ist: wenn es sich

dabei um öffentlich zugängliche Daten („open source“) handelt, und zwar unabhängig davon, wo sich die Daten geographisch befinden (lit. a); oder wenn sich die Daten auf dem Hoheitsgebiet der betreffenden Vertragspartei befinden und die rechtmäßige und freiwillige Zustimmung der Person, die über die Daten verfügen darf, vorliegt (lit. b).

Zu Art. 33:

Diese Bestimmung regelt die Rechtshilfeleistung bei der Echtzeitüberwachung von Verkehrsdaten und stellt daher das zwischenstaatliche Gegenstück zu Art. 20 dar. Klargestellt wird, dass sich diese grundsätzlich nach dem innerstaatlichen Recht der ersuchten Vertragspartei richtet (Abs. 1). Abs. 2 statuiert allerdings die Verpflichtung zur Entsprechung derartiger Ersuchen unter der Voraussetzung, dass die Erhebung von Verkehrsdaten in Echtzeit in einem gleichartigen nationalen Fall möglich wäre.

Zu Art. 34:

Dieser Artikel statuiert die Verpflichtung zur Rechtshilfeleistung im Zusammenhang mit der Erhebung oder Aufzeichnung von Inhaltsdaten in Echtzeit und stellt daher das zwischenstaatliche Gegenstück zu Art. 21 dar. Diese Form der Rechtshilfe muss nur im Einklang mit den anwendbaren völkerrechtlichen Verträgen und dem innerstaatlichen Recht der ersuchten Vertragspartei geleistet werden.

Zu Art. 35:

Art. 35 sieht die Einrichtung einer Kontaktstelle vor, 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 -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat unverzüglich für Unterstützung zu sorgen. Im Bundesministerium für Inneres/Bundeskriminalamt ist derzeit eine via Email (against-cybercrime@bmi.gv.at) erreichbare Meldestelle im Büro 1.3 „Single Point of Contact (SPOC)“ des Bundeskriminalamtes eingerichtet, welche allerdings noch nicht vollständig die Anforderungen des Art. 35 der Konvention erfüllt. Ergänzend dazu ist daher im Büro 5.2 „Computer- und Netzwerkkriminalität“ des Bundeskriminalamtes eine täglich via SPOC erreichbare 24/7 Rufbereitschaft für notwendige technische Unterstützungen verfügbar. Eine den Erfordernissen des Art. 35 vollständig entsprechende 24/7 Kontaktstelle wird mit Aufnahme des Echtbetriebes des derzeit in Umsetzung befindlichen Cyber-Crime-Competence-Center (C4) im Bundesministerium für Inneres verfügbar sein.

KAPITEL XIII – Schlussbestimmungen

Zu Art. 36:

Art. 36 normiert, dass das Übereinkommen für die Mitgliedstaaten des Europarates und Nichtmitgliedstaaten, die sich an seiner Ausarbeitung beteiligt haben (Kanada, Japan, Südafrika und USA) zur Unterzeichnung aufliegt. Gemäß Abs. 3 tritt das Übereinkommen am ersten Tag des Monats in Kraft, der auf einen Zeitabschnitt von drei Monaten nach dem Tag folgt, an dem fünf Unterzeichner, darunter mindestens drei Mitgliedstaaten des Europarates, nach Abs. 2 ihre Zustimmung ausgedrückt haben durch das Abkommen gebunden zu sein.

Zu Art. 37:

Art. 37 normiert, dass nach dem Inkrafttreten des Übereinkommens auch andere Nichtmitgliedstaaten eingeladen werden können, dem Übereinkommen beizutreten.

Zu Art. 38:

Art. 38 normiert die Hoheitsgebiete, auf welche das Übereinkommen Anwendung findet. Jede Vertragspartei kann durch eine an den Generalsekretär des Europarates gerichtete Erklärung die Anwendung dieses Übereinkommens auf Hoheitsgebiete erstrecken, für deren internationale Beziehungen sie verantwortlich ist oder in deren Namen Verpflichtungen einzugehen sie ermächtigt ist.

Zu Art. 39:

Diese Bestimmung regelt das Verhältnis zu anderen bereits zwischen den Vertragsparteien bestehenden Verträge oder Übereinkünfte.

Zu Art. 40:

Diese Bestimmung regelt, dass jede Vertragspartei mittels der Abgabe einer Erklärung von der Möglichkeit Gebrauch machen kann, nach Art. 2, 3,6 Abs.1 lit.b, 7, 9 Abs.3 und 27 Abs.9 lit.e, zusätzliche Merkmale als Voraussetzung anzusehen.

Zu Art. 41:

Diese Bestimmung normiert die Übernahme von Verpflichtungen nach Kapitel II des Übereinkommens innerhalb eines Bundesstaates („Bundesstaatsklausel“).

Zu Art. 42:

Art. 42 normiert, dass die Vertragsparteien nur jene Vorbehalte anbringen können, die nach den Bestimmungen dieses Übereinkommens ausdrücklich zulässig sind.

Zu Art. 43:

Art. 43 regelt den Status und die Rücknahme von Vorbehalten und legt u.a. fest, dass durch eine an den Generalsekretär des Europarates gerichtete Notifikation Vorbehalte gemäß Art. 42 ganz oder teilweise zurückgenommen werden können.

Zu Art. 44:

Gemäß Art. 44 kann jede Vertragspartei Änderungen zu diesem Übereinkommen vorschlagen kann. Jede vorgeschlagene Änderung wird den Mitgliedstaaten des Europarats, den Nichtmitgliedstaaten, die sich an der Ausarbeitung dieses Übereinkommens beteiligt haben, jedem Staat, der nach Art. 37 beigetreten ist oder zum Beitritt eingeladen wurde sowie dem Europäischen Ausschuss für Strafrechtsfragen (CDPC) übermittelt, der dem Ministerkomitee seine Stellungnahme zu dem Änderungsvorschlag unterbreitet. Nach einer Prüfung und vorheriger Konsultation jeder Nichtmitgliedstaaten, die Vertragsparteien des Übereinkommens sind, kann das Ministerkomitee diesen Änderungsvorschlag annehmen. Dieser tritt am 30. Tag nach dem Tag der angenommenen Änderung in Kraft, an dem alle Vertragsparteien dem Generalsekretär mitgeteilt haben, dass sie die Änderung angenommen haben.

Zu Art. 45:

Art. 45 legt im Falle der Beilegung von Streitigkeiten den Europäischen Ausschuss für Strafrechtsfragen (CDPC) als zuständige Stelle fest.

Zu Art. 46:

Art. 46 legt fest, dass die Vertragsparteien sich regelmäßig über die wirksame Anwendung und Durchführung dieses Übereinkommens konsultieren.

Zu Art. 47:

Gemäß Art. 47 kann jede Vertragspartei dieses Übereinkommen kündigen.

Zu Art. 48:

In Art. 48 werden die Notifikationen, welche der Generalsekretär des Europarates vorzunehmen hat, und die Empfänger dieser Notifikationen definiert.

Die Bundesregierung hat beschlossen, dem Nationalrat vorzuschlagen, anlässlich der Genehmigung des Staatsvertrages zu beschließen, dass die französische Sprachfassung dieses Staatsvertrages gemäß Art. 49 Abs. 2 B-VG dadurch kundzumachen ist, dass sie zur öffentlichen Einsichtnahme im Bundesministerium für europäische und internationale Angelegenheiten aufliegt.

Daran anknüpfend wurde mit Rücksicht auf eine sparsame und zweckmäßige Verwaltung gemäß § 23 Abs. 2 GOG-NR von der Vervielfältigung und Verteilung dieser Sprachfassung Abstand genommen. Die gesamte Regierungsvorlage liegt in der Parlamentsdirektion zur Einsicht auf. Überdies ist diese Regierungsvorlage mit allen Sprachfassungen auf der Homepage des Parlaments unter http://www.parlament.gv.at abrufbar.