Vernehmlassungsentwurf

Eidgenössisches Justiz- und Polizeidepartement

Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität

Vorentwurf und Erläuternder Bericht

Bundesamt für Justiz
Bern, März 2009

Übersicht

Der Bundesversammlung soll beantragt werden, das Übereinkommen des Europarates vom 23. November 2001 über die Cyberkriminalität zu genehmigen. Das am 1. Juli 2004 in Kraft getretene Übereinkommen ist die erste und bisher einzige internationale Konvention, die sich mit Computer- und Netzwerkkriminalität befasst. Sie verpflichtet die Vertragsstaaten, ihre Gesetzgebung den Herausforderungen neuer Informationstechnologien anzupassen. Die Schweiz erfüllt die Anforderungen des Übereinkommens bereits weitgehend; kleinere Anpassungen des Strafgesetzbuches und des Rechtshilfegesetzes sowie die Anbringung von verschiedenen Vorbehalten und Erklärungen sind notwendig.

In einem ersten Teil enthält die Konvention materielle Strafbestimmungen; Ziel ist eine Harmonisierung des Strafrechts unter den Staaten. In einem zweiten Teil des Übereinkommens werden Regelungen für das Strafverfahren getroffen. Es geht vorrangig um Fragen der Beweiserhebung und Beweissicherung von elektronischen Daten in der Strafuntersuchung. Schliesslich behandelt das Übereinkommen die internationale Zusammenarbeit in Strafsachen zwischen den Staaten. Das Zusammenwirken zwischen den verschiedenen Vertragsparteien soll in seinem Ablauf schnell und effizient gestaltet werden.

Die Schweiz hat das Übereinkommen am 23. November 2001 unterzeichnet. Die durch das Parlament verabschiedete Schweizerische Strafprozessordnung vom 5. Oktober 2007, die am 1. Januar 2011 in Kraft treten soll, ermöglicht eine schweizweit einheitliche Umsetzung der verfahrensrechtlichen Bestimmungen des Übereinkommens. Am 27. Februar 2008 hat der Bundesrat die Annahme der Motion Glanzmann-Hunkeler (07.3629) beantragt, welche die Ratifikation der Europaratskonvention fordert.

Das materielle Strafrecht mit seinen am 1. Januar 1995 in Kraft getretenen Bestimmungen im Bereich "Computerstrafrecht" vermag den Erfordernissen der Konvention über weite Strecken zu genügen. Anpassungsbedarf ergibt sich bezüglich des Straftatbestandes des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis des Strafgesetzbuches, sog. "Hacking"-Tatbestand). Hier wird vorgeschlagen, eine Vorverlagerung der Strafbarkeit vorzunehmen: Strafbar soll sich auch machen, wer Programme oder Daten zugänglich macht im Wissen, dass diese für das illegale Eindringen in ein Computersystem verwendet werden sollen. Daneben wird, ausserhalb der Erfordernisse gemäss Konvention, vorgeschlagen, das durch die Lehre verbreitet kritisierte Merkmal der fehlenden Bereicherungsabsicht in Artikel 143bis StGB zu streichen.

In prozessualer Hinsicht vermag die durch das Parlament verabschiedete Schweizerische Strafprozessordnung vom 5. Oktober 2007 (vgl. oben) den Anforderungen des Übereinkommens zu genügen.

Im Bereich der internationalen Zusammenarbeit ist für die Umsetzung der Artikel 30 und 33 der Konvention ebenfalls eine Anpassung (neuer Art. 18b des Bundesgesetzes über internationale Rechtshilfe in Strafsachen) erforderlich. Die schweizerische Vollzugsbehörde wird ermächtigt, Verkehrsdaten vor Abschluss des Rechtshilfeverfahrens weiterzugeben. Diese Möglichkeit lässt sich mit der Kurzlebigkeit von Computerdaten rechtfertigen. Sie ist jedoch nur in zwei besonderen Fällen vorgesehen und wird so weit eingeschränkt, dass die Rechte der betroffenen Person angemessen geschützt bleiben.

Inhaltsverzeichnis

1 Grundzüge des Übereinkommens

1.1 Ausgangslage und Entstehung des Übereinkommens

Durch die beschleunigte und fortschreitende Entwicklung im Bereich der Informationstechnologie wird unsere Gesellschaft als Ganzes einem steten Wandel unterzogen. Alltägliche Handlungen und Aufgaben im Bereich der Kommunikation konnten vereinfacht werden. Daten werden, unabhängig vom Herkunfts- oder Aufbewahrungsort, innert Sekunden an beliebige Empfänger auf der ganzen Welt versandt oder an eine Vielzahl von Personen und Einrichtungen verbreitet. In Computersystemen gespeicherte Informationen können für einen kaum bestimmbaren Personenkreis zugänglich gemacht, gezielt gesucht und entsprechend heruntergeladen werden.

Den positiven wirtschaftlichen, politischen und gesellschaftlichen Effekten dieser globalen Entwicklung stehen jedoch auch negative Aspekte gegenüber. Der technologische Fortschritt, aus dem weite Teile der Bevölkerung einen erheblichen Nutzen zu ziehen vermögen, erlaubt auch die Begehung von neuen Typen von Straftaten oder ermöglicht die Begehung von "herkömmlichen" Delikten mit neuen "digitalen" Mitteln. Betrug mittels Computernetzwerken, Verbreitung illegaler Inhalte über das Internet und Aufforderung zu Hass, Gewalt und Terror sind nur einige Aspekte, die die Öffentlichkeit und nationale sowie internationale Organisationen seit etlicher Zeit beschäftigen.

Im April 1997 begann eine durch das Ministerkomitee des Europarates eingesetzte Expertengruppe mit der Ausarbeitung des Entwurfes für eine Konvention über die Cyberkriminalität. Neben den Mitgliedstaaten beteiligten sich die Vereinigten Staaten von Amerika, Kanada, Südafrika und Japan an den Verhandlungen. Die Arbeiten dauerten bis ins Frühjahr 2001. Nach Verabschiedung des Texts durch die zuständigen Gremien des Europarates wurde der Vertrag am 23. November 2001 in Budapest zur Unterzeichnung aufgelegt. Die Schweiz hat das Übereinkommen bei dieser Gelegenheit unterzeichnet. Die Konvention trat am 1. Juli 2004 in Kraft und wurde bisher von 23 Staaten ratifiziert[1].

1.2 Überblick über den Inhalt des Übereinkommens

Die Europaratskonvention über die Cyberkriminalität ist das erste und bisher einzige internationale Übereinkommen, das sich mit Computer- und Netzwerkkriminalität befasst. Sie verpflichtet die Vertragsstaaten, das materielle Strafrecht, das Strafprozessrecht sowie die Rechtshilfe den Herausforderungen neuer Informationstechnologien anzupassen.

In einem ersten Teil enthält die Konvention materielle Strafbestimmungen; Ziel ist eine Harmonisierung des Strafrechts unter den Staaten. Die Vertragsstaaten werden unter anderem dazu verpflichtet, Computerbetrug, Datendiebstahl, Fälschung von

[1] Stand: Dezember 2008. Die Texte der Konvention sowie des Erläuternden Berichts des Europarates zum Übereinkommen (auf diesen wird in der Folge mehrfach Bezug genommen) sind abrufbar unter http://conventions.coe.int/Treaty/GER/v3DefaultGER.asp (ETS Nr. 185).

Dokumenten mit Hilfe eines Computers oder das Eindringen in ein geschütztes Computersystem unter Strafe zu stellen (Art. 2 bis 8). Die Mitgliedstaaten sollen zudem jede Form von Kinderpornografie auf dem Internet und deren Verbreitung bestrafen (Art. 9). Ebenso sind Verletzungen des Immaterialgüterrechts, welche auf elektronischem Weg erfolgen, strafrechtlich zu ahnden (Art. 10). Weiter müssen auch Unternehmungen für Straftaten im Sinne der Konvention verantwortlich gemacht werden können (Art. 12).

In einem zweiten Teil der Konvention werden Regelungen für das Strafverfahren getroffen. Es geht um Fragen der Beweiserhebung und Beweissicherung von elektronischen Daten in der Strafuntersuchung (Art. 16 bis 21). Computerdaten können durch Zugriff über grosse Distanzen innerhalb von Sekunden verändert werden. Es soll daher sichergestellt werden, dass elektronisch bearbeitete Daten, wenn sie für den Zweck einer Strafuntersuchung verwendet werden, in authentischer Form beigebracht werden können und im Laufe des Verfahrens nicht verfälscht oder vernichtet werden. Von Bedeutung ist dabei, dass Untersuchungsbehörden einen raschen Zugriff auf die betreffenden Daten vornehmen und diese sichern können.

Der dritte Teil der Europaratskonvention schliesslich behandelt die internationale Zusammenarbeit in Strafsachen zwischen den Staaten (Rechtshilfe, Auslieferung, vorläufige Massnahmen u.a.; Art. 23 bis 35). Das Zusammenwirken zwischen den verschiedenen Vertragsparteien soll in seinem Ablauf schnell und effizient gestaltet werden. Die Zusammenarbeit ist, so der Konventionstext, in grösstmöglichem Umfang durchzuführen.

1.3 Würdigung des Übereinkommens

Die vorliegende Europaratskonvention über die Cyberkriminalität nimmt sich der neuen Herausforderungen der Informationstechnologie[2] an die Staaten und die internationale Gemeinschaft an und erkennt die Notwendigkeit, international vernetzte Delinquenz nicht bloss national, sondern über Grenzen hinweg zu bekämpfen und zu verhindern. Das Ansinnen der Konvention, die nationalen Gesetzgebungen im europäischen Raum und darüber hinaus zu harmonisieren und die internationale Zusammenarbeit zu verstärken, ist zu begrüssen. Erste positive Auswirkungen des Vertrages im Rahmen seiner Umsetzung in den Staaten sind zu verzeichnen. In verschiedenen Ländern wurde die entsprechende Gesetzgebung im Bereich der Computerkriminalität angepasst; die Konvention diente dabei als massgebliche Bezugsgrösse und der Europarat als nützlicher Wissensvermittler.

Jedoch darf die Bedeutung des Übereinkommens über die Cyberkriminalität zum heutigen Zeitpunkt auch nicht überschätzt werden. In zahlreichen Ländern bedarf die Infrastruktur bei der Bekämpfung der Cyber-Kriminalität (technische Ausrüstung und Kapazität auf Seiten der Behörden, Überwachungsmöglichkeiten) nach wie vor einer grossen Verbesserung. Die praktischen Auswirkungen der Konvention werden von Mitgliedstaaten mit einem differenzierten, funktionierenden Instrumentarium gegen Computerdelikte als eher gering eingestuft, dies nicht zuletzt aufgrund des fehlenden Monitoring-Mechanismus und eines zurzeit schwach ausgeprägten Austausches zwischen den Mitgliedstaaten.

[2] Vgl. Kap. 1.1.

2 Die Bestimmungen des Übereinkommens und ihr Verhältnis zum schweizerischen Recht

2.1 Kapitel I: Begriffsbestimmungen

2.1.1 Artikel 1 - Begriffsbestimmungen

Artikel 1 umschreibt, für die Anwendung der Konvention, die Begriffe "Computersystem", "Computerdaten", "Diensteanbieter" ("Service Provider") sowie "Verkehrsdaten". Letztgenannte geben insbesondere Aufschluss über Absender und Empfänger, Zeitpunkt, Dauer, Grösse und Weg einer Nachricht. Die Terminologie des Übereinkommens weicht hier von Artikel 2 Buchstabe g der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs[3] ab, wo auf Daten verwiesen wird, welche der Dienstanbieter als Belege für die Tatsache der Sendung aufzeichnet. Im Rahmen des prozessualen Teils der Konvention[4] wird, soweit wesentlich, näher auf den Begriff eingegangen. Die Begriffsbestimmungen des Übereinkommens unterscheiden sich in praktischer Hinsicht jedoch nicht wesentlich von den in der Schweiz angewendeten Begriffen.

2.2 Kapitel II: Innerstaatlich zu treffende Massnahmen

2.2.1 Artikel 2 - Rechtswidriger Zugang

Artikel 2 der Konvention strebt die international einheitliche Kriminalisierung des "Hacking" an. Bestraft werden soll, wer sich vorsätzlich und unrechtmässig Zugang zu einem Computersystem oder einem Teil davon verschafft. Vertragsstaaten können eine Erklärung[5] abgeben, wonach als weitere Voraussetzung für den Eintritt der Strafbarkeit eine Umgehung von Sicherheitsmassnahmen, der Vorsatz, Daten zu erhalten, ein anderer unredlicher Vorsatz oder eine Verbindung mit einem anderen Computersystem vorliegen muss.

Artikel 143bis des Schweizerischen Strafgesetzbuches (StGB)[6] erfasst unbefugte Zugriffe auf Daten durch Eindringlinge, sogenannte "Hacker". Strafbar macht sich, wer ohne Bereicherungsabsicht auf dem Weg von Datenübertragungseinrichtungen unbefugt in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt.

Artikel 2 der Konvention wird durch Artikel 143bis StGB im Wesentlichen abgedeckt. Eine Differenz besteht bezüglich der geforderten Sicherung des Systems. Von einer entsprechenden Abänderung des Strafartikels kann jedoch abgesehen werden. Statt dessen ist eine Erklärung abzugeben, wonach das Überwinden einer Zugangssicherung vorliegen muss[7]. Die Abgabe weiterer Erklärungen zu Artikel 2 der Konvention erscheint hingegen nicht als notwendig. Die Konvention erfordert an dieser Stelle keine gesetzgeberischen Anpassungen.

3 VÜPF, SR **780.11**.
4 Art. 14 ff.
5 Vgl. Art. 40 der Konvention.
6 SR **311**.
7 Diese oder eine ähnliche Erklärung wurde bezüglich Art. 2 bereits durch einige Mitgliedstaaten abgegeben; vgl. die entsprechende Liste der Erklärungen von Staaten unter http://conventions.coe.int/ . Die Möglichkeit der Abgabe von Erklärungen und Vorbehalten wurde bei der Erarbeitung der Konvention ausdrücklich als Bestandteil des einfach gehaltenen Texts vorgesehen (vgl. Ziff. 49 und 50 des Erläuternden Berichts zur Konvention, Fussnote 1).

Die Formulierung von Artikel 143bis StGB, wonach die Tat ohne Bereicherungsabsicht strafbar ist, ist in der Lehre jedoch wiederholt auf Kritik gestossen[8]. Es wird gerügt, dass der aus Neugierde handelnde Täter nach Artikel 143bis bestraft wird, während er im Falle seiner Bereicherungsabsicht unter Umständen straflos bleibe. Diese Auffassung lässt ausser Acht, dass das Eindringen in ein Datenverarbeitungssystem mit Bereicherungsabsicht häufig darum erfolgt, um sich elektronische Daten zu beschaffen, das heisst um diese für sich oder für eine Drittperson zwecks weiterer Verwendung festzuhalten. Strafbarkeit gemäss dem mit höherer Strafe bedrohten Artikel 143 StGB[9] ist in diesem Fall gegeben[10]. Beschafft sich der Eindringling keine Daten, versucht er jedoch, aus seinem Vorgehen einen Vorteil zu schlagen und beispielsweise einen Dritten aufgrund des blossen Eindringens in ein System oder der drohenden Datenbeschädigung zu einer Leistung zu bewegen, so finden die entsprechenden Strafbestimmungen zum Schutze des Vermögens oder der Freiheit Anwendung[11]. Das Kriterium der fehlenden Bereicherungsabsicht in Artikel 143bis StGB erscheint jedoch als irritierend und war in seiner ausschliessenden Anwendung vom Gesetzgeber offenbar nicht eindeutig beabsichtigt. Dem Rechtsanwender stellt sich die nicht leichthin zu beantwortende Frage nach dem Grund der sprachlichen Einschränkung und nach der Grundlage der Strafbarkeit des verwerflicheren Handelns in Bereicherungsabsicht[12]. Auch gerät das Kriterium der fehlenden Bereicherungsabsicht zwangsläufig in Konflikt mit der im Rahmen der Umsetzung von Artikel 6 der Konvention vorgeschlagenen Vorverlagerung der Strafbarkeit[13], wo - zur Vermeidung einer Strafbarkeitslücke - auch das Verbreiten eines Passwortes *mit* Bereicherungsabsicht unter Strafe gestellt werden soll.

Aus diesem Grunde wird im Rahmen der Umsetzung der Europaratskonvention über die Cyberkriminalität vorgeschlagen, eine Streichung des Merkmals der fehlenden Bereicherungsabsicht in Artikel 143bis StGB vorzunehmen (zum Wortlaut siehe Ausführungen zu Artikel 6 der Konvention[14]). Der Kerninhalt des "Hacking" (zuweilen immer noch mit einer fehlenden Bereicherungsabsicht assoziiert) wird auf Taten mit Bereicherungsabsicht ausgedehnt. Dadurch kann dem gesetzgeberischen Willen, wonach das Eindringen in ein System mit Bereicherungsabsicht in jedem Fall strafbar sein soll, explizit entsprochen sowie der ins Feld geführten Kritik Rechnung getragen werden. Dem nicht vollumfänglich auszuschliessenden Risiko einer Strafbarkeitslücke von Artikel 143bis kann begegnet werden. Dringt der Täter mit Bereicherungsabsicht auf elektronischem Weg in ein geschütztes System ein und eignet er sich Daten an, macht er sich wie bisher der unbefugten Datenbeschaffung (Art. 143) schuldig, wodurch Artikel 143bis strafrechtlich konsumiert wird.

8 Ph. Weissenberger, in: Basler Kommentar, Strafrecht II, N 25 zu Art. 143bis, Basel 2007; S. Trechsel et al., Schweizerisches Strafgesetzbuch, Praxiskommentar, St. Gallen 2008, N 10 zu Art. 143bis.

9 Unbefugte Datenbeschaffung.

10 Diese Auffassung wurde auch im Rahmen der parlamentarischen Beratungen vertreten, vgl. Sten. Bulletin des Nationalrates, 1993, S. 935 ff.

11 So etwa Art. 156 (Erpressung) oder Art. 181 StGB (Nötigung).

12 Die beiden Normen von Art. 143 und Art. 143bis fanden sich im ursprünglichen Gesetzesentwurf des Bundesrates vereint (vgl. BBl **1991** II 1009). In dieser ursprünglichen Fassung war die Tatbegehung ohne Bereicherungsabsicht als privilegierte Variante dem Grundtatbestand nachgestellt.

13 Siehe dort.

14 Kap. 2.2.5.

2.2.2 Artikel 3 - Unrechtmässiges Abfangen

Gemäss Artikel 3 der Konvention macht sich strafbar, wer mit technischen Mitteln vorsätzlich und unrechtmässig nicht öffentlich übertragene Computerdaten einschliesslich der elektromagnetischen Abstrahlung abfängt. Abfangen beinhaltet das Abhören, Überwachen, SichBeschaffen oder auch Aufnehmen von Daten[15]. Vertragsstaaten haben angesichts der vergleichbaren Ausgangslage wie bei Artikel 2 der Konvention wiederum die Möglichkeit, mittels Erklärung den Eintritt der Strafbarkeit von weiteren Voraussetzungen abhängig zu machen, und zwar von der Verbindung mit einem anderen Computersystem oder dem Bestehen eines zusätzlichen deliktischen Vorsatzes.

Im schweizerischen Strafrecht findet sich keine mit Artikel 3 der Konvention deckungsgleiche Regelung. Mehrere Strafnormen sorgen für einen jeweils teilweisen Schutz. Artikel 321ter StGB schützt das Post- und Fernmeldegeheimnis, eine Verletzung desselben wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. Der Anwendungsbereich beschränkt sich aber, im Gegensatz zu den Anforderungen der Konvention, grundsätzlich auf Beamte und andere Personen in besonderer Stellung. Die Strafbarkeit gemäss Artikel 143bis StGB ("Hacking") beschränkt sich auf das Eindringen in ein Computersystem. Nicht geschützt werden demnach Übertragungseinrichtungen als solche, es sei denn, diese stellen wiederum Computeranlagen im Sinne der Strafnorm dar[16].

Gemäss Artikel 143 StGB[17] macht sich strafbar, wer sich in Bereicherungsabsicht elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind. Als "Beschaffen" im Sinne des Gesetzes gilt das Erlangen der Verfügungsmacht über die Daten. Nicht notwendig ist, dass der Täter die Informationen auf einen eigenen Datenträger speichert. Es genügt, dass er die erlangten Erkenntnisse für seine Zwecke einsetzen kann[18]. Als Beschaffungshandlung im Sinne des Strafgesetzbuches kommt insbesondere auch das Auffangen und Abhorchen elektromagnetischer Abstrahlung, ausgehend von einem Computersystem oder einer Datenübertragungsanlage, in Frage[19].

Durch die geforderte Sicherung wird der Anwendungsbereich von Artikel 143 StGB auf Fälle beschränkt, wo der Datenberechtigte seinen Willen zum Ausdruck bringt, dass Daten nicht oder nur eingeschränkt zugänglich sein sollen. Ausser dem Verschliessen von Räumen und Behältern kann solches auch mittels Verwendung von Verschlüsselungen, Zugangscodes, biometrischen Schlüsseln oder Passwörtern erreicht werden. Die Sicherung muss *üblicherweise ausreichen*, um einen unbefugten Zugriff zu verhindern[20]. Es ist zum Beispiel nicht erforderlich, dass neben einem marktüblichen Zugangs- und Virenschutz noch spezifische Sicherungsmassnah-

15 Ziff. 53 des Erläuternden Berichts zur Konvention (vgl. Fussnote 1).
16 N. Schmid, Computerkriminalität, Zürich 1994, § 5 N 16.
17 Unbefugte Datenbeschaffung.
18 Evtl. aber ohne sie wirklich einzusetzen (N. Schmid, a.a.O., § 4 N 40 f.).
19 N. Schmid, a.a.O., §4 N 30 und N 51.
20 Vgl. Weissenberger, a.a.O., N 18 zu Art. 143.

men[21] getroffen werden. Der unbefugte Zugriff auf nicht gesicherte Daten oder deren unbefugte Verwendung[22] fällt nicht unter den Tatbestand.

Artikel 3 des Übereinkommens erfasst jedoch nur das unbefugte Abfangen von Computerdaten*übermittlungen*. Bei der Übermittlung von Daten dürfen an die Sicherungsmassnahmen in aller Regel nur geringe Anforderungen gestellt werden[23]. Für den Eintritt der Strafbarkeit nach Artikel 143 StGB sollen in diesen Fällen grundsätzlich keine Sicherheiten wie die Anwendung von Verschlüsselungstechniken vorausgesetzt werden. Artikel 143 StGB entspricht daher insoweit der Bestimmung von Artikel 3 der Konvention. An die Sicherung des nicht-öffentlichen Datenverkehrs sind, wie ausgeführt, keine erhöhten Anforderungen zu stellen. Die Strafbestimmung sieht jedoch vor, dass die tatbestandsmässige Handlung in Bereicherungsabsicht erfolgen muss. Daher ist es notwendig, eine entsprechende Erklärung abzugeben.

Gemäss Erläuterndem Bericht zur Konvention[24] soll auch der Informationsfluss innerhalb eines Computers als Datenübertragung im Sinne von Artikel 3 gelten. Hierunter fallen unter anderem die angesichts der technologischen Entwicklung stetig zunehmenden drahtlosen Übertragungen zwischen Rechnern und peripheren Geräten (beispielsweise Drucker, Tastaturen, Bildschirmen). Diese Daten sind zuweilen, technische Ausrüstung und Kenntnisse vorausgesetzt, relativ leicht abzufangen, gelten aber aufgrund ihres nicht-öffentlichen Charakters, der in der Regel beschränkten Reichweite sowie wegen des Umstandes, dass der gezielt handelnde Täter erhebliche Vorkehrungen treffen muss, um Zugang zu einer solchen Datenübertragung zu erhalten, als gegen einen unbefugten Zugriff besonders gesichert. Artikel 143 StGB ist auch in diesem Fall anwendbar. Eine gesetzgeberische Anpassung ist, neben der Vornahme der erwähnten Erklärung, nicht notwendig.

2.2.3 Artikel 4 - Eingriff in Daten

Artikel 4 der Konvention stellt das vorsätzliche und unbefugte Beschädigen, Löschen, Beeinträchtigen, Verändern oder Unterdrücken von Computerdaten unter Strafe. Eine Vertragspartei kann mittels Vorbehalt erklären[25], dass als Strafbarkeitsvoraussetzung ein grosser Schaden resultieren muss.

Gemäss Artikel 144bis StGB (Datenbeschädigung) wird auf Antrag bestraft, wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte Daten verändert, löscht oder unbrauchbar macht. Daten unbrauchbar macht, wer - auch mit bloss vorübergehender Wirkung - dem Berechtigten den Gebrauch der Daten verunmöglicht[26]. Das Unterdrücken von Daten im Sinne der Konvention wird durch das geltende Recht damit ebenfalls abgedeckt. Gleiches gilt für die Beschädigung und Beeinträchtigung, welche durch die Tatvarianten der Veränderung / Unbrauchbar-

21 Bspw. im Falle eines Angriffs mit sog. "Trojaner-Viren"; vgl. Urteil der 2. Strafkammer des Obergerichts des Kantons Bern vom 13. November 2007, SK-Nr. 2007/187.

22 Bspw. im Falle eines gemeinsam benutzten Computers oder der rechtswidrigen Verwendung von anvertrauten Daten.

23 Vgl. Chr. Schwarzenegger, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in: Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zürich 2002, S. 305 ff..

24 Ziff. 55; vgl. Fussnote 1.

25 Art. 42 der Konvention. Von der Möglichkeit dieses Vorbehaltes haben bereits einige Staaten Gebrauch gemacht, vgl. http://conventions.coe.int/.

26 N. Schmid, a.a.O., N 29 zu Art. 144bis; Stratenwerth, a.a.O., N 49 zu § 14; vgl. auch Ziff. 61 des Erläuternden Berichts (Fussnote 1).

machung erfasst werden. Die geforderte Strafbarkeit ist durch Artikel 144bis StGB gewährleistet.

2.2.4 Artikel 5 - Eingriff in ein System

Gemäss Artikel 5 der Konvention macht sich strafbar, wer vorsätzlich und unbefugt die Funktionsweise eines Computersystems in schwerer Weise hemmt, indem er Daten eingibt, übermittelt, beschädigt, löscht, verschlechtert, abändert oder unterdrückt. Als schwerwiegendes Hemmnis gilt insbesondere auch das Versenden von Daten in solcher Form, Menge oder Frequenz, dass die Funktion eines Rechners erheblich eingeschränkt wird[27]. Der unaufgeforderte Massenversand von E-Mails[28] wird durch die Norm grundsätzlich nicht umfasst[29].

Der Sachverhalt wird abgedeckt durch den Straftatbestand der Datenbeschädigung nach Artikel 144bis StGB, wo das (auch vorübergehende) Unbrauchbarmachen von Daten und das Verhindern des Zugangs zu Daten während einer erheblichen Zeitspanne[30] unter Strafe gestellt werden.

2.2.5 Artikel 6 - Missbrauch von Vorrichtungen

2.2.5.1 Vorgaben des Übereinkommens

In Artikel 6 der Konvention wird das unbefugte vorsätzliche Herstellen, Abgeben, Verschaffen zum Gebrauch, Einführen, Verbreiten oder anderweitig Zur-Verfügung-Stellen von Vorrichtungen, Programmen[31], Zugangscodes sowie Passwörtern, die zur Begehung einer Straftat im Sinne der vorstehenden Artikel gebraucht werden[32], unter Strafe gestellt. Der Vorsatz muss sich, neben der Tathandlung an sich, auch auf die Begehung der genannten Straftat gemäss Artikel 2 bis 5 beziehen[33]. Mit anderen Worten: Der Verkauf oder die Weitergabe eines Programms muss mit Wissen und Willen erfolgen, wonach dieses im Rahmen einer beschriebenen Straftat gebraucht werden soll. Ebenso strafbar erklärt wird der Besitz solchen Materials mit dem Vorsatz, dass dieses im Rahmen einer der genannten Straftaten zum Einsatz gelangt[34].

Auch hier gewährt die Konvention den Mitgliedstaaten verschiedene Möglichkeiten von Vorbehalten und Abweichungen im innerstaatlichen Recht. So kann der strafbare Besitz an eine Mindestanzahl solcher Vorrichtungen gekoppelt werden. Absatz 3 von Artikel 6 sieht die Möglichkeit eines generellen Vorbehaltes vor[35]. Lediglich der Verkauf, das Verbreiten und das Verfügbarmachen von Passwörtern, Codes oder ähnlichen Daten, die den Zugang zu einem Computersystem ermöglichen, muss unter Strafe gestellt werden.

27 Vorsätzliches Blockieren oder Lahmlegen eines Rechners, vgl. Ziff. 67 des Erläuternden Berichts (Fussnote 1).
28 "Spamming". Am 1. April 2007 ist eine entsprechende Strafbestimmung im Schweizer Recht in Kraft getreten (Art. 3 Bst. o des Bundesgesetzes gegen den unlauteren Wettbewerb, SR **241**, BBl **2003** 7951).
29 Ziff. 69 des Erläuternden Berichts (vgl. Fussnote 1).
30 Etwa durch den Versand von grossen, modifizierten Datenpaketen an Server, deren Funktion in der Folge zum Erliegen gebracht wird (vgl. Weissenberger, a.a.O., N 35 zu Art. 144bis, m.w.Hinweisen).
31 Z.B. Virusprogramme, vgl. Ziff. 72 des Erläuternden Berichts (Fussnote 1).
32 Art. 6 Abs. 1 Bst. a.
33 Art. 6 Abs. 1 Bst. a in fine.
34 Art. 6 Abs. 1 Bst. b.
35 Art. 42 der Konvention.

2.2.5.2 Ergänzung von Artikel 143bis StGB

Gemäss Artikel 144bis Ziffer 2 StGB wird bestraft, wer Programme, von denen er weiss oder annehmen muss, dass sie zum Zwecke der Datenbeschädigung oder -veränderung verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt. Es handelt sich um eine Strafbestimmung gegen sogenannte Computerviren, welche Vorbereitungshandlungen zu Datenbeschädigung unter Strafe stellt. Eventualvorsatz im Hinblick auf eine durch einen Dritten begangene Datenbeschädigung genügt[36].

Artikel 6 der Konvention wird durch den erwähnten Strafartikel in seinem Kernbereich abgedeckt. Daneben können, insbesondere in Fällen, wo nicht die Änderung oder Löschung von Daten angestrebt wird oder wo nicht Programme in Verkehr gebracht werden, auch die Bestimmungen über die Gehilfenschaft sowie den Versuch[37] in Verbindung mit den Artikeln 143 und 143bis StGB Anwendung finden.

Bei der Herstellung oder beim Besitz von Vorrichtungen, Programmen oder Ähnlichem mit beabsichtigter illegaler Nutzung kann in Anbetracht von Lehre und Rechtsprechung zum strafrechtlichen (unvollendeten) Versuch im Sinne von Artikel 22 Absatz 1 StGB[38] unter Umständen von einem solchen Versuch und der damit einhergehenden Strafbarkeit ausgegangen werden. Kann dem Hersteller oder Besitzer der entsprechende beabsichtigte Zweck rechtsgenüglich nachgewiesen werden - und hiervon geht der Konventionstext aus -, so dürfte der Betreffende seinen Vorsatz im Sinne der Überschreitung der Versuchsschwelle manifestiert haben (aber noch nicht alles getan haben, um die Tat zu vollenden).

Als Gehilfe wird bestraft, wer zu einem Verbrechen oder Vergehen vorsätzlich Hilfe leistet, mithin also in untergeordneter Stellung die Vorsatztat eines Anderen fördert[39]. Der Gehilfe braucht weder das Opfer noch den Täter noch die bestimmten Tatmodalitäten zu kennen[40]. Das Einführen, Verschaffen und Verbreiten von entsprechenden Vorrichtungen, Passwörtern und Programmen mit Wissen und Willen, dass damit strafbare Handlungen begangen werden, kann eine Gehilfenschaft zu den Straftatbeständen des Computerstrafrechts darstellen. Hierbei ist jedoch zu beachten, dass - neben der versuchten Gehilfenschaft - auch die Beihilfe zu einer (noch) nicht versuchten Haupttat straflos bleibt. Wie beschrieben, muss eine Verbindung und inhaltliche und zeitliche Nähe zu einem konkret geplanten Delikt bestehen.

Nicht strafbar macht sich hingegen, gemäss dem Grundsatz der tatsächlichen Akzessorietät[41], in der Regel derjenige, welcher eine entsprechende Vorrichtung besitzt oder herstellt mit dem Vorsatz, dass diese zu einem unbestimmten zukünftigen Zeitpunkt durch einen unbestimmten Täter zu deliktischen Zwecken eingesetzt wird. Der notwendige Konnex zu einer - zumindest versuchten - Haupttat fehlt. Liegt damit der Fall vor, wo eine Person zum Beispiel einen Zugangscode[42] weitergibt mit dem Vorsatz, dass dieser für ein unbestimmtes Delikt verwendet wird, und wird noch nicht mit der Ausführung einer spezifischen Straftat begonnen, kann gemäss geltendem Recht nicht von einem strafbaren Verhalten ausgegangen werden. Dies

36 Vgl. BGE 129 IV 230.
37 Art. 22 und Art. 25 StGB.
38 Vgl. BGE 114 IV 114, 119 IV 227; S. Trechsel / P. Noll, Schweizerisches Strafrecht, AT I, Zürich 1998, S. 174 ff.
39 Vgl. S. Trechsel, Kurzkommentar, Zürich 1997, N 1 zu Art. 25.
40 Forster, in: Basler Kommentar, StGB I, 2003, N 19 zu Art. 25.
41 Vgl. S. Trechsel, Kurzkommentar, Zürich 1997, N 21 ff. zu VorArt. 24.
42 Und kein Programm im Sinne des Gesetzes.

wird jedoch durch die Konvention gefordert[43]. Eine Ergänzung von Artikel 143bis, die sich auf die illegale Verbreitung von Zugangscodes oder ähnlicher Daten beziehen und damit, ähnlich wie Artikel 144bis Ziffer 2 StGB (Datenbeschädigung), gewisse Vorbereitungshandlungen zum "Hacking" unter Strafe stellen soll [44], ist wie folgt vorzunehmen:

> [1] *Wer ~~ohne Bereicherungsabsicht~~ auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*
>
> [2] ***Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zu dem in Absatz 1 genannten Zweck verwendet werden sollen, in Verkehr bringt oder zugänglich macht**, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.*

Die neu als strafbar erklärte Verbreitung von Zugangscodes und anderen Daten soll als Offizialdelikt ausgestaltet werden. Im Gegensatz zur Tatbestandsvariante des tatsächlichen Eindringens kann bei der blossen Verbreitung von Programmen in aller Regel kein konkretes Angriffsobjekt und kein entsprechender Strafantragsberechtigter ausgemacht werden. Dies gilt zum Beispiel für die Bereitstellung von Daten im Internet, mittels welcher grundsätzlich eine Vielzahl von Systemen "geknackt" werden könnte, die mit demselben Schutz ausgestattet sind.

Daneben wird die Streichung des gesetzlichen Erfordernisses der fehlenden Bereicherungsabsicht vorgeschlagen (vgl. die Ausführungen zu Artikel 3 der Konvention[45]), wodurch die Strafbarkeit der erwähnten "Vortaten", unabhängig von einer Bereicherungsabsicht, auch in systematischer Hinsicht plausibel wird.

Die vorgeschlagene Ergänzung orientiert sich an den Erfordernissen der Konvention und sieht, gegenüber dem geltenden Straftatbestand der Datenbeschädigung, eine geringfügige, als verhältnismässig erachtete Einschränkung der möglichen Tathandlungen[46] vor. Kriminalisiert werden die (weit auszulegenden und zum Teil inhaltlich überlappenden) Tathandlungen des *Zugänglichmachens* und *Inverkehrbringens* von Daten.

Bezüglich des Besitzes, Einführens und Herstellens von entsprechenden Daten, soweit nicht im Hinblick auf die Beschädigung oder Veränderung von Daten erfolgend oder als Gehilfenschaft oder strafbarer Versuch eines anderen Straftatbestandes[47] zu qualifizieren, erscheint es als angebracht, dass die Schweiz einen einschränkenden Vorbehalt anbringt.

2.2.6 Artikel 7 - Fälschung mittels Computer

Strafbar erklärt wird in Artikel 7 das vorsätzliche und unbefugte Einspeisen, Abändern, Löschen oder Unterdrücken von Daten, wodurch nicht-authentische Daten entstehen, mit dem Vorsatz, dass diese für rechtliche Zwecke als authentisch betrachtet werden. Vertragsstaaten können eine Erklärung[48] abgeben, wonach betrügerische oder ähnlich unredliche Absicht vorliegen muss.

43 Vgl. Art. 6 Abs. 3.
44 Vgl. Schmid, a.a.O., N 31 zu Art. 143bis.
45 Kap. 2.2.1.
46 Namentlich bezüglich der Herstellung und Einfuhr von Daten.
47 Insbesondere Art. 143 und 143bis StGB.
48 Art. 40 der Konvention.

Soweit der Täter keinen befugten Zugriff auf die entsprechenden Daten hat, findet die Strafbestimmung der Datenbeschädigung[49] Anwendung. Wirkt der Täter auf einen Datenverarbeitungsvorgang ein und liegt eine Vermögensverschiebung respektive ein Schaden vor, findet Artikel 147 StGB[50] Anwendung. Im Übrigen gilt, dass der Straftatbestand der Urkundenfälschung[51] oder des Versuchs hierzu auch auf elektronische Dateien und Daten Anwendung findet, womit die entsprechende Bestimmung der Konvention durch das geltende Recht abgedeckt wird. Notwendig ist jedoch die Abgabe einer Erklärung, wonach als zusätzliches Tatbestandsmerkmal die Absicht besteht, einen Schaden zu verursachen oder einen Vorteil zu erwirken.

2.2.7 Artikel 8 - Computerbetrug

Artikel 8 der Konvention erklärt das vorsätzliche, unrechtmässige Bewirken eines Vermögensverlustes zu Lasten einer anderen Person mit der betrügerischen oder unredlichen Absicht, sich oder einem Anderen einen Vermögensvorteil zu verschaffen, als strafbar. Der Verlust muss durch Eingabe, Änderung, Unterdrücken oder Löschen von Computerdaten bewerkstelligt (Bst. a) oder durch eine andere Beeinträchtigung der Funktionsweise eines Computersystems (Bst. b) bewirkt werden.

Gemäss Artikel 147 StGB wird der betrügerische Missbrauch einer Datenverarbeitungsanlage unter Strafe gestellt. Im Gegensatz zum "klassischen" Betrugstatbestand[52] wird der Fall abgedeckt, in welchem die Vermögensverschiebung nicht auf einem durch den Täter hervorgerufenen Irrtum eines menschlichen Opfers beruht, sondern durch reine Manipulation von Daten bewirkt wird[53]. Von einer Verwendung von unrichtigen Daten im Sinne des Strafartikels ist beispielsweise auszugehen, wenn der Täter Daten verändert, löscht, umplatziert oder sonstwie tatsachenwidrig abändert. Unrichtig können Daten auch dann sein, wenn sie zum falschen Zeitpunkt eingespeist werden. Ebenso strafbar ist, wer "in vergleichbarer Weise" auf einen Datenverarbeitungs- oder Datenübermittlungsprozess einwirkt und dadurch eine Vermögensverschiebung herbeiführt oder eine solche verdeckt.

Artikel 8 der Konvention wird durch Artikel 147 StGB abgedeckt. Die erfolgte Vermögensverschiebung gehört zum objektiven Tatbestand und muss für die Vollendung des Delikts vorliegen. Nicht erforderlich ist hingegen, dass der Täter tatsächlich profitiert. Beruht die Vermögensverschiebung auf einem durch den Täter hervorgerufenen Irrtum einer Person, findet, auch wenn Datenverarbeitungsvorgänge im Spiel sind, der "ordentliche" Betrugstatbestand Anwendung. Dieser geht der besprochenen Strafbestimmung diesfalls vor[54].

2.2.8 Artikel 9 - Kinderpornografie

Gemäss Artikel 9 der Konvention macht sich strafbar, wer mittels eines Computersystems vorsätzlich Kinderpornografie anbietet, zugänglich macht, verbreitet, übermittelt, sich verschafft, besitzt oder für die Verbreitung mittels Computer herstellt.

Artikel 197 Ziffern 3 und 3^{bis} StGB stellen die entsprechenden Tathandlungen, insbesondere auch den Besitz von kinderpornografischem Material auf elektronischen Datenträgern oder das Herunterladen von solchen Daten, unter Strafe. Durch

49 Art. 144^{bis} Ziff. 1 StGB.
50 Betrügerischer Missbrauch einer Datenverarbeitungsanlage.
51 Art. 251 i.V.m. Art. 110 Abs. 4 StGB.
52 Gemäss Art. 146 StGB.
53 Vgl. hierzu auch N. Schmid, a.a.O., N 1 zu § 7.
54 Vgl. N. Schmid, a.a.O., N 161 zu § 7.

das schweizerische Strafrecht ebenso erfasst werden "real erscheinende Bilder" ("realistic images") im Sinne von Artikel 9 Absatz 2 Buchstabe c der Konvention[55]. Von den entsprechenden Vorbehaltsmöglichkeiten muss kein Gebrauch gemacht werden.

Artikel 9 Absatz 2 Buchstabe b der Konvention bezieht sich auf die Darstellung einer Person mit dem Erscheinungsbild einer minderjährigen Person ("a person appearing to be a minor"). Die Bestimmung des Übereinkommens ist in ihrem Gehalt nicht völlig klar; auch der Erläuternde Bericht vermag keine abschliessende Klärung herbeizuführen. Geht es um Personen, deren Minderjährigkeit nicht abschliessend feststellbar ist, so kann der schweizerische Richter im Rahmen der Beweiswürdigung den Schluss ziehen, inwieweit von einer Handlung mit einem Kind auszugehen ist, und den Täter einer Bestrafung zuführen. Den diesbezüglichen Anforderungen wäre Genüge getan. Geht es in der Konvention, und hierauf deuten verschiedene Sprachfassungen hin, aber um die Darstellung einer erwachsenen Person, die als Kind erscheint, ist die Darstellung gemäss dem geltenden schweizerischen Recht nicht strafbar. Es ist zwar zutreffend, dass sich solche Darstellungen auf den Betrachter korrumpierend auswirken können. Das Gefährdungspotential und die faktische Bedeutung solcher Darstellungen sind jedoch ungleich geringer als die fatalen Auswirkungen der Darstellung von "realer" Kinderpornografie für Betroffene wie Betrachter. Eine entsprechende Ausweitung der Strafbarkeit erscheint daher nicht als opportun. Es wird die Erklärung eines Vorbehaltes vorgeschlagen, wonach Buchstabe b von Absatz 2 nicht Anwendung findet.

Als "Kinder" im Sinne von Artikel 197 StGB gelten gemäss herrschender Lehrmeinung und Praxis Personen unter 16 Jahren[56]. Dies entspricht dem Schutzalter im Sinne von Artikel 187 StGB[57]. Diese Altersgrenze soll jedoch gemäss verschiedentlich geäusserter Auffassung nicht das alleinige Kriterium für das absolute Verbot von entsprechenden Darstellungen sein. Als strafwürdig erweisen könne sich auch die Abbildung von älteren, körperlich jedoch wenig entwickelten Jugendlichen; massgeblich müsse auch der vermittelte Eindruck und die offensichtliche Ausrichtung auf den pädophilen Betrachter sein. Im Rahmen der Umsetzung und Ratifikation der Konvention besteht die Möglichkeit zur Erklärung[58], wonach das Alter von 16 Jahren auch bezüglich Artikel 9 Absatz 3 der Konvention zur Anwendung gelangen soll. Von dieser Möglichkeit soll durch die Schweiz angesichts der (zwar nicht ausnahmslos geltenden) Altersgrenze von 16 Jahren Gebrauch gemacht werden.

Auf internationaler Ebene wird vermehrt eine strikte Alterslimite von 18 Jahren postuliert. Die Notwendigkeit und Angemessenheit einer Anpassung der Altersgrenze der Strafbarkeit von sexuellen Handlungen mit Kindern respektive für entsprechende Darstellungen muss im gesamten Kontext einer allfälligen Umsetzung der Europaratskonvention zum Schutze von Kindern gegen sexuelle Ausbeutung und sexuellen Missbrauch vom 15. Oktober 2007 später vertieft geprüft werden.

55 Vgl. Botschaft über die Änderung des StGB und MStG vom 10. Mai 2000, BBl **2000** 2983.
56 Vgl. Schwaibold/Meng, Basler Kommentar, a.a.O., N 21 ff. zu Art. 197.
57 Sexuelle Handlungen mit Kindern.
58 Art. 40 der Konvention.

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

In dieser Bestimmung weicht die französische Fassung, im Gegensatz zur deutschen, von der in der Schweiz gebräuchlichen Terminologie ab[59]. Die Schweiz hat sämtliche in Artikel 10 der Europaratskonvention über die Cyberkriminalität aufgeführten Übereinkommen ratifiziert. Es sind dies:

- die Berner Übereinkunft zum Schutze von Werken der Literatur und Kunst, in der Pariser Fassung vom 24. Juli 1971[60];
- das Internationale Abkommen vom 26. Oktober 1961 über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen[61];
- das Abkommen über handelsbezogene Aspekte der Rechte an geistigem Eigentum[62];
- der WIPO-Urheberrechtsvertrag vom 20. Dezember 1996[63];
- der WIPO-Vertrag vom 20. Dezember 1996 über Darbietungen und Tonträger[64].

Mit der Teilrevision des Urheberrechtsgesetzes[65], die am 1. Juli 2008 in Kraft getreten ist, wurde die schweizerische Gesetzgebung an die beiden WIPO-Verträge (WCT und WPPT) angepasst. Das WCT und das WPPT sind ratifiziert und für die Schweiz gleichzeitig mit dem revidierten Urheberrecht in Kraft getreten.

Wie der Erläuternde Bericht des Europarates präzisiert, wird mit dem Zusatz "aufgrund ihrer Verpflichtungen" in beiden Absätzen "klargestellt, dass eine Vertragspartei dieses Übereinkommens nicht verpflichtet ist, aufgeführte Übereinkünfte anzuwenden, bei denen sie nicht Vertragspartei ist"[66]. Die Konvention ist demnach so formuliert, dass den Vertragsstaaten aus internationalen Übereinkommen, die sie nicht ratifiziert haben, keine Verpflichtungen erwachsen. Die Schweiz ist gleichermassen an die Berner Übereinkunft, das Rom-Abkommen, das TRIPS-Abkommen sowie das WCT und WPPT gebunden. Deshalb ist mit Blick auf diese Übereinkommen zu prüfen, welche Verpflichtungen sie aufgrund der Europaratskonvention über die Cyberkriminalität erfüllen muss.

Die Schweiz hat im URG die Rechte anerkannt, die in den von ihr ratifizierten Übereinkommen vorgesehen sind. In den Artikeln 67 bis 69a dieses Gesetzes hat sie die entsprechenden Verletzungen des Urheberrechts und der verwandten Schutzrechte zu Straftatbeständen erhoben. Diese Strafbestimmungen erlauben auch, wie dies Artikel 10 der Konvention verlangt, die Verfolgung von Straftaten, die "mittels eines Computersystems" begangen werden.

59 In der französischen Fassung von Art. 10 wird eine etwas eigentümliche Terminologie verwendet. So wird "copyright" mit "propriété intellectuelle" (geistiges Eigentum) übersetzt statt mit "droit d'auteur" (Urheberrecht). Auch wurden nicht immer die offiziellen französischen Titel der zitierten internationalen Abkommen übernommen (vgl. TRIPS-Abkommen und WCT). Auf internationaler Ebene wird im Französischen der Ausdruck "droits connexes" verwendet, während diese Rechte in der Schweiz als "droits voisins" (verwandte Schutzrechte) bezeichnet werden.

60 SR **0.231.15**.

61 Rom-Abkommen; SR **0.231.171**.

62 TRIPS-Abkommen, Anhang 1C des Abkommens vom 15. April 1994 zur Errichtung der Welthandelsorganisation; SR **0.632.20**.

63 WCT; SR **0.231.151**.

64 WPPT; SR **0.231.171.1**.

65 URG; SR **231.1**.

66 Ziff. 110 in fine des Erläuternden Berichts (Fussnote 1).

Das URG wird auch dem Erfordernis der Vorsätzlichkeit gerecht, indem es explizit "vorsätzlich" begangene Taten unter Strafe stellt. Ebenso erfüllt es die Voraussetzung, dass die Rechtsverletzungen "in gewerbsmässigem Umfang" begangen werden, indem es vorschreibt, "gewerbsmässig" begangene Taten von Amtes wegen zu verfolgen. Das URG geht hier noch weiter und ermöglicht in den anderen Fällen die Verfolgung auf Antrag.

Ausserdem wurde das URG so revidiert und an das WCT und WPPT angepasst, dass die Schweiz sämtliche durch Artikel 10 der Konvention auferlegten Verpflichtungen erfüllt.

2.2.10 Artikel 11 - Versuch, Anstiftung und Gehilfenschaft

Artikel 11 der Konvention wird durch das geltende schweizerische Strafrecht, insbesondere Artikel 22, 24 und 25, abgedeckt.

2.2.11 Artikel 12 - Verantwortlichkeit juristischer Personen

Gemäss Artikel 12 der Konvention sollen juristische Personen für strafbare Handlungen im Sinne der Konvention haftbar gemacht werden können, die zu ihren Gunsten von einer natürlichen, eine leitende Position im Unternehmen innehabende Person begangen werden (Abs. 1). Die Unternehmung soll ebenso haften für die Begehung einer Straftat im Sinne der Konvention, ausgeführt zu ihren Gunsten durch eine Person unter ihrer Führung, wenn eine mangelhafte Kontrolle von Seiten einer leitenden Person nachgewiesen wird (Abs. 2).

Die Haftung kann zivil-, verwaltungs- oder strafrechtlicher Natur sein (Abs. 3) und soll der allfälligen Strafbarkeit einer natürlichen Person, welche die Straftat begangen hat, nicht entgegen stehen (Abs. 4).

Zahlreiche internationale Strafrechtsübereinkommen der letzten Jahre kennen ähnliche, zum Teil identische Regelungen der Verantwortlichkeit von Unternehmen. So sieht etwa die Strafrechtskonvention des Europarates über die Korruption vom 27. Januar 1999[67] ebenfalls die Verantwortlichkeit für Unternehmen vor, ohne jedoch ausdrücklich auf den zivil-, verwaltungs- oder strafrechtlichen Aspekt einzugehen[68]. Der - trotz einer gegenläufigen internationalen Tendenz - nach wie vor verbreitete Grundsatz, wonach sich Unternehmen nicht strafbar machen können, wird durch die Übereinkommen geschützt. Jedoch müssen die Staaten sicherstellen, dass auch juristische Personen angemessenen Sanktionen oder Massnahmen, darunter Geldsanktionen, unterliegen[69].

Die strafrechtliche Unternehmungshaftung wurde am 1. Oktober 2003 in das Schweizer Recht eingefügt[70]. Eine primäre Verantwortlichkeit des Unternehmens besteht für eine beschränkte Zahl bestimmter Deliktskategorien, wenn dem Unternehmen vorzuwerfen ist, dass es nicht alles Erforderliche und Zumutbare vorgekehrt hat, um eine solche Straftat zu verhindern[71]. Die durch die Europaratskonvention umfassten Straftaten[72] fallen nicht unter die erwähnten Deliktskategorien[73].

In die Schweizer Rechtsordnung wurde gleichzeitig auch eine allgemeine subsidiäre strafrechtliche Verantwortlichkeit der juristischen Person eingeführt für den Fall, dass die Tat im Rahmen des Unternehmenszwecks begangen wurde und wegen mangelhafter Organisation des Unternehmens keiner bestimmten natürlichen Person zugeordnet werden kann[74]. Die Strafe ist Busse bis zu fünf Millionen Franken. Diese strafrechtliche Haftung bezieht sich auf die Gesamtheit der Verbrechen und Vergehen gemäss schweizerischer Rechtsordnung[75] und deckt alle Delikte gemäss Konvention ab. Sie geht, im Vergleich zum Konventionstext, in dem Sinne weiter, als dass dieser sich auf Straftaten beschränkt, die zum Vorteil der juristischen Person und durch einen Vertreter des Managements begangen werden, während die Haftung gemäss StGB bei jedem Verbrechen oder Vergehen, begangen im Rahmen des Unternehmungszwecks durch eine Person in Ausübung einer geschäftlichen Verrichtung, greift. Gemäss Artikel 102 Absatz 1 StGB ist jedoch die Bestrafung der juristischen Person grundsätzlich nur dann möglich, wenn das Verhalten keiner natürlichen Person zugerechnet werden kann.

Artikel 12 Absatz 4 der Konvention statuiert in diesem Zusammenhang, dass die Strafbarkeit der juristischen Person nicht die Verantwortlichkeit des Täters berühren soll. Es stellt sich die Frage, ob damit die Verpflichtung der Staaten zu einer parallelen strafrechtlichen Haftung eingeführt wird. Der Erläuternde Bericht zum Übereinkommen gibt hierzu keine weiteren Hinweise.

Die subsidiäre Verantwortlichkeit der juristischen Person im Schweizer Recht steht der Strafbarkeit der natürlichen Person nicht entgegen, verhindert diese also nicht. Sie findet dann Anwendung, wenn der Täter aufgrund der mangelhaften Organisation des Unternehmens nicht einer Bestrafung zugeführt werden kann. Artikel 102 Absatz 1 StGB steht daher nicht im Widerspruch zu Artikel 12 Absatz 4 der Konvention, weil die strafrechtliche Haftung der handelnden natürlichen Personen durch die subsidiäre Unternehmenshaftung nicht ausgeschlossen wird. Dies verdeutlicht die folgende Konstellation: Wird die fehlbare natürliche Person und ihr Verhalten nach Verurteilung der Unternehmung doch noch festgestellt und lag der Grund für die zunächst unmögliche Zurechnung in der Organisation der Unternehmung, so steht einer Bestrafung beider Parteien - der natürlichen sowie der juristischen Person - grundsätzlich nichts entgegen[76].

Neben der strafrechtlichen Haftung steht zudem das Instrument der verwaltungsrechtlichen Haftung und die entsprechenden Sanktionen zur unmittelbaren Verhütung zukünftiger Schädigungen, beispielsweise durch Entzug einer Bewilligung oder der Verweigerung der Zulassung einer Unternehmung in einem Marktsegment oder Tätigkeitsbereich, zur Verfügung. Die Schweizer Rechtsordnung kennt verschiedene

67 SEV 173, Art. 18; SR **0.311.55**.
68 Im betreffenden Erläuternden Bericht (Ziff. 86) wird jedoch wiederum ausgeführt, dass die Staaten nicht dazu verpflichtet werden, Strafbarkeit bezüglich juristischer Personen einzuführen.
69 Vgl. Art. 13 der Konvention.
70 Heute Art. 102 und 102*a* StGB.
71 Art. 102 Abs. 2 StGB.
72 Art. 2 bis 9 der Konvention.
73 Im Katalog finden sich insbesondere Korruptionstatbestände sowie das Delikt der Geldwäscherei.
74 Art. 102 Abs. 1 StGB.
75 Mit Freiheitsstrafe oder mit Geldstrafe bedrohte Delikte; vgl. Art. 10 StGB.
76 Vgl. Niggli/Gfeller, Basler Kommentar, Basel 2007, N 113 zu Art. 102.

solcher Mechanismen, welche jedoch nicht umfassend auf alle Unternehmungen angewendet werden können und auch nur in gewissen Bereichen des Marktes und der Wirtschaft bedeutsam sind. So können gegen Unternehmen, die einer staatlichen Aufsicht unterstellt sind, verwaltungsrechtliche Sanktionen verhängt werden. Die Eidgenössische Finanzmarktaufsicht kann beispielsweise einem Bankinstitut, welches die Voraussetzungen der Bewilligung nicht mehr erfüllt oder seine gesetzlichen Pflichten grob verletzt, die Bewilligung zur Geschäftstätigkeit entziehen[77].

Daneben können Personenverbindungen und Anstalten mit unsittlichem oder widerrechtlichem Zweck das Recht der Persönlichkeit nicht erlangen. Entsprechend sind sie aufzuheben, und ihr Vermögen fällt dem Gemeinwesen zu[78]. Schliesslich stehen zivilrechtliche Mittel und Instrumente zur Verfügung, damit Unternehmen, zu deren Gunsten ein leitender Angestellter Straftaten verübt oder seine Aufsichtspflichten bezüglich der Tatbegehung durch einen Angestellten vernachlässigt hat, für den eingetretenen Schaden haftbar gemacht werden können.

Es kann daher gesamthaft betrachtet davon ausgegangen werden, dass das schweizerische Recht den Anforderungen von Artikel 12 der Konvention genügt. Die geltenden Regelungen der subsidiären strafrechtlichen Verantwortlichkeit gehen zum Teil weiter als durch das Übereinkommen gefordert und stellen sicher, dass Verbrechen und Vergehen, begangen im Rahmen des Zwecks einer Unternehmung, auch dann nicht ungesühnt bleiben, wenn die Tat keiner natürlichen Person zugerechnet werden kann. Die subsidiäre Unternehmenshaftung dürfte zudem gerade bei den hier in Frage stehenden Delikten von grösserer Bedeutung sein, da sich die handelnden natürlichen Personen bei Netzwerkdelikten mit erhöhter Wahrscheinlichkeit nicht ermitteln lassen. Von einer Aufnahme der Delikte gemäss Konvention in den erwähnten Deliktskatalog der primären strafrechtlichen Unternehmungshaftung im Schweizer Recht oder einer generellen Ausweitung des Katalogs kann daher abgesehen werden[79].

2.2.12 Artikel 13 - Sanktionen und Massnahmen

Absatz 1 von Artikel 13 verpflichtet die Vertragsstaaten, sicherzustellen, dass Straftaten gemäss Übereinkommen mit angemessenen Sanktionen, darunter auch Freiheitsstrafe, geahndet werden können. Das geltende schweizerische Recht entspricht diesem Erfordernis, indem die einschlägigen Delikte alle mit Freiheitsstrafe bedroht sind.

Gemäss Absatz 2 sollen auch juristische Personen im Sinne von Artikel 12 angemessenen Sanktionen oder Massnahmen, welche strafrechtlicher oder anderer Natur sein können und jedenfalls auch Geldsanktionen umfassen, unterliegen. Das schweizerische Recht vermag auch diesen Anforderungen zu genügen, indem neben der subsidiären strafrechtlichen Verantwortlichkeit von Unternehmen[80] mit Bussenandrohung bis fünf Millionen Franken auch mittels zivil- oder verwaltungsrechtlichen Urteilen oder Verfügungen Sanktionen gegen fehlbare Unternehmungen erlassen werden können, welche wirksam, verhältnismässig sowie abschreckend sind.

77 Art. 23^{quinquies} des Bankengesetzes vom 8. November 1934, SR **952.0**.
78 Art. 52 und Art. 57 ZGB.
79 Dies im Gegensatz zu den erwähnten internationalen Strafrechtsübereinkommen gegen Korruption, wo die Verknüpfung der Konventionsdelikte mit der wirtschaftlichen Tätigkeit von Unternehmungen ungleich grösser ist.
80 Vgl. oben, Art. 12.

2.2.13 Artikel 14 - Geltungsbereich der verfahrensrechtlichen Bestimmungen

Absatz 2 Buchstabe b der Bestimmung stellt den Grundsatz auf, wonach die folgenden prozessrechtlichen Bestimmungen nicht nur für die Verfolgung von Straftaten im Sinne der Konvention, sondern allgemein bei mittels eines Computersystems begangenen Delikten Anwendung finden. Absatz 2 Buchstabe c hält darüber hinaus fest, dass die Bestimmungen auch auf die Sammlung elektronisch verfügbarer Beweise zur Aufklärung beliebiger Straftaten[81] Anwendung finden. Die Konvention will damit sicherstellen, dass elektronisch gespeicherte Daten im Rahmen von Strafverfahren im selben Rahmen als Beweismittel genutzt werden können wie "analoge", herkömmliche Beweismittel[82].

Aus diesem erweiterten Anwendungsbereich heraus ist zu prüfen, ob sich in prozessrechtlicher Hinsicht Anpassungsbedarf ergibt und inwieweit zum Beispiel die prozessualen Regeln betreffend Überwachung, Beschlagnahme, Einziehung und allgemeine Beweiserhebung auch auf elektronische Medien anwendbar sind.

Die nationale Grundlage für die Regelung des Prozessrechts im weiten Sinne bilden zum Einen die verschiedenen Strafprozessordnungen auf Stufe Bund und Kantone sowie, zum Anderen, das seit dem 1. Januar 2002 in Kraft stehende Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs[83] und die dazugehörige Verordnung[84]. Das BÜPF wird auch nach Inkrafttreten der Schweizerischen Strafprozessordnung vom 5. Oktober 2007[85] Geltung haben (Vollzug der Überwachung); dagegen werden die strafprozessualen Regeln[86] in die StPO überführt. Vorliegend wird auf das geltende Recht Bezug genommen. Wo die Regelungen der StPO wesentliche Neuerungen beinhalten, wird hingegen auch auf diese verwiesen.

Artikel 14 Absatz 3 Buchstabe b befasst sich mit sogenannten "geschlossenen Nutzergruppen", also beispielsweise mit firmeninternen elektronischen Netzwerken. Gemäss Artikel 1 Absatz 4 und Artikel 15 Absatz 8 BÜPF haben Betreiber von internen Fernmeldenetzen und Hauszentralen die Überwachung zu dulden sowie die notwendigen Auskünfte zu erteilen; das Gewinnen und die Sicherstellung entsprechender Daten ist damit auch in diesem nicht-öffentlichen Bereich grundsätzlich möglich[87].

2.2.14 Artikel 15 - Bedingungen und Garantien

Artikel 15 beinhaltet die Verpflichtung der Vertragsstaaten, die Menschenrechte und Grundfreiheiten zu respektieren und im Zusammenhang mit der Umsetzung des vorliegenden Übereinkommens zu garantieren. Insbesondere soll auch das Prinzip der Verhältnismässigkeit von Verfahrenshandlungen Berücksichtigung finden. So soll die Art von prozessualen Zwangsmassnahmen der Schwere und Art des untersuchten Delikts entsprechen und nicht unverhältnismässig bezüglich der Einwirkungen oder des Aufwandes sein.

81 "De toute infraction pénale".
82 Vgl. EB Ziff. 141.
83 BÜPF, SR **780.1**.
84 VÜPF, SR **780.11**.
85 StPO, BBl **2007** 6977, Inkrafttreten geplant auf 1.1.2011.
86 Art. 3-10 BÜPF.
87 Unter der Voraussetzung der Verfügbarkeit der Daten.

2.2.15 Artikel 16 - Umgehende Sicherung gespeicherter Computerdaten

Artikel 16 der Konvention verpflichtet die Staaten, dafür zu sorgen, dass die zuständigen Untersuchungsbehörden die beschleunigte Sicherung von gespeicherten Computerdaten[88] anordnen oder bewirken können. Erfolgt die Anordnung der Sicherung gegenüber einer anderen Person, zum Beispiel einem Dienstanbieter, so kann dieser verpflichtet werden, die Daten für einen beschränkten Zeitraum unverändert aufzubewahren.

Die verschiedenen Strafprozessordnungen entsprechen dem Erfordernis der beschleunigten Sicherung, indem elektronische Daten im Rahmen der Erhebung und Sicherung von Beweismitteln durch die Untersuchungsbehörden unter Wahrung der Verhältnismässigkeit auch beschleunigt gesichert werden können. Gemäss Schweizerischer Strafprozessordnung vom 5. Oktober 2007[89] fallen elektronische Datenträger und Dateien unter den Begriff der sachlichen Beweismittel und können entsprechend zu den Akten genommen[90] oder mittels Durchsuchung sichergestellt werden[91].

Die Konvention regt darüber hinaus an, dass eine erste Sicherung auch erreicht werden kann, indem (vertrauenswürdige) Drittpersonen mittels Verfügung dazu verpflichtet werden, Daten aufzubewahren. Es besteht jedoch keine Verpflichtung für Vertragsstaaten, solche "preservation orders" einzuführen[92]. Es genügt vielmehr, wenn die entsprechende Sicherung durch die Behörden selber vorgenommen wird.

Das geltende Schweizer Recht kommt dieser Anregung der Konvention zumindest teilweise, und zwar bezüglich spezifischer Daten bei Internet-Diensteanbietern, in genereller Manier nach. Provider werden gemäss BÜPF dazu verpflichtet, Verkehrs- und Rechnungsdaten für die Dauer von sechs Monaten aufzubewahren[93]. Sie können jedoch auch, im Einzelfall, mittels Verfügung der zuständigen Behörde dazu angehalten werden, eine vorübergehende Sicherung von Datenmaterial vorzunehmen. Die Möglichkeit, jedermann mittels Verfügung zur Aufbewahrung von Daten zu verpflichten, ginge jedoch in diesem Kontext zu weit und wäre auch kaum mit Artikel 15 der Konvention (Grundsatz der Verhältnismässigkeit) vereinbar. Den Erfordernissen der Konventionsbestimmung wird durch das geltende Recht Genüge getan.

88 Einschliesslich Verbindungsdaten, d.h. Daten über Teilnehmer, Zeitpunkt, Dauer und Weg einer Kommunikation; vgl. auch Art. 2 Bst. g VÜPF.
89 Vgl. Ausführungen zu Art. 14 der Konvention.
90 Art. 192 ff. StPO.
91 Art. 246 ff. StPO.
92 Vgl. EB Ziff. 160 des Erläuternden Berichts (Fussnote 1).
93 Art. 15 Abs. 3 BÜPF: Aufbewahrung von Identifikations- sowie von Verkehrs- und Rechnungsdaten. Die Verlängerung der Frist auf ein Jahr ist absehbar (jedoch nicht durch die Konvention gefordert; vgl. Ziff. 161 in fine des Erläuternden Berichts).

2.2.16 Artikel 17 - Umgehende Sicherung und teilweise Weitergabe von Verkehrsdaten

Artikel 17 der Konvention verlangt, dass die Sicherung von Verkehrsdaten[94] gemäss Artikel 16 auch gewährleistet wird für den Fall, wo mehrere Dienstanbieter an einer Kommunikation beteiligt waren (Abs. 1 Bst. a).

Die Schweizer Rechtsordnung entspricht dem Erfordernis von Absatz 1 Buchstabe a. Gemäss Artikel 15 Absatz 3 BÜPF werden Anbieterinnen dazu verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie Verkehrs- und Rechnungsdaten für die Dauer von sechs Monaten aufzubewahren. Sind mehrere Anbieterinnen beteiligt, erteilt die Behörde einer Anbieterin einen behördlichen Überwachungsauftrag, worauf die übrigen Anbieterinnen ihre Daten an diese liefern (Abs. 2 von Art. 15). Der Umstand, wonach mehrere Dienstanbieter an einer Kommunikation beteiligt sind, steht damit einer umgehenden Sicherung von Verkehrsdaten nicht entgegen.

Artikel 17 Absatz 1 Buchstabe b des Übereinkommens sieht vor, dass der Dienstanbieter, gegenüber welchem die Sicherung von Verkehrsdaten erwirkt wird, den zuständigen Behörden die notwendigen Verkehrsdaten eröffnet, damit weitere Provider und der Kommunikationsweg eruiert werden können. Die ersuchenden Behörden haben die erwünschten Daten genügend zu spezifizieren. Es geht zu diesem Zeitpunkt noch nicht darum, dass Urheber oder Empfänger von Nachrichten namentlich festgestellt werden können[95].

Mit Inkrafttreten der Schweizerischen Strafprozessordnung vom 5. Oktober 2007[96] wird die Staatsanwaltschaft für sämtliche Verbrechen und Vergehen Auskunft verlangen können über Verbindungen (Absender und Empfänger, Zeitpunkt) und andere Verkehrs- sowie Rechnungsdaten (Art. 273 StPO). Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht, ist aber unabhängig von einem Deliktskatalog und kann auch rückwirkend verlangt werden. Der Ausschluss von blossen Übertretungstatbeständen steht, unter Berücksichtigung des Prinzips der Verhältnismässigkeit[97], der Erfüllung der Erfordernisse gemäss Konvention nicht entgegen. Den Anforderungen der Konvention kann damit durch das geltende Recht entsprochen werden.

Im Übrigen bleibt Artikel 14 Absatz 4 BÜPF für alle über das Internet begangene Straftaten[98], mithin auch für Übertretungen, anwendbar. Gemäss dieser Bestimmung wird die Anbieterin dazu verpflichtet, der zuständigen Behörde alle Angaben zu machen, damit der Urheber der Straftat eruiert werden kann. Hierzu gehören auch Informationen und Daten, mittels welcher der Kommunikationspfad festgestellt werden kann. Artikel 14 Absatz 4 ist im Bereich "Internet" umfassend anzuwen-

94 "Traffic data" betreffen Herkunft, Empfänger, Zeitpunkt und -dauer oder Weg der Kommunikation. Verkehrsdaten geben jedoch nicht zwangsläufig direkten Aufschluss über die Identität und Anschrift des Absenders (Art. 1 Bst. d der Konvention, vgl. Ziff. 30 des Erläuternden Berichts, Fussnote 1). Es kann sich hierbei auch um die IP-Adresse handeln. Vertragsstaaten sind in diesem Zusammenhang frei, verschiedene Arten von Verkehrsdaten zu schützen (Ziff. 31 des Erläuternden Berichts).

95 Ziff. 169 des Erläuternden Berichts (vgl. Fussnote 1).

96 Geplant auf dem 1.1.2011.

97 Art. 15 der Konvention.

98 Dieser Terminus kann gegenüber Delikten, welche "mittels eines Computersystems begangen" werden, eine Einschränkung darstellen.

den[99] und bezieht sich sowohl auf statische wie auf dynamische IP-Adressen[100]. In beiden Fällen ist daher nicht von einer Überwachungsmassnahme im herkömmlichen Sinne des BÜPF auszugehen; die Untersuchungsbehörde kann direkt und unabhängig von der geltend gemachten Straftat[101] eine Anfrage beim zuständigen Dienst vornehmen.

2.2.17 Artikel 18 - Anordnung der Herausgabe

Gemäss Artikel 18 Absatz 1 Buchstabe a der Konvention kann die zuständige Untersuchungsbehörde jede Person dazu verpflichten, sich in ihrem Besitz befindliche gespeicherte Computerdaten herauszugeben. Diese Bestimmung wird durch das schweizerische Recht abgedeckt (Editionspflicht der nicht beschuldigten Person) und findet sich inhaltlich auch im Rahmen der Schweizerischen Strafprozessordnung wieder[102]. Im Falle der Weigerung besteht die Möglichkeit von Zwangsmassnahmen.

Des Weiteren werden Dienstanbieter (Abs. 1 Buchst. b) dazu verpflichtet, auf Anordnung der zuständigen Behörden Kundendaten[103], jedoch keine Verbindungsdaten oder Inhaltsdaten, mitzuteilen. Damit regelt Artikel 18 der Konvention[104] nicht die Teilnehmeridentifikation im Rahmen von unmittelbaren spezifischen Datenübertragungen, sondern befasst sich - unabhängig vom erfolgten oder bevorstehenden Datenverkehr - mit der Identifikation von Teilnehmern im Netz. Es stellt sich an dieser Stelle nicht die Frage der Überwachung derselben[105]. Wie zu Artikel 17 der Konvention ausgeführt, kann die Untersuchungsbehörde für sämtliche Verbrechen und Vergehen Auskunft verlangen über Verbindungen und andere Verkehrs- sowie Rechnungsdaten[106]. Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht, ist aber unabhängig von einem Deliktskatalog und kann auch rückwirkend verlangt werden.

Artikel 14 Absatz 4 BÜPF findet auch an dieser Stelle Anwendung[107]. Zu liefern sind insbesondere Name und Adresse des Teilnehmers sowie andere Adressierungselemente gemäss dem Fernmeldegesetz vom 30. April 1997[108].

Artikel 18 Absatz 1 Buchstabe b der Konvention beschränkt sich auf Daten, welche durch den Provider gehalten werden, und schreibt diesen nicht vor, in welchem Umfang und für wie lange die Informationen gespeichert und damit verfügbar gemacht werden müssen. Sind entsprechende Daten im einzelnen Fall aufgrund der

99 Vgl. Entscheid der Rekurskommission Reko UVEK vom 27.4.2004, J-2003-162, abrufbar unter www.reko-inum.admin.ch.

100 Eine *statische* IP (Internet-Protokoll)-Adresse besteht aus einer eindeutigen viergliedrigen Zahl, die einem mit dem Internet verbundenen Rechner zugewiesen ist. Demgegenüber ist eine *dynamische* IP-Adresse nicht dauerhaft oder zeitunabhängig einem festen Anschluss zugeordnet. Sie stellt heute nach wie vor den Regelfall dar und wird dem Benutzer vom angewählten Anbieter jeweils für die Dauer der Internet-Sitzung zur Verfügung gestellt. Damit wird eine dynamische Adresse täglich von einer Vielzahl von Personen benutzt. Technisch betrachtet muss rückwirkend in den sogenannten "Logfiles" gesucht werden, um zu einem spezifizierten Zeitpunkt den Adressenbenutzer ermitteln zu können.

101 Der Katalog von Art. 3 BÜPF ist nicht anwendbar.

102 Vgl. Art. 263 ff. StPO, insb. Art. 265: Herausgabepflicht.

103 "Subscriber information", z.B. Identität des Kunden, Angaben über Zahlungsverkehr.

104 Abs. 1 Buchst. b.

105 Der Deliktskatalog von Artikel 3 BÜPF findet auch an dieser Stelle keine Anwendung.

106 Art. 273 StPO.

107 Vgl. oben.

108 FMG, SR **784.10**.

innerstaatlichen Regelungen nicht (mehr) greifbar, ergibt sich keine Abweichung zu den Erfordernissen der Konvention.

Das Schweizerische Recht entspricht, insbesondere unter Berücksichtigung der Regelungen der Schweizerischen Strafprozessordnung, den Anforderungen von Artikel 18 der Konvention.

2.2.18 Artikel 19 - Durchsuchung und Beschlagnahme gespeicherter Computerdaten

Artikel 19 Absatz 1 und 3 der Konvention verpflichten die Vertragsparteien, Regelungen vorzusehen, wonach gespeicherte Computerdaten und Datenträger auf ihrem Hoheitsgebiet von den zuständigen Behörden durchsucht und sichergestellt werden können. Computerdaten sollen, ähnlich wie bewegliche Sachen, beschlagnahmt und greifbar gemacht werden. Ebenso soll es auch möglich sein, dass ganze Rechner beschlagnahmt werden können[109]. Die Voraussetzungen für solche Durchsuchungen sollen grundsätzlich dieselben sein wie bei der Suche nach "herkömmlichen" Beweismitteln.

Vorliegend geht es nicht in erster Linie um fernmelderechtliche Fragen oder um die Überwachung dieses Verkehrs. Anwendung finden die nationalen Regelungen betreffend Beweisbeschaffung und -sicherung. Zahlreiche Beispiele aus der Praxis der vergangenen Jahre[110] haben gezeigt, dass die kantonalen Strafprozessordnungen den diesbezüglichen Anforderungen grundsätzlich genügen und die Durchsuchung und Beschlagnahme von Daten und Rechnern vorgenommen werden kann. Auch die Schweizerische Strafprozessordnung vom 5. Oktober 2007 sieht die Durchsuchung und Beschlagnahme von elektronischen Daten und Datenträgern, zum Teil explizit, vor[111].

Artikel 19 bezieht sich auf gespeicherte Computerdaten und kann grundsätzlich gegenüber jedermann angewendet werden. Es stellt sich damit die Frage, inwieweit diese Zugriffsmöglichkeit der Strafverfolgungsbehörden auch für gespeicherte Daten (z.B. Inhaltsdaten von Kunden) bei Providern gilt und ob damit eine Beschränkung des Schutzes des Fernmeldegeheimnisses einhergeht. Im Konventionstext finden sich dazu keine Ausführungen. Jedoch hält der Erläuternde Bericht fest, dass es den Staaten unbenommen bleibt, Kommunikation als solche auch in diesem Bereich zu schützen. So kann zum Beispiel eine beim Provider zwischengespeicherte Nachricht, die vom Adressaten noch nicht abgefragt worden ist, als Teil der Kommunikation betrachtet werden[112], womit sie den entsprechenden Schutz geniesst und nur aufgrund einer Verfügung, unter gewissen Voraussetzungen, durch den Anbieter herausgegeben wird. Den Schutz des Fernmeldegeheimnisses verlieren die Daten jedenfalls zu demjenigen Zeitpunkt, in welchem sie im Speichermedium des Empfängers Eingang finden und dort mittels Beschlagnahme sichergestellt werden können[113]. Artikel 19 der Konvention ist folglich kein Instrument, um bestehende nationale Grundsätze betreffend Fernmeldegeheimnis auszuhöhlen.

109 Ziff. 187 des Erläuternden Berichts (vgl. Fussnote 1).
110 Etwa im Rahmen polizeilicher und untersuchungsrichterlicher Ermittlungen im Kampf gegen Kinderpornografie.
111 Art. 246 ff. und 263 ff. StPO.
112 Ziff. 190 des Erläuternden Berichts (vgl. Fussnote 1).
113 Vergleichbar etwa einer Briefpostsendung, die entsprechenden Schutz durch das Postgeheimnis geniesst, während der Brief am Tag danach - etwas als Teil der Buchhaltung des Empfängers - mittels Hausdurchsuchung beschlagnahmt und anschliessend ausgewertet werden kann.

Absatz 2 von Artikel 19 sieht vor, dass Behörden, nachdem sie Zugriff auf ein erstes Computersystem genommen haben, wo rechtlich zulässig, auch auf ein weiteres verbundenes System zugreifen, um dieses zu durchsuchen. Diese Ausdehnung kann damit durch das innerstaatliche Recht ausgestaltet werden. Durch die Bestimmung ausdrücklich nicht autorisiert wird das Durchsuchen von Datenträgern auf fremdem Staatsgebiet, ohne zusätzliche Erfordernisse zu erfüllen (vgl. Art. 32 der Konvention) oder den Rechtshilfeweg zu beschreiten. Es bestehen, gemäss innerstaatlichem Recht, Möglichkeiten, im Rahmen einer Durchsuchung auf ein anderes, verbundenes Datensystem zuzugreifen[114]. Dies bedingt allerdings, dass sich die behördliche Befugnis auch auf den erweiterten Bereich erstreckt. Dem trägt die Formulierung der Konventionsbestimmung[115] Rechnung.

Absatz 4 von Artikel 19 der Konvention statuiert, auf behördliches Ansuchen hin, eine Informationspflicht von Drittpersonen, etwa eines Systemadministrators, damit ein Zugriff auf Daten vorgenommen werden kann. Das BÜPF sieht solche Pflichten für bestimmte Bereiche vor[116]. Die Mitwirkungspflicht gemäss Konvention besteht in einem angemessenen, verhältnismässigen Umfang. So kann zum Beispiel die Enthüllung eines Passwortes auf behördliche Anfrage hin in einem Fall angemessen sein, während sie in einem anderen Fall unverhältnismässig wäre[117].

Es stellt sich die Frage, ob diese Pflichten der Konvention über die gewöhnliche strafprozessuale Zeugnispflicht oder die Editionspflicht von Dritten[118] hinausgeht. Angesichts der Einschränkung der Konvention auf angemessene Fälle einer Informationspflicht, die erst nach behördlicher Aufforderung erwächst, vermag das geltende Recht mit der Möglichkeit für Untersuchungsbehörden, Editionsverfügungen zu erlassen, den Anforderungen der Konvention zu genügen. Aus dem Erläuternden Bericht[119] geht insbesondere hervor, dass die Bestimmung sich an Systemadministratoren oder Personen mit ähnlicher Aufsichtsfunktion über ein Computersystem richtet. In diesen Fällen kann aber innerstaatlich im Einzelfall zu prüfen sein, inwieweit eine Garantenpflicht des Betroffenen vorliegt, wodurch die Widerhandlung gegen eine Editionsverfügung gemäss Artikel 305 StGB[120] strafbar sein kann.

2.2.19 Artikel 20 - Erhebung von Verkehrsdaten in Echtzeit

Artikel 20 der Konvention regelt die Echtzeit-Erhebung von Verkehrs- oder Verbindungsdaten durch die zuständigen Behörden, wobei die Vertragsstaaten die Behörden auch ermächtigen können, Verbindungsdaten durch Dienstanbieter in Echtzeit erheben oder aufzeichnen zu lassen. Die Konvention gestattet den Staaten, als Voraussetzung für die Datenerhebung einen Deliktskatalog einzuführen und einen entsprechenden Vorbehalt zur Konvention anzubringen[121].

114 Im Falle gewisser Netzwerke wird dieser Umstand der Untersuchungsbehörde fallweise kaum bewusst sein.
115 "Where lawfully accessible".
116 Art. 14 Abs. 4 und Art. 15 Abs. 8 BÜPF (Pflicht von Betreibern interner Fernmeldenetze und Hauszentralen, Zutritt zu gewähren und notwendige Auskunft zu geben).
117 Vgl. Ziff. 202 des Erläuternden Berichts (Fussnote 1) sowie Art. 15 der Konvention.
118 Welche in der Regel keine weitergehende aktive Mitwirkungspflicht bei der Suche nach Beweismitteln umfasst; vgl. Art. 265 StPO.
119 Ziff. 200 ff. des Erläuternden Berichts (Fussnote 1).
120 Tatbestand der Begünstigung; vgl. BGE 120 IV 106.
121 Art. 14 Abs. 3 in Verb. mit Art. 42 der Konvention.

Das geltende schweizerische Recht sieht vor, dass Verbindungsdaten (wie auch Inhaltsdaten) durch Echtzeitüberwachung erhoben werden können, wobei die Überwachung im Rahmen des Deliktskatalogs gemäss BÜPF[122] vorgenommen werden darf. Dieser Katalog wird bezüglich Inhaltsdaten in die Schweizerische Strafprozessordnung übernommen. In Bezug auf Verkehrs- und Rechnungsdaten sowie Verbindungsdaten findet im Rahmen der StPO eine Ausweitung statt, indem bei Vorliegen eines Verbrechens oder Vergehens durch die Behörden entsprechend Auskunft verlangt werden kann[123]. Mit dem Anbringen eines entsprechenden Vorbehaltes im Sinne von Artikel 14 Absatz 3 der Konvention besteht kein gesetzgeberischer Anpassungsbedarf.

2.2.20 Artikel 21 - Erhebung von Inhaltsdaten in Echtzeit

Artikel 21 der Konvention regelt die Echtzeit-Erhebung von Inhaltsdaten, wobei diese durch die zuständigen Behörden im Hinblick auf eine Reihe schwerer Straftaten, zum Beispiel mittels Deliktskatalog autonom bestimmbar, durchgeführt oder angeordnet werden kann. Für die schweizerische Gesetzgebung gilt, dass die Echtzeitüberwachung und Aufzeichnung von Inhaltsdaten abhängig vom Deliktskatalog von Artikel 3 BÜPF angeordnet werden kann. Es besteht kein Anpassungsbedarf im geltenden Recht.

2.2.21 Artikel 22 - Gerichtsbarkeit

Die Konvention unterscheidet zwischen obligatorischer und fakultativer Zuständigkeit der Vertragsstaaten bei der Verfolgung der im Übereinkommen umschriebenen Straftaten. Absatz 1 verpflichtet jeden Vertragsstaat, seine Zuständigkeit zu begründen, wenn sich die Straftat in seinem Hoheitsgebiet ereignet hat (Territorialitätsprinzip, Bst. a von Abs. 1, zwingende Vertragsbestimmung) oder, optional, wenn die Tat an Bord eines Schiffes, das die Flagge dieses Staates führt (Flaggenprinzip, Bst. b), oder an Bord eines Luftfahrzeugs, das nach dem Recht dieses Vertragsstaates eingetragen ist (Bst. c), begangen wird. Die Zuständigkeit der Schweizer Gerichte ist gemäss geltendem Recht gegeben und ergibt sich aus Artikel 3 StGB, Artikel 4 Absatz 2 des Seeschifffahrtsgesetzes[124] und Artikel 97 Absatz 1 des Luftfahrtgesetzes[125].

Gemäss Buchstabe d von Absatz 1 begründet der Staat seine Gerichtsbarkeit, wenn die Straftat von einem Staatsangehörigen begangen wird und die Tat am Begehungsort strafbar ist oder die Tat ausserhalb des Hoheitsbereichs irgendeines Staates begangen wird. In diesen Fällen wird die Zuständigkeit der Schweizer Gerichte durch Artikel 7 Absatz 1 Buchstabe a StGB abgedeckt (aktives Personalitätsprinzip). Von der Vorbehaltsmöglichkeit gemäss Absatz 2 von Artikel 22 (diese bezieht sich auf die Bst. b bis d) ist somit nicht Gebrauch zu machen.

Der Vertragsstaat muss sodann gemäss Absatz 3 seine Zuständigkeit über Straftaten gemäss Übereinkommen[126] auch dann begründen, wenn sich der Verdächtige in seinem Hoheitsgebiet befindet und er nur deshalb nicht ausgeliefert wird, weil er Staatsangehöriger ist. Dieser Pflicht zur Strafverfolgung bei Nichtauslieferung ("aut

122 Art. 3 BÜPF.
123 Art. 273 StPO, unabhängig vom Deliktskatalog.
124 Bundesgesetz vom 23. September 1953 über die Seeschifffahrt unter der Schweizer Flagge, SR **747.30**.
125 Bundesgesetz vom 21. Dezember 1948 über die Luftfahrt, SR **748.0**.
126 Die Tat muss in diesem Fall mit einer Strafe von mindestens einem Jahr Freiheitsentzug bedroht sein; vgl. Art. 24 Abs. 1 der Konvention.

dedere aut iudicare") kommt die Schweiz aufgrund von Artikel 6 StGB nach. Artikel 7 des Bundesgesetzes über die internationale Rechtshilfe in Strafsachen[127] hält fest, dass kein Schweizer Bürger ohne seine Zustimmung zum Zweck der Strafverfolgung ausgeliefert werden darf. Die Europaratskonvention über die Auslieferung vom 13. Dezember 1957[128] regelt die Auslieferung eigener Staatsangehöriger in ihrem Artikel 6. Hier findet sich bereits dieselbe Verpflichtung wie in der vorliegenden Konvention. Die Regeln für die stellvertretende Strafverfolgung durch die Schweiz finden sich in den Artikeln 85 ff. IRSG, wobei die Effizienz dieser Strafverfolgung wesentlich von den gelieferten Akten und zur Verfügung gestellten Beweismitteln abhängt.

2.3 Kapitel III: Internationale Zusammenarbeit

2.3.1 Allgemeines

Die Europaratskonvention über die Cyberkriminalität zielt darauf ab, ein schnelles und wirksames System der internationalen justiziellen Zusammenarbeit in Strafsachen zu errichten. Insoweit nicht ausdrücklich etwas anderes vorgesehen ist, sollen die zwischen den Vertragsstaaten geschlossenen internationalen Verträge sowie deren innerstaatliches Recht weiterhin gelten. Die Konvention enthält jedoch für bestimmte Massnahmen besondere Normen, die von der bestehenden Regelung abweichen können[129]. Dies hängt insbesondere auch mit der geforderten raschen Durchführung der Massnahmen zusammen, die sich mit der Dauer der Verfahren kaum vereinbaren lassen. In Anbetracht der heutigen Regelung der internationalen justiziellen Zusammenarbeit in Strafsachen erfordert die Umsetzung der Konvention eine Änderung des IRSG (siehe Kap. 2.3.9.1).

2.3.2 Artikel 23 - Allgemeine Grundsätze der internationalen Zusammenarbeit

Gemäss Artikel 23 sollen die Vertragsparteien untereinander "im grösstmöglichen Umfang" zusammenarbeiten. Dies verlangt, dass Hindernisse, welche die rasche und reibungslose Zirkulation von Informationen und Beweismitteln hemmen, auf zwischenstaatlicher Ebene soweit wie möglich abzubauen sind. Diese Bestimmung, die in Verträgen zur Bekämpfung der Kriminalität gebräuchlich ist, umfasst im Bereich der Cyberkriminalität einen besonderen Aspekt: Der Informationsaustausch soll schneller ablaufen als in den üblichen Verfahren der internationalen justiziellen Zusammenarbeit in Strafsachen[130]. Die in Artikel 23 enthaltene Verpflichtung zur Zusammenarbeit bezieht sich auf: a) sämtliche Straftaten in Zusammenhang mit Computersystemen und -daten[131] sowie b) die Erhebung von Beweismaterial in elektronischer Form für eine Straftat[132]. Die Bestimmungen von Kapitel III gelten demnach sowohl bei Straftaten, die mittels eines Computersystems begangen werden, als auch in Fällen, in denen bei herkömmlichen, ohne Computersystem began-

127 Rechtshilfegesetz, IRSG; SR **351.1.**
128 SR **0.353.1**.
129 Im Falle der Schweiz gilt dies für die in Art. 30 der Konvention geregelte rasche Weitergabe gespeicherter Computerdaten, die *vor* Abschluss des Verfahrens an die ersuchende Behörde übermittelt werden müssen, sowie für die Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit nach Art. 33 der Konvention.
130 Ziff. 16, 20 und 242 des Erläuternden Berichts (Fussnote 1).
131 Das heisst die Straftaten nach Art. 14 Abs. 2 Bst. a und b der Konvention.
132 Art. 14 Abs. 2 Bst. c.

genen Delikten die Erhebung von Beweismitteln in elektronischer Form erforderlich ist[133].

2.3.3 Art. 24 - Auslieferung

Gemäss Artikel 24, einer üblichen Bestimmung, besteht die Auslieferungspflicht nur[134] bei in den Artikeln 2 bis 11 der Konvention bezeichneten Straftaten. Für diese Auslieferungspflicht nach Artikel 24 müssen zwei Bedingungen, die in Artikel 2 Absatz 1 des Europäischen Auslieferungsabkommens formuliert sind, kumulativ erfüllt sein: a) die beidseitige Strafbarkeit[135] und b) die Androhung einer Freiheitsstrafe im Höchstmass von mindestens einem Jahr. Auf die für eine Auslieferung erforderliche Strafdrohung wird in den Ausführungen zu den Artikeln 2 bis 11 näher eingegangen. Die schweizerische Gesetzgebung stimmt mit der Konvention überein, denn nach Artikel 35 IRSG ist die Auslieferung zulässig, wenn aufgrund der Unterlagen des Ersuchens die Tat nach dem Recht sowohl der Schweiz als auch des ersuchenden Staates mit einer freiheitsbeschränkenden Sanktion im Höchstmass von mindestens einem Jahr oder mit einer schwereren Sanktion bedroht ist. Was Artikel 24 Absatz 1 bis 4 der Konvention betrifft, knüpft die Schweiz die Auslieferung nicht an das Vorhandensein eines Vertrages[136].

Nach Artikel 24 Absatz 5 unterliegt die Auslieferung den im innerstaatlichen Recht vorgesehenen Bedingungen. Die Schweiz regelt diese in den Artikeln 32 ff. IRSG. So ist unser Land als ersuchte Vertragspartei nicht zur Auslieferung verpflichtet, wenn die im betreffenden Vertrag oder innerstaatlichen Recht vorgesehenen Bedingungen[137] seiner Ansicht nach nicht erfüllt sind. Massgebend für die Zusammenarbeit sind nämlich die geltenden Abkommen zwischen den Parteien, wie das Europäische Auslieferungsübereinkommen vom 13. Dezember 1957 (EAUe) mit den beiden Zusatzprotokollen[138].

In Artikel 24 Absatz 6 wird der Grundsatz "aut dedere aut iudicare" (Auslieferung oder Strafverfolgung) angewendet. Schweizer Bürger und Bürgerinnen dürfen ohne ihre schriftliche Zustimmung nicht ausgeliefert werden[139]. Verweigert die betroffene Person die Zustimmung, verfolgt die Schweiz sie[140] auf Antrag des ersuchenden

133 Ziff. 243 des Erläuternden Berichts (Fussnote 1).

134 Hier ist auf den Unterschied zur Zusammenarbeit im Rahmen der Rechtshilfe hinzuweisen, deren Anwendungsbereich gemäss Art. 23 wesentlich grösser ist: Die Verpflichtung zur Zusammenarbeit gilt ebenso bei Straftaten in Zusammenhang mit Computersystemen und -daten wie bei der Erhebung von Beweismitteln in elektronischer Form für eine Straftat.

135 Aufgrund der betreffenden Rechtsvorschriften beider Vertragsparteien.

136 Art. 1 Abs. 1 Bst. a IRSG.

137 Art. 37 IRSG sieht u.a. vor, dass die Auslieferung abgelehnt wird, wenn dem Ersuchen ein Abwesenheitsurteil zugrunde liegt und im vorausgegangenen Verfahren nicht die Mindestrechte der Verteidigung gewahrt worden sind, die anerkanntermassen jedem einer strafbaren Handlung Beschuldigten zustehen; ausgenommen sind Fälle, in denen der ersuchende Staat eine als ausreichend erachtete Zusicherung gibt, dem Verfolgten das Recht auf ein neues Gerichtsverfahren zu gewährleisten, in dem die Rechte der Verteidigung gewahrt werden. Gemäss dieser Bestimmung wird die Auslieferung auch abgelehnt, wenn der ersuchende Staat keine Gewähr bietet, dass der Verfolgte im ersuchenden Staat nicht zum Tode verurteilt oder dass eine bereits verhängte Todesstrafe nicht vollstreckt wird oder der Verfolgte nicht einer Behandlung unterworfen wird, die seine körperliche Integrität beeinträchtigt.

138 SR **0.353.1**, **0.353.11** und **0.353.12**.

139 Art. 7 IRSG.

140 Die Ermittlungen und die Strafverfolgung müssen rasch und ebenso sorgfältig durchgeführt werden wie bei jeder anderen vergleichbaren Straftat.

Staates in Anwendung von Artikel 24 Absatz 6 der Konvention und von Artikel 7 Absatz 1 StGB. Die Schweiz unterrichtet die ersuchende Partei über das Ergebnis des Verfahrens. Ersucht die Partei, deren Auslieferungsersuchen abgelehnt worden ist, nicht darum, dass der Fall den zuständigen Behörden zu Ermittlungszwecken oder zur Strafverfolgung unterbreitet wird, ist die Schweiz nicht verpflichtet, sich einzuschalten[141].

Aufgrund von Artikel 24 Absatz 7 muss die Schweiz dem Generalsekretär des Europarates mitteilen, dass in der Schweiz das Bundesamt für Justiz (BJ) für Ersuchen um Auslieferung oder vorläufige Festnahme zuständig ist[142]. Diese Bestimmung ist nur anwendbar, wenn die beiden betroffenen Parteien keinen Vertrag abgeschlossen haben[143]. Die Bezeichnung einer Behörde schliesst jedoch die Möglichkeit, auf diplomatischem Weg vorzugehen, nicht aus[144].

2.3.4 Artikel 25 - Allgemeine Grundsätze der Rechtshilfe

Artikel 25 verpflichtet die Vertragsparteien, bei einer sehr umfangreichen Gruppe von Straftaten zusammenzuarbeiten, was auch aus Artikel 23 hervorgeht[145]. Gemäss Artikel 25 Absatz 2 der Konvention muss die Schweiz die rechtlichen Grundlagen schaffen, welche ihr erlauben, die bezeichneten besonderen Formen der Zusammenarbeit zu gewähren, insbesondere die in den Artikeln 27 sowie 29 bis 35 der Konvention genannten. Solche Regelungen sind unerlässlich für eine wirksame Zusammenarbeit in Strafsachen wegen Computerdelikten[146]. Die Einzelheiten dieser gesetzlichen Anpassungen werden in Kapitel 2.3.9.1 ausgeführt.

In Artikel 25 Absatz 3 der Konvention wird eine schnelle Rechtshilfemassnahme eingeführt. Computerdaten sind äusserst flüchtig. Es genügt, einige Tasten zu drücken oder ein Automatikprogramm laufen zu lassen, um sie zu löschen, wodurch die Ermittlung des Täters verunmöglicht wird oder die Beweise für seine Schuld vernichtet werden. Einige Arten von Daten werden nur kurzfristig gespeichert, bevor sie gelöscht werden. In solchen dringenden Fällen muss das Ersuchen rasch eingereicht und beantwortet werden. Artikel 25 Absatz 3 ermöglicht deshalb die beschleunigte Rechtshilfe, wodurch verhindert werden soll, dass wesentliche Informationen oder Beweismittel verloren gehen, weil sie gelöscht worden sind, bevor ein Rechtshilfeersuchen erstellt und übermittelt werden konnte und eine Antwort eingegangen ist. Erreicht wird dies, indem einerseits den Vertragsparteien in dringenden Fällen gestattet wird, ein Ersuchen um Zusammenarbeit mit schnellen Kommunikationsmitteln einzureichen[147], und andererseits die ersuchte Partei dazu angehalten wird, ein solches Ersuchen mit schnellen Kommunikationsmitteln zu beantworten.

141 Wurde kein Auslieferungsersuchen gestellt oder wurde die Auslieferung aus einem anderen Grund als der Staatsangehörigkeit abgelehnt, ist die Schweiz nicht verpflichtet, ihren Behörden die Strafverfolgung zu übertragen (Ziff. 251 des Erläuternden Berichts, Fussnote 1).

142 Art. 17 Abs. 2 IRSG.

143 Besteht nämlich ein für die Parteien verbindlicher bilateraler oder multilateraler Auslieferungsvertrag, wie das genannte EAUe, wissen diese, an wen die Ersuchen um Auslieferung oder vorläufige Festnahme zu richten sind, womit sich das Führen eines Verzeichnisses erübrigt.

144 Ziff. 252 des Erläuternden Berichts (Fussnote 1).

145 Die Art. 33 und 34 gestatten die Änderung des Geltungsbereichs dieser Massnahmen; vgl. die Ausführungen zu diesen Bestimmungen.

146 Ziff. 254 des Erläuternden Berichts (Fussnote 1).

147 Und nicht über die klassischen und wesentlich langsameren Übermittlungswege, d.h. als versiegeltes Schriftstück im diplomatischen Kuriergepäck oder per Post.

Jede Vertragspartei muss die erforderlichen Voraussetzungen schaffen, damit sie diese Massnahme anwenden kann[148]. In sensiblen Angelegenheiten können die Vertragsparteien besondere Sicherheitsmassnahmen, wie die Verschlüsselung, vereinbaren[149]. Die ersuchte Vertragspartei kann verlangen, dass ihr nachträglich auf einem der klassischen Übermittlungswege eine formelle Bestätigung zugestellt wird, was der schweizerischen Praxis entspricht.

In Artikel 25 Absatz 4 der Konvention ist der allgemeine Grundsatz verankert, wonach die Rechtshilfe den in den anwendbaren Rechtshilfeverträgen und im innerstaatlichen Recht vorgesehenen Bedingungen unterliegt[150]. Diese übliche Bestimmung gilt insbesondere auch bei eingreifenden Massnahmen wie einer Durchsuchung oder Beschlagnahme, die nur dann vorgenommen wird, wenn die ersuchte Vertragspartei die Gewissheit hat, dass die für die Anordnung einer solchen Massnahme erforderlichen Bedingungen erfüllt sind[151]. Diese Regelung gilt jedoch nicht, wenn in den Artikeln von Kapitel III ausdrücklich etwas anderes vorgesehen ist. Die Konvention enthält mehrere Abweichungen von dem allgemeinen Grundsatz[152], insbesondere hinsichtlich der Gründe für die Verweigerung der Rechtshilfe[153]. Die Zusammenarbeit darf gemäss Artikel 25 Absatz 4 bei Straftaten nach den Artikeln 2 bis 11 nicht allein mit der Begründung verweigert werden, dass die betreffende Straftat als fiskalisches Delikt angesehen wird. Dies ist unproblematisch, weil diese Straftaten gemäss Konvention nicht an sich fiskalische Delikte darstellen, auch wenn solche Methoden zur Begehung fiskalischer Delikte angewendet werden können. Es lässt sich nicht ausschliessen, dass einige Staaten versuchen könnten, die mit der Konvention über die Cyberkriminalität eingeführten schnellen Rechtshilfemassnahmen zu verwenden, um Informationen zu erlangen, welche die Schweiz nicht liefern will, indem sie zum Beispiel eine Computerstraftat oder als Beweismaterial dienende Computerdaten als Vorwand benutzen.

148 Telefax und elektronische Post werden lediglich beispielhalber genannt. Jedes im Einzelfall angemessene schnelle Kommunikationsmittel kann eingesetzt werden. Mit dem technologischen Fortschritt können weitere schnelle Kommunikationsmittel entstehen, die sich für die Einreichung von Rechtshilfeersuchen eignen.

149 Ziff. 256 des Erläuternden Berichts (Fussnote 1).

150 Damit werden die Rechte der Personen garantiert, die sich im Hoheitsgebiet der ersuchten Partei aufhalten und von einem Rechtshilfeersuchen betroffen sein können.

151 Ziff. 257 des Erläuternden Berichts (Fussnote 1).

152 Ziff. 258 des Erläuternden Berichts (Fussnote 1): Eine solche Abweichung ergibt sich aus Art. 25 Abs. 2 der Konvention, wonach jede Vertragspartei die in den anderen Artikeln des Kapitels aufgeführten Formen der Zusammenarbeit (wie Speicherung, Datenerhebung in Echtzeit, Durchsuchung und Beschlagnahme, Beteiligung am Netzwerk 24/7) gewähren muss, unabhängig davon, ob diese Massnahmen bereits in ihren internationalen Rechtshilfeverträgen oder ihrer Rechtshilfegesetzgebung festgeschrieben sind. Eine weitere Abweichung findet sich in Art. 27, der bei der Erledigung von Ersuchen stets anwendbar ist und Vorrang hat vor einer innerstaatlichen Bestimmung der ersuchten Vertragspartei, welche die internationale Zusammenarbeit regelt, wenn kein Rechtshilfevertrag oder eine gleichwertige Vereinbarung zwischen der ersuchenden und der ersuchten Vertragspartei besteht (System von Bedingungen und Gründen für die Verweigerung der Rechtshilfe).

153 Vgl. auch die Ausführungen zu Art. 27 Abs. 4.

Artikel 25 Absatz 5 enthält eine übliche Bestimmung zur beidseitigen Strafbarkeit[154].

2.3.5 Artikel 26 - Unaufgeforderte Übermittlung von Informationen

In Artikel 26 wird eine Bestimmung, die aus Artikel 10 des Übereinkommens vom 8. November 1990 über Geldwäscherei sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten[155] und Artikel 28 des Strafrechtsübereinkommens vom 27. Januar 1999 über Korruption[156] übernommen wurde, auf die Rechtshilfe ausgedehnt. Eine entsprechende Regelung findet sich auch in den meisten der bestehenden bilateralen Verträge über die Rechtshilfe in Strafsachen sowie in Artikel 11 des Zweiten Zusatzprotokolls vom 8. November 2001 zum Europäischen Übereinkommen über die Rechtshilfe in Strafsachen[157], welcher, wie Artikel 26 der Konvention, auch eine Vertraulichkeitsklausel enthält. Artikel 26, eine Kann-Bestimmung, gibt den beiden Vertragsparteien die Möglichkeit, einander ohne vorheriges Ersuchen und, gemäss Absatz 2, eventuell unter bestimmten Bedingungen[158] Informationen über Ermittlungen oder Verfahren zu übermitteln, welche für die von beiden angestrebte Bekämpfung der Kriminalität dienlich sind[159]. Der Informationsaustausch richtet sich nach dem innerstaatlichen Recht. In der Schweiz sind die Bedingungen in Artikel 67*a* IRSG[160] festgelegt.

2.3.6 Artikel 27 - Verfahren für Rechtshilfeersuchen ohne anwendbare völkerrechtliche Übereinkünfte

In Artikel 27 wurden die Grundsätze anderer von der Schweiz abgeschlossener Abkommen übernommen. Artikel 27 Absatz 1 sieht vor, dass die Rechtshilfe nach den entsprechenden Übereinkommen und Rechtshilfeverträgen, wie dem Europäischen Übereinkommen vom 20. April 1959 über die Rechtshilfe in Strafsachen[161] oder dem weiter oben genannten Zusatzprotokoll, abgewickelt wird. Die in den Artikeln 29 bis 35 der Konvention festgelegten Rechtshilfemassnahmen bei Computerstraftaten setzen jedoch die Schaffung der erforderlichen Rechtsgrundlagen voraus, insoweit das geltende Recht der jeweiligen Vertragspartei nicht ausreicht.

Artikel 27 Absätze 2 bis 10 enthält Bestimmungen, die zur Anwendung gelangen, wenn keine Verträge vorhanden sind. Sie betreffen das Bezeichnen einer zentralen Behörde, die Festlegung von Bedingungen, die Gründe für den Aufschub oder die

154 Ziff. 259 des Erläuternden Berichts (Fussnote 1): Wegen der unterschiedlichen einzelstaatlichen Rechtsordnungen bestehen nämlich Unterschiede in der Terminologie und der Einstufung krimineller Verhaltensweisen. Wird ein Verhalten in beiden Rechtsordnungen als Straftat gewertet, sollten diese rein juristischen Unterschiede der Gewährung der Rechtshilfe nicht entgegenstehen. In Fällen, in denen das Kriterium der beidseitigen Strafbarkeit anwendbar ist, sollte es flexibel gehandhabt werden, um die Gewährung der Rechtshilfe zu erleichtern.

155 SR **0.311.53**.

156 SR **0.311.55**; Ziff. 260 des Erläuternden Berichts (Fussnote 1).

157 SR **0.351.12**.

158 Die empfangende Vertragspartei ist gegenüber der übermittelnden Vertragspartei nur verpflichtet, wenn sie die unaufgefordert übermittelten Informationen annimmt: Mit deren Annahme akzeptiert sie auch, dass sie die mit der Übermittlung dieser Informationen verbundenen Bedingungen einhalten muss. Somit stellt Artikel 26 der Konvention vor die Wahl, das Angebotene anzunehmen oder darauf zu verzichten.

159 Kriminalität macht nicht Halt vor Grenzen, und die Informationen, welche eine Vertragspartei bei ihren Ermittlungen gewinnt, sind häufig auch für die Behörden der anderen Vertragspartei von Interesse.

160 Unaufgeforderte Übermittlung von Beweismitteln und Informationen.

161 EUeR; SR **0.351.1**.

Verweigerung der Rechtshilfe sowie die entsprechenden Verfahren, die Vertraulichkeit von Ersuchen und die direkte Übermittlung. Diese Regelung geht somit dem innerstaatlichen Recht vor. Andere Punkte werden in Artikel 27 nicht geregelt[162].

Gemäss Artikel 27 Absatz 2 der Europaratskonvention über die Cyberkriminalität muss die Schweiz, sofern kein internationales Abkommen besteht, dem Generalsekretär des Europarates mitteilen, welche Stelle als zentrale Behörde für den Versand und die Beantwortung von Rechtshilfeersuchen zuständig ist. Wie bei der Erklärung zum EUeR ist demnach zu präzisieren, dass das "Bundesamt für Justiz des Eidgenössischen Justiz- und Polizeidepartementes in Bern für die Entgegennahme aller Rechtshilfeersuchen des Auslands und für die Übermittlung aller schweizerischen Rechtshilfeersuchen" zuständig ist. In diesen Zusammenhang gehört auch Artikel 27 Absatz 9 Buchstabe e, aufgrund dessen die Vertragsparteien eine Erklärung abgeben können, dass Ersuchen nach diesem Absatz aus Gründen der Effizienz an ihre zentrale Behörde zu richten sind. In Anwendung dieser Bestimmung sind die Ersuchen an das BJ zu richten, was einen zusätzlichen Arbeitsaufwand und Personalbedarf mit sich bringt[163]. Denn Rechtshilfeersuchen, die aufgrund der Konvention über die Cyberkriminalität an das Amt gerichtet werden, betreffen nicht nur die Verfolgung von Computerstraftaten, sondern auch die Erhebung von Beweismaterial in elektronischer Form für andere Straftaten[164]. Solche Rechtshilfeersuchen sind in der Regel komplexer als andere Ersuchen, die üblicherweise eingehen, und müssen prioritär behandelt werden. Wegen der Komplexität der Thematik hat das BJ auch damit zu rechnen, dass es von schweizerischen und ausländischen Behörden regelmässig konsultiert wird, und es wird Stellungnahmen und Empfehlungen zu den anwendbaren Verfahren abgeben. Neben dieser Informationsaufgabe kommt ihm bei der Erledigung der an die Schweiz gerichteten Rechtshilfeersuchen auch die Aufgabe zu, die von den Schweizer Vollzugsbehörden getroffenen Entscheide vermehrt zu kontrollieren. Aufgrund des neuen Artikels 18*b* IRSG[165] wird nämlich ein Teil der Entscheide, die bis anhin vom Amt und von der betroffenen Person angefochten werden konnten, nur noch der Kontrolle des BJ unterliegen, das die Glaubwürdigkeit des mit dieser Bestimmung eingeführten Systems gewährleisten muss. Mit dieser Änderung geht auch die Verpflichtung einher, der ausländischen Behörde die in Artikel 18*b* IRSG aufgestellten Bedingungen zu erläutern und für deren Einhaltung zu sorgen. Um den Erfordernissen der Konvention Rechnung zu tragen, ist innerhalb des BJ eine auf Cyberkriminalität spezialisierte Gruppe zu bilden. Der Aufwand für die Erledigung dieser Aufgaben dürfte einer zusätzlichen Vollzeitstelle (einschliesslich Pikettdienst) entsprechen. Dies ermöglicht der Schweiz das rasche Reagieren, das für die Bekämpfung der Computerkriminalität so wichtig ist. Auch Kantone müssen bei der Bekämpfung der Kriminalität, gegen die sich die Konvention richtet, rasch handeln und die benötigten Fachleute sowie die entsprechende Informatikausrüstung bereitstellen.

162 So findet sich darin zum Beispiel keine Bestimmung zu Form und Inhalt der Ersuchen, zur Zeugeneinvernahme in der ersuchten oder ersuchenden Vertragspartei, zur Erstellung amtlicher Unterlagen, Überstellung inhaftierter Zeugen oder Hilfe bei Einziehungen. Was diese Fragen anbelangt, ergibt sich aus Art. 25 Abs. 4, dass die Gewährung dieser Arten von Rechtshilfe sich nach dem innerstaatlichen Recht der ersuchten Vertragspartei richtet, sofern in Kapitel III nichts anderes bestimmt wird. In der Schweiz ist somit das IRSG massgebend. Ziff. 264 des Erläuternden Berichts (Fussnote 1).

163 Insbesondere auch für den Pikettdienst und die Ausbildung.

164 Art. 25 Abs. 1.

165 Siehe Kap. 2.3.9.1.

Artikel 27 Absatz 3 verpflichtet die ersuchte Vertragspartei, Rechtshilfeersuchen nach den von der ersuchenden Vertragspartei bezeichneten Verfahren zu erledigen, sofern dies mit dem Recht der ersuchten Vertragspartei nicht unvereinbar ist. Eine solche Regelung, die sich auch in anderen internationalen Verträgen[166] findet, soll gewährleisten, dass den bestehenden Beweisanforderungen entsprochen wird[167]. Gemäss Artikel 27 Absatz 4 kann die Rechtshilfe verweigert werden: a) aus Gründen nach Artikel 25 Absatz 4 der Konvention[168], b) bei Straftaten, welche die ersuchte Vertragspartei als politische Straftaten oder als mit solchen zusammenhängende Straftaten ansieht, und c) in Fällen, in denen die staatliche Souveränität, die Sicherheit, öffentliche Ordnung oder andere wesentliche Interessen der ersuchten Vertragspartei beeinträchtigt werden könnten[169]. Artikel 27 Absatz 5, eine übliche Bestimmung, gestattet der ersuchten Vertragspartei die Erledigung eines Rechtshilfeersuchens zwar nicht zu verweigern, aber aufzuschieben, wenn die unverzügliche Durchführung der in dem Ersuchen genannten Massnahmen die von ihren Behörden geführten strafrechtlichen Ermittlungen und Verfahren beeinträchtigen könnte[170]. Gemäss Artikel 27 Absatz 6 kann die ersuchte Vertragspartei in Fällen, in denen sie die Rechtshilfe normalerweise verweigern oder aufschieben würde, Bedingungen daran knüpfen. Erscheinen diese Bedingungen der ersuchenden Vertragspartei nicht annehmbar, kann die ersuchte Vertragspartei diese ändern oder die Rechtshilfe verweigern oder aufschieben. In Artikel 27 Absatz 7 der Konvention wird die ersuchte Vertragspartei verpflichtet, der ersuchenden Vertragspartei das Ergebnis der Erledigung des Rechtshilfeersuchens mitzuteilen und die Verweigerung oder den Aufschub der Rechtshilfe zu begründen[171]. Gemäss Artikel 27 Absatz 8 kann die ersuchende Vertragspartei die ersuchte Vertragspartei bitten, das Vorliegen eines

166 Insbesondere Art. V des Vertrags vom 10. September 1998 zwischen der Schweiz und Italien zur Ergänzung des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen vom 20. April 1959 und zur Erleichterung seiner Anwendung, SR **0.351.945.41**, und Art. 9 des Staatsvertrags vom 25. Mai 1973 zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen, SR **0.351.933.6**.

167 Es geht darum, sicherzustellen, dass die im ersuchenden Staat geltenden Rechtsvorschriften über die Zulässigkeit von Beweismitteln eingehalten werden, damit er die Beweismittel vor Gericht verwenden kann. Vgl. Ziff. 267 des Erläuternden Berichts (Fussnote 1).

168 D.h. aus den im innerstaatlichen Recht der ersuchten Partei vorgesehenen Gründen.

169 Entsprechend dem übergeordneten Grundsatz, dass die Rechtshilfe im grösstmöglichen Umfang gewährt werden soll, sind die von einer ersuchten Partei festgelegten Ablehnungsgründe einzuschränken und massvoll anzuwenden. Demzufolge soll die Rechtshilfe, abgesehen von den in Artikel 28 der Konvention genannten Gründen, nur in Ausnahmefällen aus Datenschutzgründen abgelehnt werden können. Ziff. 268 und 269 des Erläuternden Berichts (Fussnote 1).

170 Wenn beispielsweise die ersuchende Vertragspartei um die Übermittlung von Beweismitteln oder Zeugenaussagen gebeten hat, die sie für Ermittlungen oder ein Verfahren benötigt, und dieselben Beweismittel und Zeugenaussagen für ein unmittelbar bevorstehendes Verfahren im Hoheitsgebiet der ersuchten Vertragspartei erforderlich sind, ist es gerechtfertigt, dass die ersuchte Partei die Rechtshilfe aufschiebt. Ziff. 270 des Erläuternden Berichts (Fussnote 1).

171 Die Verpflichtung der ersuchten Vertragspartei, ihre Gründe mitzuteilen, soll die Effizienz der Rechtshilfe erhöhen und der ersuchenden Vertragspartei Zugang zu ihr unbekannten Informationen über das Vorhandensein von Zeugen oder Beweismitteln und die damit verbundenen Umstände verschaffen. Ziff. 272 des Erläuternden Berichts (Fussnote 1).

Ersuchens und dessen Inhalt vertraulich zu behandeln[172]. Die Schweiz hat im Zweiten Zusatzprotokoll zum EUeR einer solchen Klausel zugestimmt[173].

Artikel 27 Absatz 9 ermöglicht eine schnelle Kommunikation: Die zentralen Behörden nach Artikel 27 Absatz 2 verkehren unmittelbar miteinander. In dringenden Fällen können jedoch Richter und Staatsanwälte der ersuchenden Vertragspartei Rechtshilfeersuchen direkt an die Richter und Staatsanwälte der ersuchten Vertragspartei übermitteln. Dabei müssen sie eine Kopie des Ersuchens der zentralen Behörde ihres Landes zukommen lassen, welche diese an die zentrale Behörde der ersuchten Vertragspartei weiterleitet. Ersuchen können auch über Interpol übermittelt werden[174]. Behörden der ersuchten Vertragspartei, die ein Ersuchen erhalten, das nicht in ihren Zuständigkeitsbereich fällt, müssen a) das Ersuchen an die zuständige Behörde der ersuchten Vertragspartei weiterleiten und b) die Behörden der ersuchenden Vertragspartei darüber in Kenntnis setzen[175]. Ersuchen können, selbst wenn sie nicht dringend sind, auch direkt, ohne Beteiligung der zentralen Behörde übermittelt werden, sofern die Behörde der ersuchten Vertragspartei diese ohne Anwendung von Zwangsmassnahmen erledigen kann. Eine Vertragspartei kann den anderen Parteien über den Generalsekretär des Europarates mitteilen, dass Ersuchen aus Effizienzgründen direkt an ihre zentrale Behörde zu richten sind[176]. So wird es die Schweiz handhaben.

2.3.7 Artikel 28 - Vertraulichkeit und Beschränkung der Verwendung

Artikel 28 sieht Beschränkungen der Verwendung von Informationen oder Unterlagen vor, damit die ersuchte Vertragspartei, wenn es sich um besonders sensible Informationen oder Unterlagen handelt, sicherstellen kann, dass deren Verwendung sich auf die Zwecke beschränkt, für welche die Rechtshilfe gewährt wird. Wie Artikel 27 der Konvention ist Artikel 28 nur anwendbar, wenn kein Übereinkommen zwischen der ersuchenden und der ersuchten Partei in Kraft ist[177].

Artikel 28 Absatz 2 erlaubt der ersuchten Vertragspartei, zwei Arten von Bedingungen zu stellen: a) Die Informationen oder Unterlagen bleiben vertraulich, wenn dem

172 Es kann nämlich vorkommen, dass eine Partei ein Rechtshilfeersuchen in einer besonders sensiblen Angelegenheit stellt oder ein Ersuchen in einem Fall einreicht, in dem es schwerwiegende Folgen hätte, wenn die dem Ersuchen zugrunde liegenden Tatsachen zu früh öffentlich gemacht würden. Vertraulichkeit kann jedoch nur insoweit verlangt werden, als dadurch der ersuchten Partei nicht verunmöglicht wird, die gewünschten Beweismittel oder Informationen zu erlangen. Dies ist beispielsweise von Bedeutung, wenn Informationen offengelegt werden müssen, um einen für die Erledigung des Ersuchens benötigten Gerichtsbeschluss zu erlangen, oder wenn Privatpersonen, die im Besitz von Beweismitteln sind, über das Ersuchen in Kenntnis gesetzt werden müssen, damit es erledigt werden kann. Ziff. 273 des Erläuternden Berichts (Fussnote 1).

173 Kann die ersuchte Vertragspartei einem Ersuchen um Vertraulichkeit nicht entsprechen, teilt sie dies der ersuchenden Vertragspartei mit, worauf diese ihr Ersuchen zurückziehen oder ändern kann.

174 Art. 27 Abs. 9 Bst. b.

175 Art. 27 Abs. 9 Bst. c.

176 Art. 27 Abs. 9 Bst. e; vgl. Ausführungen zu Art. 27 Abs. 2.

177 Sofern die Vertragsparteien nichts anderes beschliessen. Damit werden Überschneidungen mit anderen bestehenden bilateralen und multilateralen Rechtshilfeverträgen und ähnlichen Vereinbarungen vermieden, so dass die Zuständigen sich in der Praxis weiterhin an die übliche Regelung halten können und nicht versuchen müssen, zwei konkurrierende oder gar widersprüchliche Übereinkünfte anzuwenden. Vgl. Ziff. 276 des Erläuternden Berichts (Fussnote 1).

Ersuchen ohne diese Bedingung nicht entsprochen werden könnte[178]; b) die übermittelten Informationen oder Unterlagen dürfen nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet werden. In der Schweiz ist der in Artikel 67 IRSG verankerte Grundsatz der Spezialität in der Praxis von zentraler Bedeutung. Nach diesem Grundsatz dürfen übermittelte Schriftstücke und Auskünfte im ersuchenden Staat in Verfahren wegen Taten, in denen Rechtshilfe nicht zulässig ist, weder für Ermittlungen benutzt noch als Beweismittel verwendet werden[179]. Die Beschränkung der Verwendung der übermittelten Informationen und Unterlagen gilt nur, wenn sie von der ersuchten Vertragspartei ausdrücklich verlangt wird. Andernfalls besteht für die ersuchende Vertragspartei keine solche Beschränkung. Mit dieser Beschränkung wird sichergestellt, dass die Informationen und Unterlagen nur zu den in dem Ersuchen vorgesehenen Zwecken verwendet werden, und somit ausgeschlossen, dass sie ohne Zustimmung der ersuchten Vertragspartei für andere Zwecke benutzt werden. Hinsichtlich der Möglichkeit, die Verwendung zu beschränken, sieht die Europaratskonvention über die Cyberkriminalität jedoch zwei Ausnahmen vor[180]. Kann die ersuchende Vertragspartei einer Bedingung nicht entsprechen, teilt sie dies der ersuchten Vertragspartei umgehend mit, woraufhin diese entscheidet, ob sie die Informationen dennoch zur Verfügung stellen will[181]. Von der ersuchenden Vertragspartei kann verlangt werden, dass sie Angaben zur Verwendung der Informationen oder Unterlagen macht, die sie unter den in Absatz 2 genannten Bedingungen erhalten hat, damit die ersuchte Vertragspartei die Einhaltung dieser Bedingungen überprüfen kann[182]. Aufgrund des oben erwähnten Grundsatzes der Spezialität nach Artikel 67 IRSG wird die Schweiz zuweilen überprüfen müssen, ob die an die Übermittlung geknüpften Bedingungen eingehalten werden.

2.3.8 Artikel 29 - Umgehende Sicherung gespeicherter Computerdaten

Nach Artikel 29 Absatz 1 kann eine Vertragspartei darum ersuchen, dass Daten, die mittels eines Computersystems im Hoheitsgebiet der ersuchten Vertragspartei gespeichert sind, umgehend gesichert werden, und nach Absatz 3 ist jede Vertragspartei verpflichtet, die gesetzlichen Voraussetzungen dafür zu schaffen. Dadurch soll vermieden werden, dass die Daten während des Zeitraums, der für die Ausarbeitung, Übermittlung und Erledigung eines Rechtshilfeersuchens zur Erlangung der Daten erforderlich ist, verändert, entfernt oder gelöscht werden. Die Sicherung ist eine

178 Wie bei der vertraulich zu behandelnden Identität eines Informanten. Vgl. Ziff. 277 des Erläuternden Berichts (Fussnote 1).

179 Dieses Verbot bezieht sich insbesondere auf Taten, die nach schweizerischer Auffassung politischen, militärischen oder fiskalischen Charakter haben. Vgl. Art. 3 Abs. 1 und 3 IRSG: Als Tat mit fiskalischem Charakter gilt eine Tat, die auf eine Verkürzung fiskalischer Abgaben gerichtet erscheint oder Vorschriften über währungs-, handels- oder wirtschaftspolitische Massnahmen verletzt. Unterlagen und Informationen, die im Rahmen der Rechtshilfe übermittelt werden, dürfen jedoch auch in einem Verfahren wegen Abgabebetrug verwendet werden.

180 a) Wenn das zur Verfügung gestellte Material eine angeklagte Person entlastet, wird es gegenüber der Verteidigung oder einer Gerichtsbehörde offengelegt. b) Wenn das im Rahmen von Rechtshilfeabkommen zur Verfügung gestellte Material grossenteils in Verhandlungen, häufig in öffentlichen Verfahren, in denen die Offenlegung obligatorisch ist, verwendet wird, so wird es mit seiner Offenlegung allgemein zugänglich. In solchen Fällen ist es nicht möglich, hinsichtlich der Ermittlungen und Verfahren, für die um Rechtshilfe ersucht wurde, Vertraulichkeit zu gewährleisten. Ziff. 278 des Erläuternden Berichts (Fussnote 1).

181 Art. 28 Abs. 3.

182 Art. 28 Abs. 4.

begrenzte, vorläufige Massnahme. Computerdaten sind äusserst flüchtig. Deshalb soll das Verfahren nach Artikel 29 gewährleisten, dass diese Daten bis zum Abschluss des langwierigeren und komplizierteren Verfahrens der Erledigung eines formellen Rechtshilfeersuchens verfügbar bleiben. Diese Massnahme ist schneller als ein übliches Rechtshilfeverfahren und stellt einen geringeren Eingriff dar. In diesem Stadium wird von den für die Rechtshilfe zuständigen Personen der ersuchten Vertragspartei nicht verlangt, dass sie sich die betreffenden Daten von deren Verwahrer übergeben lassen. Vielmehr soll die ersuchte Vertragspartei dafür sorgen, dass der Verwahrer (häufig ein Dienstanbieter oder eine andere Drittpartei) die Daten sichert, das heisst nicht löscht, bis die spätere Übergabe der Daten angeordnet wird[183]. Im schweizerischen Recht wird dieses Erfordernis durch vorläufige Massnahmen erfüllt, welche die Schweizer Vollzugsbehörde gemäss Artikel 18 IRSG anordnen kann. So kann ein Dienstanbieter aufgefordert werden, auf einem separaten Datenträger eine Sicherungskopie (Backup) der für die ausländischen Behörden relevanten Daten zu erstellen, wodurch diese vor einer späteren Löschung durch den Benutzer oder den Dienstanbieter bewahrt werden. Die ausländische Behörde muss innert der gesetzten Frist ein formelles Rechtshilfeersuchen einreichen. Andernfalls darf die Sicherungskopie vernichtet werden. Das Verfahren nach Artikel 29 der Konvention ist schnell durchführbar und wahrt das Recht der betroffenen Person auf Achtung der Privatsphäre, denn die Daten werden nur weitergegeben, wenn die Kriterien für die vollständige Offenlegung gemäss den Rechtshilfeabkommen erfüllt sind. Diese Bestimmung ermöglicht ein äusserst schnelles Verfahren, mit dem sich vermeiden lässt, dass Daten unwiederbringlich verloren gehen. Dabei werden die Daten gesichert, bis sie zu einem späteren Zeitpunkt übergeben werden können. Diese Massnahmen kommen jedoch nur in Betracht, wenn der Dienstanbieter nicht selbst in die im Ausland verfolgte Tat verwickelt ist. In einem solchen Fall braucht es eine Durchsuchung, um die vorläufigen Massnahmen durchführen zu können.

Artikel 29 Absatz 2 gibt den Inhalt eines solchen Sicherungsersuchens vor. Das Ersuchen ist rasch zu verfassen und zu übermitteln. Deshalb müssen die darin enthaltenen Informationen kurz gefasst sein und sich auf die Angaben beschränken, welche für die Sicherung der Daten erforderlich sind[184]. Danach muss die ersuchende Vertragspartei nachträglich ein Rechtshilfeersuchen um Herausgabe der Daten einreichen.

Die beidseitige Strafbarkeit ist grundsätzlich keine Voraussetzung für die Vornahme einer Sicherung[185], denn im Zusammenhang mit einer Sicherung ist die Anwendung dieses Kriteriums kontraproduktiv[186]. Artikel 29 Absatz 4 sieht jedoch einen beschränkten Vorbehalt vor. Die Schweiz wird einen solchen Vorbehalt hinsichtlich

183 Ziff. 282 des Erläuternden Berichts (Fussnote 1).

184 Neben der Angabe der um Sicherung ersuchenden Behörde und der Straftat, welche dem Ersuchen zugrunde liegt, muss das Ersuchen eine kurze Darstellung des Sachverhalts sowie die für die Bestimmung und Lokalisierung der zu sichernden Daten erforderlichen Angaben enthalten. Zudem ist darin der Zusammenhang zwischen diesen Daten und den wegen dieser Straftat eingeleiteten Ermittlungen oder Verfahren aufzuzeigen und darzulegen, weshalb die Sicherung erforderlich ist. Ziff. 284 des Erläuternden Berichts (Fussnote 1).

185 Art. 29 Abs. 3.

186 Die Sicherung ist nämlich keine besonders eingreifende Massnahme, da a) der Verwahrer lediglich Daten, die sich rechtmässig in seinem Besitz befinden, weiterhin in seinem Besitz behält und b) die Daten erst an die Zuständigen der ersuchten Vertragspartei weitergegeben oder von diesen geprüft werden, wenn einem formellen Rechtshilfeersuchen um Weitergabe der Daten entsprochen worden ist.

der beidseitigen Strafbarkeit anbringen, da diese für unser Land bei sämtlichen eingreifenden Massnahmen erforderlich ist. Die Schweiz wird sich somit das Recht vorbehalten, bei anderen als den in den Artikeln 2 bis 11 der Konvention umschriebenen Straftaten[187] ein Sicherungsersuchen nach Artikel 29, das im Hinblick auf die Durchsuchung oder einen ähnlichen Zugriff[188], die Beschlagnahme oder eine ähnliche Sicherstellung oder die Weitergabe gespeicherter Daten gestellt wird, abzulehnen, wenn sie Grund zu der Annahme hat, dass im Zeitpunkt der Weitergabe die Voraussetzung der beidseitigen Strafbarkeit nicht erfüllt werden kann. Der von der Schweiz anzubringende Vorbehalt wird weitgehend dem Wortlaut des auf Artikel 5 EUeR Bezug nehmenden Vorbehalts entsprechen und folgendermassen formuliert sein:

"Die Schweiz behält sich das Recht vor, die Ausführung eines Rechtshilfeersuchens, welches die Anwendung einer Zwangsmassnahme erforderlich macht, der Voraussetzung gemäss Artikel 29 Absatz 4 zu unterstellen."

In Artikel 29 Absatz 5 der Konvention sind strenge Voraussetzungen für die Ablehnung eines Sicherungsersuchens festgelegt[189]. Deren Anwendung in der Praxis richtet sich nach der Auslegung der Artikel 29 und 30. Diese sehen vorläufige Massnahmen vor, die als solche einem formellen Rechtshilfeersuchen vorausgehen. Die ausländische Behörde kann nach Artikel 29 die umgehende Sicherung und nach Artikel 30 die umgehende Weitergabe gespeicherter Daten verlangen. Die Schweiz wird jedoch Artikel 29 Absatz 5 und Artikel 30 Absatz 2 differenziert auslegen: Zeigt sich zum Zeitpunkt, in dem sie über die Anordnung der vorläufigen Massnahmen zu entscheiden hat, dass dem Rechtshilfeersuchen um Übergabe der Daten nicht entsprochen werden kann, sollte die Schweiz von der Anordnung dieser vorläufigen Massnahmen absehen. Denn Artikel 31 ermöglicht die Verweigerung der Rechtshilfe aufgrund des geltenden innerstaatlichen Rechts und der anwendbaren Verträge. Lehnt die Schweiz ein Rechtshilfeersuchen ab, besteht für sie kein Grund, die Daten, auf welche sich das abgelehnte Ersuchen bezieht, zu sichern.

Stellt die ersuchte Vertragspartei fest, dass der Verwahrer der Daten die Ermittlungen beeinträchtigen könnte[190], ist die ersuchende Vertragspartei umgehend darüber zu informieren[191]. Diese kann daraufhin entscheiden, ob sie das mit der Erledigung des Sicherungsersuchens verbundene Risiko eingehen oder stattdessen eine eingreifendere, aber auch sicherere Form der Rechtshilfe wählen will[192]. Gemäss Artikel

187 Die Voraussetzung der beidseitigen Strafbarkeit ist bei Straftaten nach den Artikeln 2 bis 11 der Konvention ohnehin erfüllt, sofern die Vertragsparteien nicht einen in der Konvention vorgesehenen Vorbehalt hinsichtlich dieser Straftaten angebracht haben. Demnach können die Vertragsparteien die Voraussetzung der beidseitigen Strafbarkeit nur bei anderen als den in der Konvention bezeichneten Straftaten verlangen.

188 Vgl. den entsprechenden Vorbehalt der Schweiz im EUeR.

189 Die ersuchte Vertragspartei kann das Sicherungsersuchen nur ablehnen, wenn dessen Erledigung ihre Souveränität, Sicherheit, öffentliche Ordnung oder andere wesentliche Interessen beeinträchtigen könnte oder wenn sie die Straftat als politische oder mit einer solchen zusammenhängende Straftat ansieht. Diese Massnahme ist erforderlich, um eine wirksame Untersuchung und Verfolgung von Computerstraftaten zu gewährleisten. Dementsprechend dürfen für die Ablehnung eines Sicherungsersuchens keine anderen Gründe geltend gemacht werden. Vgl. Ziff. 287 des Erläuternden Berichts (Fussnote 1).

190 Z.B. wenn die zu sichernden Daten von einem Dienstanbieter aufbewahrt werden, der von einer kriminellen Organisation kontrolliert wird oder gegen den sich die Ermittlungen richten.

191 Art. 29 Abs. 6.

192 Wie die Anordnung der Herausgabe, die Durchsuchung oder die Beschlagnahme. Ziff. 288 des Erläuternden Berichts (Fussnote 1).

29 Absatz 7 der Konvention müssen die Daten bis zum Eingang des Rechtshilfeersuchens um Weitergabe der Daten für mindestens 60 Tage gesichert werden und nach Eingang des Ersuchens gesichert bleiben[193]. Dies ist für die Schweiz kein Problem, weil das Gesetz keine Mindestdauer für die Datensicherung vorschreibt und die Festlegung der Dauer im freien Ermessen der Vollzugsbehörde liegt. Deren Entscheide unterliegen der Kontrolle des BJ, das nötigenfalls dagegen Beschwerde einlegt.

2.3.9 Artikel 30 - Umgehende Weitergabe gesicherter Verkehrsdaten

2.3.9.1 Erforderliche Anpassung des geltenden Rechts

Die rasante Entwicklung der Informationstechnologie hat unsere Gesellschaft grundlegend verändert. Infolge des Austauschs riesiger Datenmengen[194] hat sie mittlerweile in sämtlichen Bereichen menschlichen Handelns Einzug gehalten. Sie hat beispiellose wirtschaftliche und gesellschaftliche Veränderungen mit sich gebracht, aber auch neue Formen von Kriminalität entstehen lassen. Die neuen Technologien stellen die bestehenden Rechtsgrundsätze in Frage und erfordern technische Massnahmen zum Schutz der Computersysteme und rechtliche Massnahmen zur Verhütung der Kriminalität und zur Abschreckung. Für eine wirksame Bekämpfung der Computerkriminalität braucht es eine schnelle Übermittlung der gewonnenen Informationen. Im Unterschied zu den herkömmlichen Beweismitteln, die eine gewisse zeitliche und räumliche Beständigkeit aufweisen[195] und auch bei mehrmonatiger Verfahrensdauer brauchbar bleiben, können Computerdaten innert kürzester Zeit von einem Land in ein anderes gelangen und werden in der Regel nicht dauerhaft, sondern selten länger als ein paar Monate gespeichert. Die Durchführung schneller vorläufiger Massnahmen (Beschlagnahme der relevanten Daten) allein reicht nicht aus. Zusätzlich sind die Daten möglichst rasch an die ersuchende Behörde zu übermitteln, weil sie sonst unbrauchbar werden. Dieses Erfordernis ist Gegenstand von Artikel 30 der Konvention.

Das schweizerische Recht genügt nicht für die Umsetzung von Artikel 30 der Konvention. Auf Ersuchen einer Vertragspartei, in deren Hoheitsgebiet eine Straftat begangen wurde, sichert die ersuchte Vertragspartei häufig die Verkehrsdaten zur Übermittlung einer Kommunikation, die über ihre Computer gelaufen ist. Damit wird die Möglichkeit geschaffen, die Kommunikation bis zu ihrem Ursprung zurückzuverfolgen, den Täter zu ermitteln oder entscheidendes Beweismaterial aufzufinden. Dabei kann die ersuchte Vertragspartei anhand der in ihrem Hoheitsgebiet entdeckten Verkehrsdaten feststellen, dass die Kommunikation von einem Dienstanbieter eines Drittstaates oder einem Anbieter im ersuchenden Staat ausgegangen ist. In einem solchen Fall muss die ersuchte Vertragspartei der ersuchenden Vertragspartei rasch eine ausreichende Menge von Verkehrsdaten zur Verfügung stellen, damit der Dienstanbieter des Drittstaates und der Übertragungsweg ermittelt werden können. Wurde die Kommunikation von einem Drittstaat aus übermittelt, kann die ersuchende Vertragspartei aufgrund der vorliegenden Informationen an diesen Staat

193 Ziff. 289 des Erläuternden Berichts (Fussnote 1).

194 Der bequeme Zugriff auf die in Computersystemen enthaltenen Informationen, die einfache Suche danach sowie die nahezu unbegrenzten Möglichkeiten des Austauschs und der Verbreitung dieser Informationen, ungeachtet geografischer Entfernungen, haben zu einem explosionsartigen Anstieg der verfügbaren Informationsmenge und des daraus zu schöpfenden Wissens geführt.

195 Beispielsweise muss eine Bank ihre Buchführungsunterlagen zehn Jahre lang aufbewahren.

ein Ersuchen um Sicherung und beschleunigte Rechtshilfe stellen, um den Dienstanbieter und den Übertragungsweg zu ermitteln. Artikel 30 verlangt die rasche Weitergabe von Verkehrsdaten ans Ausland, wobei diese Randdaten dank einer Überwachungsanordnung nach BÜPF zugänglich sind. Diese Verpflichtung lässt sich mit dem heutigen Rechtshilfesystem der Schweiz kaum vereinbaren. Dieses verlangt nämlich, dass vor der Übermittlung von Informationen aus dem Geheimbereich[196] dem Besitzer dieser Informationen stets eine beschwerdefähige Schlussverfügung zugestellt wird[197]. Erst nach Abschluss dieses Verfahrens, das mehrere Monate dauert, dürfen die Daten an die ausländische Behörde übermittelt werden. Diese lange Dauer hat zur Folge, dass die Daten sich für die ausländische Behörde als unbrauchbar erweisen, weil sie inzwischen veraltet sind. Zudem gibt dies den betroffenen Personen, die von den Schweizer Behörden informiert wurden, die Möglichkeit, belastendes Beweismaterial verschwinden zu lassen[198]. Somit ist das schweizerische Recht in dieser Hinsicht anzupassen, damit es den Anforderungen von Artikel 30 gerecht wird. Hierzu dient Absatz 1 Buchstabe a des nachstehenden neuen Artikels 18*b* IRSG, dessen Absatz 1 Buchstabe b auch die Anforderungen für die Umsetzung von Artikel 33 erfüllt:

Art. 18b Verkehrsdaten

[1] Die mit dem Ersuchen befasste Behörde des Bundes oder des Kantons kann die Übermittlung von Verkehrsdaten ans Ausland vor Abschluss des Rechtshilfeverfahrens anordnen, wenn:

a. die vorläufigen Massnahmen zeigen, dass sich der Ursprung der Kommunikation, die Gegenstand des Ersuchens ist, in einem anderen Staat befindet; oder wenn

b. diese Daten von der Vollzugsbehörde aufgrund der Anordnung einer bewilligten Echtzeitüberwachung (Art. 269 bis 281 StPO) erhoben wurden.

[2] Diese Daten dürfen nicht als Beweismittel verwendet werden, bevor die Verfügung über die Gewährung und den Umfang der Rechtshilfe rechtskräftig ist.

[3] Die Verfügung nach Absatz 1 und die allfällige Anordnung und Bewilligung der Überwachung sind dem Bundesamt unverzüglich mitzuteilen.

196 Art. 9 IRSG und Art. 69 des Bundesgesetzes über die Bundesstrafrechtspflege (SR **312.0**).

197 Art. 80*e* IRSG. Ein solches Verfahren ist nicht erforderlich, wenn die untersuchte Mitteilung selbst eine über das Internet begangene Straftat darstellt. In diesem Fall ist die Internet-Anbieterin verpflichtet, in einem vereinfachten Verfahren sämtliche Informationen weiterzuleiten, welche die Identifikation des Urhebers oder der Urheberin ermöglichen (Art. 14 Abs. 4 BÜPF).

198 Verdunkelungsgefahr rechtfertigt die unverzügliche Übermittlung. Diese ist z.B. angezeigt, wenn die ausländische Behörde die Identität einer Person feststellen will, die schweizerische Internetdienste benutzt, um Dateien mit Kinderpornografie auszutauschen. Bisher dürfen Daten, welche die Identifikation des Benutzers eines solchen Dienstes ermöglichen, nicht an die ausländische Behörde übermittelt werden, bevor der Benutzer über die gegen ihn gerichtete Verfügung informiert wurde und Gelegenheit hatte, innert einer Frist von dreissig Tagen dagegen Beschwerde einzulegen. Allerdings gab diese Frist ihm die Möglichkeit, sämtliche auf seinem PC gespeicherten belastenden Daten zu löschen.

Der neue Artikel 18*b* gestattet die Übermittlung von Verkehrsdaten aus dem Geheimbereich an die ausländische Behörde vor Abschluss des Rechtshilfeverfahrens in zwei Fällen: a) Absatz 1 Buchstabe a (Bestimmung zur Umsetzung von Artikel 30): Die vorläufigen Massnahmen zeigen, dass sich der Ursprung der Kommunikation, die Gegenstand des Ersuchens ist, in einem anderen Staat befindet; b) Absatz 1 Buchstabe b (Bestimmung zur Umsetzung von Artikel 33): Diese Daten werden von der Vollzugsbehörde aufgrund der Anordnung einer bewilligten Echtzeitüberwachung erhoben. Eine solche Übermittlung weicht vom heutigen Rechtshilfesystem ab, weshalb die betroffene Person einen in Artikel 18*b* Absätze 2 und 3 vorgesehenen grösseren Rechtsschutz geniesst, falls die Rechtshilfe später verweigert wird. Hierfür sind dreierlei Schutzmassnahmen vorgesehen:

a) Die Überwachungsmassnahme bedarf der Genehmigung eines unabhängigen Gerichts nach Artikel 272 StPO (vgl. neuer Art. 18*b* Abs. 1 Bst. b in fine IRSG); b) die übermittelten Daten dürfen vor Abschluss des Rechtshilfeverfahrens nicht als Beweismittel verwendet werden, so dass die Möglichkeit besteht, die übermittelten Informationen aus den ausländischen Akten entfernen zu lassen, wenn eine Beschwerde gutgeheissen wurde (vgl. neuer Art. 18*b* Abs. 2 IRSG); und
c) diese Übermittlung unterliegt der unverzüglichen Kontrolle des BJ (vgl. neuer Artikel 18*b* Abs. 3 IRSG).

Es können nur Daten übermittelt werden, die aufgrund der Anordnung einer bewilligten Überwachung erhoben wurden. Damit wird gewährleistet, dass die Daten in Übereinstimmung mit dem schweizerischen Recht erhoben wurden und dass das Rechtshilfeersuchen nicht nur von der Vollzugsbehörde, sondern auch von einem unabhängigen Gericht überprüft wurde[199]. Zusätzlich verstärkt wird diese Kontrolle dadurch, dass jede Übermittlungsverfügung dem BJ unverzüglich mitzuteilen ist. Dieses sorgt für die Einhaltung des Gesetzes und kann bei den schweizerischen ebenso wie den ausländischen Behörden intervenieren, wenn diese Bestimmung missbräuchlich angewendet oder missachtet wird. Diese Bestimmung stellt im schweizerischen Rechtshilfesystem eine gewisse Neuerung dar, weil sie die Übermittlung von Informationen aus dem Geheimbereich an die ausländische Behörde gestattet, ohne dass die betroffene Person vorher benachrichtigt wurde und Gelegenheit erhielt, ihre Argumente geltend zu machen. Eine solche Übermittlung ist notwendig, um den Anforderungen der Konvention, welche den zwingenden Erfordernissen der Strafverfolgung Rechnung trägt, zu genügen. Diese Bestimmung schränkt die Möglichkeit der betroffenen Person ein, sich unverzüglich gegen die Übermittlung von Informationen aus dem Geheimbereich ans Ausland zu wehren. Dennoch ist der Schutz der betroffenen Person durch andere Massnahmen weiterhin gewährleistet. Denn das Rechtshilfeersuchen wird nicht nur von der Vollzugsbehörde geprüft, sondern vermehrt auch vom BJ. Zudem muss auch die Behörde, welche die Überwachung genehmigt[200], überprüfen, dass das Ersuchen eine Reihe von Kriterien erfüllt, welche materiell weitgehend mit denen des Rechtshilfeverfahrens übereinstimmen[201]. Der betroffenen Person werden nicht alle Rechte entzogen: Sobald

199 Obwohl die Überprüfung durch dieses Gericht nicht die eigentliche Rechtshilfe betrifft, bezieht sie doch einen Grossteil der in der Rechtshilfe angewendeten Kriterien ein.
200 Art. 7 Abs. 1 BÜPF.
201 Dies gilt für die beidseitige Strafbarkeit (gemäss Art. 3 BÜPF), die Verhältnismässigkeit (Subsidiarität der Massnahmen: Art. 3 Abs. 1 Bst. a bis c BÜPF) sowie die Aussonderung von Dokumenten (Art. 8 BÜPF).

es die Situation erlaubt[202], muss sie über die erfolgte Übermittlung benachrichtigt werden und kann sie nicht nur gegen die Schlussverfügung, sondern auch gegen die Überwachungsverfügung Beschwerde einlegen. Wird ihre Beschwerde gutgeheissen, muss die ausländische Behörde die Informationen aus ihren Akten entfernen und dies den Schweizer Behörden bescheinigen. Bis die betroffene Person ihre Rechte geltend machen konnte, dürfen die sie betreffenden Informationen nicht als Beweismittel, sondern lediglich zu Ermittlungszwecken verwendet werden[203]. Damit trägt die vorgeschlagene Regelung den Erfordernissen der Strafverfolgung hinreichend Rechnung und stellt gleichzeitig sicher, dass die berechtigten Interessen der betroffenen Person weiterhin angemessen geschützt sind. Diese Änderung ist überdies auch im Auslieferungsverfahren für das Auffinden verdächtiger Personen von Nutzen.

Formal gesehen muss die zuständige Behörde, an die ein Ersuchen um Echtzeitüberwachung von Verkehrsdaten gerichtet wird, eine Eintretensverfügung erlassen und die allenfalls erforderlichen Genehmigungen nach Artikel 272 StPO einholen. In dieser Verfügung oder einer separaten Zwischenverfügung ordnet die Vollzugsbehörde auch die vorzeitige, an Bedingungen geknüpfte Übermittlung der aufgrund der Überwachungsanordnung erhobenen Daten an. Die Verfügung ist dem BJ unverzüglich zu übermitteln. Dieses kann dagegen Beschwerde einlegen[204], wenn die gesetzlichen Voraussetzungen nicht erfüllt sind. Die Anordnung und die Bewilligung der Überwachung sind dem BJ ebenfalls mitzuteilen, damit es kontrollieren kann, dass die Voraussetzungen von Artikel 18*b* erfüllt sind.

Massnahmen zur Echtzeitüberwachung sollten aufgrund der Natur der Sache den überwachten Personen nicht zur Kenntnis gelangen. In der internationalen Zusammenarbeit lässt sich dieses Erfordernis nur schwer mit dem Grundsatz des IRSG vereinbaren, wonach keine Information aus dem Geheimbereich einer Person an das Ausland übermittelt werden darf, ohne dass diese Person vorher die Möglichkeit hatte, sich dagegen zu wehren. Unterschiedliche Interessen bestehen jedoch nicht nur hinsichtlich der Übermittlung von Verkehrsdaten, die in Artikel 33 der Konvention geregelt ist, sondern auch in Bezug auf die Übermittlung des Inhalts von Kommunikationen, die in Echtzeit überwacht werden. Die Lehre hat diesen möglichen Konflikt erkannt und die gegenwärtigen Probleme bei der Ausführung von Rechtshilfeersuchen aufgezeigt, die sich in Zusammenhang mit der Echtzeitüberwachung des Fernmeldeverkehrs ergeben[205]. Die Revision beschränkt sich jedoch darauf, den Anforderungen für die Umsetzung von Artikel 33 zu genügen, und berücksichtigt lediglich Verkehrsdaten, aber keine Inhaltsdaten. Mit Artikel 18*b* IRSG wird somit keine umfassende gesetzliche Regelung geschaffen, welche die Durchführung von

202 In jedem Fall jedoch spätestens vor Abschluss der Strafuntersuchung oder der Einstellung des Verfahrens (Art. 10 Abs. 2 BÜPF).

203 Vgl. hierzu die Botschaft des Bundesrates vom 1. Oktober 2004 zu Art. 30 des Abkommens über die Zusammenarbeit zwischen der Europäischen Gemeinschaft und ihren Mitgliedstaaten einerseits und der Schweizerischen Eidgenossenschaft andererseits zur Bekämpfung von Betrug und sonstigen rechtswidrigen Handlungen, die ihre finanziellen Interessen beeinträchtigen, in BBl 2004 S. 6196 f. Im schweizerischen Recht wird dasselbe Kriterium angewendet; siehe z.B. Art. 10 Abs. 3 IRSG und Art. 22 des Bundesgesetzes vom 20. Juni 2003 über die verdeckte Ermittlung (BVE).

204 Art. 80*e*, 80*h* und 80*l* IRSG.

205 Thomas Hansjakob, BÜPF / VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, St. Gallen 2006; Robert Zimmermann, La coopération judiciaire internationale en matière pénale, Bern, 2004, N 246-13 ff., S. 285 ff.

Überwachungsmassnahmen im Rahmen der Rechtshilfe ermöglicht und sowohl Verkehrs- als auch Inhaltsdaten einbezieht.

Auf den neuen Artikel 18*b* Absatz 1 Buchstabe b IRSG wird auch in den Ausführungen zu Artikel 33 der Konvention eingegangen.

2.3.9.2 Weitere Erläuterungen zu Artikel 30

Gemäss Artikel 30 Absatz 2 darf die ersuchte Vertragspartei die Weitergabe von Verkehrsdaten nur ablehnen, wenn dadurch ihre Souveränität, Sicherheit, öffentliche Ordnung oder andere wesentliche Interessen beeinträchtigt werden könnten, oder wenn sie die betreffende Straftat als politische oder mit einer solchen zusammenhängende Straftat ansieht. Wie bei Artikel 29 der Konvention ist diese Art von Informationen auch hier für die Ermittlung der Täter oder das Auffinden von entscheidendem Beweismaterial derart wichtig, dass die Gründe für die Verweigerung der Weitergabe eingeschränkt wurden[206].

2.3.10 Artikel 31 - Rechtshilfe beim Zugriff auf gespeicherte Computerdaten

Artikel 31 gibt jeder Vertragspartei die Möglichkeit, für die andere Vertragspartei Daten, die mittels eines auf ihrem Hoheitsgebiet befindlichen Computersystems gespeichert sind, zu durchsuchen oder in ähnlicher Weise darauf zuzugreifen, diese zu beschlagnahmen oder in ähnlicher Weise sicherzustellen und diese weiterzugeben, wie sie es aufgrund von Artikel 19[207] der Konvention zu innerstaatlichen Zwecken tun kann[208]. Dass Artikel 31 keine Beschränkung der vorgesehenen Massnahmen auf eine bestimmte Kategorie von Delikten zulässt und keine Möglichkeit einräumt, Vorbehalte anzubringen[209], erscheint unproblematisch, weil Artikel 31 in Anwendung der in Artikel 23 genannten geltenden Übereinkommen und innerstaatlichen Rechtsvorschriften umgesetzt wird.

Nach Artikel 31 Absatz 1 kann jede Vertragspartei um eine darin vorgesehene Form von Rechtshilfe ersuchen und muss die ersuchte Vertragspartei die erforderlichen Voraussetzungen schaffen, um diese Rechtshilfe leisten zu können. Artikel 31 Absatz 2 sieht vor, dass sich diese Zusammenarbeit nach den Bedingungen richtet, die in den anwendbaren Verträgen, Vereinbarungen und innerstaatlichen Rechtsvorschriften festgelegt sind. Gemäss Artikel 31 Absatz 3 ist ein solches Ersuchen umgehend zu erledigen, wenn a) Gründe zu der Annahme vorliegen, dass bei den einschlägigen Daten eine besondere Gefahr des Verlusts oder der Veränderung besteht, oder b) die anwendbaren Verträge, Vereinbarungen oder Rechtsvorschriften eine umgehende Zusammenarbeit vorsehen.

2.3.11 Artikel 32 - Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind

Artikel 32 des Übereinkommens regelt den grenzüberschreitenden Zugriff auf öffentlich zugängliche Daten[210] sowie auf Daten mit Zustimmung der zur Weiterleitung befugten Person. Die Bestimmung behandelt diejenigen Szenarien, wo ein nicht

206 Ziff. 291 des Erläuternden Berichts (Fussnote 1).
207 Durchsuchung und Beschlagnahme gespeicherter Computerdaten.
208 Ziff. 292 des Erläuternden Berichts (Fussnote 1).
209 Art. 42.
210 Open source data.

abgesprochenes Vorgehen eines einzelnen Staates unbestrittenermassen zulässig ist[211], ohne dass die Souveränität eingeschränkt wird; die Konventionsbestimmung vollzieht damit in rechtlicher Hinsicht zwei Arten der praktisch durchgeführten Datenbeschaffung im Ausland nach. Im Verlauf der Vertragsverhandlungen stellte sich heraus, dass kein Konsens erreicht werden konnte für weitergehende Regeln, unter welchen Voraussetzungen ein unilateraler Zugriff eines Staates auf Daten, die sich in einem anderen Vertragsstaat befinden, ohne Genehmigung desselben[212] erfolgen kann.

Zum Einen wird in Artikel 32 der Fall geregelt, in welchem eine Vertragspartei auf öffentlich zugängliche Daten grenzüberschreitend zugreifen darf. Sind Daten, beispielsweise auf dem Internet unter der Domainadresse einer Firma, öffentlich abrufbar, so soll die Vertragspartei nicht dazu verpflichtet werden, dieses Material nur mit Zustimmung des Staates, in welchem sich die Daten befinden, abzurufen und zu verwenden. Zum Anderen darf die Vertragspartei auf Daten, die sich in einem anderen Vertragsstaat befinden, zugreifen oder diese empfangen, wenn sie über die rechtmässige und freiwillige Zustimmung einer Person im Inland verfügt, die rechtmässig befugt ist, die Daten an eine inländische Strafverfolgungsbehörde weiterzuleiten. Handelt es sich aber um vertrauliches Datenmaterial einer Drittperson, zu deren Offenlegung diese keine Zustimmung erteilt hat, liegt keine Befugnis im Sinne von Artikel 32 der Konvention vor.

Die Bestimmung von Artikel 32 des Übereinkommens ist damit, insbesondere bezüglich ihres zweiten Teilbereichs, eng auszulegen, um der Gefahr des Missbrauchs unter Umgehung der Rechtshilfe oder in Verletzung der Privatsphäre Dritter entgegenzuwirken[213]. Die rechtmässige Befugnis der Person, über die Daten zu verfügen und sie an eine staatliche Stelle weiterzuleiten, beurteilt sich primär nach dem nationalen Recht des Staates, indem die betreffende Person handelt. Sie liegt zum Beispiel dann vor, wenn die Person eigene E-Mails bei einem ausländischen Service-Provider gespeichert hat und sie diese Daten an eine inländische Behörde weitergibt[214]. Konkret wird damit diejenige Person im Ausland, die Daten in der Schweiz gespeichert hat, diese ohne Information der Schweizer Behörden wie bisher einer ausländischen Stelle freiwillig zur Verfügung stellen können, soweit sie dazu rechtmässig befugt ist und kein Eingriff in den geschützten Geheimbereich Dritter vorliegt.

2.3.12 Artikel 33 - Rechtshilfe bei der Erhebung von Verkehrsdaten in Echtzeit

Nach Artikel 33 muss jede Vertragspartei für eine andere Vertragspartei Verkehrsdaten in Echtzeit erheben und sind die Vertragsparteien verpflichtet, in diesem Bereich zusammenzuarbeiten. Die für eine solche Zusammenarbeit geltenden Bestimmungen und Bedingungen richten sich nach den anwendbaren Verträgen und

211 Erläuternder Bericht, Ziff. 293 (vgl. Fussnote 1).

212 Und ohne Einhalten des ordentlichen Rechts- oder Amtshilfeweges. Andere Zugriffsmöglichkeiten werden durch das Übereinkommen nicht autorisiert; vgl. Art. 39 Abs. 3 der Konvention.

213 Diese Auffassung wird von Deutschland im Rahmen seines Umsetzungsprozesses geteilt, vgl. die Ausführungen im Gesetzesentwurf der deutschen Bundesregierung vom 16. November 2007 zur Konvention über die Cyberkriminalität, Drucksache 16/7218, S. 55, abrufbar unter http://dip21.bundestag.de/dip21/btd/16/072/1607218.pdf .

214 Eine Speicherung im Ausland kann, da nicht ohne Weiteres erkennbar, auch ohne Wissen der berechtigten Person vorliegen.

Rechtsvorschriften über die Rechtshilfe in Strafsachen. Häufig können nämlich die Ermittler nicht gewährleisten, dass sich eine Kommunikation anhand der Aufzeichnungen früherer Übermittlungen bis zu ihrem Ursprung zurückverfolgen lässt, weil wesentliche Verkehrsdaten von einem Dienstanbieter in der Übertragungskette möglicherweise automatisch gelöscht wurden, bevor sie gesichert werden konnten. Deshalb müssen die Ermittler jedes Vertragsstaates unbedingt die Möglichkeit haben, sich Verkehrsdaten zu beschaffen, die über ein Computersystem in einem anderen Vertragsstaat übermittelt wurden[215]. Nach Artikel 33 Absatz 2 ist zumindest bei den Straftaten Rechtshilfe zu leisten, "bei denen die Erhebung von Verkehrsdaten in Echtzeit in einem gleichartigen inländischen Fall möglich wäre". Nach geltendem schweizerischem Recht werden Verkehrsdaten aus dem Geheimbereich unter entsprechender Geheimhaltung erhoben und muss vor deren Übermittlung eine Schlussverfügung vorliegen. Mit dem in Kapitel 2.3.9.1 vorgeschlagenen neuen Artikel 18*b* IRSG wird die Möglichkeit geschaffen, die Daten unverzüglich an das Ausland zu übermitteln, ohne dass der in der Schweiz wohnhaften betroffenen Person die Verfügung zugestellt werden muss[216]. Damit sind auch die ausländischen Ermittlungen nicht mehr gefährdet.

Artikel 33 der Konvention enthält keine Einschränkung hinsichtlich der Schwere der Straftat als Rechtfertigungsgrund für die Anwendung von Überwachungsmassnahmen. Der neue Artikel 273[217] StPO wird die Echtzeitüberwachung von Verkehrsdaten nur bei Ermittlungen in Zusammenhang mit Vergehen und Verbrechen gestatten. Artikel 15 Absatz 1 der Europaratskonvention über die Cyberkriminalität sieht jedoch vor, dass für die Befugnisse und Verfahren der Grundsatz der Verhältnismässigkeit gilt, wobei jede Vertragspartei diesen Grundsatz im Einklang mit den anderen Grundsätzen ihres innerstaatlichen Rechts anwendet[218]. Die Vertragsparteien der Konvention dürfen somit Ersuchen nicht entsprechen, welche dem Grundsatz der Verhältnismässigkeit zuwiderlaufen. Dies erlaubt der Schweiz, die Zusammenarbeit zu verweigern, wenn der Tatbestand im schweizerischen Recht als Übertretung eingestuft ist. Bei Online-Wetten, mit denen sich sehr hohe Erträge erzielen lassen, könnte es sich etwas schwierig verhalten, weil solche Wetten in der Schweiz als Übertretungen gelten[219].

2.3.13 Artikel 34 - Rechtshilfe bei der Erhebung von Inhaltsdaten in Echtzeit

Artikel 34 schränkt die Verpflichtung zur Rechtshilfe bei der Erhebung von Inhaltsdaten ein, weil das Abfangen von Daten stark in die Privatsphäre eingreift. Diese Form der Rechtshilfe wird gewährt, soweit die anwendbaren Verträge und innerstaatlichen Rechtsvorschriften dies gestatten. Die Rechtshilfepraxis in diesem Bereich steht erst am Anfang, weshalb die bestehenden Rechtshilferegelungen und das innerstaatliche Rechtshilferecht massgebend sind für den Umfang der Verpflichtung zur Zusammenarbeit und die Beschränkungen dieser Verpflichtung[220]. Gemäss dem

215 Ziff. 295 des Erläuternden Berichts (Fussnote 1).
216 Art. 80*m* IRSG.
217 Nach dem neuen Strafprozessrecht wird eine rückwirkende Überwachung möglich sein, wenn die Schwere der Straftat diese rechtfertigt und sie für die Untersuchung erforderlich ist (Art. 273 und Art. 269 Abs. 1 Bst. b und c StPO), auch wenn diese Straftat im Deliktskatalog von Art. 269 StPO nicht aufgeführt ist.
218 Ziff. 146 des Erläuternden Berichts (Fussnote 1).
219 Art. 42 des Bundesgesetzes vom 8. Juni 1923 betreffend die Lotterien und die gewerbsmässigen Wetten; LG; SR **935.51**.
220 Ziff. 297 des Erläuternden Berichts (Fussnote 1).

in Kap. 2.3.9.1 vorgeschlagenen neuen Artikel 18*b* IRSG dürfen vor Abschluss eines Verfahrens nur Verkehrsdaten an das Ausland übermittelt werden, aber keine Inhaltsdaten. Somit dürfen die Schweizer Behörden nach Artikel 30 Absatz 1 IRSG[221] einen anderen Staat nicht um die Echtzeit-Erhebung von Inhaltsdaten ersuchen.

2.3.14 Artikel 35 - 24/7-Netzwerk

Gemäss Artikel 35 der Konvention stellen die Vertragsstaaten sicher, dass eine Kontaktstelle an sieben Wochentagen 24 Stunden täglich zur Verfügung steht und besetzt ist. Diese Stelle sorgt für die Unterstützung von innerstaatlichen und internationalen Strafuntersuchungen in Fällen von Computerkriminalität. Die Kontaktstelle muss nicht selber unmittelbar Massnahmen in den Bereichen juristische Beratung, Rechtshilfe, Beweiserhebung, Datensicherung oder Strafuntersuchung im Allgemeinen ergreifen können[222]. Sie hat, um den verbindlichen Anforderungen der Konvention zu entsprechen, lediglich zur Aufgabe, als Anlaufstelle den Kontakt zwischen den mit den jeweiligen Aufgaben betrauten ausländischen und inländischen Behörden zu erleichtern.

Die Funktion der geforderten Kontaktstelle kann von der Einsatzzentrale des Bundesamtes für Polizei (fedpol) wahrgenommen werden. Das Bundesamt für Justiz mit seinem Pikettdienst wird die in Artikel 35 Absatz 1 Buchstaben a bis c der Konvention genannten Aufgaben betreffend Rechtshilfe und Auslieferung wahrnehmen (insbesondere die Entscheidfindung über die Zulässigkeit einer Massnahme).

Der Mehraufwand für die Erledigung von Rechtshilfefällen und Ersuchen im Bereich des Übereinkommens über die Cyberkriminalität kann schwerlich beziffert werden und ist abhängig von der Anzahl Vertragsstaaten der Europaratskonvention, der Komplexität der einzelnen Fälle sowie der technologischen Entwicklung, zum Einen im Hinblick auf die Delinquenz in den Staaten, zum Anderen mit Bezug auf die Mittel der Strafverfolgung[223]. Der sich aus der Umsetzung und Ratifikation der Europaratskonvention ergebende Mehraufwand (Pikettdienst und ordentliche Behandlung von Fällen) wird beim Bundesamt für Justiz auf eine Vollzeitstelle geschätzt. Bei fedpol, dessen Einsatzzentrale rund um die Uhr Meldungen entgegennehmen wird, wird für die Umsetzung der Minimalforderungen der Konvention ein Mehrbedarf von ebenfalls einer Stelle geschätzt.

Von den betroffenen Stellen im Bundesamt für Polizei wird jedoch, über die unmittelbaren Erfordernisse der Konvention hinaus, ein weiterer Ausbau der Kapazitäten als angemessen und wünschbar erachtet. Um mit der Einrichtung der Kontaktstelle einen zusätzlichen Mehrwert bei der Bekämpfung der Cyberkriminalität gegenüber dem status quo zu schaffen, könnte diese über die Minimalanforderungen der Konvention hinaus mit einem breiteren Aufgabenbereich versehen werden. Insbesondere die Wahrnehmung der in Artikel 35 Absatz 1 Buchstaben a bis c genannten Aufgaben würde mit einer unverzüglichen technischen und juristischen Unterstützung durch eine spezialisierte Einheit gewährleistet werden. Auch die für die Interaktionen zwischen den Strafverfolgungsbehörden und den Internet Service Providern

221 Die schweizerischen Behörden dürfen an einen anderen Staat keine Ersuchen richten, denen sie selbst nach diesem Gesetz nicht entsprechen können.

222 Vgl. Art. 35 Abs. 1 der Konvention mit Ziff. 298 ff. des Erläuternden Berichts (Fussnote 1).

223 Ressourcen und Ausrüstung im Bereich der Überwachung, Sicherung und Kontrolle des elektronischen Datenverkehrs.

notwendigen Kontakte und Abläufe wären durch die Kontaktstelle zu etablieren, um eine schnelle, effiziente Strafverfolgung sicherstellen zu können[224].

Diese Kooperation der Internet Service Provider mit den Strafverfolgungsbehörden bedingt einen konstanten Austausch zwischen den beteiligten Akteuren und Ausbildungen im technischen wie auch im rechtlichen Bereich. Bei einer solchen umfassenderen Ausgestaltung der Kontaktstelle würden diese Aufgaben organisatorisch und fachlich der nationalen Koordinationsstelle von Bund und Kantonen zur Bekämpfung der Internetkriminalität (KOBIK[225]) zugeordnet, da dort ein Kontaktnetz zu den IT-Ermittlern der Kantonspolizeien und auch zu verschiedenen Internet Service Providern bereits besteht. Eine Angliederung der dafür – auf Grund des heutigen Wissenstandes - notwendigen zusätzlichen zwei Stellen ermöglichte eine verbesserte Nutzung von Synergien[226].

Um eine rasche Unterstützung bei Rechtshilfefällen oder Strafverfahren in Bundeskompetenz gewährleisten zu können, wäre es bei der Etablierung einer effizienten Kontaktstelle sinnvoll und angemessen, auch im Kommissariat IT-Ermittlungen der Bundeskriminalpolizei ein Pikett einzurichten. Weil im Bereich der Cyberkriminalität bei den Kantonen das notwendige Know-how zum Vollzug der geforderten Rechtshilfe und ganz allgemein im Bereich der IT-Ermittlungen unterschiedlich verfügbar ist, könnte das Kommissariat IT-Ermittlungen auch verstärkt die kantonalen Strafverfolgungsbehörden unterstützen. Der hierfür benötigte Aufwand beliefe sich auf geschätzte zwei weitere Stellen.

Über einen entsprechenden Ressourcenantrag und die Frage einer budgetneutralen Kompensation innerhalb des EJPD wird im Rahmen der Botschaft zu Handen des Parlaments zu entscheiden sein.

2.4 Kapitel IV: Schlussbestimmungen

Die Schlussbestimmungen der Europaratskonvention über die Cyberkriminalität entsprechen - von wenigen Besonderheiten abgesehen - denjenigen in anderen Übereinkommen des Europarates.

Gemäss *Artikel 36* der Konvention steht der Beitritt nicht nur den Mitgliedstaaten des Europarates offen, sondern auch den Nicht-Mitgliedstaaten, welche an der Ausarbeitung des Übereinkommens beteiligt waren[227]. Darüber hinaus können weitere Staaten eingeladen werden, dem Übereinkommen beizutreten[228].

Die Konvention ist am 1. Juli 2004 in Kraft getreten, nachdem die dafür erforderlichen fünf Ratifikationen[229] erfolgt waren. Mittlerweile weist das Übereinkommen 23 Mitgliedstaaten auf, darunter als einziges Nicht-Mitglied des Europarates die Vereinigten Staaten.

224 Vgl. hierzu die „Richtlinien für die Zusammenarbeit zwischen Strafverfolgungsbehörden und Internet Service Providern gegen Internetkriminalität“ (Guidelines for the cooperation between law enforcement and internet service providers) des Europarates, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_FR.asp.

225 Vgl. www.cybercrime.ch.

226 Auf Grund der Konstituierung von KOBIK könnten die neuen Stellen nicht in diese Stelle integriert, sondern ihr nur organisatorisch zugeordnet werden.

227 Japan, Kanada, Südafrika und die Vereinigten Staaten von Amerika.

228 *Art. 37* der Konvention. Eingeladen sind zur Zeit (November 2008) Costa Rica, Mexiko und die Philippinen.

229 *Art. 36 Abs. 3* der Konvention.

Die Möglichkeit der Abgabe von Erklärungen und Vorbehalten wurde bei der Erarbeitung der Konvention ausdrücklich als Bestandteil des einfach gehaltenen Texts vorgesehen[230]. Entsprechend enthält *Artikel 40* die Liste derjenigen sechs Konventionsbestimmungen, zu welchen die Vertragsstaaten einschränkende Erklärungen abgeben können. Wie anlässlich der Kommentierung der einzelnen Bestimmungen erläutert, wird vorgeschlagen, dass die Schweiz Erklärungen abgibt zu den Artikeln 2, 3, 7, 9 Ziffer 3 sowie 27 Ziffer 9 Buchstabe e.

Mittels Vorbehalt kann ein Staat aufgrund von *Artikel 41* (Bundesstaatsklausel) erklären, dass er aufgrund seiner Struktur den Verpflichtungen aus dem II. Kapitel der Konvention[231] nicht nachzukommen vermag[232]. Vorausgesetzt bleibt, dass der Bereich der Internationalen Zusammenarbeit[233] durch einen solchen Vorbehalt nicht tangiert wird. Angesichts der Schweizerischen Bundeszuständigkeit im Bereich der Strafgesetzgebung und der in naher Zukunft in Kraft tretenden Schweizerischen Strafprozessordnung vom 5. Oktober 2007 muss von dieser Vorbehaltsmöglichkeit kein Gebrauch gemacht werden.

Eine Besonderheit des Übereinkommens bildet der *numerus clausus* von möglichen Vorbehalten in *Artikel 42*. Demnach können die Vertragsstaaten ausschliesslich zu den dort aufgeführten neun Konventionsbestimmungen Vorbehalte anbringen. Es ist vorgesehen, dass die Schweiz vier dieser Möglichkeiten in Anspruch nimmt, und zwar zu den Artikeln 6 Ziffer 3, 9 Ziffer 4, 14 Ziffer 3 sowie 29 Ziffer 4. Auch diesbezüglich kann für die Einzelheiten auf die Kommentierung der jeweiligen Bestimmungen verwiesen werden.

Die im Vorentwurf zum Bundesbeschluss enthaltenen Schweizer Vorbehalte und Erklärungen sind dem Generalsekretär des Europarates anlässlich der Hinterlegung der Ratifikationsurkunde bekannt zu geben.

Bei Streitigkeiten bezüglich der Auslegung oder Anwendung des Übereinkommens steht die friedliche Beilegung durch Verhandlungen zwischen den involvierten Parteien im Vordergrund (*Art. 45*). Im Unterschied zu anderen Konventionen des Europarates neueren Datums enthält das vorliegende Übereinkommen keinen wechselseitigen Überwachungs- oder Evaluationsmechanismus.

Das Übereinkommen kann jederzeit, mit einer Frist von drei Monaten, mittels Notifikation an den Generalsekretär des Europarates gekündigt werden (*Art. 47*).

2.5 Das Zusatzprotokoll gegen Rassismus und Fremdenfeindlichkeit vom 28. Januar 2003

Das Zusatzprotokoll zum Übereinkommen über die Cyberkriminalität betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art vom 28. Januar 2003 verpflichtet die Vertragsstaaten zur Bestrafung von Diskriminierung sowie Aufstachelung zu Hass und Gewalt gegen Personen aufgrund deren Rasse, Hautfarbe, Abstammung, Herkunft oder Religion. Im Übrigen werden die Bestimmungen der Konvention gegen die Cyberkriminalität

230 Vgl. die Ausführungen im Erläuternden Bericht des Europarates zur Konvention, Ziff. 49 und 50 (Fussnote 1).
231 Innerstaatliche Massnahmen.
232 Eine nicht sehr gebräuchliche Klausel, welche auf massgebliche Intervention der Vereinigten Staaten hin in den Text aufgenommen worden ist.
233 III. Kapitel der Konvention.

für anwendbar erklärt. Das Protokoll ist am 1. März 2006 in Kraft getreten und wurde bisher durch 13 Länder, darunter drei EU-Staaten, ratifiziert.

Die Schweiz hat das Zusatzprotokoll am 9. Oktober 2003 unterzeichnet. Die Schweizer Rechtsordnung entspricht den zwingenden Anforderungen des Zusatzprotokolls weitgehend. Obwohl die geltende Rassismusstrafnorm von Artikel 261bis StGB auf die im Zusatzprotokoll genannten Kriterien der Farbe, Abstammung sowie der nationalen Herkunft keinen Bezug nimmt, werden diese Tatbestandsvarianten faktisch durch die Begriffe der Rasse und der Ethnie abgedeckt.

Das geltende Schweizer Recht geht in verschiedener Hinsicht über das durch das Zusatzprotokoll Geforderte hinaus. So findet sich das Element der Religion, im Gegensatz zu den Anforderungen des Protokolls, als vollständiges Kriterium, und das schweizerische Strafrecht reduziert den Begriff der Ethnie nicht auf die ethnische Herkunft, was in der Praxis bedeutsam sein kann.

Trotz der weitgehenden Kompatibilität unserer Rechtsordnung mit dem Zusatzprotokoll wird mit dieser Vorlage nur die Ratifikation der Konvention über die Cyberkriminalität vorgeschlagen. Die Umsetzung des Protokolls, welches eine grundsätzlich andere Materie betrifft, soll in einem späteren selbständigen Schritt geprüft werden. Dieses Vorgehen erlaubt eine Fokussierung auf die materiellrechtlichen Fragen der Computerkriminalität, des Strafprozessrechts im Bereich der elektronischen Beweismittel und auf die Rechtshilfefragen in diesem Zusammenhang. Des Weiteren sind die Resultate der zur Zeit hängigen Arbeiten des EJPD betreffend Strafbarkeit der Verwendung rassistischer Symbole[234] abzuwarten und bei der Prüfung einer Umsetzung des Zusatzprotokolls zu berücksichtigen.

2.6 Verhältnis zu anderen Revisionen im Bereich des Strafrechts

Am 5. Oktober 2007 haben die Eidgenössischen Räte die Schweizerische Strafprozessordnung (StPO) verabschiedet, welche die verschiedenen kantonalen Ordnungen sowie den Bundesstrafprozess ersetzen wird. Die StPO soll am 1. Januar 2011 in Kraft treten. Im Rahmen des vorliegenden Berichts wird an verschiedener Stelle auf Bestimmungen der StPO verwiesen[235], die für die Umsetzung der Europaratskonvention über die Cyberkriminalität wesentlich sind oder welche eine lückenlose und nachvollziehbare Abdeckung durch das Schweizer Recht gewährleisten. Das Inkrafttreten der Konvention für die Schweiz setzt daher das Inkrafttreten der StPO voraus. Eine zeitliche Verzögerung dieser Vorlage ist dadurch jedoch nicht zu erwarten.

Eine Arbeitsgruppe des Bundes hat im Hinblick auf die Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) ihre Arbeit aufgenommen. Sollten sich Berührungspunkte zu dieser Vorlage ergeben, ist die Koordination zwischen den beiden Geschäften sichergestellt.

234 Vgl. hierzu das Arbeitspapier des Bundesamtes für Justiz für das Hearing betreffend die Rassismusstrafnorm von Mai 2007, abrufbar unter www.bj.admin.ch/etc/medialib/data/kriminalitaet/gesetzgebung/rassismus.

235 Vgl. insb. die Ausführungen zu den Artikeln 16 bis 21 sowie 23, 25, 30 und 33 der Konvention.

3 Auswirkungen

3.1 Finanzielle und personelle Auswirkungen auf den Bund

Auf Grund der steigenden Anzahl Fälle von Internetkriminalität ist unabhängig von der vorliegenden Europaratskonvention mit einer generell stärkeren Beanspruchung der Strafverfolgungsbehörden sowie des dem EJPD angegliederten Dienstes für die Überwachung des Post- und Fernmeldeverkehrs zu rechnen. Da Sachverhalte im Zusammenhang mit Internet in den meisten Fällen internationale Bezüge aufweisen, werden auch die für die Erfüllung von Rechtshilfeersuchen zuständigen Stellen zukünftig verstärkt gefordert sein.

Die Umsetzung und Ratifikation der Europaratskonvention über die Cyberkriminalität kann eine erhöhte qualitative und quantitative Auslastung der zuständigen Rechtshilfestelle beim Bundesamt für Justiz mit sich bringen und schafft eine zusätzliche Koordinierungsfunktion für die Einsatzzentrale der Bundeskriminalpolizei. Über einen entsprechenden Personalantrag und eine departementsinterne Kompensation wird im Rahmen der Botschaft zu Handen des Parlaments zu entscheiden sein.

3.2 Volkswirtschaftliche Auswirkungen

Die Umsetzung der Europaratskonvention über die Cyberkriminalität lässt keine Auswirkungen auf die Volkswirtschaft erwarten.

3.3 Auswirkungen auf die Informatik

Die Umsetzung der Europaratskonvention über die Cyberkriminalität lässt keine Auswirkungen auf die Informatik erwarten. Die bestehende Ausrüstung der Strafverfolgungsbehörden des Bundes und des Bundesgerichts sowie des Bundesstrafgerichts im Bereich der Informatik entsprechen den Anforderungen der Konvention und sind ausreichend, um die Verfolgung und Beurteilung in diesen Bereichen sicherzustellen.

3.4 Auswirkungen auf die Kantone

Aufgrund der nach wie vor raschen technologischen und gesellschaftlichen Entwicklung im Bereich der modernen Kommunikationstechnologien ist grundsätzlich mit einem Anstieg der Fallzahlen im Bereich der Cyberkriminalität zu rechnen. Die Umsetzung der Europaratskonvention über die Cyberkriminalität an sich lässt jedoch kaum Auswirkungen auf die Kantone erwarten. Es ist insbesondere nicht mit signifikant steigenden Fallzahlen von Strafverfolgungen wegen Delikten im Sinne der Konvention oder einer starken Zunahme von Rechtshilfefällen zu rechnen[236]. Die durch die Konvention geforderte Kontaktstelle wird in das Bundesamt für Polizei integriert. Als Anlaufstelle für Rechtshilfebelange und entsprechende Auskünfte fungiert das Bundesamt für Justiz.

4 Verhältnis zur Legislaturplanung

Die Vorlage ist in der Botschaft über die Legislaturplanung 2007-2011 angekündigt[237].

236 Vgl. auch Kap. 1.3: Würdigung der Konvention.
237 BBl **2008** 822.

5 Rechtliche Aspekte

5.1 Verhältnis zur Europäischen Union

Die Umsetzung der Europaratskonvention über die Cyberkriminalität bereitet hinsichtlich der Vereinbarkeit des Schweizer Rechts mit dem Recht der Europäischen Union (EU) keine Probleme. Unter den Vertragsstaaten zur Konvention befindet sich bereits eine beschränkte Anzahl Mitgliedsstaaten der EU, in verschiedenen anderen Mitgliedsstaaten ist die Umsetzung des Übereinkommens im Gange.

5.2 Verfassungsmässigkeit

Die Verfassungsmässigkeit des Bundesbeschlusses zur Genehmigung des Europaratsübereinkommens über die Cyberkriminalität beruht auf Artikel 54 Absatz 1 der Bundesverfassung (BV)[238], welcher den Bund ermächtigt, völkerrechtliche Verträge abzuschliessen. Artikel 184 Absatz 2 BV ermächtigt den Bundesrat, völkerrechtliche Verträge abzuschliessen und zu ratifizieren. Die Bundesversammlung ist nach Artikel 166 Absatz 2 BV für die Genehmigung völkerrechtlicher Verträge zuständig.

Internationale Verträge werden dem fakultativen Referendum unterstellt, wenn sie unbefristet und unkündbar sind, den Beitritt zu einer internationalen Organisation vorsehen, wichtige rechtsetzende Bestimmungen enthalten oder wenn ihre Umsetzung den Erlass von Bundesgesetzen erfordert[239]. Die vorliegende Konvention wird auf unbestimmte Zeit abgeschlossen, kann aber jederzeit gekündigt werden und sieht keinen Beitritt zu einer internationalen Organisation vor. Jedoch bedingt der Beitritt zum Übereinkommen Anpassungen des Strafgesetzbuches sowie des Rechtshilfegesetzes. Der Genehmigungsbeschluss wird deshalb dem fakultativen Staatsvertragsreferendum gemäss Artikel 141 Absatz 1 Buchstabe d Ziffer 3 BV zu unterstellen sein.

Die Gesetzesentwürfe stützen sich auf Artikel 54 Absatz 1 sowie 123 Absatz 1 BV.

238 SR **101**.
239 Art. 141 Abs. 1 Bst. d BV.

Anhang

Bundesbeschluss über die Genehmigung und die Umsetzung der Europaratskonvention über die Cyberkriminalität (Vorentwurf)