Kinderpornographie im Internet

Internationale Fachtagung, Balsthal 13./14. Juni 2002

Workshop 2

Anpassungsbedarf des kantonalen Strafprozessrechts an die Cybercrime Convention

Prof. Dr. Christian Schwarzenegger[1]

Einleitung

Seit einer Empfehlung des Ministerrats[2] vom 13. September 1989, die den Mitgliedsstaaten Leitlinien betreffend die Definition bestimmter Computerstraftaten vorlegte, ergriff der Europarat mehrfach die Initiativen zur Harmonisierung der strafrechtlichen Rahmenbedingungen im Bereiche der Informationstechnologie[3]. Gestützt auf diese Empfehlungen und weitere Untersuchungen kam der Lenkungsausschuss für Strafrechtsfragen des Europarates (CDPC) zum Schluss, das einzig wirksame Instrument zur Bekämpfung der Internet- und sonstigen Datennetzkriminalität sei ein verbindliches internationales Regelwerk. Ende 1996 rief er deshalb ein Komitee von Experten auf dem Gebiete der Datennetzkriminalität (PC-CY) ins Leben und betraute es mit der Ausarbeitung einer Konvention, welche Fragen des materiellen Rechts, der strafprozessualen Zwangsmassnahmen im Bereiche der Telekommunikation und Teledienste, der Tatortsbestimmung bzw. des Strafanwendungsrechts und der Rechtshilfe bei der Ermittlung von Datennetzkriminalität regeln sollte. Das Komitee nahm seine Arbeit im April 1997 auf und legte dem Lenkungsausschuss für Strafrechtsfragen im Juni 2001 die revidierte und endgültige Fassung des Übereinkommensentwurfs sowie einen erläuternden Bericht vor[4]. Um eine möglichst weitgehen-

---

1 Rechtswissenschaftliches Institut, Universität Zürich, Wilfriedstrasse 6, 8032 Zürich. Weitere Informationen unter: www.rwi.unizh.ch/schwarzenegger

2 Recommendation No. R (89) 9 on computer-related crime, CoE Recommendations können auf folgender Webseite abgerufen werden: http://cm.coe.int (Stand: 29.1.2002).

3 Hinzuweisen ist vor allem auf die Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services und die Recommendation No. R (95) 13 concerning problems of criminal procedure law connected with information technology.

4 Die Convention on Cybercrime (ETS no. 185), der Explanatory Report und weitere Dokumente sind abrufbar unter: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185 (Stand: 27.2.2002).

de internationale Harmonisierung zu erzielen, wurden Sachverständige von Nicht-Europaratsmitgliedern wie den USA, Kanada und Japan in die Vorbereitungsarbeiten miteinbezogen. Nach einigen geringfügigen Änderungen durch den Lenkungsausschuss für Strafrechtsfragen wurde das Übereinkommen schliesslich am 8. November 2001 vom Ministerkomitee des Europarates angenommen und am 23. November 2001 in Budapest anlässlich der Internationalen Konferenz über Datennetzkriminalität zur Unterzeichnung aufgelegt. Neben der Schweiz haben bis dato 28 Mitgliedsstaaten des Europarats sowie die USA, Kanada, Japan und Südafrika die Convention on Cybercrime (CCC) unterzeichnet. Eine Unterzeichnung und spätere Ratifikation steht neben den Mitgliedsstaaten des Europarates auch Nichtmitgliedsstaaten offen, die an der Ausarbeitung des Übereinkommens mitgewirkt haben (Art. 36 Abs. 1 CCC). In den Unterzeichnerstaaten sind derzeit gesetzgeberische Vorbereitungen zur Ratifikation im Gange.

Die Regelungsmaterie der Convention on Cybercrime

Das Übereinkommen verfolgt erstens das Ziel, eine Harmonisierung der materiellen Strafbestimmungen auf dem Gebiete der Computer- und Datennetzkriminalität herbeizuführen[5]. Zweitens schafft es ein einheitliches strafprozessuales Instrumentarium zur Ermittlung und Verfolgung von Computer- und Datennetzdelikten. Insbesondere soll damit die rechtzeitige Sicherung von „flüchtigen" Beweismitteln und Verbindungsdaten in elektronischer Form ermöglicht bzw. erleichtert werden[6]. Ergänzend enthält Art. 22 CCC eine Regelung über den räumlichen Geltungsbereich, wobei diese aber nicht zu einer Beseitigung kollidierender staatlicher Strafhoheiten dient, sondern im Gegenteil sicherstellen will, dass immer eine Vertragspartei für die Verfolgung

---

[5] Neben verschiedenen Begriffsbestimmungen in Kapitel I (Art. 1 CCC) definiert das Übereinkommen in Kapitel II Abschnitt 1 folgende Straftatbestände: Unrechtmässiger Zugriff (Art. 2 CCC), Eingriff in die Datenintegrität (Art. 4 CCC), Eingriff in die Systemintegrität (Art. 5 CCC), Missbrauch von Vorrichtungen (Art. 6 CCC), Computerurkundenfälschung (Art. 7 CCC), Computerbetrug (Art. 8 CCC), Straftaten in Bezug auf Kinderpornographie (Art. 9 CCC) und Straftaten in Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (Art. 10 CCC). Ausserdem enthält dieserAbschnitt eine Bestimmung über die Verantwortlichkeit juristischer Personen (Art. 12 CCC). Ein 1. Zusatzprotokoll zur Harmonisierung der materiellen Strafnormen im Bereich der Rassendiskriminierung und Fremdenfeindlichkeit ist derzeit in Vorbereitung.

[6] Kapitel II Abschnitt 2. Von besonderer Bedeutung ist der erweiterte Geltungsbereich dieser Normen. Sie sind nicht nur auf Straftaten gemäss den Art. 2–11 CCC anwendbar, sondern vielmehr auf alle mittels Computersystemen begangenen Straftaten und alle Massnahmen zur Sicherung elektronischer Beweismittel (Art. 14 Abs. 2 lit. b und c CCC)! Es ist bisher völlig unklar, ob die Kantone entsprechende Anpassungen in ihren StPO vornehmen oder diese erst im Rahmen der Ausarbeitung einer Eidgenössischen StPO erfolgen werden. Gemäss Art. 3 Abs. 2 lit. a des am 1.1.2002 in Kraft getretenen Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF, SR 780.1) ist beispielsweise die Überwachung der Internetkommunikation einschliesslich der Rand- bzw. Verbindungsdaten eines vermeintlichen Hackers (Art. 143bis StGB) oder einer Person, die Com-

der Konventionsstrafbestimmungen zuständig ist[7]. Drittens versucht das Übereinkommen ein schnelleres und effizienteres Rechtshilfe- und Auslieferungssystems bei herkömmlichen und computerbezogenen Delikten zu etablieren, das bestehende Rechtshilfeübereinkommen oder bilateralen Verträge ergänzt oder in die Lücke springt, wo solche nicht existieren[8]. Vorgesehen sind auch provisorische Massnahmen wie die beschleunigte Sicherung gespeicherter Computerdaten (Art. 29 CCC) oder die beschleunigte Weitergabe gesicherter Verbindungsdaten (Art. 30 CCC). Im abschliessenden Kapitel IV, das die üblichen Standardvertragsklauseln für im Rahmen des Europarates geschlossene Übereinkünfte enthält[9], ist in Art. 41 CCC eine für die Schweiz bedeutungsvolle „Bundesstaatsklausel" eingefügt. Danach können Bundesstaaten den Vorbehalt anbringen, die Verpflichtungen nach Kapitel II nur soweit zu übernehmen, wie sie mit den Grundprinzipien der innerstaatlichen Kompentenzausscheidung zwischen Bund und Gliedstaaten vereinbar ist. Bringt ein Bundesstaat einen solchen Vorbehalt an, muss er gleichwohl eine umfassende und wirksame Strafverfolgung nach den Grundsätzen des II. Kapitels garantieren. Da der Vorbehalt nicht auf Kapitel III ausgeweitet werden kann, sind auch alle Verpflichtungen zur grenzüberschreitenden Zusammenarbeit einzuhalten[10].

Mögliche Diskussionspunkte und Fragen des Workshops

1. Beschleunigte Sicherung gespeicherter Computerdaten (Art. 16 CCC) und beschleunigte Sicherung und Teilweitergabe von Verbindungsdaten (Art. 17 CCC)

Ist es möglich, gegenüber einer Person, die bestimmte Computerdaten besitzt (bzw. daran berechtigt ist), anzuordnen, dass sie diese Daten speichern muss?

Ist es möglich, eine Person, die bestimmte Computerdaten besitzt (bzw. daran berechtigt ist), zum Schweigen über Untersuchungshandlungen zu verpflichten?

2. Herausgabeanordnung (Art. 18 CCC)

Wie wird im Stadium der Untersuchung die Herausgabe von spezifischen Computerdaten angeordnet?

---

puterviren zugänglich macht (Art. 144bis Ziff. 2 Abs. 1 StGB), grundsätzlich nicht möglich. Vgl. dagegen die sich aus Art. 17 und 20 CCC ergebenden Pflichten der Vertragsparteien.

7 Dazu eingehend CHRISTIAN SCHWARZENEGGER, Der räumliche Geltungsbereich des Strafrechts im Internet. Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 118 (2000) 117 ff.

8 Kapitel III.

9 Z.B. über die Bedingungen des Inkraftretens (Art. 36 CCC), des Beitritts (Art. 37 CCC) usw.

10 Ausführlicher Explanatory Report (FN4) N 315 ff.

Welche Massnahmen bestehen, um die Durchsetzung dieser Verpflichtung zu sichern? Gibt es irgendwelche Sanktionen im Falle der Zuwiderhandlung gegen die Anordnung?

Ist es möglich, die Person, welche zur Herausgabe der Daten verpflichtet wurde, zum Schweigen zu verpflichten?

Ist es möglich, einen Internet Service Provider zur Herausgabe von Kundeninformationen zu verpflichten? Wie geschieht das?

3. Durchsuchung und Beschlagnahme gespeicherter Computerdaten (Art. 19 CCC)

Gibt es im kantonalen Strafprozessrecht eine Zwangsmassnahme, um die Herausgabe alleine von Computerdaten, ohne das physische Medium, auf welchem die Daten gespeichert sind, anzuordnen?

Kann die Strafverfolgungsbehörde die Daten, nachdem sie herausgegeben wurden, löschen oder – falls sie diese nicht löschen will – unzugänglich machen? Falls das Unzugänglichmachen möglich ist, welche spezifischen Massnahmen stehen zur Verfügung?

Sieht das kantonale Strafprozessrecht eine spezielle Authentifikation oder andere Massnahme vor, um die Echtheit der als Beweismittel herausverlangten Daten zu erhalten und sichern?

4. Verpflichtung der Person, gegen die eine Zwangsmassnahme angeordnet wird, mit der Untersuchungsbehörde zu kooperieren

Ist es im Moment der Vollstreckung von Zwangsmassnahmen, die auf ein Speichermedium oder gespeicherte Daten abzielen, möglich, dass die Untersuchungsbehörde eine Person, die von den Zwangsmassnahmen betroffen ist, verpflichtet, Daten auf dem Computersystem zu lokalisieren oder verschlüsselte Daten zu dekodieren?

Falls ja, gibt es eine Beschränkung hinsichtlich des Personenkreises, der dazu verpflichtet werden kann?

5. Erhebung von Verbindungsdaten (Art. 20 CCC)

Nach welchen Regeln richten sich Nicht-Echtzeit-Erhebungen von Verbindungsdaten?

Sind Zwangsmassnahmen zum Zwecke der Echtzeit-Erhebung von Verbindungsdaten zulässig?

6. Überwachung von Inhaltsdaten (Art. 21 CCC)

Unter welchen Voraussetzungen ist die Überwachung von Inhaltsdaten zulässig? Bei welchen Computer- und Internetdelikten ist eine Überwachung möglich?

Ist es möglich, einen Service Provider zu verpflichten, bei der Überwachung zu kooperieren?

Ist es möglich, den Service Provider zu verpflichten, die Überwachung geheimzuhalten?

7. Aufbewahrung (Speicherung) von Verbindungsdaten

Sind Service Provider verpflichtet, die Verbindungsdaten ohne Bezug zu einem spezifischen Straffall für eine bestimmte Zeit aufzubewahren (zu speichern)?

8. Fern- oder Remote-Zugriff (einschliesslich Online-Durchsuchung, Art. 19 Abs. 2 CCC)

Wie kann die Untersuchungsbehörde Daten erlangen, falls sich während der Durchführung einer Zwangsmassnahme, die auf einen bestimmten Computer gerichtet ist, um bestimmte Computerdaten zu erlangen, herausstellt, dass die Daten auf einem anderen Computer abgespeichert sind, der mit dem durchsuchten Computer durch eine Netzwerk verbunden ist?

9. Grenzüberschreitende Durchsuchung (Art. 32 CCC)

Ist es möglich, dass die Untersuchungsbehörde durch den Zugriff auf einen Computer, der im Ausland steht, Daten erlangen, die dort abgespeichert sind?

AUSZUG AUS DER CONVENTION ON CYBERCRIME IN DEUTSCHER ÜBERSETZUNG (ART. 14–21)[11]

Abschnitt 2 – Verfahrensrecht

Titel 1 – Allgemeine Bestimmungen

Artikel 14 – Geltungsbereich verfahrensrechtlicher Bestimmungen

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

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

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

b) andere mittels eines Computersystems begangene Straftaten und

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

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

b) Kann eine Vertragspartei aufgrund von Beschränkungen in ihren Rechtsvorschriften, die im Zeitpunkt der Annahme dieses Übereinkommens in Kraft sind, die in den Artikeln 20 und 21 bezeichneten Maßnahmen nicht auf Kommunikationen anwenden, die innerhalb eines Computersystems eines Dienstanbieters übertragen werden, das

i) für eine geschlossene Nutzergruppe betrieben wird und

ii) sich keiner öffentlichen Kommunikationsnetze bedient und nicht mit einem anderen öffentlichen oder privaten Computersystem verbunden ist,

so kann diese Vertragspartei sich das Recht vorbehalten, diese Maßnahmen auf solche Kommunikationen nicht anzuwenden. Jede Vertragspartei prüft die Möglichkeit, einen solchen Vorbehalt zu beschränken, damit die in Artikel 20 und 21 bezeichneten Maßnahmen im weitesten Umfang angewendet werden kann.

Artikel 15 – Bedingungen und Garantien

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

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

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

Titel 2 – Beschleunigte Sicherung gespeicherter Computerdaten

Artikel 16 – Beschleunigte Sicherung gespeicherter Computerdaten

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

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

---

[11] Arbeitsübersetzung aus dem Englischen, Bundesministeriums der Justiz, Berlin.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den Verwahrer oder eine andere Person, welche die Computerdaten zu sichern hat, zu verpflichten, die Durchführung dieser Verfahren für den nach ihrem innerstaatlichem Recht vorgesehenen Zeitraum vertraulich zu behandeln.
(4) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Artikel 17 – Beschleunigte Sicherung und Teilweitergabe von Verbindungsdaten
(1) Jede Vertragspartei trifft in Bezug auf Verbindungsdaten, die nach Artikel 16 zu sichern sind, alle erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen,
a) dass diese beschleunigte Sicherung von Verbindungsdaten unabhängig davon zu möglich ist, ob ein oder mehrere Dienstanbieter an der Übertragung dieser Kommunikation mitgewirkt haben;
b) dass Verbindungsdaten in so ausreichender Menge beschleunigt an die zuständige Behörde der Vertragspartei oder an eine von dieser Behörde bezeichnete Person weitergegeben werden, dass die Vertragspartei die Dienstanbieter und den Weg feststellen kann, auf dem die Kommunikation übertragen wurde.
(2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Titel 3 – Herausgabeanordnung

Artikel 18 – Herausgabeanordnung
(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, anzuordnen,
a) dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder ihrer Verfügungsgewalt befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und
b) dass ein Dienstanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Kundendaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder seiner Verfügungsgewalt befinden, vorzulegen hat.
(2) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.
(3) Im Sinne dieses Artikels bedeutet der Ausdruck „Kundendaten“ alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Dienstanbieter über Kunden seiner Dienste vorliegen, mit Ausnahme von Verbindungsdaten oder inhaltsbezogenen Daten, und durch die folgendes festgestellt werden kann:
a) die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dienstdauer;
b) die Identität des Kunden, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen.
c) gegebenenfalls andere Informationen über den Ort der Installation der Kommunikationsanlage, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen.

Titel 4 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten

Artikel 19 – Durchsuchung und Beschlagnahme gespeicherter Computerdaten
(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen,
a) ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und
b) einen Computerdatenträger, auf dem Computerdaten gespeichert sein können,
in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen.
(2) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon in ihrem Hoheitsgebiet gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.
(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, Computerdaten, auf die nach Absatz 1 oder 2 Zugriff genommen wurde, zu beschlagnahmen oder in ähnlicher Weise sicherzustellen. Diese Maßnahmen umfassen die Befugnis,
a) ein Computersystem oder einen Teil davon oder einen Computerdatenträger zu beschlagnahmen oder in ähnlicher Weise sicherzustellen,
b) eine Kopie dieser Computerdaten anzufertigen und zurückzubehalten,
c) die Integrität der einschlägigen gespeicherten Computerdaten zu erhalten,
d) diese Computerdaten in dem Computersystem, auf das Zugriff genommen wurde, unzugänglich zu machen oder sie daraus zu entfernen.
(4) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen, anzuordnen, dass jede Person, die Kenntnisse über die Funktionsweise des Computersystems oder Maßnahmen zum Schutz der darin enthaltenen Daten hat, in vernünftigem Maß die notwendigen Auskünfte zu erteilen hat, um die Durchführung der in den Absätzen 1 und 2 genannten Maßnahmen zu ermöglichen.
(5) Die Befugnisse und Verfahren nach diesem Artikel unterliegen den Artikeln 14 und 15.

Titel 5 – Echtzeit-Erhebung von Computerdaten

Artikel 20 – Echtzeit-Erhebung von Verbindungsdaten

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

a) Verbindungsdaten, die mit bestimmten in ihrem Hoheitsgebiet mittels eines Computersystems übertragenen Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und

b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,

i) solche Verbindungsdaten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder

ii) bei der Erhebung oder Aufzeichnung solcher Verbindungsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

(2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht ergreifen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass Verbindungsdaten, die mit bestimmten in ihrem Hoheitsgebiet übertragenen Kommunikationen in Zusammenhang stehen, durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Dienstanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

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

Artikel 21 – Abfangen von Inhaltsdaten

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden in Bezug auf eine Reihe schwerer Straftaten, die nach ihrem innerstaatlichen Recht zu bestimmen sind, die Befugnis zu erteilen,

a) inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mit einem Computersystem übertragen wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und

b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,

i) solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder

ii) bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

(2) Kann eine Vertragspartei die in Absatz 1 Buchstabe a bezeichneten Maßnahmen aufgrund der in ihrer innerstaatlichen Rechtsordnung festgelegten Grundsätze nicht ergreifen, so kann sie stattdessen die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um sicherzustellen, dass inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet durch Anwendung technischer Mittel in diesem Hoheitsgebiet in Echtzeit erhoben oder aufgezeichnet werden.

(3) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um einen Dienstanbieter zu verpflichten, die Tatsache, dass eine nach diesem Artikel vorgesehene Befugnis ausgeübt wird, sowie alle Informationen darüber vertraulich zu behandeln.

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