DuD
Datenschutz und Datensicherheit

Die Cyber-Crime-Konvention des Europarats

Patrick Breyer

Die Cyber-Crime-Konvention (CCC) ist nach Fahrplan Mitte September im Ministerkomitee des Europarates verabschiedet worden. Für Ende November ist die Unterzeichnung des Dokuments geplant, an die sich die Ratifizierung durch die nationalen Parlamente anschließen wird. Insbesondere der letzte Schritt lässt eine weitere kritische Debatte der Cyber-Crime-Konvention erwarten, wie ein Expertengespräch am 5. Juli 2001 vor dem Unterausschuss Neue Medien des Deutschen Bundestages gezeigt hat. Patrick Breyer setzt sich mit der Konvention kritisch auseinander.

Patrick Breyer,

Stud. jur. Universität Frankfurt am Main.

Email: P.Breyer@breyers.de

1 Gegenstand des Vertragsentwurfs

Ziel der geplanten Cyber-Crime-Konvention des Europarats (im folgenden CCC)[1], die nunmehr in der „endgültigen“ 28. Entwurfsfassung vom 29. Juni 2001[2] vorliegt, ist die Effektivierung der Strafverfolgung im Computerbereich.[3] Sie bezweckt den Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit von Computersystemen, Netzwerken und Computerdaten, aber auch den Schutz anderer Güter, soweit diese mittels solcher Einrichtungen beeinträchtigt zu werden drohen (vgl. Präambel).

Zu diesem Zweck verpflichten sich die Vertragsstaaten, bestimmte Handlungen unter Strafe zu stellen (Kapitel II Abschnitt 1) und die Ermittlungsbehörden mit Kompetenzen zur effektiven Verfolgung der Straftaten auszustatten (Kapitel II Abschnitt 2). Schließlich sind auch Pflichten zur internationalen Kooperation in Strafsachen vorgesehen, soweit ein Bezug zur Computertechnologie gegeben ist (Kapitel III).

Regelungsgegenstand der CCC ist nicht nur die Computerkriminalität. Vielmehr verpflichtet etwa Art. 23 die Staaten zur internationalen Zusammenarbeit „*in größtmöglichem Umfang und zum Zwecke von Ermittlungen oder Verfahren in Bezug auf Straftaten, welche mit Computersystemen und -daten zusammen hängen, oder zur Sammlung von Beweisen in elektronischer Form für eine Straftat*“. In der letzten Alternative ist also jede Straftat erfasst, sei sie computerbezogen oder auch nicht. Ähnlich verhält es sich mit den Vorschriften über innerstaatliche Ermittlungsbefugnisse (Art. 14 ff.).

In den Schlussbestimmungen des Entwurfs schließlich ist unter anderem vorgesehen, dass auch Staaten, die nicht Mitglied des Europarats sind, dem Vertrag beitreten können. Die Vereinigten Staaten, Kanada, Japan und Südafrika waren und sind an seiner Ausarbeitung bereits aktiv beteiligt[4]; die Öffnung des Vertrags für weitere Staaten ist geplant[5].

2 Debatte der Überwachungsbefugnisse

Welche Argumente für die geplante Konvention vorgebracht werden, liegt auf der Hand: Die Effektuierung der Strafverfolgung im Computerbereich sei unbedingt erforderlich[6]; die bestehenden Möglichkeiten seien unzureichend. Die weitreichendste Verfolgung des Ziels der Kriminalitätsbekämpfung, nämlich die Totalüberwachung der Kommunikation der Bürger, würde jedoch einen unverhältnismäßigen Eingriff in deren allgemeines Persönlichkeitsrecht darstellen, wie das Bundesverfassungsgericht (BVerfG) festgestellt hat[7], so dass Strafverfolgungsinteressen nicht Grund-

[1] Internetadresse des Europarats: <http://www.coe.int>. Kontaktmöglichkeit für Eingaben bezüglich der Cyber-Crime-Konvention (CDPC): <dmitri.marchenkov@coe.int>,<sabine.zimmer@coe.int> oder allgemein <daj@coe.int>. Zuständiges Referat beim Bundesjustizministerium: Abteilung II A 4, Fax 030-20259525.

[2] <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>. Die jeweils aktuelle Fassung ist über <http://conventions.coe.int> abrufbar.

[3] Vgl. Präambel des Konventionsentwurfs. Zitierte Rechtsnormen sind, wenn nicht anders angegeben, solche des Entwurfs vom 29.06.2001.

[4] Krempl in: Fette Bugs im Cybercrime-Abkommen (28.03.2001), Telepolis (Heise Verlag), <http://www.heise.de/tp/deutsch/inhalt/te/7239/1.html>.

[5] Geiger, Vorlesung an der Universität Frankfurt am Main vom 26.06.2001.

[6] Vgl. Präambel des Konventionsentwurfs.

[7] Vgl. Stellungnahme der Datenschutzbeauftragten aller Bundesländer außer Thüringens zu Forderungen der Innenministerkonferenz vom 30.11.2000, DuD 2001, 50.

rechtseingriffe jeder Art legitimieren können.

Aber bereits bezüglich der Frage, wie geeignet Kommunikationsüberwachung zur Bekämpfung von Straftaten überhaupt ist, werden Zweifel geäußert. Der bildungs- und forschungspolitische Sprecher und Bundestagsabgeordnete der SPD Jörg Tauss etwa ist der Ansicht, dass durch die Eingriffsbefugnisse nach der CCC allenfalls die „Dümmsten der Kriminellen schlechte Karten“ hätten und dass ansonsten lediglich „Kleinkriminalität“ erreicht werden könnte.[8] Ein Umstand, der für andere die Unverhältnismäßigkeit der geplanten Überwachungsmaßnahmen begründet, da nur Nutzer abgehört werden könnten, die sich wegen ihrer technischen Unbedarftheit nicht dagegen wehren können.[9]

In der Tat ist unbestritten, dass heute Verschlüsselungsmechanismen frei verfügbar sind, die Kriminellen eine mit an Sicherheit grenzender Wahrscheinlichkeit abhörfreie Kommunikation ermöglichen.[10] Angesichts dieser Tatsache erscheint es zweifelhaft, ob das hohe Maß an Eingriffsbefugnissen in Fällen mit Computerberührung überhaupt angemessen ist.

Leider existieren keine seriösen Statistiken auf dem Gebiet der Computerkriminalität[11], so dass die Erforderlichkeit und Angemessenheit der geplanten Überwachungsmaßnahmen empirisch weder bestätigt noch abgelehnt werden kann. Die Steigerung in der Kriminalitätsstatistik[12] scheinen kein zuverlässiger Indikator für die tatsächliche Verbreitung solcher Verhaltensweisen zu sein. Die erhöhten Ziffern können etwa auf den inzwischen besseren Verfolgungsmöglichkeiten seitens der zuständigen Behörden beruhen, zum Beispiel wegen besserer Ausstattung mit technischen Mitteln oder wegen Schulungen des Personals. Umgekehrt ist aber auch nicht geplant, zuverlässige Erkenntnisse über Cybercrime zu gewinnen. Die CCC sieht keinen Evaluierungsmechanismus vor, der es erlauben würde, anhand von objektiven Daten einige Jahre nach dem Inkrafttreten des Abkommens die Effektivität der Eingriffsbefugnisse zu überprüfen.

Man kann daher davon ausgehen, dass die Befugnisse, die den Strafverfolgungsbehörden durch die CCC eingeräumt werden, auf lange Zeit erhalten bleiben werden. Zwar entscheidet jeder Staat theoretisch frei, ob er der geplanten CCC beitritt oder nicht. Auch sieht der Vertrag eine Austrittsmöglichkeit mit dreimonatiger Frist vor (Art. 47). Jedoch ist angesichts der gewichtigen Interessen, die hinter dem Abkommen stehen – Polizeibehörden, Geheimdienste, aber auch befreundete ausländische Staaten wie die USA – kaum anzunehmen, dass es einzelnen Staaten gelingen wird, sich dem Sog „der Masse“ von Unterzeichnerstaaten zu entziehen.

Immer wieder taucht auch das Argument auf, dass gegen eine staatliche Überwachung nur derjenige etwas einwenden könne, der selbst die Strafverfolgung zu befürchten habe, nach dem Motto: „Der redliche Bürger wehrt sich nicht“. Diese Argumentation hieße aber, die Gefahren und Nebeneffekte zu verkennen, die mit der staatlichen Kommunikationsüberwachung verbunden sind. Zunächst einmal haben die Praktiken einiger Staaten traurige Berühmtheit erlangt, Kommunikationsüberwachung zum Zwecke von Wirtschaftsspionage einzusetzen. In Großbritannien und den USA z.B. ist staatliche Wirtschaftsspionage im Ausland legal.[13] Auch zur Ausforschung wissenschaftlicher Forschungserkenntnisse könnten die Überwachungsbefugnisse eingesetzt werden.

Selbst wenn sich die Ermittlungen auf den weiteren Bereich der Strafverfolgung beschränkten, bleibt immer noch das Problem, welche Daten gespeichert werden dürfen. An sich sind alle personenbezogenen Daten geeignet, die Strafverfolgung in künftigen Verfahren zu erleichtern. Man muss die Grenze der Zulässigkeit daher bedeutend enger ziehen, um nicht in den in Deutschland verfassungswidrigen Bereich der Totalüberwachung zu geraten. Die CCC hingegen lädt zu unverhältnismäßig umfangreichen Datensammlungen geradezu ein, indem sie keinerlei Beschränkungen zum Zwecke des Datenschutzes vorsieht. Bezeichnenderweise findet sich das Wort „Datenschutz“ an keiner Stelle des Vertragstextes.

Zwar ist die Frage des Datenschutzes zumeist in den nationalen Rechtsordnungen aufgrund anderer internationaler Übereinkommen bereits geregelt. Dies gilt für die Mitgliedsstaaten der EU[14], die insbesondere aufgrund der EG-Datenschutzrichtlinie 95/46/EG[15] zur Gewährleistung eines angemessenen Datenschutzniveaus verpflichtet sind. Während einige der übrigen europäischen Staaten wenigstens das weniger strenge Europaratsabkommen 108/81 zum Datenschutz[16] umgesetzt haben, steht die Gewährleistung von Datenschutz in außereuropäischen Staaten nicht selten nur auf dem Papier. Zwar lässt nicht nur die CCC (Art. 37), sondern auch die Datenschutzkonvention (Art. 23) den Beitritt außereuropäischer Staaten zu. Aber nur die CCC lockt mit dem Recht, im Wege der Rechtshilfe Beweismittel aus anderen Unterzeichnerstaaten anfordern zu dürfen. Ähnliches hat die Datenschutzkonvention nicht zu bieten, so dass ihre Unterzeichnung für Staaten mit einem geringen oder keinem Datenschutzniveau wenig attraktiv ist, vor allem für ausgeprägt souveränitäts- und selbstbewusste Staaten wie die USA.

Nach alledem muss man sich ernsthaft fragen, ob angesichts der vielschichtigen Nachteile und Gefahren staatlicher Überwachung die in der CCC vorgesehenen Befugnisse noch angemessen sind.

3 Rechtsstaatliche Anforderungen

Aus rechtsstaatlicher Sicht, in Deutschland insbesondere aufgrund des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und des Fernmeldegeheimnisses (Art. 10 GG) auf Seiten der Betroffenen, der Berufs- und Eigentumsfreiheit (Art. 12, 14 Abs. 1 GG) auf Seiten der Wirtschaft sowie allgemein des Rechtsstaatsprinzips, wird man strenge Anforderungen an die Zulässigkeit von Grundrechtseingriffen stellen müssen.

[8] Zitiert bei Schulzki-Haddouti in: Ein großer Schritt in Richtung europäischer Überwachungsstaat (25.04.2001), Telepolis, <http://www.heise.de/tp/deutsch/inhalt/te/7472/1.html>.

[9] A. Pfitzmann von der TU Dresden, Stellungnahme vor dem Unterausschuss „Neue Medien“ des Deutschen Bundestages am 05.07.2001.

[10] Siehe Fußnote 9.

[11] Krempl in: Brüssel gibt Gas bei der Bekämpfung der Computerkriminalität (11.03.2001), Telepolis, <http://www.heise.de/tp/deutsch/inhalt/te/7108/1.html>.

[12] Vgl. Sicherheitsbericht der Bundesregierung 2001, S. 197 ff.

[13] Schulzki-Haddouti in: Widerstände gegen Cybercrime-Abkommen aus eigenen Reihen (09.11.2000), Telepolis <http://www.heise.de/tp/deutsch/inhalt/te/4228/1.html>.

[14] Kugelmann, Die „Cyber-Crime“ Konvention des Europarates, DuD 2001, 215 ff.; Krader, Kampf gegen Internetkriminalität, DuD 2001, 344 ff.

[15] <http://europa.eu.int/eur-lex/de/lif/dat/1995/de_395L0046.html>.

[16] <http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm>; im Folgenden kurz „Datenschutzkonvention“ genannt.

Die Maßnahmen müssen strikt den Verhältnismäßigkeitsgrundsatz wahren und dürfen nur bei Vorliegen eines Verdachts einer hinreichend schweren Straftat ergriffen werden. Fällt dieser Verdacht weg oder ist das Strafverfahren abgeschlossen, so dürfen die Daten allenfalls aufgrund besonderer Umstände gespeichert bleiben. Überhaupt dürfen nur solche Daten gespeichert werden, die für die jeweiligen Ermittlungen erforderlich sind, nicht etwa Informationen über Lebensweise, Religion, sexuelle Gewohnheiten oder Orientierung. Zu denken ist außerdem an eine Benachrichtigung des Betroffenen von der Datenspeicherung, soweit dies den Zweck der Speicherung nicht wesentlich erschwert.[17]

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation fordert, dass private Kommunikation nur unter den folgenden Voraussetzungen überwacht werden darf:[18] Vorherige richterliche Anordnung, nachträgliche Benachrichtigung der Betroffenen, Beschränkung der Nutzung, Verpflichtung zur Protokollierung der Maßnahmen, Überwachung und Kontrolle der Durchführung sowie öffentliche Rechenschaftspflicht der die Überwachung anordnenden Stellen.

Auch die Parlamentarische Versammlung des Europarats fordert die „*Sicherstellung unabhängiger und effektiver Kontrolle, die in jedem einzelnen Verfahrensstadium auf Tatsachenbefunden bezüglich der Straftat beruht. Die Person, in deren Privatsphäre eingegriffen werden soll, ist zu bezeichnen. Dabei ist gebührend zu berücksichtigen, dass die einzelnen Befugnisse und Verfahren nicht außer Verhältnis zur Schwere des Delikts nach seiner Art und seiner Begehung im Einzelfall stehen dürfen*“.[19]

Die „*unabhängige und effektive Kontrolle*“ sollte aus rechtstaatlichen Gesichtspunkten den allgemeinen Gerichten obliegen, nicht speziellen Gremien oder Ausschüssen, wie dies in sensiblen Bereiche (vgl. etwa Art. 10 GG) bisweilen vorgesehen ist. Nur so kann die Unabhängigkeit und Neutralität der Kontrolle gewährleistet werden. Die „*Kontrolle*“ muss die Eröffnung des Rechtsweges für Betroffene einschließen. Zudem ist auch eine flächenmäßige Erfassung der Praktiken der Strafverfolger zu wünschen, etwa durch ein Monitoring-Verfahren, in dem ein spezielles Gremium regelmäßig Berichte über die staatliche Überwachungstätigkeit der Öffentlichkeit vorstellt. Nur so kann effektiv sicher gestellt werden, dass die Überwachung von Kommunikationsinhalten eine deutliche Ausnahme gegenüber dem Grundsatz der Kommunikationsfreiheit bleibt. Unverhältnismäßig wäre es nämlich, generell alle Nutzer des Internet unter Kriminalitätsverdacht zu stellen.

4 Entstehung und Hintergründe

Der seit 1997 in Ausarbeitung befindliche Entwurfstext einer Cybercrime-Konvention wurde im Juni 2001 vom ständigen Ausschuss des Europarats für Strafsachen (CDPC) endgültig beschlossen[20] und dem Ministerrat zur möglichen Annahme im Herbst 2001 übergeben[21]. Das Verfahren, in dem die CCC ausgehandelt wurde und zustande kommen soll, wird oft kritisiert.[22].

Die Natur des Abkommens als völkerrechtlicher Vertrag ist in einer Demokratie dann bedenklich, wenn so weitreichende und kontroverse Eingriffsbefugnisse des Staates in die Rechte der Bürger vorgesehen sind, wie dies bei der CCC der Fall ist. Die Verhandlung völkerrechtlicher Verträge ist in parlamentarischen Systemen typischerweise der Exekutive vorbehalten. Wenn sich die Bürokraten dann hinter verschlossenen Türen treffen, ist die Öffentlichkeit und die Vertretung des Volkes, das Parlament, nicht beteiligt. Das Europäische Rechthilfeabkommen etwa wurde überhaupt erst veröffentlicht, nachdem es bereits unterzeichnet war.[23] Undemokratisch ist im Falle der CCC besonders, dass die mit der Ausarbeitung des Entwurfs betraute Spezialistengruppe „PC-CY“ nur von sehr eingeschränkter gesellschaftlicher Repräsentanz war: Weder Bürgerrechtsaktivisten noch Rechtsberater waren vertreten.[24] Überhaupt waren die Verhandlungen ganz deutlich von Staatsinteressen geprägt. Laut Jörg Tauss (MdB) haben vor allem die europäischen Polizeistäbe, etwa das deutsche Bundeskriminalamt, hinter den Kulissen und ohne jegliche öffentliche Debatte für das Abkommen „gekämpft“; die Entwürfe seien vor allem von den Polizeiabteilungen formuliert worden.[25]

Auch nach dem Bekanntwerden der Verhandlungen gelang es nur noch der Lobby der Internetwirtschaft, Nachbesserungen in ihrem Interesse durchzusetzen. Die einzige Gruppe, deren Interessen kaum zur Geltung gekommen sind, ist die der Bürger. Teilweise wird von Absprachen zwischen Strafverfolgern und der Industrie zu Lasten der Bürger gesprochen, was die inhaltliche Ausgestaltung des Abkommens erklären würde. Es drängt sich insgesamt der Eindruck auf, dass das Cybercrime-Abkommen jetzt von den beteiligten Regierungen mit allen Mitteln „durchgedrückt” werden soll. Die Strategie der an der Ausarbeitung Beteiligten scheint zu sein, so wenig wie möglich an die Öffentlichkeit dringen zu lassen und das Abkommen möglichst schnell „durchzupeitschen“, um

[17] Bäumler, Sichere Informationsgesellschaft, Bekämpfung der Computerkriminalität und Datenschutz, DuD 2001, 348 ff.

[18] Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation, Gemeinsamer Standpunkt zu Datenschutzaspekten des Entwurfs einer Konvention zur Datennetzkriminalität des Europarates vom 13./14.9.2000. Brandenburgischer Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht / Berliner Beauftragter für Datenschutz und Akteneinsicht (Hrsg.), Dokumente zum Datenschutz 2000, S. 69, <http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm>.

[19] Stellungnahme Nr. 226 (2001) zum Entwurf des Cybercrime-Abkommens (24.04.2001), Unterpunkt xv., <http://stars.coe.fr/ta/ta01/EOPI226.htm>.

[20] <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>.

[21] Vertragsbüro des Europarats, <http://conventions.coe.int/treaty/EN/cadreprojets.htm>.

[22] Vgl. etwa Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarats über Cyberkriminalität vom 22.03.2001, S. 10, <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp41de.pdf>, sowie Anmerkungen der American Civil Liberties Union, des Electronic Privacy Information Center und von Privacy International vom 07.06.2001 zur 27. Entwurfsfassung der Cybercrime Konvention, Unterpunkt A, <http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm>.

[23] Schulzki-Haddouti in: Bundesregierung nimmt Stellung zu Cybercrime-Abkommen (27.06.2000), Telepolis, <http://www.heise.de/tp/deutsch/inhalt/te/8290/1.html>.

[24] Campbell in: Schlacht um die Privatsphäre im Rampenlicht (03.10.2000), Telepolis, <http://www.heise.de/tp/deutsch/inhalt/konf/8846/1.html>. Ebenso Anmerkungen der American Civil Liberties Union, des Electronic Privacy Information Center und von Privacy International vom 07.06.2001 zur 27. Entwurfsfassung der Cybercrime Konvention, Unterpunkt A, <http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm>.

[25] Zitiert bei Schulzki-Haddouti in: Ein großer Schritt in Richtung europäischer Überwachungsstaat (25.04.2001), Telepolis, <http://www.heise.de/tp/deutsch/inhalt/te/7472/1 .html>.

es anschließend bald wieder in Vergessenheit geraten zu lassen.

In Deutschland hat das Bundesinnenministerium bereits seine Absicht angekündigt, die CCC in der hier diskutierten Fassung so bald wie möglich zu verabschieden.[26] Auch Hansjörg Geiger, Staatssekretär des Bundesjustizministeriums, sieht einen erheblichen Druck auf Deutschland, das Abkommen zu ratifizieren.[27] Dass das Abkommen nicht ratifiziert wird, hält er daher für ebenso unwahrscheinlich wie die Hoffnung, der Entwurf könne noch einmal in größerem Umfang überarbeitet werden. Als „wahrscheinlich" bezeichnet er das Szenario, dass Deutschland bis zum Abschluss der Vertragsverhandlungen im Herbst 2001 noch versuchen wird, Nachbesserungen kleineren Umfangs durchzusetzen, dass das Abkommen letztendlich – mit einschränkenden Vorbehalten und Erklärungen seitens Deutschlands – aber dann doch ratifiziert werden wird. Die Bundesrepublik müsse schon froh sein, ihren bisherigen Rechtschutzstandard auch der Konvention gemäß beibehalten zu dürfen.[28]

Angesichts der massiven Bedenken gegen den Vertragsentwurf fragt sich, welche inhaltlichen Bestimmungen denn nun im Einzelnen am problematischsten sind. Im Folgenden wird nur auf die zwei wichtigsten Problemfelder eingegangen[29]: Die Bestimmungen über innerstaatliche Ermittlungsbefugnisse (siehe unten 5) und über die internationale Zusammenarbeit (siehe unten 6).

5 Ermittlungsbefugnisse (Art. 14 bis 21)

Wie bereits beschrieben, werden im zweiten Abschnitt des zweiten Kapitels der Konvention einheitliche Ermittlungsbefugnisse der Strafverfolgungsbehörden vorgesehen. Diese Befugnisse bestehen nicht nur in Bezug auf die nach den Artikeln 2 bis 11 festgelegten Straftaten, sondern auch bezüglich anderer mittels eines Computersystems begangener Straftaten und der Erhebung von in elektronischer Form vorhandenen Beweisen für eine beliebige Straftat (Art. 14 Abs. 2). Dabei wird den Ermittlungsbehörden unter anderem die Befugnis eingeräumt, folgende Maßnahmen anzuordnen bzw. zu ergreifen: Die beschleunigte Sicherung gespeicherter Inhaltsdaten (Art. 16), die beschleunigte Sicherung und Übermittlung von Verbindungsdaten (Art. 17), die Übermittlung von Daten durch eine Privatperson, soweit diese über die Daten verfügen kann (Art. 18), die Herausgabe von Informationen über die Identität von Kunden durch einen Provider (Art. 18), die Durchsuchung und Beschlagnahme gespeicherter Daten (Art. 19), die Erhebung von Verbindungsdaten in Echtzeit (Art. 20) und das Abhören von Inhaltsdaten in Echtzeit (Art. 21). Da diese Vorschriften Befugnisse weitgehend nur einräumen, ohne sie zu begrenzen – eine der umstrittensten Normen ist Art. 19 Abs. 4, der grundsätzlich jedermann zur Mitwirkung bei der Beschlagnahme und Entschlüsselung von Daten verpflichtet, auch etwa zur Herausgabe von Verschlüsselungscodes –, stellt sich am dringlichsten die Frage, ob die Gewährleistung der in einem Rechtsstaat unabdingbaren Menschenrechte sicher gestellt ist.

5.1 Bedingungen und Garantien (Art. 15)

Die Frage nach der Gewährleistung von Menschenrechten zielt zunächst auf Art. 15, die einzige Bestimmung der CCC, die sich ausdrücklich mit dem Problem rechtstaatlicher Garantien befasst:

Art. 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. [...]

Art. 15 ist erst gegen Ende der Verhandlungen, nämlich erst im Mai 2001, in die CCC aufgenommen hat. Damit ist nun eindeutig festgelegt, dass die Eingriffsbefugnisse nach dem zweiten Abschnitt des zweiten Kapitels (Art. 14-21) nur im Rahmen grund- und menschenrechtlicher Gewährleistungen ermöglicht werden dürfen. Eine Korrektur, die ebenso zu begrüßen ist wie die Aufnahme zentraler rechtstaatlicher Grundsätze wie das Verhältnismäßigkeitsprinzip, die unabhängige Kontrolle und die Bestimmtheit der Eingriffsermächtigungen.

5.2 Kritik

Gleichwohl ist kritisch zu bewerten, dass nach Art. 15 die Gewährleistung einer unabhängigen Kontrolle und die Beschränkung der Eingriffsbefugnisse nur gelten sollen, soweit dies *„in Anbetracht der Natur der jeweiligen Befugnis oder des jeweiligen Verfahrens angemessen ist*" (Abs. 2). Damit werden eingriffsfreundliche Staaten praktisch von der Übernahme der verfahrensrechtlichen Sicherungen der Menschenrechte suspendiert. Es ist nicht ersichtlich, bei welcher der Maßnahmen nach den Art. 14-21 eine unabhängige Kontrolle oder Begrenzungen der Eingriffsermächtigung entbehrlich sein sollten. Jedenfalls müsste, wenn man die genannte Einschränkung nicht gänzlich streicht, genau festgelegt werden, bei welchem Artikel welche Einschränkung nicht vorgenommen werden muss. Den einzelnen Staaten darf dies nicht überlassen bleiben.

Das Verbot flächendeckender Überwachung vermag man allenfalls im Verhältnismäßigkeitsgrundsatz zu entdecken. Jedoch fehlt eine Konkretisierung des Verhältnismäßigkeitsgrundsatzes insbesondere in Hinblick auf die Frage, bei welchen Straftaten welche Maßnahmen ergriffen werden dürfen. Ein Kontroll- und Berichtsverfahren zur Untersuchung der Auswirkungen des Abkommens fehlt ebenfalls.

Angesichts der weitreichenden Pflichten von Privatpersonen zur Mitwirkung an Ermittlungen (vgl. Art. 19 Abs. 4, 20, 21) muss nach Art. 6 EMRK ferner vorgesehen

[26] Hottelet in: Cybercrime-Konvention unter Beschuss (06.07.2001), FAZ.NET, http://www.faz.net.

[27] Vorlesung an der Universität Frankfurt am Main vom 26.06.2001.

[28] Siehe Fußnote 27.

[29] Ausführliche Analyse unter <http://internet.breyers.de>

werden, dass sich niemand selbst belasten muss. Auch die gebotenen Aussage- und Zeugnisverweigerungsrechte (vgl. der Sache nach etwa §§ 136 Abs. 1 S. 2, 243 Abs. 4 StPO) sind in der CCC mit keinem Wort erwähnt. Man stelle sich vor, die Staatsanwaltschaft würde von einem Arzt verlangen, die auf seinem Computer gespeicherten Patientendaten heraus zu geben. Für einen solchen Fall ließen sich verfahrensrechtliche Beschränkungen allenfalls aus der unbestimmten Generalklausel herleiten. Auch wird die Eröffnung des Rechtswegs dem Betroffenen durch Art. 15 nicht garantiert, ebenso wenig wie die Verwertung rechtswidrig erlangter Informationen verboten wird.

Die Parlamentarische Versammlung des Europarats hat wegen dieser Unzulänglichkeiten verlangt, Art. 15 durch eine Vorschrift zu ersetzen, die einen adäquaten Schutz der Menschenrechte nach der Europäischen Menschenrechtskonvention gewährleisten würde.[30] Gefordert wurde außerdem die „*Sicherstellung unabhängiger und effektiver Kontrolle, die in jedem einzelnen Verfahrensstadium auf Tatsachenbefunden bezüglich der Straftat beruht. Die Person, in deren Privatsphäre eingegriffen werden soll, ist zu bezeichnen. Dabei ist gebührend zu berücksichtigen, dass die einzelnen Befugnisse und Verfahren nicht außer Verhältnis zur Schwere des Delikts nach seiner Art und seiner Begehung im Einzelfall stehen dürfen.*“

Vergleicht man Art. 15 mit dem Vorschlag der Parlamentarischen Versammlung, dann fehlt eine Regelung, wonach die unabhängige Kontrolle der Eingriffsmaßnahmen effektiv sein muss. In den Bestimmungen der CCC fehlt ferner eine Bestimmung, wonach die Kontrolle auf Tatsachenbefunden zu beruhen hat und die Person, in deren Rechte eingegriffen wird, zu bezeichnen ist. Dass diese Ausprägungen zentraler rechtstaatlicher Anforderungen in die Konvention nicht aufgenommen wurden, ist ein elementares Versäumnis. Es mag zwar sein, dass – wie die amtliche Begründung andeutet – die erforderlichen Ergänzungen nicht bei allen Vertragsstaaten durchsetzbar waren. Dies ändert jedoch nichts an ihrer Erforderlichkeit.

> Insgesamt gesehen ist es nicht angemessen, dass die Konvention Eingriffsbefugnisse einseitig zu Lasten der Bürger nur einräumt, es dann aber den einzelnen Staaten überlässt, ob und inwieweit sie rechtsstaatliche Sicherungen vorsehen. Eine derartige Vorgehensweise ist unausgewogen und begünstigt die Einräumung unangemessener Eingriffsbefugnisse, insbesondere in Staaten ohne rechtsstaatliche Tradition nach europäischem Verständnis.

5.3 Außereuropäische Vertragsstaaten

Auffällig ist, dass Art. 15 nur die Staaten, die bereits Vertragspartei der EMRK sind, zur Beachtung derer Menschenrechtsstandards verpflichtet. Dabei wäre es gerade am wichtigsten, auch die Staaten, die nicht dem Europarat angehören, zur Einhaltung vergleichbarer Menschenrechtsstandards zu verpflichten.

Die in den Art. 14 ff. vorgesehenen Ermittlungsbefugnisse erlauben Eingriffe in weltweit gewährleistete Menschenrechte. Nicht erst die Art. 7 und 8 der rechtlich unverbindlichen Europäischen Grundrechtscharta schützen das Recht auf Achtung des Privat- und Familienlebens und der Kommunikation. Bereits der Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte von 1966[31] garantiert den Schutz jedes Menschen vor „*willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben [...] und seinen Schriftverkehr [...].*“ Eine erheblich substanziellere Klausel findet sich in Art. 8 der Europäischen Menschenrechtskonvention (EMRK), wobei diese Konvention vor allem den nicht groß genug einzuschätzenden Vorteil hat, dass ihre Bestimmungen durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EuGMR) konkretisiert und durchgesetzt werden (Art. 19 ff. EMRK).

Nach dessen Rechtsprechung zu Art. 8 EMRK müssen Eingriffe auf gesetzlich bestimmten Tatbeständen beruhen. Effektive gerichtliche Kontrolle und der Rechtsweg müssen gewährleistet sein. Der Verhältnismäßigkeitsgrundsatz gilt umfassend, jede Maßnahme muss in jedem einzelnen Fall erforderlich und angemessen sein und darf nicht ganz außer Verhältnis zu ihrem Zweck stehen. Ein vergleichbarer Schutz ist weltweit nicht gewährleistet. Die im Pakt von 1966 enthaltene Bestimmung zum Schutz der Privatsphäre ist bereits vom Wortlaut her sehr eng und schützt nur vor „*willkürlichen oder rechtswidrigen*“ Eingriffen. Vor allem aber gibt es kein Gericht zur Konkretisierung und Durchsetzung der Klausel. Zwar erlaubt es ein Zusatzprotokoll, ein Kontrollverfahren einzurichten, das auch von Einzelpersonen in Gang gesetzt werden kann.[32] Jedoch haben sich nur wenige außereuropäische Staaten diesem weniger verbindlichen und effektiven Verfahren unterworfen.

Um diese Defizite auszugleichen, müsste man die verfahrensrechtlichen Sicherungen nach der EMRK und der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in die CCC selbst aufzunehmen, um einen universellen Schutzstandard zu gewährleisten. Die Wirksamkeit dieser Schutzbestimmungen muss durchgesetzt werden, indem den Betroffenen durch die CCC selbst der Rechtsweg gegen eingreifende Maßnahmen garantiert wird.

Besonders problematisch ist das Fehlen von Menschenrechtsgewährleistungen angesichts der Tatsache, dass die CCC prinzipiell auch Drittstaaten zur Unterzeichnung offen steht (Art. 37). Wenn solche Staaten keine ausreichenden rechtstaatlichen Sicherungen vorsehen, sind ihre Bürger ebenso wie Europäer, die sich in diesem Land aufhalten oder deren Daten sich dort befinden, unangemessenen Ermittlungsbefugnissen ausgesetzt. Hiergegen lässt sich zwar einwenden, dass diese Drittstaaten ihren Behörden auch ohne die CCC unangemessene Ermittlungsbefugnisse einräumen könnten. Jedoch bliebe dabei außer Acht, dass die Konvention die Einräumung unangemessen weiter Ermittlungsbefugnisse durch ihre Formulierungen geradezu begünstigt[33], und zwar auch in Staaten, in denen solche Befugnisse bislang nicht existierten. Insofern übt auch die CCC eine für internationale Abkommen typische Sogwirkung aus.

Im übrigen sind die europäischen Staaten nicht nur verpflichtet, die Menschenrechte ihrer eigenen Bevölkerung zu wahren, sondern nach dem Charakter der Menschenrechte als universelle Rechte die der Menschen überall. Es wäre daher angemessen, im Gegenzug zur Einräumung weitreichender Ansprüche auf internationale Rechtshilfe (Art. 23 ff.) allen Vertragsparteien die adäquate Gewährleistung von Menschen– und Bürgerrechten vorzuschreiben. Gerade außereuropäische Staaten, die

[30] Stellungnahme Nr. 226 (2001). Unterpunkt xv (Fußn. 19).

[31] BGBl. 1973 II, S. 1534.

[32] Fakultativprotokoll vom 19.12.1966, BGBl. 1992 II S. 1247.

[33] Bäumler (Fn. 17), DuD 2001, 348.

von dem Anspruch auf Rechtshilfe durch andere Vertragsstaaten profitieren wollen, müssen im Gegenzug strenge Beschränkungen der Eingriffsbefugnisse auch für sich akzeptieren. Sollte dazu keine Bereitschaft bestehen, dann sollten diese Drittstaaten von einer weiteren Beteiligung an der Ausarbeitung der Konvention absehen.

Gegebenenfalls müssen die Verhandlungen, anders als gegenwärtig, auf den Kreis der Europaratsmitglieder beschränkt werden, denen das Vorsehen von Menschenrechtssicherungen erheblich leichter fallen dürfte. Drittstaaten dürfte dann erst im Anschluss an den Verhandlungsprozess der Beitritt zur Konvention ermöglicht werden, um deren negativen Einfluss auf die Ergebnisse der Verhandlungen auszuschalten. Inoffiziell ist etwa zu hören, dass die USA die Aufnahme von Datenschutzbestimmungen in das dritte Kapitel der CCC mit der Drohung verhindert haben, den Verhandlungstisch sonst zu verlassen. Wenn aber nicht einmal sicher ist, ob die außereuropäischen Staaten, insbesondere die USA, die CCC überhaupt ratifizieren werden[34], dann ist nicht einzusehen, warum sie einen derart großen Einfluss auf die Formulierung des Vertragstextes haben sollten wie gegenwärtig. Auf sie sollte bei den Verhandlungen im Rahmen des Europarats keine Rücksicht genommen werden.

5.4 Datenschutz

Was nun speziell den Datenschutz anbelangt, der als Menschenrecht noch keine allgemeine Anerkennung gefunden hat, so vermisst man jegliche Regelung in der CCC. Die Beteiligten mögen dabei zwar die bereits existierende Datenschutzkonvention des Europarats[35] im Hinterkopf gehabt haben (vgl. Präambel). Diese Konvention gilt aber gerade nicht für alle potentiellen – insbesondere nicht für die außereuropäischen – Vertragsstaaten.

Man stelle sich vor, dass in Drittstaaten nicht einmal die grundlegenden Datenschutzgrundsätze gewährleistet sein müssen, wenn diese Staaten die Ergebnisse einer Kommunikationsüberwachung speichern oder sonst Daten verarbeiten. Zwar kann sowohl nach Art. 9 der Datenschutzkonvention wie auch nach Art. 13 der Datenschutzrichtlinie der EG von den Datenschutzbestimmungen abgewichen werden, soweit dies u.a. zur Strafverfolgung erforderlich ist.

Ein gänzliches Fehlen solcher Bestimmungen und deren Kontrolle lässt jedoch befürchten, dass es in Drittstaaten zu regelrechten „Big Brother“-Datensammlungen kommen könnte. Daher wird auch von der Art. 29-Gruppe gefordert, dass Datenschutzbestimmungen integraler Bestandteil der CCC sein müssen.[36] Leider ist keine einzige Vorschrift zum Datenschutz in die CCC aufgenommen worden, insbesondere nicht in Art. 15.

5.5 Eigene Stellungnahme

Angesichts der restriktiven und schwammigen Formulierung des Art. 15 wird deutlich, dass die CCC eindeutig auf die Effektivität des Abhörens ausgerichtet ist – was angesichts der an der Ausarbeitung des Vertragsentwurfs beteiligten Kreise nicht verwundert (siehe oben 4). Einschränkungen der Abhörbefugnisse sollen nur zulässig sein, soweit dies ausdrücklich im Vertragstext vorgesehen ist. Umso mehr enttäuscht die Formulierung des Art. 15, die klare Maßstäbe bei der Begrenzung der staatlichen Eingriffsbefugnisse vermissen lässt. Dies führt zu dem Schluss, dass es aufgrund des Verhandlungsverfahrens, dem „Geburtsfehler“ des Abkommens, kaum noch möglich sein wird, den Entwurf entsprechend zu korrigieren. Wenn nicht noch substanzielle Verbesserungen in diesem Punkt vorgenommen werden, verbieten es rechtsstaatliche Erwägungen, die CCC in ihrer gegenwärtigen Fassung zu unterzeichnen.

6 Internationale Zusammenarbeit (Art. 23 bis 35)

6.1 Der Anspruch auf Rechtshilfe

Im dritten Kapitel der CCC bestimmt Art. 25 Abs. 1: *„Die Vertragsparteien leisten einander im größtmöglichen Umfang Rechtshilfe für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten im Zusammenhang mit Computersystemen und Computerdaten oder für die Erhebung von in elektronischer Form vorliegenden Beweisen für eine Straftat.“* Gemäß den Art. 29-34 kann insbesondere die Sicherung und Übermittlung gespeicherter Verbindungs- und Inhaltsdaten sowie die Erhebung von Verbindungs- und Inhaltsdaten in Echtzeit durch einen anderen Vertragsstaat verlangt werden. Im Bezug auf die Vorschriften über die internationale Zusammenarbeit stellt sich aus rechtstaatlicher Sicht zum einen die Frage, welchen Voraussetzungen dieser Anspruch auf Rechtshilfe unterliegt, zum anderen, wie mit den erlangten Daten verfahren werden darf.

Während auf die zweite Frage noch einzugehen sein wird, ist in Bezug auf die erste Frage zunächst einmal festzustellen, dass Rechtshilfe grundsätzlich in dem Umfang zu gewähren ist, in dem sie angefordert wird, wobei auch hier – im Rahmen der zulässigen Zwecke gemäß Art. 25 – keinerlei materielle Beschränkungen vorgesehen sind. Zwar muss der ersuchte Staat nur Maßnahmen nach den Art. 29-34 ergreifen. Andererseits hindert ihn aber auch keine Bestimmung daran, freiwillig weiter gehende Eingriffe vorzunehmen.

Die Art. 29-34 sind wiederum äußerst weit gefasst und lassen Einschränkungen zum Grundrechtsschutz vermissen. Wenn also etwa die südafrikanische Polizei wegen eines Bagatell-Diebstahls gegen eine Person ermittelt, die auf einem deutschen Server einen Email-Account hat, dann sind die deutschen Behörden auf Anforderung grundsätzlich verpflichtet, sich die dort gespeicherten Daten – ggf. mittels Durchsuchung und Beschlagnahme – zu verschaffen und sie nach Südafrika zu übermitteln.

Keine Voraussetzung eines Rechtshilfeersuchens ist, dass ein auf Tatsachen beruhender Verdacht bezüglich einer bestimmten Straftat vorliegt. Unter die Generalklausel in Art. 25 lassen sich vielmehr auch Ermittlungen zur vorbeugenden Bekämpfung von Straftaten fassen. Unter rechtstaatlichen Gesichtspunkten, insbesondere angesichts des Verhältnismäßigkeitsprinzips, erscheint dies nicht vertretbar.

Angesichts dessen fragt sich der kritische Beobachter, in welchen Fällen die Gewährung von Rechtshilfe denn überhaupt aus Menschenrechts- oder Datenschutzgründen ausgeschlossen sein soll. Eine zwingende Bestimmung hierzu sucht man vergeblich; der Vertragstext schreibt keinerlei Einschränkungen zum Schutz der

[34] Vgl. US-Department of Justice unter Ziff. 6, <http://www.usdoj.gov:80/criminal/cybercrime/COEFAQs.htm>.

[35] Convention 108/81 for the protection of individuals with regard to automatic processing of personal data, <europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm>.

[36] Stellungnahme 4/2001 (Fußn. 22).

Betroffenen vor. Ähnlich wie schon bei den Art. 14 ff. sieht die CCC auch im Bereich der Rechtshilfe lediglich Eingriffsbefugnisse vor, ohne diese zu begrenzen. Dass diese Vorgehensweise unausgewogen und verfehlt ist, liegt auf der Hand.

6.2 Möglichkeiten des Menschenrechts- und Datenschutzes

Die Verfasser begnügten sich stattdessen mit der Aufnahme von Vorschriften, die es dem ersuchten Staat erlauben, die Gewährung von Rechtshilfe zu verweigern. Dies kann dann möglicherweise auch aus Menschenrechts- oder Datenschutzgründen geschehen. Eine zwingende Verpflichtung des ersuchten Staates, von diesem Instrumentarium Gebrauch zu machen, besteht jedoch nicht, so dass diese Vorgehensweise bereits im Ansatz gänzlich ungenügend ist.

Dies gilt insbesondere angesichts der Tatsache, dass selbst ein rechtstaatlich geprägter Staat nach der CCC nur äußerst eingeschränkte Möglichkeiten hat, die Gewährung von Rechtshilfe aus Menschenrechts- und Datenschutzgründen zu verweigern, wie sich anhand der im Folgenden zu diskutierenden Ausnahmebestimmungen zeigen wird.

Art. 25 Abs. 4, der auf Bedingungen für die Gewährung von Rechtshilfe nach nationalem Recht verweist, ist schon seinem Wortlaut nach zu unklar formuliert, um als substanzielle Einschränkungsmöglichkeit ausgelegt werden zu können. Insbesondere verweisen die amtlichen Anmerkungen auf eine Vielzahl von Fällen, in denen die Bestimmung keine Anwendung finden soll.[37] Die Art. 29-Datenschutzgruppe der EU sieht in Art. 25 Abs. 4 daher lediglich für die Fälle der Art. 33 (Aufzeichnung von Verbindungsdaten in Echtzeit) und 34 (Aufzeichnung von Inhaltsdaten in Echtzeit) eine effektive Einschränkungsmöglichkeit der Eingriffsbefugnisse nach nationalem Recht.[38]

Art. 27 Abs. 4 erlaubt zwar die Ablehnung von Rechtshilfeersuchen durch eine Vertragspartei, wenn „*die Erledigung des Ersuchens wahrscheinlich ihre Souveränität, Sicherheit, öffentliche Ordnung (*ordre public*) oder andere zentrale Interessen beeinträchtigen würde*“. Der Menschenrechts- und Datenschutz liegt hingegen zuvörderst im Interesse der betroffenen Bürger. Es ist daher sehr zweifelhaft, ob er als zentrales Staatsinteresse angesehen werden kann.[39] Auch der Begriff „*ordre public*“ wird nur als Unterfall eines zentralen Staatsinteresses genannt.

Zudem bekräftigen die Anmerkungen, dass Art. 27 Abs. 4 eng auszulegen und zurückhaltend anzuwenden sei.[40] Die Vorschrift dürfe nicht dazu führen, dass Amtshilfeersuchen in ganzen Fallgruppen verweigert werden dürften.[41] Insbesondere aus Datenschutzgründen komme eine „weitgehende, kategorische oder systematische“ Ablehnung der Zusammenarbeit nicht in Betracht.[42] Somit kann auch in Art. 27 Abs. 4 keine ausreichende Ermächtigung für hinreichende Einschränkungen zum Menschenrechts- und Datenschutz gesehen werden.

Schließlich kommt noch Art. 28 in Betracht, demzufolge jeder Staat die Übermittlung von Informationen im Rahmen der Rechtshilfe von der Bedingung abhängig machen kann, dass die Daten „*nicht für andere als die in dem Ersuchen genannten Ermittlungen oder Verfahren verwendet werden*“ (Art. 28 Abs. 2 lit. b).

Im Umkehrschluss zu den in Art. 28 Abs. 2 vorgesehenen Einschränkungsmöglichkeiten lässt sich allerdings zunächst einmal entnehmen, dass der ersuchende Staat in keiner Weise an Datenschutzbestimmungen gebunden ist und die erlangten Daten sogar veröffentlichen darf. Einmal erlangt, kann er über sie grundsätzlich voll verfügen, auch über das konkrete Strafverfahren, welches Anlass für das Ersuchen war, hinaus.

Die einzige Möglichkeit, dies zu verhindern, besteht in der sehr aufwendigen Lösung, dass sich der ersuchte Staat in jedem Einzelfall auf Art. 28 beruft. Aber selbst wenn dies geschieht, ist nur die Verwendung, nicht auch die Speicherung der übermittelten Daten eingeschränkt. Eine Löschungspflicht ist nicht vorgesehen.

Zur Durchsetzung des eingeschränkten Nutzungsrechts wurde zwar in Abs. 4 vorgesehen, dass der übermittelnde Staat vom Empfängerstaat Angaben bezüglich der vertragsgemäßen Verwendung der Daten verlangen kann. Diese Angaben unterliegen aber keiner Kontrolle. Sogar wenn der Empfängerstaat eine unzulässige Verwendung eingestehen würde, bestünde keinerlei Sanktionsmöglichkeit seitens des übermittelnden Staates. Insbesondere wird dem betroffenen Bürger selbst kein Rechtsschutz garantiert.

Angesichts der Formulierung in Art. 28 Abs. 2 lit. b, übermittelte Informationen dürften in keinen anderen als den im Ersuchen genannten Verfahren verwendet werden, stellt sich zudem die Frage, welche Verfahren im Ersuchen denn genannt werden dürfen. Wie oben gezeigt, ist der durch Art. 25 gesteckte Rahmen sehr weit. Insbesondere ist nicht ausgeschlossen, dass ein Staat Informationen etwa für zukünftige Strafverfahren anfordert, ohne dass bereits ein konkreter Verdacht vorliegt. Die CCC ermöglicht nicht einmal die Ablehnung eines Rechtshilfeersuchens, das über den in Art. 25 Abs. 1 genannten Rahmen hinaus geht oder aus sonstigen Gründen rechtswidrig ist.

Nicht zuletzt fehlt sowohl ein Katalog schwerer Straftaten, wegen derer ermittelt werden muss, noch ist es erforderlich, dass dieses möglicherweise begangene Delikt im ersuchten Staat strafbar ist. Der Einwand der fehlenden doppelten Strafbarkeit kann nur erhoben werden, wenn sich dies der Vertragsstaat bei der Ratifikation der Konvention ausdrücklich vorbehalten hat (vgl. Art. 29 Abs. 4). Im Übrigen sind Vorbehalte nicht zulässig (Art. 42), so dass auch dieses Rechtsinstitut keine ausreichende Lösung für eine „Nachbesserung“ des verfehlten Vertragstexts ermöglicht.

6.3 Gewährung von Rechtshilfe

Im Ergebnis ist festzustellen, dass jeder Vertragsstaat in extrem weitem Maße zur Gewährung von Amtshilfe verpflichtet ist. Es wäre denkbar, dass Südafrika ein Amtshilfeersuchen an Deutschland stellt mit dem Zusatz, dass die übermittelten Informationen in einem laufenden Ermittlungsverfahren, aber auch zur zukünftigen, vorbeugenden Verbrechensbekämpfung eingesetzt werden sollen. Ein solches Amtshilfeersuchen könnte Deutschland nach den Bestimmungen des Entwurfs nicht ablehnen.

Dies gilt auch dann, wenn in Südafrika kein angemessenes Datenschutzniveau sichergestellt wäre und wenn die übermittelten Daten dort unverhältnismäßig lange gespeichert würden. Stellt man sich noch

[37] Amtliche Anmerkung 258.
[38] Stellungnahme 4/2001 (Fußn. 22).
[39] So auch Dix Stellungnahme vor dem Unterausschuss „Neue Medien“ des Deutschen Bundestages am 05.07.2001 = in diesem Heft.
[40] Amtliche Anmerkung 268.
[41] Amtliche Anmerkung 268.
[42] Amtliche Anmerkung 269.

vor, dass die übermittelten Daten einen deutschen Staatsbürger betreffen, liegt auf der Hand, dass in einem solchen Fall den deutschen Behörden von Verfassungs wegen die Datenübermittlung verboten wäre. Gleichwohl wären sie dazu nach der CCC verpflichtet. In einem solchen Fall, in dem übermittelte Informationen in ausländischen Staaten in einer Weise gebraucht werden, die in Deutschland als offensichtlich rechtswidrig anzusehen wäre, ist der Betroffene auch weitgehend schutzlos gestellt. Jedenfalls die CCC garantiert ihm keinen Rechtsschutz.

6.4 Gefahr „internationaler Ermittlungsoasen“

Auch einzelne Nachbesserungen am Text, wie sie die Bundesregierung anstrebt[43], können die grundsätzliche Problematik des dritten Kapitels der CCC kaum entschärfen. Der schleswig-holsteinische Landesdatenschutzbeauftragte Helmut Bäumler äußerte insbesondere die Befürchtung, dass „*internationale Ermittlungsoasen*“ geschaffen werden könnten.[44] So könnte etwa die deutsche Staatsanwaltschaft, die gegen einen Deutschen nach deutschem Recht in einer bestimmten Weise nicht ermitteln dürfte, die USA um Amtshilfe ersuchen. Die dortigen Behörden sind möglicherweise nicht an vergleichbare Schutzvorschriften gebunden, so dass die deutschen Strafverfolger unter Umgehung der hiesigen Vorschriften Beweismittel erlangen könnten.

Verschärfend tritt hinzu, dass in Deutschland nicht die aus den USA bekannte „fruits of the poisonous tree doctrine“ gilt, wonach Beweise, die rechtswidrig erlangt wurden, sowie jegliche Ergebnisse von Folgeermittlungen in Strafverfahren nicht verwertet werden dürfen. In Deutschland ist man in diesem Punkt sehr viel großzügiger. Das BVerfG betont jedenfalls in Fällen schwerer Straftaten den Vorrang des staatlichen Ermittlungsinteresses („Interesse an der Wahrheitsfindung“).[45]

Kurz, es besteht ein gewisser Anreiz für die deutsche Staatsanwaltschaft, nationale Schutzvorschriften durch internationale Amtshilfeersuchen zu umgehen. Da die CCC keinen grenzüberschreitenden Bezug des Ermittlungsverfahrens verlangt, wäre ein solches Vorgehen auch durchaus möglich.

Offensichtliche Missbräuche wird man zwar in Deutschland zu verhindern wissen. Dies gilt aber nicht für durch Amtshilfe der deutschen Behörden erlangte Daten, die im Ausland missbräuchlich eingesetzt werden. Die CCC stellt insbesondere nicht sicher, dass in ausländischen Staaten „Ermittlungsoasen“ nicht gezielt ausgenutzt werden.

Aus rechtstaatlicher Sicht ist eine Übernahme der Regelung im Europäischen Rechtshilfeübereinkommen wünschenswert, wonach Amtshilfeersuchen nur dann nachgekommen werden muss, wenn sie auch nach dem Recht des ersuchten Staates rechtmäßig hätten gestellt werden dürfen.[46] Weit davon entfernt schreibt das dritte Kapitel der CCC nicht einmal das – auch menschenrechtlich gebotene – Verhältnismäßigkeitsprinzip fest, von materiellen Bestimmungen zum Menschenrechts- und insbesondere Datenschutz ganz zu schweigen.

6.5 Kritik der Art. 29-Datenschutzgruppe

Ähnliche grundsätzliche Bedenken bringt die Art. 29-Datenschutzgruppe der EU vor.[47] Sie verweist darauf, dass einige Mitgliedsstaaten der EU die Datenschutzrichtlinie 95/46/EG auch auf die Weitergabe von Informationen durch die Strafverfolgungsbehörden anwenden. Diese Datenschutzrichtlinie erlaubt die Übermittlung von Daten in Drittstaaten grundsätzlich nur, wenn diese ein adäquates Datenschutzniveau aufweisen. Es könne den Behörden dieser Staaten, so die 29er-Gruppe, unter Umständen nicht oder nur eingeschränkt erlaubt sein, einem Amtshilfeersuchen nach der CCC nachzukommen. Das Gleiche könne aufgrund von Verfassungsrecht einiger Mitgliedsstaaten der Fall sein.

Die EU-Datenschützer schlagen daher zwei Lösungsmöglichkeiten vor: Als *„reines Minimum“* wird gefordert, dass es dem ersuchten Staat generell erlaubt sein muss, die Übermittlung von Daten von Bedingungen zum Zwecke des Datenschutzes abhängig zu machen.[48] Dies alleine würde aber noch keine effektive Gewährleistung eines angemessenen Schutzniveaus in allen Unterzeichnerstaaten bedeuten.

Daher wird zusätzlich gefordert, dass ein einheitlicher Schutzstandard durch materielle Bestimmungen in der CCC selbst sicher gestellt werden muss, insbesondere im Hinblick auf den Schutz des Rechts auf Privatleben und informationelle Selbstbestimmung (Datenschutz). Die Unterzeichnerstaaten sollen außerdem verpflichtet werden, der Datenschutzkonvention des Europarats beizutreten. Staaten, die von dem Anspruch auf Amtshilfe profitieren wollten, müssten sich auch auf einen angemessenen Schutz der übermittelten Daten einlassen.

6.6 Eigene Stellungnahme

Zusammenfassend ergibt sich, dass alles andere als die Aufnahme substanzieller, materieller Menschenrechts- und Datenschutzbestimmungen aus Bürgersicht gänzlich unbefriedigend wäre und die grundsätzlichen Bedenken gegen das dritte Kapitel der CCC nicht ausräumen könnte.

Wenn man die Aufnahme von ausführlichen Datenschutzregelungen in die CCC angelehnt etwa an die Datenschutzkonvention des Europarats vermeiden will, müsste als Minimallösung wenigstens der Art. 28 Abs. 2 lit. b wie folgt gefasst werden:

„The requesting Party shall use information or material furnished in response to its request only insofar as necessary for a current investigation or proceeding concerning a criminal offence related to computer systems and data, or concerning any criminal offence and involving the necessity to collect evidence in electronic form. At the end of this investigation or proceeding, at the latest five years after the transmission, the information or material shall be destroyed by the requesting Party. As far as possible in view of the purpose of the request, the data subject shall be informed of and have the right to demand what personal data of theirs is stored by the requesting Party.“

Nur durch die Aufnahme einer derartigen, materiellen Datenschutzbestimmung lässt sich die Aufnahme einer Generalklausel über ein „angemessenes Datenschutzniveau“ als Bedingung für die Übermittlung

[43] Geiger, in seiner Vorlesung an der Universität Frankfurt am Main vom 26.06.2001.

[44] Bäumler, DuD 2001, 348, 352.

[45] „Tagebuch-Urteil“, BVerfGE 80, S. 367 ff.

[46] Vgl. etwa Art. 18 Abs. 5 des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, ABl. C 197 vom 12.07.2000 S. 3-23; siehe auch Bäumler, DuD 2001, 348, 352.

[47] Stellungnahme 4/2001 (Fußn. 22)

[48] Ebenso die Parlamentarische Versammlung der Europarats in ihrer Stellungnahme Nr. 226 (2001) (Fußn.19), Unterpunkt xix.

von Informationen vermeiden. Unabdingbar ist eine wie auch immer geartete, effektive Vorsorge für den Fall, dass in einem ersuchenden Staat die Einhaltung fundamentaler Grundrechte bezüglich des Schutzes der Privatsphäre Einzelner nicht sicher gestellt ist.

Die Datenschutzbestimmungen müssen auch für die freiwillige Übermittlung von Daten gem. Art. 26 gelten. Sie dürfen nicht durch bilaterale Rechtshilfeverträge (sog. „MLATs“) untergraben werden können, so dass Art. 28 Abs. 1, der die Subsidiarität der CCC gegenüber solchen Abkommen vorsieht, zu hinterfragen ist.

Das Rechtshilfeverfahren muss über die rein zwischenstaatliche Ebene hinaus so gestaltet werden, dass dem betroffenen Bürger unmittelbar Möglichkeiten zur Durchsetzung seines Rechts auf Schutz seiner Privatsphäre eingeräumt werden, insbesondere ein gerichtlich durchsetzbares Recht auf Benachrichtigung sowie ein effektiver Auskunfts-, Berichtigungs- und Löschungsanspruch. Auch im Bereich der Strafverfolgung muss der Umgang mit personenbezogenen Daten den Grundsätzen der Verhältnismäßigkeit und der Datensicherheit unterworfen werden.

Zudem muss eine effektive Kontrollmöglichkeit bezüglich der Einhaltung der vorzusehenden Datenschutzbestimmungen vorgesehen werden. Nur ein „stumpfes Schwert“ ist Art. 28 Abs. 4. Um ein effektives Sicherungsinstrument darzustellen, müsste die dort vorgesehene Unterrichtung obligatorisch sein und veröffentlicht werden; bei ihrer Missachtung müssten Sanktionen drohen.

Zusätzlich ist die Einrichtung eines Monitoring-Verfahrens in Betracht zu ziehen, in dem ein spezielles Gremium regelmäßig Berichte über die staatliche Überwachungstätigkeit und die Einhaltung der Menschenrechtsschutzbestimmungen der Öffentlichkeit vorstellt. Dieses Gremium wäre mit substanziellen Befugnissen auszustatten, insbesondere mit dem Recht, den gegen die CCC verstoßenden Staat namentlich und öffentlich zu benennen. Besonders ist darauf zu achten, dass das Monitoring-Gremium nicht mit Personen besetzt wird, die staatliche Sicherheitsinteressen wahrnehmen.

Eine weitere Sanktionsmöglichkeit wäre es, den Vertragsstaaten generell die Möglichkeit einzuräumen, Amtshilfeersuchen zu verweigern, wenn der ersuchende Staat wiederholt gegen die Datenschutzbestimmungen der Konvention verstoßen hat und dies durch das Monitoring-Gremium auch festgestellt wurde. In Betracht käme schließlich auch, eine Vertragsstrafe vorzusehen.

In jedem Fall aber müssen Datenschutzbestimmungen nicht nur vorgesehen, sondern auch effektiv durchgesetzt werden. Leider ist schon in Bezug auf das erstere Erfordernis nicht abzusehen, dass eine befriedigende Lösung gefunden oder auch nur gesucht werden wird.

Nur „zweite Wahl“ wäre die vorgeschlagene Lösung der Parlamentarischen Versammlung des Europarats, wonach dem ersuchten Staat durch Ergänzung des Art. 27 Abs. 4 gestattet werden soll, die Amtshilfe zu verweigern, wenn die Einhaltung „allgemein anerkannter“ Datenschutzbestimmungen nicht sicher gestellt ist.[49] Damit läge der Datenschutz in der Hand des jeweils ersuchten Staats, was wiederum keine effektive Gewährleistung des Datenschutzniveaus ermöglichen würde. Um eine Aufnahme materieller Datenschutzbestimmungen und effektiver Mechanismen zu ihrer Durchsetzung im dritten Kapitel wird man daher nicht umhin kommen.

7 Fazit

Festzuhalten bleibt, dass die CCC einseitig auf die Effektivität der Strafverfolgung ausgerichtet ist, während der Schutz der beteiligten Bürger, soweit er überhaupt zugelassen wird, allein den einzelnen Vertragsstaaten überlassen bleibt. Weder die Bestimmungen über innerstaatliche Ermittlungsbefugnisse noch die Vorschriften über die internationale Zusammenarbeit sehen substanzielle rechtsstaatliche Sicherungen zum Menschenrechts- und Datenschutz vor; stattdessen wird deren Missachtung Vorschub geleistet.

Materiell fehlen jegliche konkrete Bestimmungen bezüglich der Frage, unter welchen Voraussetzungen der jeweilige Grundrechtseingriff verhältnismäßig ist. Grundrechtsschutz muss auch durch Verfahren gewährleistet werden, insbesondere durch das Erfordernis vorheriger richterlicher Anordnung von Maßnahmen, durch nachträgliche Benachrichtigung der Betroffenen, durch Beschränkung der Nutzung erlangter Daten, durch Verpflichtung zur Protokollierung der Maßnahmen, durch richterliche Überwachung und Kontrolle ihrer Durchführung sowie durch eine öffentliche Rechenschaftspflicht der die Überwachung anordnenden Stellen.

Keinem dieser Erfordernisse wird der vorliegende Entwurf der CCC gerecht. Er ist damit fundamental unvereinbar mit den Menschenrechten aus europäischer Sicht. Dennoch ist zu befürchten, dass er sich, einmal ratifiziert, faktisch durchsetzen und den Menschenrechtsschutz unterhöhlen wird, ohne dass dies von der Öffentlichkeit wahrgenommen würde.

Aus diesem Grund ist die Unterzeichnung der Konvention in ihrer derzeit geplanten Fassung strikt abzulehnen. Zu überdenken wäre dieses Ergebnis allenfalls nach einer umfassenden Überarbeitung des Entwurfs unter durchgehender Aufnahme konkreter und effektiver materieller Bestimmungen zum Grundrechtsschutz.

Potentiellen außereuropäischen Vertragsstaaten ein europäisches Menschenrechtsverständnis „aufzuzwingen“, erscheint angesichts der Tatsache gerechtfertigt, dass diesen Staaten im Gegenzug ein umfassendes Recht auf internationale Rechtshilfe eingeräumt wird. Wenn sie sich darauf nicht einlassen, bleibt allein ein Vorgehen nur im europäischen Rahmen möglich.

[49] Stellungnahme Nr. 226 (2001). Unterpunkt xix (Fußn. 19).