Christian Schwarzenegger

Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001

Am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Fernmeldegeheimnisses

aus: DONATSCH, Andreas / FORSTER, Marc / SCHWARZENEGGER Christian (Hrsg.): Strafrecht, Strafprozessrecht und Menschenrechte. Festschrift für Stefan Trechsel zum 65. Geburtstag. Zürich: Schulthess, 2002, S. 305-324

Inhaltsverzeichnis

I. Einleitung

"Ohne Internet läuft nichts mehr", so betitelte eine grosse Tageszeitung unlängst einen Artikel über die Verbreitung des Internets in Schweizer Unternehmen[1]. Mittlerweile nutzen bereits 85% aller Betriebe mindestens einen der verschiedenen Internetdienste. Darunter ist der Einsatz von E-Mails am weitesten verbreitet (ca. 78%), gefolgt vom Webzugang für Firmenangehörige (ca. 71%). Rund 55% der untersuchten Unternehmen unterhalten eine eigene Website. Obschon sich die Interneteuphorie der 90er Jahre etwas abgekühlt hat, wird die Schweizer Wirtschaft im Jahre 2002 schätzungsweise 6 Mia. Franken in das Datennetz investieren und mehr als 15 Mia. Franken im E-Commerce umsetzen[2]. Allerdings

haben sich die Akzente vom direkten Online-Verkauf und Online-Brokering, die sich mehrheitlich nicht den Erwartungen entsprechend etablieren konnten, auf die effizienzsteigernden Bereiche der betriebsinternen Kommunikation, der B2B-Kontakte[3] und des Marketings verschoben.

Auch in der Entwicklung der privaten Nutzung des Internets spiegelt sich seine grosse Popularität und zunehmende Bedeutung. Im Jahre 2001 soll die Zahl der Menschen mit Zugang zum Internet weltweit auf 429 Mio. angestiegen sein, wobei innerhalb Europas die skandinavischen Länder und die Niederlanden die höchsten "Penetrationsraten" aufweisen[4]. Innerhalb eines Jahrzehnts haben die Fortschritte der Informationstechnologie somit eine grundlegende Veränderung der Gesellschaft herbeigeführt. Sowohl im nichtkommerziellen Umfeld der Universitäten und privaten Nutzer als auch im Gebiete der wirtschaftlichen Beziehungen sind Informationen ungeachtet der geographischen Entfernung in einem Ausmass verfügbar und austauschbar geworden, wie es vor 20 Jahren noch kaum möglich erschien. Auch in den Bereichen der öffentlichen Verwaltung und der Volksrechte wird immer mehr Internet-Tauglichkeit angestrebt. Nach einer Botschaft des Bundesrates zur Teilrevision des Bundesgesetzes über die politischen Rechte[5] sollen in der Schweiz schon bald erste Versuche mit der Stimmabgabe per Internet beginnen, während in den Kantonen mit webbasierten Formen der Online-Steuererklärung experimentiert wird.

Die Schattenseiten dieser Entwicklung werden ebenfalls immer deutlicher: Auf der einen Seite erleichtern die Anonymität und Globalität der Internetkommunikation und des elektronischen Handels die Begehung traditioneller Straftaten wie beispielsweise der Inhalts- und Informationsverbreitungsdelikte, der verschiedenen Varianten des Betruges, der Delikte gegen den Geheim- oder Privatbereich oder der immaterialgüter- und wettbewerbsrechtlichen Delikte[6]. So mussten im Jahre 2000 europaweit bereits 767 Websites durch die Behörden geschlossen werden,

Schwarzenegger — Festschrift Trechsel, S. 307

weil darauf illegale Softwarekopien angeboten wurden[7]; hinzu tritt hier wohl ein beträchtliches Dunkelfeld. Auf der anderen Seite bieten Computertechnologie und Netzwerke Angriffsflächen für neue Kriminalitätsformen, wie die Beispiele des illegalen Zugriffs auf ein Computersystem (Hacking) oder des Ausserfunktionsetzens eines Netzwerkcomputers durch Überfluten mit Datenpaketen oder E-Mails (Denial of Service Attacks[8]) zeigen.

In regelmässigen Abständen dringen international operierende Hacker, deren Alter häufig unter 18 Jahren liegt 9, in die Rechner von wichtigen Einrichtungen ein. Illustrativ für die grenzüberschreitende Natur solcher Aktionen ist ein aktueller Fall, in welchem 6 italienische Computerautodidakten im Alter zwischen 15 und 23 Jahren die Web-Server des US-Verteidigungsministeriums (Pentagon), der Weltraumbehörde NASA, verschiedener US-Gerichte sowie offizieller Server der chinesischen, britischen, schwedischen und mexikanischen Regierung "knackten". Die technisch aufwendige und kostenintensive Fahndung dauerte 3 Monate[10].

Im Jahr 2001 nahm auch die Verbreitung von Computerviren sprunghaft zu. Diese bösartigen Codes, die häufig per Mail-Attachment, aber auch über infizierte Websites verbreitet werden, bergen ein erhebliches Schädigungspotential[11]. So war jüngst zu lesen, dass die Schweizer FDP Opfer einer Virenattacke geworden sei, wobei der bösartige Code vertrauliche Texte von der Festplatte des betroffenen Computers abrief und per E-Mail an zufällig ausgewählte Personen aus der Adressdatei des Mailprogramms versandte[12]. Gemäss Erhebungen der Hersteller

Schwarzenegger — Festschrift Trechsel, S. 308

von Anti-Viren-Programmen war im Jahr 2001 durchschnittlich jedes 370ste E-Mail mit einem Virus infiziert, während die Werte im Jahr 2000 bei 1 Virus pro 700 E-Mails und

im Jahr 1999 noch bei 1 Virus pro 1400 E-Mails lagen[13].

Diese negativen Ereignisse stellen klar unter Beweis, dass sowohl private Nutzer als auch E-Commerce-Anbieter und die öffentliche Hand von Internetkriminalität betroffen sind und alle ein vitales Interesse an einer Verbesserung der Sicherheit im Internet haben. Lösungen sind auf verschiedenen Ebenen anzustreben:

• Der technische Schutz der Computersysteme und der Datenübertragung muss verbessert werden.

• Die verschiedenen Diensteanbieter und die Nutzer müssen besser über die Missbrauchsgefahren informiert und durch Schulungsprogramme zum Selbstschutz angeregt werden.

• Auf nationaler, aber auch internationaler Ebene sind rechtliche Rahmenbedingungen zu schaffen oder zu verbessern, die eine koordinierte Bekämpfung der Internetkriminalität ermöglichen[14].

II. Entstehung und Inhalt der Convention on Cybercrime

1. Die Entstehung der Convention on Cybercrime

Seit einer Empfehlung des Ministerrats[15] 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[16]. 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 PC-CY nahm seine Arbeit im April 1997 auf und legte dem CDPC im Juni 2001 die revidierte und endgültige Fassung des Übereinkommensentwurfs sowie einen erläuternden Bericht vor[17]. Um eine möglichst weitgehende internationale Harmonisierung zu erzielen, wurden Sachverständige von Nicht-Europaratsmitgliedern wie den USA, Kanada und Japan in die Vorbereitungsarbeiten miteinbezogen. Einzigartig war auch das offene Konsultationsverfahren, welches seit April 2000 durch die Publikation der jeweils aktuellsten Fassungen des Übereinkommensentwurfs im Internet in Gang gesetzt wurde[18].

Nach einigen geringfügigen Änderungen durch den CDPC 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. Bis dato haben 29 Mitgliedsstaaten des Europarats sowie die USA, Kanada, Japan und Südafrika die Convention on Cybercrime (CCC) unterzeichnet[19]. 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 Kraft tritt es drei Monate

nachdem mindestens fünf Staaten, wovon mindestens drei Mitgliedsstaaten des Europarates sein müssen, ihre Zustimmung ausgedrückt haben, durch das Übereinkommen

gebunden zu sein (Art. 36 Abs. 3 CCC). Nach dem Inkrafttreten kann das Ministerkomitee des Europarates auch andere Nichtmitgliedsstaaten zum Beitritt einladen (Art. 37 Abs. 1 CCC).

2. 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[20]. Zweitens schafft sie 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[21]. 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 der Konventionsstrafbestimmungen zuständig ist[22]. 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[23]. 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[24], 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 innerstaatli-

chen 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[25].

III. Die Delikte gegen die Vertraulichkeit von Computerdaten und -systemen

Mit der Revision des Vermögens- und Urkundenstrafrechts[26] wurden Strafbestimmungen in das schweizerische Strafgesetz eingeführt, welche die neuen Deliktsformen im Zusammenhang mit der elektronischen Datenverarbeitung und Datenübertragung[27] kriminalisieren sollten[28]. "Nicht unbedenklich ist, dass man sich

weitgehend an den Delikten gegen das Eigentum orientierte, obgleich hier ganz andere Sachverhalte zu regeln waren[29]."

Tabelle: Verurteilungen wegen Computerdelikten (1995-1999)

Jahr	1995	1996	1997	1998	1999
Unbefugte Datenbeschaffung (Art. 143)	1	2	2	2	3
Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143bis)	0	1	0	1	1
Datenbeschädigung (Art. 144bis Ziff. 1)	13	17	na	20	8
Herstellung usw. von Programmen zur Datenbeschädigung (Art. 144bis Ziff. 2)	1	0	na	2	1
Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147)	52	224	368	394	396

Quelle: Bundesamt für Statistik, Strafurteilsstatistik 2002 (persönliche Mitteilung).

Obschon die in der Einleitung genannten Fälle auf eine Zunahme der Computer- und Internetkriminalität hinweisen, lässt sich ihr Ausmass nur ungenau beziffern, fehlen doch Angaben zu den polizeilich bekanntgewordenen Fällen in der Schweiz[30]. Ähnlich wie in

Deutschland enden in der Schweiz nur ganz wenige Fälle mit einer Verurteilung (siehe Tabelle). Im übrigen betreffen die Verurteilungen wegen betrügerischen Missbrauchs einer Datenverarbeitungsanlage nur zu einem geringen Teil Netzwerkdelikte. In der Mehrzahl der Fälle handelt es sich hierbei um Missbräuche von Zahlungskarten. Damit wird deutlich, dass die Strafverfolgungsbemühungen im Bereich der Computer- und Internetkriminalität gemessen an den Schäden und Gefahren, die mit dem Hacking oder der Verbreitung von Computerviren verbunden sind[31], noch völlig hinterherhinken.

Nachdem die Schweiz am 23. November 2001 die Convention on Cybercrime unterzeichnet hat, stellt sich nunmehr die Frage, inwiefern die geltenden Strafnormen den Vorgaben des Übereinkommens entsprechen bzw. ob ein Anpassungsbedarf im materiellen Strafrecht besteht[32]. Anhand der Delikte gegen die Vertraulichkeit

von Computerdaten und -systemen (Art. 2-3 CCC) und der damit verknüpften Fragen (Art. 1 und 11 CCC) soll dies im folgenden geprüft werden.

1. Der Datenbegriff (Art. 1 CCC)

Im Gegensatz zum schweizerischen aber auch deutschen Strafrecht enthält die CCC in Art. 1 neben Definitionen für die Begriffe "Computersystem", "Diensteanbieter" und "Verbindungsdaten" auch eine Begriffsbestimmung der "Computerdaten". Als solche gelten alle "Darstellungen von Tatsachen, Informationen oder Begriffen in einer zur Verarbeitung in einem Computer geeigneten Form einschliesslich eines Programmes, das geeignet ist, ein Computersystem zur Ausführung einer Funktion zu veranlassen"[33] (Art. 1 lit. b CCC). Die Vertragsparteien sind nicht verpflichtet, diese Definition wörtlich zu übernehmen, sondern es soll genügen, wenn sie in einer den Grundsätzen des Übereinkommens entsprechenden Weise im innerstaatlichen Recht verankert werden[34]. Es stellt sich somit die Frage, ob sich die bisherigen Auslegungsansätze bezüglich des Daten-

begriffs im schweizerischen Strafgesetz mit Art. 1 lit. b CCC decken oder in Einklang bringen lassen.

Daten sind bestimmte Informationen über einen Sachverhalt, die in einer Vielzahl von Formen festgehalten werden können: Texte, Zahlen, Zeichen, Musik oder Geräusche, Stand- oder Bewegungsbilder auf Papier, als Ladungs- oder Magnetisierungszustand auf einem elektronischen Speicher, als Materialveränderung auf einem optischen Speicher oder auch als Vorstellung im menschlichen Gehirn[35]. Nachdem Artikel 143 StGB[36] von "elektronisch oder in vergleichbarer Weise gespeicherten oder übermittelten Daten" spricht, ist der Begriff im Zusammenhang mit den Computerstrafnormen einzuschränken auf Informationen, die in codierter Form von einer Datenverarbeitungsanlage verarbeitet, gespeichert oder übermittelt werden können. Dazu werden abweichend von der Terminologie der Informatik auch die Programme gezählt[37]. Aus dieser Begrenzung folgt, dass Informationen,

die in einer körperlichen, bildlich-visuell erkennbaren Form vorliegen 38, keine Daten im Sinne der Computerstrafnormen sind. Ebensowenig soll dies der Fall sein, wenn die Daten in Geräten gespeichert sind, die nicht als Datenverarbeitungsanlage zu qualifizieren sind, bzw. von solchen übermittelt werden[39]. Somit hängt die Reichweite des Datenbegriffs von der Definition der Datenverarbeitungsanlage ab, wobei der Gesetzgeber als solche "offensichtlich nur Systeme höherer Funktionsstufen" habe erfassen wollen[40]. Der gestützt darauf getroffene Ausschluss beispielsweise von telephonisch übermittelten Informationen, von durch Registriermedien aufgenommenen Tönen (Musik) oder Bildern ist aber angesichts der technischen Entwicklung unhaltbar geworden. Neuere "Personal Digital Assistants" (PDA), d.h. elektronische Terminplaner im Westentaschenformat mit Datenverarbeitungsfunktionen (etwa Textverarbeitung, Rechner, Datenbank, E-Mail), verfügen über die Fähigkeit, Daten per Mobiltelephonteil über das Funknetz oder per Infrarotverbindung an einen beliebigen Computer zu übermitteln[41]. Gleiches gilt für neuere Mobiltelephone, die einen schnellen, ortsungebundenen Zugang ins Internet ermögli-

chen. Wozu vor 10 Jahren nur ein Computer in der Lage war, ist heute problemlos mit solchen Geräten möglich. Programmierte Mikroprozessoren sorgen für das Verarbeiten und Übermitteln von E-Mails oder EMS (Enhanced Messaging Service), d.h. die Verbreitung von Texten, Bildern, Gesprächen oder Musik. Mit WAP-Micro- oder HTML-Browsern ausgerüstet erlauben diese Mobiltelephone auch den Zugriff auf Web-Inhalte und Online-Services. Ausserdem können derzeit alle auf Speichermedien wie CDs, DVDs oder MDs festgehaltenen Photos, Videos, Filme, Musikstücke usw. sowohl von den herkömmlichen Abspielgeräten als auch von Computern "gelesen" und verarbeitet werden[42]. Bei allen angesprochenen Informationen besteht daher ein Zusammenhang

zu einer "Datenverarbeitungsanlage", weshalb sie heute richtigerweise unter den Datenbegriff der Computerstrafnormen zu fassen sind[43]. Dieser weite Datenbegriff korrespondiert mit der Formulierung der Art. 1 lit. b CCC, der keinerlei Beschränkungen auf "Schriftdaten" enthält.

2. Unrechtmässiger Zugriff (Art. 2 CCC)

Nach Art. 2 CCC haben die Vertragsparteien "den vorsätzlichen und unrechtmässigen Zugriff[44] auf das Ganze oder einen Teil eines Computersystems ... unter Strafe zu stellen". Einschränkend können sie dabei auf der Tatbestandsebene zusätzliche Merkmale vorsehen[45]: objektiv eine Tatbegehung "durch Verletzung von Sicherheitsmassnahmen" oder "in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist", subjektiv eine "Absicht, Computerdaten zu erlangen", oder eine "andere deliktische[46] Absicht". Darin spiegelt sich die Meinung des Expertenkomitees (PC-CY), wonach es den Vertragsparteien freigestellt bleiben soll, geringfügige und unbedeutende Fälle vom Anwendungsbereich der in den Artikeln 2 bis 10 CCC festgeschriebenen Straftatbestände auszunehmen[47]. Die Strafbestimmung des "unrechtmässigen Zugriffs" strebt eine einheitliche Kriminalisierung des Hackings auf internationaler

Ebene an. Der Zusatz "unrechtmässig" hebt hervor, dass die beschriebenen Tathandlungen unter bestimmten Umständen rechtmässig oder zumindest gerechtfertigt sein können[48]. Art. 2 CCC schützt das Rechtsgut der unbeeinträchtigten Verfügungsmacht

und Kontrolle der natürlichen oder juristischen Personen über ihre Computersysteme. Mit dem unrechtmässigen Zugriff ist dieses Interesse schon verletzt, weshalb der Tatbestand nicht etwa als abstraktes Gefährdungsdelikt aufzufassen ist[49]. Die Tathandlung besteht in einem Zugriff auf ein Computersystem, d.h. der Täter gelangt via öffentliche Telekommunikationsnetze, ein lokales Netzwerk oder - falls dies vom Vertragsstaat nicht ausgeschlossen wird - auch via Tastatur in das Computersystem. Dabei genügt es, wenn der Zugriff auf einen Teil des Systems erfolgt, z.B. auf die Ebene des Betriebssystems, auf Dateiverzeichnisse oder angeschlossene externe Speichermedien. Nicht notwendig ist dagegen, dass der Täter weitere Programmfunktionen in Gang setzt[50]. Die Gehilfenschaft zum unrechtmässigen Zugriff ist mit Strafe zu bedrohen, während das Übereinkommen keine Verpflichtung enthält, den Versuch zu kriminalisieren (Art. 11 Abs. 1 und 2 CCC).

Anders als die Strafgesetze Deutschlands und Österreichs enthält das schweizerische StGB eine spezielle Strafbestimmung gegen das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB), die in der gegenwärtigen Fassung mit Art. 2 CCC kompatibel erscheint[51]. Dennoch sollte die Gelegenheit nicht versäumt werden, zwei Ungereimtheiten in Art. 143bis StGB zu beseitigen. Einerseits sollte nicht vorausgesetzt werden, dass das Datenverarbeitungssystem "fremd" sein müsse, weil es nicht um die Sache, sondern um die Zugangsberechtigung geht[52], andererseits müsste die Einschränkung "ohne Bereicherungsabsicht" gestrichen werden, welche auf eine Fehlinterpretation der eidgenössischen Räte zurückgeht und eine Regelungslücke schafft[53].

Von grosser praktischer Relevanz ist dagegen die Abweichung in Bezug auf das Antragserfordernis. Art. 2 CCC sieht kein solches vor, so dass sich die Frage stellt, ob die Schweiz Art. 143bis StGB zu einem Offizialdelikt abändern muss, besteht doch ein enger Zusammenhang mit den im Übereinkommen vorgesehenen strafprozessualen Zwangsmassnahmen und der Verpflichtung zur Rechtshilfe. Nachdem der Strafantrag (Art. 28 ff. StGB) als Prozessvoraussetzung gilt[54], ist unbestritten, dass die Strafverfolgungsbehörden bei Inlandstaten erst dann einschreiten und insbesondere Zwangsmassnahmen ergreifen dürfen, wenn der Strafantrag vorliegt[55]. Ob ein nur nach dem Recht des ersuchten Staates erforderlicher Strafantrag Voraussetzung der Rechtshilfe sei, ist in der Schweiz umstritten[56]. Um Unsicherheiten auszuschliessen, aber auch weil das unbefugte Eindringen wie einleitend gesehen eine immer grössere Bedeutung erlangt hat, sollte der Tatbestand in ein Offizialdelikt überführt werden[57].

3. Unrechtmässiges Abfangen (Art. 3 CCC)

Art. 3 CCC sieht vor, dass "das vorsätzliche und unrechtmässige, mit technischen Mitteln ausgeführte Abfangen[58] nichtöffentlicher Computerdatenübertragungen an ein Computersystem, aus einem Computersystem oder innerhalb eines

Computersystems einschliesslich der elektromagnetischen Abstrahlungen von einem Computersystem, welches solche Computerdaten transportiert", unter Strafe zu stellen ist. Wie bei Art. 2 CCC kann eine Vertragspartei die Strafbestimmung zusätzlich einschränken auf die Tatbegehung "in deliktischer Absicht" oder "in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist"[59]. Aus dem erläuternden Bericht geht hervor, dass diese Strafnorm das Recht der Kommunikationsteilnehmer auf Nichtöffentlichkeit der Datenübermittlung schützen soll, wodurch das in Art. 8 Abs. 1 EMRK verankerte Recht auf Achtung der Korrespondenz bezüglich aller Formen der Datenübertragung (Telephon, Fax, E-Mail, File Transfer) umgesetzt wer-

de[60]. Die Formulierung von Art. 3 CCC lässt bedauerlicherweise erhebliche Zweifel darüber aufkommen, ob mit dem unrechtmässigen Abfangen auch das unrechtmässige Ausspähen *gespeicherter*, d.h. im Moment der Tathandlung nicht in Übermittlung befindlicher Daten erfasst werden soll[61]. Die Ausführungen des erläuternden Berichts zum geschützten Rechtsgut und die Bezeichnung des Angriffsobjekts mit "Computerdaten*übertragungen*" sprechen eindeutig dagegen. Note 53 des erläuternden Berichtes, welche den Begriff der "technischen Mittel" näher darlegt, besagt demgegenüber, dass diese sich bezögen auf "das Abhören, Kontrollieren oder Überwachen des Kommunikationsinhaltes, *das Beschaffen des Inhalts von Daten*, entweder *direkt durch den Zugriff und die Benutzung des Computersystems* oder indirekt durch die Benutzung von elektronischen Abhör- oder Abfanggeräten"[62]. Der Einbezug des Ausspähens abgespeicherter Daten liesse sich allenfalls auf die Tatsache gründen, dass der direkte Zugriff des Täters auf die Festplatte eines Computers und die programmgesteuerte Ausführung einer Abfragefunktion immer auch eine Datenübermittlung "innerhalb des Computersystems" auslöst, d.i. eine Datenübertragung im

Bus[63], welche er gleichzeitig "abfängt". Überzeugend ist das aber nicht, denn der Begriff "Abfangen" impliziert eine vom Berechtigten oder von Dritten, jedenfalls nicht vom Täter ausgelöste Datenübermittlung. Eindeutig nicht vom Regelungsbereich des Art. 3 CCC erfasst sind die auf externen Datenträgern wie Disketten, CDs oder DVDs abgespeicherten Daten, solange sie nicht über ein Laufwerk direkt in einem Computersystem abrufbar sind. Nachdem auch die weiteren Artikel 4 bis 10 CCC keinen strafrechtlichen Schutz *abgespeicherter* Daten vorsehen, können die Vertragsparteien diese empfindliche Regelungslücke wohl nur durch eine freiwillige Erweiterung der innerstaatlichen Strafbestimmungen auf das unrechtmässige Ausspähen aller, also auch gespeicherter Daten verhindern.

Die Einschränkung auf "nichtöffentliche Computerdatenübertragungen" bedeutet nicht, dass nur Kommunikation erfasst werden solle, die aufgrund ihres Inhaltes geheim ist

(Intim-, Amts-, Berufsgeheimnis u.a.); das Merkmal bezieht sich vielmehr auf die Nichtöffentlichkeit des Übertragungsvorganges selbst. Wenn also jemand per Modem via Telephonnetz eine Verbindung zu seinem Access-Provider herstellt, um öffentlich zugängliche Informationen auf dem World Wide Web - z.B. das Tageswetter - abzurufen, ist das gleichwohl eine nichtöffentliche Übertragung, weil die Tatsache, ob und welche Informationen übermittelt werden, ebenfalls geschützt wird[64]. Eine wichtige Klarstellung enthält der erläuternde Bericht auch bezüglich der Kommunikation von Firmenangehörigen (E-Mail, Internetnutzung). Auch diese ist grundsätzlich "nichtöffentlich", so dass die Vertragsparteien dafür zu sorgen haben, dass eine unrechtmässige Überwachung durch den Arbeitgeber kriminalisiert wird[65]. Die Tathandlung ist sehr weit gefasst und

fordert insbesondere kein "Beschaffen" oder "Verschaffen"[66], sondern ein blosses "Abfangen". Damit wird verdeutlicht, dass es sich nicht um eine Parallelnorm zum Diebstahl handeln soll, welche die Schaffung einer gewahrsamsähnlichen Stellung beim Täter voraussetzen würde, sondern wie gesehen um eine Verletzung des formellen[67] Kommunikationsgeheimnisses. Wenn es aber um dieses Rechtsgut geht, muss zur Vollendung die blosse Wahrnehmung durch den Täter oder einen Dritten genügen. Immerhin dürfte der technische Abfangeingriff für sich - ohne diese Wahrnehmung - nicht ausreichen bzw. nur als Versuch strafbar sein, weil damit erst eine Gefährdung des Kommunikationsgeheimnisses einherginge.

Bei der Umsetzung des Übereinkommens ist besonders darauf zu achten, dass Art. 3 CCC keine Einschränkung auf "besonders gesicherte Daten"[68] zulässt. Die Vertragsparteien dürfen somit den strafrechtlichen Schutz nicht (mehr) von einer Datensicherung, etwa einer Verschlüsselung der E-Mails, abhängig machen. Hinsichtlich der Computerdatenübertragung ist diese Lösung auch vorzuziehen, weil Daten ungleich einer Postkarte per definitionem nie unmittelbar einsehbar sind. Wer aber schon besondere Anstrengungen unternimmt, um mit Lauschprogrammen oder anderen Hilfsmitteln den Datenaustausch abzufangen, soll nicht noch zusätzlich mit Straffreiheit belohnt werden,

wenn die Daten unverschlüsselt unterwegs sind. Die Gehilfenschaft zum unrechtmässigen Abfangen ist mit Strafe zu bedrohen, ebenso der Versuch (Art. 11 Abs. 1 und 2 CCC)[69].

Da es im schweizerischen StGB keine mit Art. 3 CCC identische Regelung gibt, erweist sich die Abklärung des Anpassungsbedarfs schwieriger als bei Art. 2 CCC. Mehrere Strafnormen des StGB und Nebenstrafrechts sorgen zumindest teilweise für einen Art. 3 CCC entsprechenden Schutz, ohne die Vorgaben jedoch gänzlich einzulösen.

Bei Art. 143 StGB erweist sich zunächst schon die Grundkonzeption als "Datendiebstahl" als hinderlich. Das geschützte Rechtsgut der unbefugten Datenbeschaffung ist ein "... - zivilrechtlich vorerst nicht näher zu klassifizierende[s] - Verfügungsrecht über Computerdaten, ein Immaterialgüterrecht eigener Art"[70].

Schwarzenegger — Festschrift Trechsel, S. 321

Einbezogen wird auch das Verfügungsrecht über völlig wertlose Daten. Verlangt das Gesetz aber subjektiv neben dem Vorsatz noch eine Absicht zur unrechtmässigen Bereicherung, dann enfällt der Schutz dieses Verfügungsrechts in vielen Fällen gänzlich[71]. Zwar könnte man diskutieren, ob man die "Absicht zur unrechtmässigen Bereicherung" als einen Unterfall der in Art. 3 CCC als Einschränkung anerkannten "deliktischen Absicht" ansehen darf, in Anbetracht des zu schützenden Rechtsgutes aber gehört dieses subjektive Tatbestandsmerkmal zweifellos aus Art. 143 StGB entfernt.

Wollte man Art. 143 StGB so ausgestalten, dass er alle Fälle von Art. 3 CCC erfasst, müsste man im objektiven Tatbestand einerseits noch die "besondere Sicherung gegen seinen unbefugten Zugriff" streichen[72] und andererseits neu die elektromagnetischen Abstrahlungen von einem Computersystem der Datenübermittlung gleichstellen. Bei näherer Analyse zeigt sich jedoch, dass das von Art. 3 CCC ins Auge gefasste Rechtsgut - soweit sich dieses überhaupt klar fassen lässt (siehe oben) - nicht mit jenem von Art. 143 StGB identisch ist. Der Verweis auf Art. 8 Abs. 1 EMRK[73] zeigt, dass es nicht um

den Kommunikationsinhalt - die Daten - geht, sondern um die Vertraulichkeit der nicht-öffentlichen Computerdatenübertragung an sich: ein Rechtsgut, dass sich aus dem Grundrecht des Fernmeldegeheimnisses herleitet[74]. Obschon daraus eine staatliche Schutzpflicht auch gegen Eingriffe Privater hervorgeht[75], ist der strafrechtliche Schutz des Fernmeldegeheimnisses in der Schweiz fragmentarisch und daher ungenügend.

Dies sei sogleich am Beispiel der E-Mail-Kommunikation illustriert: Der naheliegende Schutz der elektronischen Post durch Art. 179 StGB (Verletzung des Schriftgeheimnisses) scheitert schon daran, dass Daten, solange sie nicht

ausgedruckt vorliegen[76], nicht als Schriften gelten. Art. 143 Abs. 1 StGB ist grundsätzlich anwendbar und schützt sowohl Datenpakete in der Übermittlungsphase als auch die gespeicherten Nachrichten in der Mailbox auf dem Mail-Server des Nutzers. Häufig wird die Anwendung von Art. 143 StGB daran scheitern, dass die Daten während der Übertragung nicht besonders gegen Zugriffe gesichert sind[77], noch häufiger wohl am Fehlen des subjektiven Merkmals der Absicht zur unrechtmässigen Bereicherung. Eine Strafbarkeit nach Art. 143bis StGB ist beschränkt auf das Eindringen in ein Computersystem, womit nur der Zugriff auf die Mailbox des Nutzers erfasst werden kann[78]. Die Verletzung des Post- und Fernmeldegeheimnisses (Art. 321ter StGB) schliesslich ist als echtes Sonderdelikt ausgestaltet, weshalb sich nur jene strafbar machen können[79], die als Verantwortliche oder Hilfspersonen Post- oder Fernmeldedienste erbringen. Diese Strafbestimmung entspricht daher nicht der Regelung von Art. 3 CCC, obschon das Fernmeldegeheimnis sowohl Inhaltsdaten als auch Verbindungs(rand)daten aller fernmeldetechnischer Übertragungen inklusive der Internet-Dienste umfasst[80]. Weitere relevante Straftatbestände[81] haben ebenfalls einen engeren Anwendungsbereich, so dass sie keinen generellen Schutz von E-Mail-Nachrichten gewährleisten können.

Welche Lösung ist erstrebenswert? Am sinnvollsten erscheint die Ergänzung von Art. 321ter StGB um einen Absatz, der die Verletzung des Fernmeldegeheimnisses durch beliebige Personen unter Strafe stellt. Dieser Absatz könnte sich an Art. 3 CCC orientieren, müsste aber weiter gefasst werden, um alle fernmeldetechnischen Datenübertragungen einzuschliessen (vgl. Art. 3 lit. c FMG). Als qualifizierte Varianten könnten die jetzigen Absätze bestehen bleiben. In dieser Form hätte die Bestimmung nichts mehr im achtzehnten Titel über die Amts- und Berufspflichten zu suchen, sondern sollte im dritten Titel hinter die Verletzung des Schriftgeheimnisses (Art. 179 StGB) plaziert werden. Je nachdem wie weit man den "Auftrag" von Art. 3 CCC auslegt, müssten auch an Art. 143 StGB die schon erwähnten Änderungen vorgenommen werden. Notwendig erscheint zumindest die Anpassung hinsichtlich der in Übertragung befindlichen Computerdaten (Wegfall der besonderen Sicherung und der Absicht zur unrechtmässigen Bereicherung) und die Ausdehnung der unbefugten Datenbeschaffung auf elektromagnetische Abstrahlungen, die nicht von der Strafnorm zum Schutze des Fernmeldegeheimnisses erfasst werden.

IV. Schluss

Ein Bedarf an internationaler Harmonisierung der materiellen Strafnormen des Computer- und Internetstrafrechts ist ausgewiesen. Die Convention on Cybercrime macht einen wichtigen ersten Schritt in diese Richtung. Die Detailanalyse der Vorschriften über die Vertraulichkeit der Computerdaten und -systeme lässt erkennen, das die praktische Umsetzung der Vorgaben in das innerstaatliche Strafrecht nicht leicht fällt. Selbst für das Hacking, die unbefugte Datenbeschaffung und die Verletzung des Fernmeldegeheimnisses, gegen die es im schweizerischen StGB schon spezifische Strafbestimmungen gibt, resultieren Anpassungspflichten aus der Convention on Cybercrime. Als hinderlich erweist sich die Grundkonzeption einer Parallelität zwischen Eigentums- und Computerdelikten. Die anstehende Gesetzesrevision sollte daher genutzt werden, die aufgezeigten

Ungereimtheiten der Computerstraftatbestände des geltenden StGB auszuräumen und die Normen in einen systematisch passenden Kontext zu stellen. Weitere schwierige Aufgaben stehen dem schweizerischen Gesetzgeber im Bereiche der strafprozessualen Anpassungen an die Convention on Cybercrime bevor.

Fussnoten:

[1] Siehe die Meldung in Tages-Anzeiger, Ohne Internet läuft nichts mehr, 28. Januar 2002, 25.

[2] Tages-Anzeiger (FN 1), 25, Quelle: Netzreport des Instituts für Wirtschaftsinformatik an der Universität Bern 2001. Weiterführend mit internationalem Vergleich Jonathan Coppel, E-Commerce: Impacts and policy challenges, OECD Economics Department Working Papers No. 252, Paris 2000.

[3] “Business to business", vgl. dazu Coppel (FN 2), 25: "The largest share of e-commerce takes place between businesses (at present, they account for 70 to 85 per cent of all electronic sales) and B2B e-commerce is expected to experience more rapid progression than B2C over the next few years."

[4] Zwischen 50 und 60% haben in diesen Ländern einen privaten Internetanschluss. In der Schweiz liegt dieser Anteil mit ca. 43% noch deutlich über Deutschland (ca. 35%), Italien (ca. 34%), Frankreich (ca. 22%) und Spanien (ca. 20%). Quelle: Nielsen/Netratings zit. nach Tages-Anzeiger, Internet-Gesellschaft, 16. Juni 2001, 47. Vgl. zu den Schätzungsmethoden Wolfram Gieseke, Anti-Hacker Report, Düsseldorf 2001, 560 ff.

[5] BBl 2001, 6401 ff. Vorgesehen sind die Förderung des E-Voting, d.h. des gezielten Einsatzes elektronischer Mittel zur Erleichterung der Ausübung politischer Rechte, die Erleichterung der Meinungsbildung der Stimmberechtigten durch elektronische Angebote seitens der Bundeskanzlei und die Schaffung der Rechtsgrundlagen für Pilotprojekte zur elektronischen Stimmabgabe.

[6] Ein Überblick über die Erscheinungsformen der Internetkriminalität findet sich bei Ursula Widmer/Konrad Bähler, Rechtsfragen beim Electronic Commerce, Sichere Geschäftstransaktionen im Internet, 2. Aufl., Zürich 2000, 292 ff.; Christian Schwarzenegger, E-Commerce - Die strafrechtliche Dimension, in: Internet-Recht und Electronic Commerce Law, hrsg. von Oliver Arter/Florian S. Jörg, Lachen und St. Gallen 2001, 333 ff.; Rolf H. Weber, E-Commerce und Recht, Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, Zürich 2001, 538 ff.

[7] Quelle: BSA zit. nach Tages-Anzeiger, Internetpiraterie, 19. März 2001, 59. Dabei war das Vorgehen der deutschen Behörden besonders energisch (533 Fälle), gefolgt von Grossbritannien (70 Fälle) Österreich (63 Fälle) und den Niederlanden (27 Fälle). In der Schweiz wurden 11 Websites mit illegalen Softwarekopien geschlossen.

[8] Zur Analyse der Strafbarkeit nach dem geltenden Recht Schwarzenegger (FN 6), 365 ff.; Rolf H. Weber/Roland Unternährer, Wirtschaftsterrorismus im Internet, in: Wirtschaft und Strafrecht, Festschrift für Niklaus Schmid, hrsg. von Jürg-Beat Ackermann/Andreas Donatsch/Jörg Rehberg, Zürich 2001, 375 ff.

[9] Die entsprechenden Taten sind folglich nach dem Jugendstrafrecht zu beurteilen, vgl. zu den US-amerikanischen Erfahrungen Joseph V. De Marco, It's Not Just Fun and "War Games" - Juveniles and Computer Crime, USA Bulletin May 2001, abrufbar unter: www.cybercrime.gov/usamay20017.htm (Stand: 27.2.2002).

[10] Tages-Anzeiger, Der Hacker-Chef grüsst Daniela, 17. Januar 2002, 12.

[11] Das sich im Mai 2000 weltweit verbreitende"I Love You" Virus soll nach Schätzungen der Swiss Re innert kürzester Zeit einen Schaden mehr als $ 1 Mia. verursacht haben, vgl. Swiss Re, National catastrophes and man-made disasters in 2000, sigma No. 2/2001, 7. Andere Quellen sprechen gar von einem wirtschaftlichen Schaden von $ 17 Mia., Tages-Anzeiger, Antiviren rentieren, 21. Januar 2002, 53.

[12] Tages-Anzeiger, Vertrauliches von der FDP, 19. Januar 2002, 9.

[13] Tages-Anzeiger, Von Würmern und tanzenden CEOs, 24. Dezember 2001, 49: "Das Jahr des Wurms".

[14] Vgl. dazu das EU-Aktionsprogramm "eEurope 2002 - An information society for all", Mitteilung der Kommission zur Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, KOM(2000) 890, abrufbar unter: http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComEN.pdf (Stand: 17.2.2002).

[15] 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).

[16] 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.

[17] 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). Am 24. April 2001 wurde der Entwurf der Convention on Cybercrime von der Parlamentarischen Versammlung des Europarates diskutiert und angenommen. Dabei kam es zu Kritik an den schwerwiegenden Eingriffe in die Freiheitsrechte; ausserdem wurde eine Strafnorm zur Bekämpfung der Verbreitung von rassistischer und fremdenfeindlicher Propaganda gefordert. Da aber eine solche Strafnorm die Ratifikation einiger Staaten (insbesondere der USA) gefährdet hätte, fanden sich die Parlamentarier mit dem Vorschlag des Berichterstatters ab, sofort ein Zusatzprotokoll zur CCC zu erarbeiten, das unter dem Titel "Erweiterung des Anwendungsbereichs der Konvention zur Erfassung neuer Arten von Straftaten" die Verbreitung von rassistischer Propaganda, den Menschenhandel via Internet und die Funktionsbeeinträchtigung von Computersystemen durch Spamming (unaufgeforderte Werbemails) definieren und kriminalisieren soll. Council of Europe, Parliamentary Assembly, Draft Convention on Cyber-crime, Opinion No. 226 (2001); vgl. Neue Zürcher Zeitung, Europarat berät Computerkriminalität, 9. März 2001, 83.

[18] Siehe zu den Vorbereitungsarbeiten: Explanatory Report (FN 17), N 7 ff.

[19] Stand: 27.2.2002 (bisher keine Ratifikation).

[20] Kapitel II Abschnitt 1. Neben den im nächsten Abschnitt behandelten Delikten definiert das Übereinkommen auch den Eingriff in die Datenintegrität (Art. 4 CCC), den Eingriff in die Systemintegrität (Art. 5 CCC), den Missbrauch von Vorrichtungen (Art. 6 CCC), die Computerurkundenfälschung (Art. 7 CCC), den 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 dieser Abschnitt 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.

[21] 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 Computerviren 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.

[22] Dazu eingehend Christian Schwarzenegger, Der räumliche Geltungsbereich des Straf-

rechts im Internet. Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 118 (2000) 117 ff.; ders., (FN 6), 337 ff. m.w.N.

[23] Kapitel III.

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

[25] Ausführlicher Explanatory Report (FN 17), N 315 ff.

[26] Fassung gemäss BG vom 17.6.1994, in Kraft seit 1.1.1995; vgl. Botschaft über die Änderung des Schweizerischen Strafgesetzbuches und des Militärstrafgesetzes (Strafbare Handlungen gegen das Vermögen und Urkundenfälschung), BBl 1991 II 969 ff.

[27] Die Begriffe Datennetz und Datennetzkriminalität sind weiter gefasst als Internet und Internetkriminalität. Erstere umfassen auch Local Area Networks (LAN) oder Wide Area Networks (WAN) sowie Intra- und Extranets, die ein in sich geschlossenes Computernetz - meist in einem Unternehmen - auf der Basis der Internetprotokolle darstellen, Meyers Lexikonredaktion (Hrsg.), Duden Informatik. Ein Fachlexikon für Studium und Praxis, 3. Aufl., Mannheim u.a. 2001, 311 und 544 ff. einführend zu Rechnernetzen.

[28] Insbes. die Artikel 143, 143bis, 144bis, 147, 150 ("Zeitdiebstahl"), 251 i.V.m. 110 Ziff. 5 StGB (Fälschung von Datenurkunden), s.a. Office fédéral de la justice, Rapport national de la Suisse sur la prévention et la lutte contre la cybercriminalité, Conférence sur la Cybercriminalité, Budapest, 22 novembre 2001.

[29] So der völlig berechtigte Einwand von Stefan Trechsel, Schweizerisches Strafgesetzbuch, Kurzkommentar, 2. Aufl., Zürich 1997, Art. 143 N 1.

[30] Entsprechende Daten aus der Polizeilichen Kriminalstatistik Deutschlands belegen eine steigende Tendenz, vgl. BT-Dr. 14/6321, 5 f. (Antwort der Bundesregierung auf eine Grosse Anfrage "Wirksamer Schutz vor Computerattacken"). Entsprechende Verurteilungen sind dagegen sehr selten, BT-Dr. 14/6321, 8 ff. Vgl. dazu Frankfurter allgemeine Zeitung, Gezielte Angriffe von Computer-Hackern schrecken die Unternehmen auf, 11. Februar 2002, 24.

[31] Vgl. auch die Befragungsresultate in KPMG (Hrsg.): 2001 global e.fr@ud.survey, o.O. 2001, abrufbar unter: www.kpmg.de/library/surveys/ (Stand: 27.2.2002).

[32] Ohne Bezug auf das Übereinkommen hält Laurent Moreillon, Les nouveaux délits informatiques sur Internet, Medialex 7 (2001) 21 ff., das schweizerische Computerstrafrecht für revisionsbedüftig.

[33] Diese und die unten folgenden Übersetzungen des Verfassers basieren auf dem englischen und französischen Originaltext. Die vollständige deutsche Übersetzung der Art.

1-6, 11 und 13 CCC kann abgerufen werden unter: www.rwi.unizh.ch/schwarzenegger/home.htm (Stand: 18.3.2002).

[34] Explanatory Report (FN 17), N 22.

[35] Vgl. Philip E. Margolis, Computer & Internet Dictionary, 3. ed., New York 1999, 134. Zum menschlichen Gedächtnis Daniel L. Schacter, Searching for memory, New York 1996, 39 ff.

[36] Ebenso Art. 144bis Ziff. 1 Abs. 1 StGB.

[37] Botschaft (FN 26), 988; Marcel A. Niggli, Das Verhältnis von Eigentum, Vermögen und Schaden nach schweizerischem Strafgesetz, Zürich 1992, 186 ff.; Niklaus Schmid, Zu den Begriffen der Daten, der Datenverarbeitung und der Datenverarbeitungsanlage im neuen Vermögens- und Urkundenstrafrecht, ZStrR 110 (1992) 320 ff.; ders., Computer- sowie Check- und Kreditkarten-Kriminalität, Zürich 1994, § 2 N 7 ff.; Jörg Rehberg/Niklaus Schmid, Strafrecht III. Delikte gegen den Einzelnen, 7. Aufl., Zürich 1997, 144; Trechsel (FN 29), Art. 143 N 3.

[38] Z.B. als Ausdruck, Strichcode oder früher als Lochkarte.

[39] Schmid (FN 37), § 2 N 19. Vorausgesetzt sei demnach "das Erbringen einer - hinsichtlich Schwierigkeit der zu registrierenden, zu verarbeitenden und als Resultat zu erfassenden und gegen aussen abzugebenden Daten - qualifizierten Arbeitsleistung." Keine Datenverarbeitungsanlagen wären damit "elektronische Bauteile" in Automaten und ähnlichen Geräten.

[40] Nicht als solche zu betrachten wären z.B. Telephone, Faxgeräte, Waren- und Dienstleistungsautomaten, Ladenkassen, Mess-, Kontroll- und Steuergeräte usw., solange sie nicht mit einer Datenverarbeitungsanlage verbunden sind, siehe eingehend Schmid (FN 37), § 2 N 48 ff.

[41] Die neueste Gerätegeneration verbindet Handy und PDA-Funktionen, vgl. Spiegel Online, Halb Handy, halb PDA, 5. März 2002, abrufbar unter: www.spiegel.de/netzwelt/technologie/0,1518,183613,00.html (Stand: 8.3.2002).

[42] Vgl. dazu exemplarisch den Digital Hub auf iMac Computern von Apple, welcher die Bearbeitung und Verwaltung von Photos, DVDs, Musik, Filmen und anderen multimedialen Dokumenten erlaubt: www.apple.com/imac/digitalhub.html (Stand: 8.3.2002).

[43] Die Speicherung von Texten, Bildern, Tönen usw. erfolgt in binärer Codierung, die letztlich zu Zeichenfolgen über dem zweielementigen Zeichenvorrat {0, 1} führt. Ein enger Datenbegriff, der derart registrierte Gespräche, Musik oder Bilder ausschliesst, ist nicht mehr zeitgemäss, anders noch Schmid (FN 37), § 2 N 47, und insbesondere Rehberg/Schmid (FN 37), 145. Überschneidungen mit Art. 179bis StGB (z.B. bei der Internet- oder Mobiltelephonie) sind möglich, zweifelnd Günter Stratenwerth, Schweizerisches

Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 5. Aufl., Bern 1995, § 14 N 25, ebenso mit Art. 67 URG, Art. 29 i.V.m. Art. 3 ff. UWG oder mit Art. 179^{novies} StGB. Sie sind ein Problem der Konkurrenzlehre.

[44] "Access" wird in der Informatik mit "Zugriff" übersetzt, vgl. George Kurtz/Stuart McClure/Joel Scambray, Das Anti-Hacker-Buch, Bonn 2000, 269 f. (Remote- oder Fernzugriff) und 302 (lokaler Zugriff); Meyers Lexikonredaktion (FN 27), 166.

[45] Eine entsprechende Erklärung ist bei der Ratifikation schriftlich abzugeben, vgl. Art. 40 CCC.

[46] "Dishonest intent" bzw. "intention délictueuse".

[47] Explanatory Report (FN 17), N 37 und N 49 speziell zu Art. 2 CCC.

[48] Explanatory Report (FN 17), N 38 und 47, insbesondere entfällt schon die Tatbestandsmässigkeit bei Zugriffen zur Prüfung der Sicherheit eines Computersystems, falls ein Einverständnis des Berechtigten vorliegt, oder bei Zugriffen auf Computersysteme, die für einen freien Zugriff von Dritten eingerichtet werden (z.B. Fileserver).

[49] Zur entsprechenden Schweizer Strafnorm, siehe Trechsel (FN 29), Art. 143bis N 1 f. m.N.; zu Recht hält Trechsel (FN 29), Art. 143bis N 2 die Einordnung bei den Vermögensdelikten für nicht gerechtfertigt.

[50] Explanatory Report (FN 17), N 44 ff.

[51] Wird Art. 143bis StGB in der derzeitigen Fassung belassen, müsste die Schweiz bei der Ratifikation eine Erklärung i.S.v. Art. 40 CCC abgeben, dass sie den Straftatbestand des unrechtmässigen Zugriffs durch zusätzliche, nach Art. 2 CCC zulässige Merkmale einschränke. "Auf dem Wege einer Datenübertragungseinrichtung" schliesst nach h.L. den Zugriff via Tastatur aus, vgl. Schmid (FN 37), § 5 N 23; Trechsel (FN 29), Art. 143bis N 7; "gegen seinen Zugriff besonders gesichert" schränkt den Schutzbereich objektiv auf Computersysteme mit Zugangssicherung ein, dazu Schmid (FN 37), § 4 N 28 ff.; Trechsel (FN 29), Art. 143 N 6. Während das erste Merkmal den Schutz der unbeeinträchtigten Verfügungsmacht und Kontrolle unnötig schwächt, was auch durch andere Straftatbestände wie Hausfriedensbruch nicht kompensiert wird (man denke z.B. an Laptop-Computer, anders noch Schmid [FN 37], § 5 N 23), lässt sich mit Blick auf die Verhältnismässigkeit des Mitteleinsatzes diskutieren, ob auch völlig ungesicherte Computersysteme strafrechtlich vor unrechtmässigen Zugriffen geschützt werden sollen.

[52] Stratenwerth (FN 43), § 14 N 38; Trechsel (FN 29), Art. 143bis N 4.

[53] Trechsel (FN 29), Art. 143bis N 10, "höchst unglückliche Formulierung"; s.a. Schmid (FN 37), § 5 N 27 ff.; José Hurtado Pozo, Droit pénal, Partie spéciale I, Infractions contre la vie, l'intégrité corporelle et le patrimoine, 3e éd., Zürich 1997, 255; Rehberg/Schmid (FN 37), 151 f.

[54] Vgl. Niklaus Schmid, Strafprozessrecht. Eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes, 3. Aufl., Zürich 1997, 152; Robert Hauser/Erhard Schweri, Schweizerisches Strafprozessrecht, 4. Aufl., Basel u.a. 1999, § 41 N 10.

[55] Vgl. § 24 Abs. 1 ZH-StPO; Art. 101 Abs. 2 BStP. In dringenden Fällen können vor der Stellung des Antrages sichernde Massnahmen getroffen werden, § 24 Abs. 2 ZH-StPO; Art. 101 Abs. 2 BStP.

[56] Gestützt auf Art. 35 Abs. 2 IRSG verneinend Robert Zimmermann, La coopération judiciaire internationale en matière pénale, Bern 1999, 274 f. m.H. auf einen unveröffentlichten BGE; bejahend Peter Popp, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel u.a. 2001, 182 mit Differenzierungen; offengelassen in BGE 78 I 47 f. m.N. zur älteren Literatur. Zum Teil gelten besondere staatsvertragliche Bestimmungen, vgl. BGE vom 7. Februar 2002 (1A.203/2001/sch) E. 1 f.

[57] Der unrechtmässige Zugriff auf ein Computersystem eines Angehörigen oder Familiengenossen könnte dann in einem neu zu schaffenden Abs. 2 immer noch dem Antragserfordernis unterstellt werden.

[58] Die wörtliche Übersetzung von "interception" lautet "Abfangen" oder "Unterbrechen"; der Begriff wird daneben auch mit "Abhören", "Überwachen" oder "Sniffen" ins Deutsche übertragen. Nachdem im Strafprozessrecht der Begriff "Überwachung" für das Abfangen der Telekommunikation inklusive Internetübertragung üblich ist (vgl. Art. 179^{octies} StGB; Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF], SR 780.1; s.a. Art. 21 CCC "Interception of content data", Überwachung von Inhaltsdaten), wäre es sinnvoll, von "unrechtmässiger Überwachung" zu sprechen. Dem steht jedoch entgegen, dass die bisher mit dem Begriff Überwachung assoziierte Übertragung von Telephongesprächen nach h.L. gerade nicht als *Daten*-Übertragung angesehen wird. Siehe FN 40.

[59] Diesfalls muss die Vertragspartei bei der Ratifikation eine entsprechende Erklärung abgeben (Art. 40 CCC).

[60] Explanatory Report (FN 17), N 51.

[61] Die Begriffe der Speicherung und Übermittlung werden sowohl im schweizerischen als auch im deutschen StGB deutlich voneinander unterschieden. Vgl. Schmid (FN 37), § 5 N 27 ff.; Trechsel (FN 29), Art. 143 N 3 f., und zum dStGB Roland Schmitz, Ausspähen von Daten, § 202a StGB, JA 27 (1995) 480 f.; Wolfgang Bär, Computerkriminalität und EDV-Beweissicherung, in: Handbuch des Wirtschafts- und Steuerstrafrechts, hrsg. von Heinz-Bernd Wabnitz/Thomas Janovsky, München 2000, 1124 f.: "Gespeichert sind Informationen, wenn sie auf einem körperlichen Trägermedium aufgenommen oder aufbewahrt sind. Geschützt werden sollen damit alle Formen der Verkörperung von Daten. ... Eine Übermittlung liegt demgegenüber vor, wenn Daten von einer speichernden Stelle

weitergegeben oder auf dem eigenen Rechner zum Abruf bereitgehalten werden. Gemeint sind damit aber auch die während des Übermittlungsvorganges über die Datennetze übertragenen Informationen ..." S.a. Gunther Arzt/Ulrich Weber, Strafrecht, Besonderer Teil, Lehrbuch, Bielefeld 2000, 215 f.; Theodor Lenckner, in: Adolf Schönke/Horst Schröder, Strafgesetzbuch, Kommentar, 26. Aufl., München 2001, § 202a N 8.

[62] Explanatory Report (FN 17), N 53. Übersetzung und Hervorhebung durch den Verfasser.

[63] Der Bus ist eine Sammelleitung zur Datenübertragung zwischen mehreren Funktionseinheiten (CPU, Speicher, Peripheriegeräte) innerhalb eines Computers, ausführlicher Meyers Lexikonredaktion (FN 27), 166 ff. und 725 f. Auch die Datenübertragung zwischen CPU und Tastatur soll erfasst sein, Explanatory Report (FN 17), N 55.

[64] Nicht inhalts-, sondern intentionsbestimmter Geheimnisschutz. Nicht darunter fallen daher Radio und Fernsehen, vgl. Wolfgang Wessely, Das Fernmeldegeheimnis - ein unbekanntes Grundrecht? ÖJZ 54 (1999) 492.

[65] Explanatory Report (FN 17), N 54. Kontrollen durch den Arbeitgeber sind zulässig und damit nicht "unrechtmässig", wenn sie die Eignung des Arbeitnehmers für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind (Art. 328b OR). Dazu Adrian von Kaenel, Internet und Datenschutz am Arbeitsplatz, in: Geschäftsplattform Internet II. Rechtliche und praktische Aspekte, hrsg. von Rolf H. Weber/Reto M. Hilty/Rolf Auf der Maur, Zürich 2001, 21 ff.; s.a. Eidgenössischer Datenschutzbeauftragter, Leitfaden über Internet- und E-Mail-Überwachung am Arbeitsplatz, Für öffentliche Verwaltung und Privatwirtschaft, Bern 2001, abrufbar unter: www.edsb.ch/d/doku/leitfaeden/internet/internet.pdf (Stand: 15.3.2002). Die geltenden Strafbestimmungen StGB (Art. 143, 143bis 179 ff., 321ter StGB) sind auf solche Fälle in der Regel nicht anwendbar. Vgl. zur möglichen Strafbarkeit der Überwachung und Kontrolle von Arbeitnehmern nach dem Arbeitsgesetz (SR 822.11): Art. 26 ArGV 3 i.V.m. Art. 59 Abs. 1 lit. a und Art. 60 Abs. 1 ArG.

[66] Die Reichweite dieser Begriffe ist sowohl in der schweizerischen wie auch der deutschen Lehre umstritten, zusammenfassend Trechsel (FN 29), Art. 143 N 7, und Lenckner (FN 61), § 202a N 10 beide m.w.N.

[67] Geschützt ist also das Recht, andere von der Kenntnisnahme der Daten auszuschliessen, selbst wenn die übermittelten Informationen an sich nicht geheim sind.

[68] Im Gegensatz zu Art. 143 Abs. 1 StGB ("Daten, die ... gegen seinen unbefugten Zugriff besonders gesichert sind") bzw. § 202 Abs. 1 dStGB ("Daten, die ...gegen unberechtigten Zugang besonders gesichert sind").

[69] Erklärt eine Vertragspartei einen Vorbehalt bezüglich Art. 11 Abs. 2 CCC kann sie auf eine Kriminalisierung des Versuches im innerstaatlichen Recht verzichten, Art. 11 Abs. 3 i.V.m. Art. 42 CCC.

[70] Treffend Stratenwerth (FN 43), § 14 N 22 und N 27; ähnlich Trechsel (FN 29), Art. 143 N 2. Ungleich des Eigentums an Sachen (Art. 641 ZGB), existiert im Zivilrecht keine lückenlose Regelung der "Berechtigung an immateriellen Daten". Informationen in der Form von personenbezogenen Daten (Datenschutzrecht), Geheimnissen (Persönlichkeitsrecht, Firmenrecht, Bankenrecht) oder Werken, Marken usw. (Immaterialgüterrecht) werden partikulär geschützt. Soweit Daten nicht in diese Kategorien fallen, besteht an ihnen zwar ein ungeschriebenes persönliches Recht. Dieses ist aber mangels Schutzrechtscharakters gegenüber Dritten nicht durchsetzbar.

[71] Trechsel (FN 29), Art. 143 N 8 mit Beispiel.

[72] Siehe oben bei FN 68.

[73] In der Praxis des EGMR ist der Fernmeldeverkehr sowohl dem Privatleben als auch dem Briefverkehr zuzurechnen, Eur. Court HR, Klass and others v. Germany judgment of 6 September 1978, Series A no. 28; vgl. Wessely (FN 64), 491.

[74] In der Schweiz aus Art. 13 Abs. 1 BV, vgl. Art. 43 ff. FMG.

[75] Vgl. Wessely (FN 64), 467 m.H. auf die ständige Rechtsprechung des EGMR zu Art. 8 und 11 EMRK. Bei grundlegenden Werten kann der Erlass strafrechtlicher Normen geboten sein. Die neue Bundesverfassung anerkennt, dass die Grundrechte auch unter Privaten wirksam werden, "soweit sie sich dazu eignen", Art. 35 Abs. 3 BV. Zum Stand der verfassungsrechtlichen Diskussion siehe Ulrich Häfelin/Walter Haller, Schweizerisches Bundesstaatsrecht, 5. Aufl., Zürich 2001, 87 ff.

[76] Schmid (FN 37), § 4 N 110 f.; Stratenwerth (FN 43), § 12 N 5; Trechsel (FN 29), Art. 179 N 2 (nur verkörperte Erscheinungsformen); anders BGE 116 IV 343 (zu Art. 110 Ziff. 5 StGB a.F.), wo auch Anzeigen am Bildschirm als Schriften behandelt wurden. Aus der expliziten Gleichsetzung von "Datenträgern" mit Schriften bei der Legaldefinition der Urkunde (Art. 110 Ziff. 5 Satz 2 StGB) erschliesst sich deutlich, dass Daten in einem anderen Kontext eben nicht Schriften sein können. Das Analogieverbot (Art. 1 StGB) verhindert eine Ausdehnung dieser speziellen Urkundenregelung auf die Grundmenge aller Schriften. Vgl. zur klareren Legaldefinition der Schriften im dStGB Albin Eser, in: Adolf Schönke/Horst Schröder, Strafgesetzbuch, Kommentar, 26. Aufl., München 2001, § 11 N 78 (Einbezug der "Datenspeicher", genauer wäre: gespeicherter Daten).

[77] Anders bei der Ablage in Mailboxen, die zumeist passwortgeschützt sind, was dem Kriterium der besonderen Sicherung genügt. Schmid (FN 37), § 4 N 38, will allerdings bei einem Datentransport über drahtgebundene oder eigens reservierte drahtlose Kanäle (z.B. Mobiltelephonie) ungesicherte Daten als gegen den Täterzugriff besonders gesichert ansehen (fraglich). Vgl. zur eingehenden Diskussion in Deutschland statt aller Lenckner (FN 61), § 202a N 8 m.w.N. (Verschlüsselung ist notwendig).

[78] Qualitativ wird damit ein anderes Rechtgut geschützt, siehe oben III.2.

[79] Art. 321ter Abs. 2 StGB erweitert die Strafbarkeit auf Personen, die zwar selber nicht den erforderlichen Sonderstatus haben, aber einen Adressaten des Geheimhaltegebotes als Tatmittler einsetzen, vgl. Jörg Rehberg, Änderungen im Strafgesetzbuch durch das neue Fernmeldegesetz, AJP 7 (1998) 564.

[80] BGE 126 I 50 ff. Die Erforschung und Herausgabe der Angaben über Randdaten einer E-Mail-Mitteilung bedarf einer richterlichen Genehmigung, seit 1.1.2002 geregelt im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [BÜPF], SR 780.1.

[81] Art. 179^{novies} StGB schützt vor dem unbefugten Beschaffen von Personendaten aus einer Datensammlung; Art. 6 i.V.m. Art. 23 UWG schützen auch vor dem (Online-)Auskundschaften und Verwerten bzw. Mitteilen von Fabrikations- und Geschäftsgeheimnissen. Anders als bei Art. 143 StGB wird keine besondere Sicherung der Daten gefordert, weshalb diese Bestimmungen z.B. im WEF-Hacking-Fall, wo die Kundendatei des World Economic Forums online ausgespäht und einer Zeitungsredaktion übergeben wurde, subsidiär als anwendbar erscheint, vgl. zum Fall Schwarzenegger (FN 6), 333 m.N.; Art. 50 FMG schützt vor dem unbefugten Verwerten von nichtöffentlichen Informationen, die mit einer Fernmeldeanlage empfangen wurden. Die Anwendung wird dadurch eingeschränkt, dass eine unbefugte Verwendung oder Bekanntgabe an Dritte objektiv erforderlich ist.