Die rechtlichen Aspekte der Wirtschaftskriminalität im Internet an konkreten Fällen

(Vortrag gehalten an IT-Security-Seminare mit der Trivadis AG
in Basel, Bern, Regensdorf, Stuttgart und München
im August und September 2001)
Es galt das gesprochene Wort

EINLEITUNG

Im Allgemeinen werden drei verschiedene Formen der Internetkriminalität unterschieden:

- Eine Form der Internetkriminalität zielt darauf ab, wirtschaftliche Bestrebungen einzelner Unternehmen oder ganzer Wirtschaftszweige zu behindern oder gänzlich auszuschalten, ohne dass die Täter jedoch eine Bereicherungsabsicht hegen.

- Der zweite und grösste Teil der kriminellen Aktivitäten im Internet zielt auf Bereicherung ab und fügt den Unternehmen nicht nur einen Imageschaden, sondern auch einen Vermögensschaden zu. Nebst den betroffenen Unternehmen können auch deren Kunden können zu den Geschädigten gehören.

- Eine dritte Form findet sich auf höchster Ebene zwischen Staaten wieder: Die „Cyberwars“ wie z.B. zwischen Palästina und Israel oder China und Taiwan.

- Als vierte Form kann der „*Kinderscherz*“ angesehen werden: Hier bewegt sich die Hackergemeinde auf dem schmalen Grat, einerseits ohne Absicht zu handeln und anderseits einer „sportlichen“ Motivation zu folgen, bei der jedoch zumindest eine gewisse zerstörerische Absicht festzustellen ist.

Im folgenden werden die Ausführungen in diesem Referat auf die straf- und datenschutzrechtlichen Aspekte beschränkt.

Grundlage der weiteren Ausführungen bilden die drei in technischer Hinsicht besprochenen Hacker-Attacken. Bei der juristischen Prüfung der Fälle muss einem bestimmten Prüfungsschema gefolgt werden. Nur so kann ermittelt werden, ob die Strafnorm durch den Straftäter erfüllt wurde und dieser danach bestraft werden kann, oder ob der Täter straflos bleibt.

Anzufangen ist dabei immer mit dem **objektiven Tatbestand**. Dabei ist zunächst zu prüfen, ob folgende *Tatbestandsmerkmale* erfüllt sind:

- *Täter*
- *Tatobjekt*
- *Tathandlung.*

Als *Täter* kommt in den besprochenen Fällen der Hacker in Betracht. *Tatobjekt* der sog. „Hackertatbestände" bilden automatisierte Datenverarbeitungsanlagen, also Computersysteme. Die *Tathandlung* richtet sich je nach Straftatbestand. Sie ist z.B. durch das *Eindringen in ein fremdes Computersystem* oder durch die *Datenbeschädigung* gegeben.

Unter dem Merkmal des **subjektiven Tatbestandes** ist zu prüfen, ob der Täter die Tat *absichtlich* herbeiführen wollte (Vorsatz), sie allenfalls in Kauf nahm (Fahrlässigkeit) oder diese überhaupt nicht begehen wollte (straffrei).

Fall 1: Denial of service

Ein Hacker greift von seinem in der Schweiz stehenden Computer einen sich ebenfalls in der Schweiz befindlichen Server an.

Mit seiner Attacke bewirkt der Hacker gezielt und bewusst, dass die sich auf dem Server befindlichen Internetseiten durch etwelche Benutzer nicht mehr aufgerufen werden können.

In diesem ersten Fallbeispiel liegt eine typische Hackerattacke, nämlich um eine **Denial-of-Service-Attacke**, vor. Zur Beurteilung stehen im wesentlichen zwei Straftatbestände,

nämlich das *unbefugte Eindringen in eine Datenverarbeitungsanlage* (Art. 143bis CH-StGB) sowie Datenbeschädigung (Art. 144bis Ziff. 1 CH-StGB).

Art. 143bis CH-StGB: **Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.**

Die Computeranlage muss als erstes Kriterium fremd sein, d.h. der Täter darf keine Zugangsberechtigung aufweisen, und sie muss gegen seinen Zugriff besonders gesichert sein. Wenn dies nicht der Fall ist, ist der objektive Tatbestand nicht erfüllt, da der Täter (Hacker) nicht in ein *besonders gesichertes* Datenverarbeitungssystem eindringt.

Gehen wir im weiteren davon aus, dass der Server (wie üblich) gesichert ist, dann gilt der Tatbestand als erfüllt und der Täter ist strafbar, da sämtliche Voraussetzungen des Art. 143bis CH-StGB gegeben sind („besonders gesichertes Datenverarbeitungssystem"). Das Eindringen ist aber regelmässig nur dann erfüllt, wenn der Täter zur Datenverarbeitungsanlage führende Schranken wie etwa *Codes, Chiffrierungen, Verschlüsselungen* usw. überwindet. Das Eindringen wird zudem bereits mit Überwindung der ersten Zugangssicherung, z.B. einem Code oder Passwort, vollendet. Ohne derartige Zugangssicherungen kann die dargestellte *„Hackerstrafnorm"* also nicht zur Anwendung kommen.

Der Hacker dringt in unserem Fall über das Internet in ein ihm fremdes Netzwerksystem ein. Er handelt mit voller Absicht. Die objektiven und subjektiven Tatbestandsmerkmale sind somit erfüllt. Zu beachten ist dabei, dass Art. 143bis CH-StGB nur *vorsätzliches* Eindringen erfasst.

Im gezeigten Fall beabsichtigt der Hacker zudem, den Server zum Absturz zu bringen bzw. die Internetseiten unbrauchbar zu machen.

In diesem Zusammenhang ist der Tatbestand der *Datenbeschädigung* gemäss Art. 144bis Ziff.1 CH-StGB zu untersuchen.

Art. 144bis Ziff. 1 CH-StGB: **Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.**

Neu an diesem Tatbestand ist, dass die Daten *fremd* sein müssen, d.h. nicht für den Hacker bestimmt sind. Die *Tathandlung* besteht im *unbefugten Verändern* (Abändern des Inhalts oder der Form), *Löschen* (vollständiges Vernichten) oder *Unbrauchbarmachen* (Absperren, ohne dass die Daten selbst verändert oder gelöscht würden). Unbefugt handelt der Hacker dann, wenn er die Handlung gegen den ausdrücklichen oder vermutlichen Willen des Berechtigten durchführt. Die Tathandlung führt dazu, dass der Berechtigte nicht mehr wie gewohnt über seine Daten verfügen kann.

In unserem Anschauungsfall - dem Lahmlegen eines Rechners durch eine DoS-Attacke - fällt die *Tathandlung* des *Unbrauchbarmachens* der Daten in Betracht. Die Veränderung oder Löschung bleibt in der ersten Variante unseres Beispielfalles aus.

Daten werden auch dann unbrauchbar gemacht, wenn sie *versteckt* werden. Auch können Dateinamen oder Passwörter verändert bzw. vertauscht oder sogar Verschlüsselungen eingefügt werden, ohne dass die Datei als solche verändert wird. Auf diese Weise bleiben die Daten in ihrer Ursprungsform erhalten, sind aber auf dem gewohnten Wege für den Nutzer nicht mehr abrufbar.

Dies ist in unserem Beispiel der Fall. Handelt der Täter mit Absicht, ist der objektive und der subjektive Tatbestand erfüllt.

Zusammenfassend ist festzuhalten, dass der Hacker die Straftatbestände (Art. 143bis und des Art. 144bis CH-StGB) erfüllte und auf Antrag (*Antragsdelikt*) mit Busse oder Haft bestraft werden kann. Den Geschädigten - einerseits das Unternehmen, andererseits aber auch private Nutzer – verbleibt eine Frist von 3 Monaten zur Anzeigeerstattung. Diese Frist beginnt ab Kenntnis der Tat und des Täters zu laufen.

Variante:

Der Hacker verändert oder löscht den Inhalt der Internetseiten.

Der Täter ist auch in diesem Beispiel nicht zur Veränderung oder Löschung von Daten befugt. Er erfüllt die gleichen Kriterien, wie im besprochenen Grundsachverhalt, und macht sich des *unbefugten Eindringens in eine Datenverarbeitungsanlage* und der *Datenbeschädigung* strafbar. Obwohl also ganz verschiedene Tathandlungen mit erheblich unterschiedlichen Wirkungen und unterschiedlichem Schadenspotential begangen wurden, sind dieselben Strafnormen anwendbar. Zu berücksichtigen sind die verschiedenen Tatumstände allenfalls bei der Verschuldensbewertung und damit bei der Strafzumessung.

Hinweis: Für Deutschland finden sich die wichtigsten Strafnormen für das "Hacking" in § 202a D-StGB *(Ausspähen von Daten),* in § 303a und b D-StGB *(Datenveränderung und Computersabotage)* sowie in § 263a D-StGB *(Computerbetrug).*

Fall 2: Mail bomb

Ein Hacker dringt von seinem in der *Schweiz* stehenden Computer über einen sich in *Italien* befindlichen Mailserver in einen *deutschen* Mailserver ein. Von dort sendet er eine grosse Anzahl von E-Mails (mail-bomb) mit rassistischem Inhalt. Als Absenderadressen der E-Mails figurieren beliebige (Scherz- bzw. Phantasie-)Adressen.

Folgendes ist in diesem Sachverhalt zu beachten:

1. Hacker dringt über italienischen Mailserver in einen deutschen Mailserver ein. Damit liegt ein *internationaler* Sachverhalt vor.
2. Vom deutschen Mailserver sendet er viele E-Mails mit rassistischem Inhalt. Er operiert aber von der Schweiz aus.
3. Der Hacker gibt extra „Scherz- bzw. Phantasie-„Absender“ an.

Die globale Verbreitung des Internet bringt es mit sich, dass strafbare Darstellungen, ob in Wort oder Bild, zu einem grossen Teil im Ausland oder auf Umwegen über das Ausland ins Netz gespiesen werden. Diesem Umstand muss durch eine gut funktionierende *internationale Rechtshilfe* sowie durch eine zukünftige *Harmonisierung* des Strafrechts Rechnung getragen werden. Im Rahmen des Strafrechts bestehen innerhalb der EU schon seit längerem Harmonisierungsbestrebungen (*Hinweis*: Entwurf eines "Gemeinsamen Stand-

punktes zu den Verhandlungen im Europarat über den Entwurf des Übereinkommens zur Cyber-Kriminalität des EU-Rats" vom 23. April 1999).

Das zweite Fallbeispiel tangiert drei verschiedene Länder: Schweiz – Italien – Deutschland.

In einem internationalen Strafrechtsfall ist in einer ersten Phase abzuklären, welches Recht zur Anwendung kommt. Zur Auswahl stehen hier das deutsche, das italienische und das schweizerische Recht.

Um das anwendbare Recht festzulegen, ist zu ermitteln, wo die Tat verübt wurde. Bei Internetdelikten ist dies eine schwierige und rechtlich umstrittene Frage.

Grundsätzlich können verschiedene nationale Rechte zur Anwendung gelangen. Im vorliegenden Fall gibt es nämlich zwei *Anknüpfungspunkte*:

1. Den Ort der Ausführung, d.h. der Ort, an welchem der Täter die Eingabe erstellt (hier: Schweiz).
2. Den Ort des Erfolges, d.h. der Ort, an dem die Tat verwirklicht wird (hier: Deutschland).

Zudem werden zwei *Deliktstypen* unterschieden:

1. **Erfolgs**delikt: Die Tathandlung ist die konkrete Schädigung eines Rechtsguts. Strafbar ist also die Bewirkung eines bestimmten Erfolgs.
2. **Tätigkeits**delikt: Hier ist der Tatbestand schon dann begangen, wenn der Täter ein bestimmtes Verhalten an den Tag legt. Strafbar ist also die Tat an sich.

Gegenwärtig überwiegt in der schweizerischen und deutschen Lehre die Meinung, dass Internetdelikte (*Eindringen in ein fremdes Datenverarbeitungssystem*, *Virentatbestand* und auch *Rassendiskriminierung*) als Tätigkeitsdelikte eingestuft werden. In diesem Sinne sind sie im Moment ihrer Ausführung schon vollendet und zwar am *Ort der Ausführung* (unbeschadet des Erfolges und des Ortes des Erfolgseintritts). Im vorliegenden Fall ist dies die Schweiz, weshalb schweizerisches Strafrecht zur Anwendung gelangt.

Wie im ersten Sachverhalt ist auch hier der Tatbestand des *unbefugten Eindringens in ein Datenverarbeitungssystem* (Art. 143bis CH-StGB) erfüllt. Diese Bestimmung ist eine Art "Grunddelikt", das beinahe immer erfüllt sein wird, ähnlich dem Tatbestand des Hausfriedensbruchs bei Diebstahl und anderen Vermögensdelikten.

Geht man weiter davon aus, mit der mail-bomb werden Viren verschickt, führt dies zum sogenannten *Virentatbestand* (Art. 144bis Ziff. 2 CH-StGB):

Wer *Programme*, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 [des Art. 144bis StGB] **genannten Zwecken verwendet werden sollen, herstellt, einführt, *in Verkehr bringt*, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.**

Diese schwammig formulierte Regelung hat zum Ziel, die *Virendelikte* zu erfassen.

„Viren“ sind Programme, die zum Zwecke der Datenbeschädigung verwendet werden. Ob es sich dabei um eigentliche Computerviren handeln muss oder auch um eine grosse Anzahl E-Mails mit denen das Computersystem überfordert und dadurch zum Absturz gebracht wird, ist in der Lehre umstritten.

Im gezeigten Fall verschickt der Hacker eine grosse Anzahl von E-Mails, d.h. eine sogenannte mail-bomb. Wird davon ausgegangen, dass eine beträchtliche Anzahl dieser E-Mails auf ein und denselben oder nur auf ganz wenige Server geschickt wird, ist der objektive "Virustatbestand" als erfüllt anzusehen. Denn das Versenden einer grossen Anzahl von E-Mails auf ein und dasselbe Netzwerk kann zum Absturz dieses Computersystems führen. Es spielt dabei keine Rolle, ob die E-Mails Computerviren enthalten oder nicht.

Da der Hacker vorliegend mit Vorsatz handelt, sind die Voraussetzungen erfüllt, und der Hacker ist strafbar. Der Virustatbestand ist ein Offizialdelikt, d.h. die zuständigen Behörden müssen bei Kenntnis des Sachverhaltes ohne vorherige Anzeigeerstattung tätig werden.

Werden hingegen die (nicht verseuchten) E-Mails an verschiedenste Adressen gesendet, kommt der Virustatbestand nicht zum Zuge und die Untersuchung kann hier abgebrochen werden, ausser der Täter erfüllt weitere Delikte, auf die sogleich eingegangen wird.

Der Hacker begeht vorliegend nicht nur die typischen Computerdelikte. Seine E-Mails enthalten ausserdem rassistische Inhalte. Deshalb muss hier noch die Strafnorm der *Rassendiskriminierung* (Art. 261bis CH-StGB) geprüft werden. Es geht also nicht nur um die Form, sondern auch um den Inhalt.

Art. 261 bis Abs. 4 CH-StGB: **Wer öffentlich durch Wort, Schrift, Bild, Gebärden, Tätlichkeiten oder in anderer Weise eine Person oder eine Gruppe von Personen wegen ihrer Rasse, Ethnie oder Religion in einer gegen die Menschenwürde verstossenden Weise herabsetzt oder diskriminiert oder aus einem dieser Gründe Völkermord oder andere Verbrechen gegen die Menschheit leugnet, gröblich verharmlost oder zu rechtfertigen sucht, wird mit Gefängnis oder mit Busse bestraft.**

Die Handlung besteht in der Verbreitung dieser E-Mails an die – und das ist hier von grosser Wichtigkeit – *Öffentlichkeit*. Ein kleiner Kreis ausgewählter Privatpersonen genügt nicht, um das Kriterium der Öffentlichkeit zu erfüllen. Bei einer mail-bomb ist in der Regel davon auszugehen, dass das Kriterium der Öffentlichkeit erfüllt ist.

Der Inhalt der E-Mails ist gemäss Sachverhalt rassendiskriminierend. Indessen genügt nicht jede Herabsetzung einer „Gruppe“ wie z.B. *„Ausländer sind faul!"*, vielmehr - und dies ist hervorzuheben – muss die Äusserung in einer *gegen die Menschenwürde verstossenden Weise* erfolgen. Dieser Begriff ist sehr weit auslegbar. Auch führt eine genaue Abhandlung der Strafnorm der Rassendiskriminierung an dieser Stelle viel zu weit. Anzumerken bleibt, dass der Täter absichtlich, also mit Vorsatz handelte und sich nebst den beurteilten Computerdelikten der Rassendiskriminierung strafbar macht.

Dieses Beispiel sollte jedenfalls in aller Kürze vor Augen führen, dass solche rassendiskriminierenden Aussagen - ob sie über Internet, Presse, mündlich oder sonstwie an die *Öffentlichkeit* gelangen - unter Strafe stehen. Gleiches gilt für ähnliche Strafbestimmungen wie z.B. im Bereich der Sittlichkeit (Pornographie usw.).

Fall 3: Read private inbox

Ein Hacker dringt von seinem in *Deutschland* stehenden Computer in einen *schweizerischen* Mailserver ein. Dort liest er den privaten Posteingangsordner der Kunden dieses

Mailservers, um Informationen über Pincodes zu sammeln. Mit diesen Pincodes dringt er in passwortgeschützte kommerzielle Internetseiten ein, um von deren Angebot zu profitieren.

1. Der *Ort der Ausführung*, also dort von wo der Hacker von seinem Computer in einen Mailserver eindringt, befindet sich diesmal in *Deutschland***.**
2. Der *Ort des Erfolges* hingegen befindet sich in der *Schweiz*, da dort der Hacker die privaten Mails liest. Durch das Lesen der privaten Posteingangsordner gelangt der Täter an für ihn unberechtigte Pincodes (Passwörter).
3. Die Pincodes benutzt der Hacker, um auf passwortgeschützte Internetseiten zu gelangen und für sich einen Nutzen daraus zu ziehen, d.h. sich zu bereichern.

Durch sein Vorgehen macht sich der Hacker wieder diverser strafrechtlicher Computerdelikte schuldig. Die Computerdelikte werden diesmal von Deutschland aus begangen, weshalb deutsches Strafrecht zur Anwendung gelangt.

Nachfolgend ist der deutsche Straftatbestand, das *Ausspähen von Daten* (§ 202a D-StGB), zitiert, welcher analog zu 143^{bis} CH-StGB formuliert ist.

§ 202a D-StGB: (1) **Wer unbefugt Daten, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.**

In unserem Fall erfüllt der Hacker auch hier diesen strafrechtlichen (Grund-)Tatbestand.

Auch an dieser Stelle ist hervorzuheben, dass die Strafantragsfrist 3 Monate ab **Kenntnis** der Tat und der Person des Täters (Hacker) zu erfolgen hat (§ 77b D-StGB). Wird die Tat in der Praxis bemerkt und der Täter tatsächlich eruiert – *was ein schwieriges Unterfangen ist* – verbleibt genügend Zeit, rechtlich gegen den Täter vorzugehen, d.h. Anzeige zu erstatten.

Zudem macht sich der Hacker auch des *Computerbetruges* schuldig, indem er mit den „geklauten" Pincodes in passwortgeschützte kommerzielle Internetseiten eindringt und deren Inhalt für sich nutzt, sich also u.U. einen rechtswidrigen Vermögensvorteil verschafft.

§ 263a D-StGB: (1) **Wer in der Absicht, sich oder einen Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.**

Als letztes – *aufgrund ihrer Wichtigkeit keineswegs zu vernachlässigen* – sind die **datenschutzrechtlichen** Aspekte. Wie erwähnt, werden die privaten Posteingangsordner eines schweizerischen Mailservers gelesen. Es ist davon auszugehen, dass deshalb überwiegend eine schweizerische Kundschaft betroffen ist. Aus diesem Grund ist das **schweizerische Datenschutzgesetz** anzuwenden.

Auszugehen ist von Art. 4 Abs. 1 CH-DSG:

"Personendaten dürfen nur rechtmässig beschafft werden."

Mit Personendaten werden alle Angaben bezeichnet, die sich auf eine bestimmbare Person beziehen (Art. 3 lit. a CH-DSG). In unserem Fall sind private Postordner geradezu dafür prädestiniert, *Personendaten* zu enthalten, welche sich der Hacker *unrechtmässig beschafft*.

Liegt wie im vorliegenden Sachverhalt eine Datenschutzverletzung gemäss Datenschutzgesetz vor, ist zu beurteilen, ob das für den Hacker strafrechtliche Folgen nach sich ziehen kann.

Die Strafnorm des 179^{novies} CH-StGB regelt das *Unbefugte Beschaffen von Personendaten*, aber nur für *besonders schützenswerte* Personendaten. Darunter fallen religiöse oder weltanschauliche Daten, Daten über die Gesundheit oder Intimsphäre usw. (Art.3 lit. c und d CH-DSG). Pincodes fallen indessen unter diese *besonders schützenswerten* Personendaten fallen. Pincodes sollen ja gerade verhindern, dass sich ein Fremder einen Vorteil zukommen lässt; sie erfüllen selbst eine Schutzfunktion. Art. 179^{novies} CH-StGB kommt im vorliegenden Fall deshalb nicht zur Anwendung.

Zu prüfen bleibt, ob die Geschädigten auf anderem Wege Ansprüche geltend machen können.

Wirft man noch einmal einen Blick in das Datenschutzgesetz, stellt man in Art. 12 CH-DSG fest, dass, wer Personendaten unrechtmässig beschafft (Art. 3, Art. 4 CH-DSG), die *Persönlichkeit* der betroffenen Person *verletzt*. Diese ist sodann nach Art. 15 CH-DSG klageberechtigt.

Nach zivilrechtlichen Bestimmungen kann Schadenersatz von den betroffenen Personen, deren Pincode missbraucht wurde, geltend gemacht werden (Hinweis: über Art. 28a Abs. 3 ZGB, welcher auf 41 OR verweist). Zusätzlich ist erforderlich, dass der Hacker – wie vorliegend – mit Absicht gehandelt hat.

Dem Geschädigten bleibt im konkreten Fall, wie in allen anderen Fällen auch, letztlich nur übrig, **zivilrechtliche Ansprüche** geltend zu machen. Voraussetzung ist indessen, dass ein *Vermögensschaden* nachgewiesen werden kann.

Schlussbemerkungen

Das Internet bewegt sich keineswegs in einem gesetzlichen Niemandsland, auch wenn heute nur wenige, spezifisch auf das Internet zugeschnittene Rechtssätze bestehen. Zwei technische Umstände führen dazu, dass die Internetkriminalität schwierig zu bekämpfen ist:

1. Das Internet ist ein nahezu zeitverzugloses Kommunikationsmedium!
2. Das Internet ist nicht an räumliche Distanzen gebunden, sondern überwindet mit den Staatsgrenzen auch die einzelnen staatlichen rechtlichen Massnahmen!

Aufgrund dieser Tatsache besteht die Gefahr, dass ein „*Rechtsnormenkrieg im Cyber-space*“ bevorsteht:

So konnte man Mitte August 2000 in der Presse lesen, dass die Strafuntersuchung gegen den Urheber des „I love you“-Virus in den Philippinen eingestellt wurde, weil dort der

Straftatbestand der Datenbeschädigung oder der Verbreitung von Computerviren nicht existiert. Angesichts der enormen Schäden, die durch solche Angriffe entstehen, sollte das Strafrecht oder die durch das Strafrecht zu schützenden Werte in dem Masse weltweit harmonisiert werden, dass diejenigen Handlungen, für deren Begehung sich das Internet als ideales Medium anbietet, weltweit möglichst einheitlich mit Strafe belegt werden.

Dies gilt für alle Straftatbestände, die im Internet stark vertreten sind, insbesondere natürlich die Computerdelikte, aber auch Rassendiskriminierung und Kinderpornographie!

In einem ersten Schritt hat der Europarat eine sog. „Cyber-Crime-Convention“ entworfen, welche vorsieht, dass namentlich in den genannten Bereichen einheitliche Strafnormen geschaffen werden sollen. Daran beteiligt sind neben den Nationen des Europarats die USA, Kanada, Japan und Südafrika.

Die Bekämpfung der internationalen Internetkriminalität muss an erster Stelle stehen, um die horrend ansteigenden Fälle (etwas) besser in den Griff zu bekommen. An dieser Stelle sei abschliessend auf den "WEF-Davos-Fall" oder nochmals auf den „I love you“-Virus verwiesen.

lic. iur. Patrik Häberlin, Rechtsanwalt