Preparatory Colloquium
Verona (Italy), *28 – 30 November 2012*
Section I - Information Society and Penal Law

LANDESBERICHT ÖSTERREICH*

Andrea LEHNER*

A. Einleitung

Im vorliegenden Landesbericht werden die wesentlichen computerstrafrechtlichen Regelungen Österreichs sowie Fragen aus angrenzenden Bereichen erläutert. Der Landesbericht wurde aufgrund des im AIDP-Newsletter 1/2012 zur Verfügung gestellten Fragebogens erarbeitet. Die Gliederung des Berichts entspricht der Gliederung des Fragebogens.

B. Kriminalisierung

1. Geschützte Rechtsgüter

Which specific legal interests are deemed to be in need of protection by criminal law?

Insbesondere schützt das österreichische Strafrecht im Bereich des Computerstrafrechts folgende Rechtsgüter: Privatsphäre, das Recht auf Geheimhaltung, Vermögen, die Zuverlässigkeit von Daten, sexuelle Integrität und Selbstbestimmung, die Sicherheit des Verkehrs mit unbaren Zahlungsmitteln sowie den öffentlichen Frieden.

2. Delikte des Computerstrafrechts

Please give typical examples of criminal laws concerning

a. attacksagainst IT systems

Wichtigstes Beispiel ist § 118aStrafgesetzbuch (StGB) – der **widerrechtliche Zugriff auf ein Computersystem:** § 118a will typische Fälle von unbefugtem Eindringen in fremde Computer („Hacking") erfassen.[1]Den objektiven Tatbestand des § 118a verwirklicht derjenige, der sich zu einem Computersystem (oder zu einem Teil eines solchen), über das er nicht oder nicht alleine verfügen darf, Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem überwindet. In subjektiver Hinsicht muss der Täter, neben dem Tatbildvorsatz (dolus eventualis[2] genügt), ein dreifaches Absichtserfordernis[3] als erweiterten Vorsatz erfüllen: und zwar muss es ihm darauf ankommen (i) sich oder einem anderen Unbefugten von gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen, (ii) die Daten selbst zu benützen, einem anderen, für den sie nicht bestimmt sind, zugänglich zu machen oder sie zu veröffentlichen *und* (iii) dadurch sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Die Verwirklichung des § 118a ist mit

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Mag. Andrea Lehner ist Universitätsassistentin am Institut für Strafrecht und Kriminologie der Rechtswissenschaftlichen Fakultät der Universität Wien.

[1] *Birklbauer/Hilf/Tipold,* Strafrecht Besonderer Teil I[2] (2012) 227; *Fuchs/Reindl-Krauskopf,* Strafrecht Besonderer Teil I[3] (2009) 96.

[2] Bedingt vorsätzlich handelt, wer es zumindest ernstlich für möglich hält, dass er einen Sachverhalt verwirklicht, der einem gesetzlichen Tatbild entspricht, und sich damit abfindet (§ 5 Abs 1 2. HS StGB).

[3] Absicht im Sinne von § 5 Abs 2 StGB als stärkster Vorsatzgrad, bei dem es dem Täter darauf ankommen muss den Umstand oder Erfolg zu verwirklichen, für den das Gesetz absichtliches Handeln voraussetzt.

Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen bedroht. Wer die Tat als Mitglied einer kriminellen Vereinigung[4] begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

Des Weiteren ist hier § 126b StGB–die **Störung der Funktionsfähigkeit eines Computersystems** – zu nennen. Nach § 126b ist strafbar, wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er vorsätzlich Daten eingibt oder übermittelt. Es ist eine Strafdrohung von Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen vorgesehen. Die Tat ist strenger bestraft, wenn die Störung der Funktionsfähigkeit längere Zeit andauert (Freiheitsstrafe bis zu zwei Jahre oder Geldstrafe bis zu 360 Tagessätzen) oder wenn die Tat als Mitglied einer kriminellen Vereinigung begangen wird (Freiheitsstrafe von sechs Monaten bis zu fünf Jahren).

b. violationof IT privacy

Mittels den folgenden Tatbeständen will das österreichische Strafrecht einerseits das Ausspionieren *bestimmter* Daten (§§ 123 StGB und 51 DSG, wenn die Daten in weiterer Folge auch verwendet werden) und andererseits das Ausspionieren von Daten *am Übertragungsweg* (§§ 119, 119a, 120 Abs 2a StGB) verhindern.[5]

Tathandlung des § 119 **(Verletzung des Telekommunikationsgeheimnisses)**ist die vorsätzliche[6] Benützung einer Vorrichtung, die an einer Telekommunikationsanlage oder an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde. Als erweiterter Vorsatz ist erforderlich, dass der Täter die Absicht hat, sich oder einem anderen Unbefugten vom Inhalt im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen.Voraussetzung für die Verwirklichung ist, dass es sich um Mitteilungen mit gedanklichem Inhalt (= Nachrichten) handeln muss. Bloße Verbindungsdaten eines Kommunikationsvorgangs werden vom § 119 nicht erfasst.[7]Vollendet ist § 119 bereits mit dem Benützen der Vorrichtung. Die Verwirklichung des Delikts ist mit Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen bedroht.

Den Tatbestand des § 119a **(Missbräuchliches Abfangen von Daten)**verwirklicht, wer eine Vorrichtung, die an einem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, vorsätzlich (dolus eventualis) benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt. Hier ist der erweiterte Vorsatz in Form der Absicht erforderlich, (i) sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen, (ii) die Daten selbst zu benützen, einem anderen, für den sie nicht bestimmt sind, zugänglich zu machen oder sie zu veröffentlichen und (iii) dadurch sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen. Der erweiterte Vorsatz des § 119a deckt sich demnach mit dem des § 118a. Das Missbräuchliche Abfangen von Daten ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen bedroht. Sowohl die Tathandlung als auch der Schutzbereich reichen bei § 119a weiter als bei § 119: § 119a normiert nicht nur die Benutzung einer Vorrichtung als Tathandlung, sondern auch das Abfangen elektromagnetischer Abstrahlung. Hinsichtlich des Schutzbereichs ist von § 119a generell die Übermittlung von Daten[8] erfasst und nicht nur von

[4]Kriminelle Vereinigung im Sinne von § 278 StGB als ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen, der darauf ausgerichtet ist im Gesetz aufgezählte Straftaten zu begehen.
[5]*Reindl-Krauskopf,* Computerstrafrecht im Überblick[2] (2009) 25.
[6]Werden keine weiteren Angaben gemacht, reicht als Vorsatzgrad dolus eventualis aus.
[7]*Reindl-Krauskopf,* Computerstrafrecht 30.
[8]Für eine Definition des Begriffs „Daten“ siehe Kapitel B. 3.

Nachrichten.[9] Vollendet ist § 119a bereits mit dem Benützen der Vorrichtung oder Abfangen elektromagnetischer Strahlung. Im Verhältnis zu § 119 ist § 119a ausdrücklich subsidiär.

Den Tatbestand des **Missbrauchs von Tonaufnahme- oder Abhörgeräten** (§ 120 Abs 2a StGB) verwirklicht, wer eine im Wege einer Telekommunikation übermittelte und nicht für ihn bestimmte Nachricht vorsätzlich aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht in der Absicht, sich oder einem anderen Unbefugten vom Inhalt dieser Nachricht Kenntnis zu verschaffen. § 120 Abs 2a ist mit Freiheitsstrafe bis zu drei Monaten oder Geldstrafe bis zu 180 Tagessätzen zu bestrafen. Die Tathandlungen des § 120 Abs 2a unterscheiden sich grundlegend von denen der §§ 119, 119a. Sie umfassen das Aufzeichnen, Zugänglichmachen oder Veröffentlichen von Nachrichten und knüpfen ihre Strafbarkeit damit an einen späteren Zeitpunkt als die §§ 119, 119a.[10] § 120 Abs 2a ist im Verhältnis zu den §§ 119, 119a ausdrücklich subsidiär.

Das vorsätzliche **Auskundschaften eines Geschäfts- oder Betriebsgeheimnisses** (§ 123 StGB) ist zu bestrafen, wenn es mit dem erweiterten Vorsatz geschieht, das Geheimnis zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben. § 123 ist kein spezifisches Computerstrafrechtsdelikt. Jede Möglichkeit des Ausspionierens ist unter § 123 subsumierbar, unter anderem auch das Ausspionieren von Geschäftsgeheimnissen nach einem Hackingangriff.[11]

§ 51 DSG pönalisiert eine **Datenverwendung in Gewinn- oder Schädigungsabsicht.** Demnach ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen, wer *personenbezogene* Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat. Im Unterschied zu § 123 genügt bei § 51 DSG also nicht das Ausspionieren von Daten, sondern die Daten müssen vom Täter tatsächlich verwendet werden.[12]Bei den Daten muss es sich um personenbezogene handeln; das sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist (Name, Adresse, Geburtsdatum, Kontonummer, Fingerabdrücke usw.).[13] Des Weiteren muss der Täter mit dem erweiterten Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern oder in der Absicht handeln, einen anderen dadurch in seinem Grundrecht auf Datenschutz zu schädigen.

c. forgery and manipulation of digitally stored data

§ 126a StGB **(Datenbeschädigung)** stellt die vorsätzliche Veränderung, Löschung, das sonstige Unbrauchbarmachen oder Unterdrücken von automationsunterstützt verarbeiteten, übermittelten oder überlassenen Daten, über die der Täter nicht oder nicht allein verfügen darf, unter Strafe.Kann also der Berechtigte seine Daten aufgrund der Verhaltensweise des Täters nicht mehr (wenn auch nur vorübergehend) verwenden, wurde er also geschädigt, so ist der Tatbestand des § 126a erfüllt. Der Schaden bemisst sich am Wiederbeschaffungswert der manipulierten Daten, die nicht mehr in der bisherigen Weise genutzt werden können.[14]Die Verwirklichung des Tatbestands ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen bedroht. Übersteigt der Schaden EUR 3.000,00 erhöht sich die Strafdrohung auf Freiheitsstrafe bis zu zwei Jahren oder

[9] *Birklbauer/Hilf/Tipold,* BT I 231 f.
[10] *Birklbauer/Hilf/Tipold,* BT I 231.
[11] *Reindl-Krauskopf,*Computerstrafrecht 26.
[12] *Reindl-Krauskopf,*Computerstrafrecht 27.
[13] Siehe genauer *Salimi* in Höpfel/Ratz (Hrsg), Wiener Kommentar zum Strafgesetzbuch (WK)[2] § 51 DSG Rz 27 ff.
[14] *Öhlböck/Esztegar,* Rechtliche Qualifikation von Denialof Service Attacken, Journal für Strafrecht 2011, 126 (129).

Geldstrafe bis zu 360 Tagessätzen, übersteigt der Schaden EUR 50.000,00 oder wird die Tat als Mitglied einer kriminellen Vereinigung begangen erhöht sich die Strafdrohung auf Freiheitsstrafe von sechs Monaten bis zu fünf Jahren.

Datenfälschung (§ 225a StGB) ist das vorsätzliche Herstellen von falschen Daten oder das Verfälschen von echten Daten durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten. Die Tat muss vom erweiterten Vorsatz getragen sein, dass die falschen oder gefälschten Daten im Rechtsverkehr zum Beweis eines Rechts, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden. Der Täter braucht daher bei der Datenfälschung einen Täuschungsvorsatz.Da die Täuschung eine Willensbildung beim Beweisadressaten erfordert, ist nur der Vorsatz der Täuschung eines Menschen von § 225a erfasst. Ist geplant, die falschen oder gefälschten Daten nur gegenüber einer Maschine einzusetzen, so ist § 225a nicht anwendbar.[15] Bei Verwirklichung des Delikts droht Freiheitsstrafe bis zu einem Jahr.

§§ 241a und cStGB umfassen die **Vorbereitung** der Fälschung und die **Fälschung unbarer Zahlungsmittel**[16]. Diese Delikte können auch als computerstrafrechtliche angesehen werden und zwar insofern als die Fälschung unbarer Zahlungsmittel sehr häufig unter Einsatz von EDV-Mitteln erfolgt.[17] Sie wurden 2004[18] in Ergänzung zu § 225a im österreichischen Recht verankert, da § 225a zwar das Fälschen und Verfälschen von Daten sanktioniert, allerdings den erweiterten Vorsatz auf Verwendung der Fälschung zum Beweis eines Rechts, einer Tatsache oder eines Rechtsverhältnisses im Rechtsverkehr – wie oben bereits beschrieben – verlangt. Das hätte zur Konsequenz, dass weiße Plastikkartenfälschungen, die aufgrund ihres äußeren Erscheinungsbildes nicht zur Täuschung eines Menschen eingesetzt werden können (sondern nur zur Täuschung von Maschinen), straflos wären, da sie nicht unter § 225a subsumiert werden können.

Das Fälschen unbarer Zahlungsmittel beinhaltet zwei verschiedene Tatbestände, nämlich das vorsätzliche Herstellen eines falschen unbaren Zahlungsmittels und das (vorsätzliche) Verfälschen eines echten unbaren Zahlungsmittels. Ein falsches Zahlungsmittel stellt bspw her, wer ein Zahlungsmittel nachmacht, aus dessen am Datenträger abgespeicherten Daten sich der Anschein ergibt, es läge ein echtes Zahlungsmittel vor. Beim Verfälschen verändert der Täter zB die am Zahlungsmittel abgespeicherten Daten. Beide Varianten müssen mit dem erweiterten Vorsatz begangen werden, dass das Zahlungsmittel im Rechtsverkehr wie ein echtes verwendet wird. Hier kann also auch geplant sein, dass das Falsifikat lediglich im elektronischen Rechtsverkehr zur Anwendung kommt. Die geplante Täuschung eines Menschen ist nicht erforderlich.[19]Die Strafdrohung ist Freiheitsstrafe bis zu drei Jahren. Wird die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begangen, erhöht sich die Strafdrohung auf Freiheitsstrafe von sechs Monaten bis zu fünf Jahren.

§ 241c stellt bereits die Vorbereitung der Fälschung unbarer Zahlungsmittel unter Strafe (Strafdrohung Freiheitsstrafe bis zu einem Jahr). Demnach macht sich derjenige strafbar, der vorsätzlich ein Mittel oder Werkzeug anfertigt, von einem anderen übernimmt, sich oder einem anderen verschafft, einem anderen überlässt oder sonst

[15]Siehe *Reindl* in Höpfel/Ratz (Hrsg), WK[2] § 225a Rz 20 ff.
[16]Für eine Definition des Begriffs „unbare Zahlungsmittel" siehe Kapitel B.3.
[17]*Reindl,* Das Phänomen „Phishing", SIAK-Journal 2007, 2 (6).
[18]StrÄG (Strafrechtsänderungsgesetz) 2004, BGBl I 2004/15.
[19]*Reindl-Krauskopf,* Computerstrafrecht 57 ff.

besitzt, wenn die Tat von dem erweiterten Vorsatz, dadurch sich oder einem anderen eine Fälschung eines unbaren Zahlungsmittels zu ermöglichen, getragen ist. Als Mittel oder Werkzeug können bspw Computerprogramme dienen.[20]

§ 148a StGB **(Betrügerischer Datenverarbeitungsmissbrauch)** verwirklicht, wer durch Gestaltung eines Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs das Ergebnis einer automationsunterstützten Datenverarbeitung vorsätzlich beeinflusst und dadurch einen anderen am Vermögen schädigt. Die Strafdrohung beträgt Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätze. Wer die Tat gewerbsmäßig begeht oder durch die Tat einen EUR 3.000,00 übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen EUR 50.000,00 übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.

d. distribution of computer viruses

Die Verteilung von **Computerviren** kann entweder eine **Datenbeschädigung** (§ 126a) oder eine **Störung der Funktionsfähigkeit eines Computersystems** (§ 126b) bewirken.[21]Kommt es aufgrund der Computerviren zu Datenveränderungen und in weiterer Folge auch zu einer Schädigung des Betroffenen, so ist eine Strafbarkeit wegen Datenbeschädigung zu überlegen. Dies wird bei überschreibenden Viren regelmäßig der Fall sein. Bei nicht überschreibenden Viren kommt nur eine Störung der Funktionsfähigkeit eines Computersystems in Betracht. Allerdings müssen diese Viren destruktive Funktionen ausführen und zu einer *schweren* Störung der Funktionsfähigkeit des Computersystems führen.[22]

Im Falle von Angriffen mit **Computerwürmern** kommt ebenfalls eine Strafbarkeit nach §§ 126a oder b in Betracht. Der mit dem Angriff verbundene Computerausfall kann ein Datenunterdrücken im Sinne des § 126a bedeuten. Zusätzlich müssen allerdings Schäden in Form von Wiederherstellungskosten entstehen. Ist § 126a nicht erfüllt, so kommt eine Strafbarkeit nach § 126b in Betracht. § 126b ist ausdrücklich subsidiär zu § 126a.[23]

e. crimes related to virtual identities of users, e.g. forging, stealing or damaging virtual personalities

Für den Identitätsdiebstahl und ähnliche Handlungen gibt es in Österreich derzeit keinen eigenen Straftatbestand. Jedoch können gewisse Stadien des Identitätsdiebstahls (wie zB das unbefugte Abändern von Daten) von bereits dargestellten Delikten wie zB § 225a StGB oder § 51 DSG umfasst sein.

f. Other innovative criminal prohibitions in the area of ICT and internet, e.g. criminalization of the creation and possession of certain virtual images, violation of copyright in virtual sphere

Das österreichische Strafgesetzbuch enthält ein Vorbereitungsdelikt zu den bereits besprochenen §§ 118a, 119, 119a, 126a, 126b und 148a. Es handelt sich dabei um den **Missbrauch von Computerprogrammen oder Zugangsdaten** (§ 126c StGB). Pönalisiert wird das vorsätzliche Herstellen, Einführen, Vertreiben, Veräußern, Zugänglichmachen, Verschaffen oder Besitzenbestimmter Computerprogramme, Computerpasswörter, Zugangscodes oder vergleichbarer Daten. Dabei ist der erweiterte Vorsatz erforderlich, dass das Computerprogramm, -passwort oder der Zugangscode zur Begehung eines der oben genannten Delikte gebraucht wird. Die Strafdrohung beträgt Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen.

---

[20]*Reindl-Krauskopf,* Computerstrafrecht 60.
[21]Beide Tatbestände wurden bereits oben erläutert.
[22]*Schuh,* Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich, Schweiz (2012) 219 f.
[23]*Schuh,* Computerstrafrecht 224 f.

§ 10 Zugangskontrollgesetz (ZuKG) – der **Eingriff in das Recht auf Zugangskontrolle** – ist ein ähnliches Delikt wie § 126c und schützt zugangskontrollierte Dienste (zB Pay-TV) vor unbefugten Zugriffen.[24] Strafbar ist derjenige, der in *gewerbsmäßiger* Absicht Vorrichtungen vertreibt, verkauft (oder Ähnliches), herstellt, einführt, usw., um Sicherungen bei zugangskontrollierten Diensten zu umgehen. Wichtiger Unterschied zu § 126c ist also das Erfordernis des gewerbsmäßigen Handelns in § 10 ZuKG.

§ 91 UrhG sieht eine Strafdrohung von Freiheitsstrafe bis zu sechs Monaten oder Geldstrafe bis zu 360 Tagessätzen (bei gewerbsmäßiger Begehung Freiheitsstrafe bis zu zwei Jahren) vor, wenn gegen ausgewählte **Bestimmungen des UrhG** verstoßen wird. Anwendungsbeispiel ist das Knacken des Kopierschutzes bei Computerprogrammen („Cracking").[25]

Eine weitere wichtige „Deliktsgruppe" des Computerstrafrechts stellen Regelungen zu verbotenen Inhalten dar **(Inhaltsdelikte).** Einschlägige Normen im StGB betreffen unter anderem einerseits den Schutz der sexuellen Integrität und den Schutz der Jugend vor sittlicher Gefährdung und andererseits die Wahrung des öffentlichen Friedens. Diese Delikte sind überwiegend „traditionelle" Delikte und nicht computerspezifisch ausgestaltet.

Was den Schutz der sexuellen Integrität betrifft finden sich im StGB das Verbot pornographischer Darstellungen Minderjähriger (§ 207a), der Anbahnung von Sexualkontakten zu Unmündigen (§ 208a) und der Förderung pornographischer Darbietungen Minderjähriger (§ 215a Abs 2a). Das **Verbot pornographischer *Darstellungen* Minderjähriger** pönalisiert das vorsätzliche Herstellen, Anbieten, Verschaffen, Überlassen, Vorführen, sonst Zugänglichmachen und Besitzen von einschlägigen pornographischen Darstellungen.[26]Unter den Begriff Darstellung sind lediglich wirklichkeitsnahe Abbildungen und bildliche Darstellungen eines Geschehens zu subsumieren; also keine Texte, Zeichnungen oder etwa Skulpturen (§ 207a Abs 4).Den Begriff des Herstellens können auch computertechnische Bearbeitungsmöglichkeiten erfüllen, beispielsweise das Einscannen eines Bildes.[27]Auch der wissentliche[28] Zugriff auf pornographische Darstellungen Minderjähriger im Internet steht unter Strafe. Die Strafdrohungen für die eben genannten Delikte sind unterschiedlich gestaffelt und reichen von Freiheitsstrafe bis zu einem Jahr (wissentlicher Zugriff auf pornographische Darstellungen im Internet) bis zu Freiheitsstrafe von einem bis zu zehn Jahren (Begehung als Mitglied einer kriminellen Vereinigung; besonders schwere Nachteile oder Gefährdung des Lebens der minderjährigen Person).

Die **Förderung pornographischer *Darbietungen* Minderjähriger** stellt die wissentliche Betrachtung einer pornographischen Darstellung, an der eine minderjährige Person mitwirkt, unter Strafe (Freiheitsstrafe bis zu zwei Jahren). Unter „Darbietung" ist im Unterschied zur Darstellung ein aktuelles („live") Geschehen zu verstehen. Unter „Betrachten" ist jede Form der visuellen Wahrnehmung zu verstehen, sei es im Rahmen einer Live-Aufführung oder einer Live-Übertragung mittels Web-Cam oder Phone-Cam.[29]

---

[24]*Birklbauer/Hilf/Tipold,* BT I 276.
[25]*Birklbauer/Hilf/Tipold,* BT I 229.
[26]Nach § 74 Abs 1 Z 2 StGB sind Minderjährige Personen, die das 18. Lebensjahr noch nicht vollendet haben.
[27]*Reindl-Krauskopf,* Computerstrafrecht 40 f.
[28]Die Vorsatzform der Wissentlichkeit iSd § 5 Abs 3 StGB ist für die Verwirklichung des Tatbestands erforderlich. Wissentlich handelt, wer den Umstand oder Erfolg, für den das Gesetz Wissentlichkeit voraussetzt, nicht bloß für möglich hält, sondern sein Vorliegen oder Eintreten für gewiss hält.
[29]EBRV (Erläuternde Bemerkungen zur Regierungsvorlage) 1505 BlgNR 24. GP 8.

Der Tatbestand **„Anbahnung von Sexualkontakten zu Unmündigen"**(§ 208a StGB) ist ebenfalls ein „allgemeines" Delikt, beinhaltet aber auch eine spezielle computerstrafrechtliche Ausformung **(„Cyber-Grooming").** Strafbar ist, wer einer unmündigen Person unter Verwendung eines Computersystems ein persönliches Treffen vorschlägt oder ein solches mit ihr vereinbart und eine konkrete Vorbereitungshandlung zur Durchführung dieses Treffens setzt, wenn eine dieser Tathandlungen von der Absicht (erweiterter Vorsatz) getragen ist an der Person eine strafbare Handlung gegen die sexuelle Integrität und Selbstbestimmung zu begehen. Strafdrohung ist Freiheitsstrafe bis zu zwei Jahren.

Was die Strafbarkeit der Anbieterseite (Produzenten und Verteiler) von pornographischem Material betrifft, ist das **Pornographiegesetz** einschlägig. Eines Verbrechens macht sich bspw schuldig, wer in *gewinnsüchtiger Absicht unzüchtige*[30] Schriften, Abbildungen oder andere unzüchtige Gegenstände vorsätzlich herstellt. Da es sich hier insgesamt, auch bei den Schriften, um Gegenstände handeln muss, ist es bspw notwendig, dass ein Text auf einem Datenträger abgespeichert ist. Strafdrohung ist Freiheitsstrafe bis zu einem Jahr.

Computerstrafrechtlich relevante Bestimmungen zum Schutz des öffentlichen Friedens im StGB sind insbesondere die strafbewehrten Verbote der **Anleitung zur Begehung einer terroristischen Straftat** (§ 278f), der **Aufforderung zu oder Gutheißung von mit Strafe bedrohten Handlungen** (§§ 282, 282a) sowie der **Verhetzung** (§ 283). Hier geht es bspw um das Anbieten einer Anleitung zum Bau einer Bombe auf einer Internet-Website, die Aufforderung zu einer terroristischen Straftat in einem Medium oderdie öffentliche Aufforderung zu Gewalt gegen unter anderem eine Religionsgesellschaft. Strafdrohung ist in allen drei Fällen bis zu zwei Jahre Freiheitsstrafe.

Relevante Bestimmungen des **Verbotsgesetzes** sind folgende: Wer unter anderem in einem Medium wie einer Internet-Website oder wer sonst öffentlich auf eine Weise, dass es vielen Menschen zugänglich wird, den Holocaust leugnet, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen (§ 3h VerbotsG – **„Ausschwitzlüge").** Bei besonderer Gefährlichkeit des Täters oder der Begehung drohen bis zu 20 Jahren Freiheitsstrafe. Des Weiteren ist das **öffentliche Auffordern**, Aneifern und Verleiten zu nationalsozialistischen Handlungen, wie etwa die Neubildung der NSDAP oder die Beteiligung an einer solchen Organisation, verboten (§ 3d VerbotsG). § 3d sieht eine Strafdrohung von fünf bis zehn Jahren Freiheitsstrafe vor, bei besonderer Gefährlichkeit des Täters oder der Betätigung bis zu 20 Jahren. Als Auffangtatbestand dient § 3g VerbotsG, der eine **sonstige Betätigung im nationalsozialistischen Sinn** verlangt (Strafdrohung wie bei § 3h VerbotsG). Die genannten Tatbestände sind subsidiär, wenn sich im Sachverhalt eine schwerere verpönte gerichtlich strafbare Handlung verbirgt.

3. Actus reus und Definitionen

How is the criminal conduct (actus reus) typically defined in these crimes (by description of the act, by consequence, other)?

Computerstrafrechtlich relevante Delikte sind überwiegend als **schlichte Tätigkeitsdelikte** ausgestaltet. Das heißt der objektive Tatbestand erschöpft sich in der Vornahme eines bestimmten Tuns. Der Eintritt einer von der Tathandlung gedanklich abtrennbaren Wirkung in der Außenwelt (Erfolg) wird nicht vorausgesetzt. Die Konzeption als schlichtes Tätigkeitsdelikt hat zur Folge, dass diese Delikte nicht durch bloßes Unterlassen begangen werden können.[31]

---

[30]Zum Erfordernis der „Unzüchtigkeit" siehe genauer *Freund,* Die Strafbarkeit von Internetdelikten – Eine Analyse am Beispiel pornographischer Inhalte (1998) 61 f.
[31]*Kienapfel/Höpfel/Kert,* Strafrecht Allgemeiner Teil[14] (2012) Z 9 Rz 14.

Ausnahmen sind allerdings etwa die Störung der Funktionsfähigkeit eines Computersystems (als Erfolg wird die schwere Störung eines Computersystems vorausgesetzt)[32] sowie die Datenbeschädigung und der betrügerische Datenverarbeitungsmissbrauch (als Erfolg wird hier der Eintritt eines Schadens verlangt)[33].

How is the object defined ("data", "writings", contents)?

„Daten" im Sinne des **StGB** sind sowohl personenbezogene als auch nicht personenbezogene Daten als auch Programme (§ 74 Abs 2 StGB). Für § 51 DSG gilt eine abweichende Definition: Nach § 4 Z 1 **DSG** sind Daten Angaben über Betroffene im Sinne des Datenschutzgesetzes, deren Identität bestimmt oder bestimmbar ist (= „personenbezogene Daten").

„Computersysteme" sind sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen (§ 74 Abs 1 Z 8 StGB).

„Unbare Zahlungsmittel" sind alle personengebundenen oder übertragbaren körperlichen Zahlungsmittel, die den Aussteller erkennen lassen, durch Codierung, Ausgestaltung oder Unterschrift gegen Fälschung oder missbräuchliche Verwendung geschützt sind und im Rechtsverkehr bargeldvertretende Funktion haben oder der Ausgabe von Bargeld dienen (§ 74 Abs 1 Z 10 StGB).

4. Beschränkungen hinsichtlich Tatsubjekt und Opfer

Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?

Grundsätzlich sind die genannten Delikte von **jedermann** begehbare Delikte.[34] **§ 51 DSG** hingegen ist als **Sonderdelikt** konzipiert: Unmittelbarer Täter kann nur der sein, der die relevanten Daten ausschließlich aufgrund seiner berufsmäßigen Beschäftigung anvertraut bekam oder dem sie zugänglich geworden sind oder der sich diese widerrechtlich verschafft hat. Da es sich um ein unrechtsbezogenes Sonderdelikt handelt, ist die Beteiligung eines Außenstehenden an § 51 DSG nach den allgemeinen Regeln des StGB möglich.[35]

Eine Beschränkung auf bestimmte Opfergruppen findet sich in den§§ 207a, 208a und 215a Abs 2a StGB, wonach das Verbot pornographischer Darstellungen und Darbietungen ausschließlich in Bezug auf **Minderjährige**[36] gilt. Das Verbot der Anbahnung von Sexualkontakten gilt nur hinsichtlich **unmündiger Personen,** also Personen, die das 14. Lebensjahr noch nicht erreicht haben (siehe § 74 Abs 1 Z 1 StGB).

5. Mensrea

Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?

Nein, im Bereich des Computerstrafrechts ist nur vorsätzliches Handeln strafbar.

---

[32] *Birklbauer/Hilf/Tipold,* BT I 272.
[33] *Birklbauer/Hilf/Tipold,* BT I 268; *Kirchbacher/Presslauer* in Höpfel/Ratz (Hrsg), WK² § 148 Rz 4 f.
[34] Siehe bspw für § 123 *Lewisch* in Höpfel/Ratz (Hrsg), WK² § 123 Rz 1 und für § 207a *Philipp* in Höpfel/Ratz (Hrsg), WK² § 207a Rz 7.
[35] Siehe *Salimi* in Höpfel/Ratz (Hrsg), WK² § 51 DSG Rz 13 f mwN.
[36] Siehe Fn 27.

6. Unterschiede computerspezifische Delikte – "traditionelle" Delikte

Are there specific differences between the definition of cyber crimes and "traditional" crimes?

Nein. Grundsätzlich ist anzumerken, dass viele traditionelle Delikte (vor allem im Bereich der Inhaltsdelikte) auch auf computerrechtlich relevante Sachverhalte angewendet werden. Der einzige Unterschied von computer*spezifischen* Delikten im Vergleich zu traditionellen Delikten kann in den überdurchschnittlich hohen Vorsatzanforderungen der computerspezifischen Delikte gesehen werden.[37]

C. Rechtsetzungstechnik

1. Computerstrafrecht und Legalitätsprinzip

Are there specific problems with respect to the principle of legality (e.g. vagueness, open-ended reference of the crime definition to other regulations?

Auffallend ist die sehr weite Definition eines Computersystems in § 74 Abs 1 Z 8, wonach sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen darunterfallen.

2. Vermeidung von übertriebenen abschreckenden Wirkungen für legitime User

How does legislation avoid undue chilling effects on legitimate use of ICT or of the internet?

Wie bereits erwähnt werden für eine Strafbarkeit oftmals hohe Anforderungen an den Vorsatz gestellt. Einerseits dadurch, dass ein extensiver erweiterter Vorsatz Voraussetzung für eine Strafbarkeit sein kann und andererseits dadurch, dass ein stärkerer Vorsatzgrad als Eventualvorsatz – also Wissentlichkeit oder Absichtlichkeit – gefordert sein kann. § 207a Abs 3a bspw verlangt den *wissentlichen* Zugriff auf pornographische Darstellungen Minderjähriger. So soll zum Beispiel gewährleistet werden, dass sich nicht bereits jener User strafbar macht, in dessen Browser eine solche Darstellung in einem Pop-up Fenster erscheint.

3. Berücksichtigung technischer Entwicklungen

How does criminal legislation avoid becoming obsolete in light of rapid technological innovation?

Viele Delikte des Computerstrafrechts sind unabhängig von der Verwendung einer bestimmten Technologie formuliert. Es ist demnach nicht von Bedeutung auf welche Weise sie genau begangen werden. Das bietet die Möglichkeit, dass auch neue technische Entwicklungen unter diese Tatbestände subsumiert werden können, ohne dass es einer Gesetzesänderung bedarf.[38] Verweise auf verwaltungsrechtliche Vorschriften kennt man im Computerstrafrecht nicht.

---

[37]Siehe bspw *Bergauer,* Kritische Anmerkungen zu § 126c, ÖJZ 2007, 532 (535); *Salimi,* Zahnloses Cyberstrafrecht? – Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012, 998 (1000 ff); vgl EBRV StrÄG 2002, 1166 BlgNR 21. GP 25.

[38]*Reindl-Krauskopf,*Computerstrafrecht 48; *Reindl,* SIAK-Journal 2007, 2 (3).

D. Umfang der Kriminalisierung

1. Strafbarkeit von Vorbereitungshandlungen

To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g. acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Havelegislaturesmadespecificeffortstoavoidover-criminalisation?

Typische Vorbereitungsdelikte sind der Missbrauch von Computerprogrammen und Zugangsdaten (§ 126c) und die Vorbereitung der Fälschung unbarer Zahlungsmittel (§ 241c).Auch der widerrechtliche Zugriff auf ein Computersystem (§ 118a), Datenspionage (§§ 119 ff), der Eingriff in das Recht auf Zugangskontrolle (§ 10 ZuKG), die Fälschung unbarer Zahlungsmittel (§ 241a) und das Anbahnen von Sexualkontakten (§ 208a) können als dem Vorfeldbereich des Computerstrafrechts angehörig gesehen werden.[39]

Die Implementierung dieser Delikte wurde im Hinblick auf die Vorverlagerung des Strafrechts in das sonst strafrechtsfreie Vorfeld diskutiert. Allerdings gab es keine spezielle computerstrafrechtliche Diskussion diesbezüglich, sondern es wurden lediglich allgemeine Problematiken von Vorbereitungsdelikten besprochen.

Der Tatbestand des Missbrauchs von Computerprogrammen sieht einschränkend vor, dass es sich beim Tatobjekt *Computerprogramm*um ein solches handeln muss, das aufgrund seiner besonderen Beschaffenheit gerade *zum Zweck der Begehung* einer der genannten strafbaren Handlungen *geschaffen oder adaptiert wurde.*Damit kommt Software, die für einen legalen Zweck geschaffen wurde, technisch gesehen aber auch für illegale Zwecke eingesetzt werden könnte – da sich die wesentlichen Programmabläufe legaler Tools nicht von illegalen unterscheiden – grundsätzlich nicht als Tatobjekt in Frage. Diese Beschränkung wird in der Literatur allerdings als zu weitgehend kritisiert. Es wird vorgeschlagen den objektiven Tatbestand dahingehend abzuändern, dass das gegenständliche Computerprogramm ersichtlich zur Begehung eines der in § 126c genannten Straftaten „geeignet" sein muss, unabhängig davon zu welchem Zweck es ursprünglich geschaffen oder adaptiert wurde.[40]

Des Weiteren ist der Tatbestand des Missbrauchs von Computerprogrammen erst dann erfüllt, wenn sich der erweiterte Vorsatz des Täters auf die vollständige Erfüllung des Unrechts der in § 126c aufgezählten Delikte erstreckt.

Ferner sieht § 126c Abs 2 die Möglichkeit einer Strafaufhebung für schadenvermeidendes Verhalten vor.[41] Demnach ist der Täter nicht zu bestrafen, wenn er freiwillig den Gebrauch des Computerprogramms, -passworts, des Zugangscodes oder der vergleichbaren Daten im Zusammenhang mit der Begehung einer in § 126c Abs 1 aufgezählten Handlungen verhindert.Bestimmungen zur „Tätigen Reue" finden sich ebenfalls in § 241d (für die Vorbereitung der Fälschung und die Fälschung unbarer Zahlungsmittel) sowie in § 208a Abs 2 (für die Anbahnung von Sexualkontakten).

---

[39]*Reindl-Krauskopf,*Computerstrafrecht 8 f.

[40]*Bergauer,* Kritische Anmerkungen zu § 126c, ÖJZ 2007, 532 (534).

[41]Die Bestimmung vereint Elemente von „Tätiger Reue" und des Rücktritts vom Versuch (§ 16 StGB): siehe genauer EBRV StrÄG 2002, 1166 BlgNR 21.GP 30.

2. Strafbarkeit des Besitzes

To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds? How is "possession" of data defined? Doesthedefinitionincludetemporarypossessionormereviewing?

Ganz allgemein lässt sich der Besitz als Tathandlung wie folgt **definieren:** Besitzer ist, wer den inkriminierten Gegenstand innehat und daher faktisch auf ihn zugreifen und über ihn verfügen kann. Entscheidend, ob Besitz vorliegt, ist also die tatsächliche unmittelbare Sachherrschaft über einen Gegenstand. Der strafrechtliche Besitzbegriff ist gleichbedeutend mit dem des Gewahrsams im Bereich der Vermögensdelikte. Bloßer Mitgewahrsam genügt. Ob wie beim Gewahrsam die tatsächliche Sachherrschaft von einem Herrschaftswillen getragen werden muss, ist unklar. Wichtig ist, dass ein geforderter Herrschaftswille nicht den für den strafbaren Besitz nötigen Vorsatz ersetzen kann. Die Tathandlung der Innehabung in § 10 Zugangskontrollgesetz kann als inhaltlich gleichbedeutend mit der des Besitzens angesehen werden.[42]

§ 207a Abs 3 verbietet das **Besitzen pornographischer Darstellungen** Minderjähriger. Auch „bloße" Konsumenten machen sich demnach strafbar, da sie aufgrund ihrer Nachfrage den Markt und somit auch die Produktion kinderpornographischen Materials beeinflussen. Für das Besitzen der Darstellung ist es in diesem Zusammenhang notwendig, dass der Täter sie bspw auf seinem Computer gezielt abspeichert. Eine im Cache des Computers automatisch abgelegte Kopie reicht dafür in der Regel nicht aus.[43] Das (bloße) Ansehen kinderpornographischen Materials kann damit keinesfalls unter die Tathandlung „besitzen" subsumiert werden. 2009 hat der österreichische Gesetzgeber aber auch das bloße Betrachten kinderpornographischer Darstellungen und Darbietungen unter Strafe gestellt (§ 207a Abs 3a und § 215a Abs 2a). Um hier zu einer Strafbarkeit zu kommen, ist allerdings der *wissentliche* Zugriff auf eine einschlägige Darstellung bzw Darbietung erforderlich. Für die anderen Tathandlungen des § 207a ist Eventualvorsatz ausreichend.

§ 126c bestraft den **Besitz von Computerprogrammen**, Computerpasswörtern, Zugangscodes oder vergleichbarer Daten, sofern es der Täter ernstlich für möglich hält und sich damit abfindet, dass diese zur Begehung eines computerspezifischen Delikts gebraucht werden.

Gemäß § 241c ist der **Besitz eines Mittels oder Werkzeugs** – getragen von dem erweiterten Vorsatz sich oder einem anderen damit eine Fälschung eines unbaren Zahlungsmittels zu ermöglichen – strafbar.

§ 10 ZuKG bestraft die **gewerbsmäßige Innehabung von Umgehungsvorrichtungen.** Darunter wird bspw verstanden, dass jemand eine technische Einrichtung zur Umgehung von Sicherungen bei zugangskontrollierten Diensten verwendet und die mit ihrer Hilfe entschlüsselten Signale gegen Gebühren anderen Nutzern zur Verfügung stellt.[44]

Auch im Pornographiegesetz findet sich eine Art Besitzstrafbarkeit, nämlich das **vorrätig halten von unzüchtigen Gegenständen zum Zweck der Verbreitung.** Im Unterschied zu § 207a sind daher aber vom Pornographiegesetz keine bloßen Konsumenten erfasst.

---

[42] *Hochmayr,* Strafbarer Besitz von Gegenständen – Zur Reichweite der Strafdrohungen für den (bloßen) Besitz von Waffen, Suchtmitteln, Kinderpornographie, etc. (2005) 8 ff.
[43] *Reindl-Krauskopf,*Computerstrafrecht 42.
[44] *Reindl,* SIAK-Journal 2007, 2 (6).

3. Verantwortlichkeit und Verpflichtungen von Provider

To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g. hosting or access providers)? What are the requirements of their liability, especially concerning mensrea? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose costs?Istherecriminalliabilityforviolating such obligations?

Vorschriften über die Verantwortlichkeit der verschiedenen Provider (Access-, Caching-, Host-Provider, Betreiber von Suchmaschinen und Setzer von Hyperlinks) finden sich im **E-Commerce-Gesetz** (ECG).[45] Die Vorschriften des ECG normieren für die Provider jeweils unterschiedliche Voraussetzungen, bei deren Einhaltung sie strafrechtlich (und auch zivilrechtlich)*nicht* zur Verantwortung gezogen werden können. Die Vorschriften des ECG wirken somit haftungsbeschränkend. Beachtet ein Provider die für ihn aufgestellten Regeln allerdings nicht *und* verwirklicht er zusätzlich auch einen strafrechtlichen Tatbestand, ist er strafbar.[46]

Entfällt die Haftungsfreistellung, so ist eine Strafbarkeit des Providers für eine Beteiligung am Delikt des Users nach allgemeinen Grundsätzen zu prüfen. Eine Strafbarkeit durch Tun wird in der Regel allerdings nicht vorliegen, außer eventuell bei Link-Setzer. Naheliegender ist eine Strafbarkeit des Providers durch Unterlassen. Um zu einer Strafbarkeit des Providers zu kommen, muss diesem allerdings eine Garantenstellung nachgewiesen werden können, was bei Accessprovider, Betreiber von Suchmaschinen und Link-Setzer grundsätzlich nicht möglich sein wird. Bei Caching- und Hostprovidern bietet § 78 Telekommunikationsgesetz (TKG) einen möglichen Ansatzpunkt für eine gesetzliche Garantenstellung. Demnach haben Inhaber von Telekommunikationsendeinrichtungen *geeignete* Maßnahmen zu treffen, um eine missbräuchliche Verwendung ihres Geräts auszuschließen, soweit ihnen dies *zumutbar* ist und die Bestimmungen des *Datenschutzgesetzes* eingehalten werden.[47] Allerdings ist des Weiteren zu beachten, dass – wie bereits erwähnt – die meisten Delikte des Computerstrafrechts schlichte Tätigkeitsdelikte sind und diese nicht durch Unterlassen begangen werden können.

Für die Haftungsfreistellung gelten im Detail folgende Regelungen:

Für den **Access-Provider** (siehe § 13 Abs 1 ECG) und für den **Betreiber einer Suchmaschine** (siehe § 14 Abs 1 ECG) gilt, dass diese für die übermittelten bzw. abgefragten Informationen dann nicht verantwortlich sind, wenn sie (i) die Übermittlung nicht veranlassen, (ii) den Empfänger der übermittelten bzw. abgefragten Information nicht auswählen und (iii) die übermittelte bzw. abgefragten Information weder auswählen noch verändern. Für den Betreiber einer Suchmaschine ist allerdings zu beachten, dass ihm das Haftungsprivileg dann nicht zugutekommt, wenn die Inhalte von Personen stammen, die dem Suchmaschinenbetreiber unterstehen oder die von ihm beaufsichtigt werden.

Das Haftungsprivileg des **Caching-Providers** ist in § 15 ECG geregelt: Demnach ist dieser nicht zur Verantwortung zu ziehen, wenn er (i) die Informationen nicht verändert, (ii) die Bedingungen für den Zugang zur Information beachtet, (iii) die Regeln für die Aktualisierung der Informationbeachtet, (iv) die zulässige Anwendung von Technologien zur Sammlung von Daten nicht beeinträchtigt und (v) unverzüglich eine von ihm gespeicherte Information entfernt oder den Zugang zu ihr sperrt, sobald er tatsächliche Kenntnis davon erhalten hat, dass die

[45]Das ECG geht zum größten Teil auf die E-Commerce-Richtlinie, ABl L 178 vom 17. 7. 2000, zurück.
[46]Siehe ausführlich *Reindl-Krauskopf,*Computerstrafrecht 103 ff.
[47]Siehe ausführlich *Reindl-Krauskopf,* Computerstrafrecht 103 ff.

Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt oder der Zugang zu ihr gesperrt wurde.

Ein **Host-Provider**(siehe § 16 Abs 1 ECG) und ein **Link-Setzer** (siehe § 17 Abs 1 ECG) bleiben frei von Verantwortung, wenn sie (i) von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis haben oder (ii) unverzüglich tätig werden, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis haben. Auch bei diesen beiden Arten von Provider ist zu beachten, dass das Haftungsprivileg nicht gilt, wenn der Nutzer oder die Person, von der die Informationen stammen, dem Provider unterstehen oder von ihm beaufsichtigt werden.

Caching-, Host-Provider und Link-Setzer sind also **verpflichtet tätig zu werden,** sobald sie von rechtswidrigen Tätigkeiten oder Informationen tatsächliche Kenntnis haben. Dabei kann der Host-Provider selbst die Informationen löschen oder sperren oder aber seinen Vertragspartner dazu anhalten. Ob der Host-Provider zum Löschen verpflichtet ist, wenn der Vertragspartner dem Auftrag nicht nachkommt ist strittig.[48]Die genannten Provider haben die dadurch entstehenden Kosten selbst zu tragen. Etwaige Sonderregeln zum Kostenersatz existieren nicht. Kommen die Provider diesen Verpflichtungen nicht nach, so verlieren sie ihr Haftungsprivileg. Erfüllen Caching-, Host-Provider und Link-Setzer auch gleichzeitig einen Straftatbestand, so ist bei ihrer strafrechtlichen Verantwortlichkeit zu beachten, dass eine solche erst dann in Betracht kommt, wenn die genannten Provider *tatsächliche Kenntnis* von der rechtswidrigen Tätigkeit oder Information haben. Im Endeffekt muss sich diese tatsächliche Kenntnis – die am ehesten der Wissentlichkeit gem § 5 Abs 2 StGB entspricht – dann auch auf den objektiven Tatbestand eines in Frage kommenden Delikts beziehen. So kommt es letztlich bei jenen Delikten, bei denen nur Eventualvorsatz gefordert ist, zu einer **Anhebung des Vorsatzerfordernisses** für die genannten Provider.[49]

Are providers obliged to monitor and control what information they provide or offer access to?

Die genannten Provider sind *nicht* verpflichtet, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf rechtswidrige Tätigkeiten hinweisen (§ 18 ECG).

Are providers obliged to provide information on the identity of users?

Siehe dazu Frage F. 1.

4. Verfassungsrechtliche Beschränkungen

What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and internet crime (e.g. freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mensrea requirements)?

Was die Inhaltsdelikte, insbesondere das Verbot nationalsozialistischer Inhalte, betrifft, wurde unter anderem diskutiert, in welchem Verhältnis dieses Verbot zum Recht auf freie Meinungsäußerung nach Art 10 EMRK und dem Recht auf Versammlungs- und Vereinsfreiheit nach Art 11 EMRK steht. Eine Beschäftigung mit oder Diskussion von nationalsozialistischen Inhalten in sachlicher Weise ist (auch im Internet) zuzulassen, allerdings nur solange keine Strafbarkeit nach dem Verbotsgesetz gegeben ist. Eine derartige Beschränkung der verfassungsrechtlich

[48]Bejahend *Reindl,* E-Commerce und Strafrecht (2003) 277 mwN.
[49]*Reindl-Krauskopf,* Computerstrafrecht 113 f, 119 und 125.

gewährleisteten Rechte ist im Sinne der Art 10 Abs 2 und Art 11 Abs 2 sowie im Einklang mit der Judikatur des EGMR, der ausgesprochen hat, dass ein Verbot nationalsozialistischer Betätigung im Interesse der nationalen Sicherheit und der territorialen Unversehrtheit in einer demokratischen Gesellschaft notwendig ist.[50]

5. Strafrechtliche Sanktionen

Does the law provide for criminal sanctions specifically targeting cyber criminals (e.g. a temporary ban from using the internet)?

Als strafrechtliche Sanktionen für Täter computerspezifischer Delikte – wie für Täter „traditioneller" Delikte– finden sich im StGB und in den entsprechenden Nebengesetzenprimär **Geld**- und/oder **Freiheitsstrafen.** Als weitere Sanktionen kommen insbesondere die **Konfiskation** nach § 19a und die **Einziehung** nach § 26 StGB – bei Vorliegen der entsprechenden Voraussetzungen – in Betracht. Der Konfiskation unterliegen alle Gegenstände, die zur Zeit der gerichtlichen Entscheidung im Eigentum des Täters stehen und (i) die er zur Begehung einer vorsätzlichen Straftat verwendet hat, (ii) die von ihm dazu bestimmt waren, dafür verwendet zu werden, oder (iii) die durch diese Handlung hervorgebracht worden sind. Eingezogen werde können alle im Inland befindlichen Werkzeuge und Produkte von Straftaten, wobei von der Sache selbst eine Gefahr ausgehen muss. Nicht einzuziehen sind Gegenstände des täglichen Gebrauchs. Von einer Einziehung ist abzusehen, wenn der Berechtigte die Gefährlichkeit des Gegenstandes beseitigt. Kann also bspw kinderpornographisches Material von einer Festplatte gelöscht werden, so ist dessen Einziehung unzulässig.[51]In den bereits besprochenen Nebengesetzen finden sich teilweise Sonderbestimmungen zur Einziehung.

E. Alternativen zur Kriminalisierung

1. Verhältnis des Strafrecht zum Zivilrecht und zum Verwaltungsstrafrecht

What role does criminal law play in relation to other ways of combating abuse of ICT and the internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?

Die **praktische Bedeutung** des Computerstrafrechts ist gering, da es kaum zu Verurteilungen kommt. Die meisten Verurteilungen gab es 2007 hinsichtlich pornographischer Darstellungen Minderjähriger (187 Verurteilungen), bezüglich der anderen Delikte bewegen sich die Verurteilungszahlen im einstelligen Bereich.[52]Im Jahr 2010 kam es hinsichtlich vieler computerspezifischer Delikte zu keiner einzigen Verurteilung.[53]

Zivilrechtlich richtet sich der Ersatz eines entstandenen Schadens nach den allgemeinen Regeln des Schadenersatzes. Handelt es sich um eine vorsätzliche Schädigung, so hat der Schädiger volle Genugtuung zu leisten, das heißt den positiven Schaden und auch den entgangenen Gewinn zu ersetzen (§ 1324 ABGB).[54]Teilweise finden sich in den entsprechenden Nebengesetzen auch Sonderregeln dazu (siehe zB § 7 ZuKG). Das Opfer hat die Möglichkeit sich dem Strafverfahren als **Privatbeteiligter** anzuschließen, um Ersatz für einen Schaden oder Beeinträchtigung zu erhalten. Dabei können nur gegen den Beschuldigten gerichtete Ansprüche geltend gemacht werden. Ein Zuspruch eines Schadenersatzes kann im Strafurteil allerdings nur dann erfolgen,

[50]Siehe *Lässig* in Höpfel/Ratz (Hrsg), WK[2] VerbotsG § 3g Rz 2 und *Reindl-Krauskopf,* Computerstrafrecht 49, jeweils mwN.
[51]OGH 20. 1. 2011, 11 Os 163/10w, siehe auch JBl 2007, 470 mit Anmerkungen *Salimi.*
[52]Siehe die Zusammenstellung bei *Reindl-Krauskopf,* Computerstrafrecht 7.
[53]Siehe die entsprechenden Hinweise bei den einzelnen Delikten bei *Birklbauer/Hilf/Tipold,* BT I.
[54] Siehe zB*Öhlböck/Esztegar,* Journal für Strafrecht 2011, 126 (131).

wenn es zu einem rechtskräftigen Schuldspruch des Angeklagten gekommen ist. Eine teilweise Zuerkennung des geltend gemachten Anspruches ist möglich. Wird der Beschuldigte freigesprochen, so muss der Privatbeteiligte auf den Zivilrechtsweg verwiesen werden. Der Privatbeteiligte kann trotz Zuspruchs im Strafverfahren darüber hinausgehende Ansprüche im Zivilverfahren einklagen. Dies kommt in der Praxis sehr häufig vor, da dem Privatbeteiligten oftmals nur ein symbolischer Betrag zugesprochen wird. Ob der Zivilrichter im nachfolgenden Prozess an die Feststellungen aus dem Strafurteil gebunden ist, ist strittig.[55]

Verwaltungsstrafrechtliche Sanktionen für computerspezifische verbotene Handlungen finden sich in Nebengesetzen wie etwa dem Telekommunikationsgesetz (§ 109 TKG), dem E-Commerce-Gesetz (§ 26 ECG), dem Datenschutzgesetz (§ 52 DSG), dem Zugangskontrollgesetz (§ 13 ZuKG)[56] oder dem Pornographiegesetz (§ 14 Pornographiegesetz). Alle genannten verwaltungsrechtlichen Strafbestimmungen enthalten eine ausdrückliche **Subsidiaritätsklausel:** Demnach liegt eine Verwaltungsübertretung nicht vor, wenn die Tat auch den Tatbestand einer gerichtlich strafbaren Handlung erfüllt.

2. Außerstrafrechtliche Sanktionen

What non-criminal means of combating offensive websites are used/propagated (e.g. closing down websites, blocking access to websites)?

Einen möglichen Ansatzpunkt bietet der bereits erwähnte § 78 TKG, wonach bestimmte Provider, soweit zumutbar und unter Einhaltung der Bestimmungen des DSG, geeignete Maßnahmen zu treffen haben, um eine missbräuchliche Verwendung ihrer Einrichtung auszuschließen. Diensteanbieter, die lediglich den Zugang zu Kommunikationsdiensten vermitteln, sind von dieser Bestimmung nicht erfasst.

3. Einsatz von Schutzmaßnahmen

To what extent are ICT users expected to protect themselves (e.g. by encryption of messages, using pass-words, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g. by using anti-virus software or protecting access to private networks by password? Does the lack of reasonable self-protection provide a defense for defendants accused of illegally entering or abusing another person's network or abusing their data?

Wie bereits dargelegt verpflichtet § 78 TKG Inhaber von Funkanlagen und Telekommunikationsendeinrichtungen, soweit ihnen dies zumutbar ist und die Bestimmungen des DSG eingehalten werden, geeignete Maßnahmen zu treffen, um eine missbräuchliche Verwendung ihrer Einrichtung auszuschließen. Diese Bestimmung kann so interpretiert werden, dass diese Verpflichtung sämtliche Inhaber von Telekommunikationsendeinrichtungen, somit auch einen gewöhnlichen Internetnutzer, der Inhaber eines Breitbandmodems ist und damit im Internet kommuniziert, trifft.[57] Wer entgegen dieser Bestimmung keine geeigneten Maßnahmen trifft, begeht eine Verwaltungsübertretung und ist mit einer Geldstrafe bis zu EUR 4.000,00 zu bestrafen (§ 109 Abs 1 Z 6 TKG). Allerdings ist hervorzuheben, dass die Verhängung einer Verwaltungsstrafe – insbesondere im Falle von gewöhnlichen Internet-Usern – nur in seltenen Fällen möglich sein wird. Ein normales Anti-Viren-Programm oder eine gewöhnliche Firewall wird in der Regel nicht geeignet sein, um bspw Hackerangriffe zu vermeiden; und die

[55] Siehe *Seiler,* Strafprozessrecht[11] (2010) Rz 266 ff mwN.
[56] Siehe § 13 ZuKG.
[57] *Bergauer,* Aktuelles zum Computerstrafrecht – Zugleich eine Buchbesprechung, jusIT 2010, 132 (133).

Installierung „professioneller" Softwareprogramme wird dem normalen Internet-User im Regelfall nicht zugemutet werden können.

Regelmäßig wird im Falle eines Hackerangriffs auch eine **zivilrechtliche Haftung** (auf Schadenersatz) des Gehackten im Raum stehen, wenn dieser keine ausreichenden Sicherheitsmaßnahmen getroffen hat.Haftet ein Unternehmen seinem Kunden aus Vertrag, so trifft das Unternehmen sogar die Beweislast, dass es die erforderlichen Sicherheitsmaßnahmen getroffen hat (siehe § 1298 ABGB). Insbesondere Unternehmen sollten daher umfassende Schutzmaßnahmen ergreifen und ein entsprechendes Sicherheitskonzept für ihr Unternehmen erstellen (Stichwort „IT-Compliance").[58]

In einem Strafverfahren kann der Angeklagte *nicht* wirksam geltend machen, dass der Inhaber seines Angriffszieles keine ausreichenden Schutzmaßnahmen ergriffen hat. Im Rahmen einer schadenersatzrechtlichen Haftung im Zivilrecht allerdings könnte das Nichtergreifen von Schutzmaßnahmen als mögliches Mitverschulden gesehen werden und damit zu einem geringeren Schadenersatzanspruch führen.

F. Einschränkungen der Anonymität

Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?

Anbieter öffentlicher Kommunikationsdienste (Internet-Zugangsdienste, öffentliche Telefondienste einschließlich Internettelefonie und E-Mail-Dienste) sind verpflichtet bestimmte Kommunikationsdaten für eine Dauer von sechs Monaten für Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten verdachtsunabhängig (als Vorratsdaten) zu speichern. Die zu speichernden Datenkategorien sind in § 102a TKG abschließend festgelegt: darunter fallen Stamm-, Zugangs- und Verkehrsdaten, aber keine Inhaltsdaten.

Internet-Zugangsdienste haben die Stammdaten (zB Name und Anschrift) der Teilnehmer hinter IP-Adressen und den Zeitraum der Zuteilung der IP-Adresse zu speichern. Des Weiteren haben sie die Kennung des Anschlusses zu speichern, über die der Internetzugang erfolgt ist. Anbieter öffentlicher Telefondienste haben Art und Zeitraum jedes Kommunikationsvorganges, die Kennung der beteiligten Anschlüsse und die Stammdaten der betroffenen Teilnehmer zu speichern. Anbieter von E-Mail-Diensten sind zur Speicherung von Kennung und Stammdaten der Teilnehmer hinter E-Mail-Adressen, Herkunft und Adressat übermittelter oder empfangener E-Mails und An- und Abmeldungen von E-Mail-Diensten verpflichtet.

In einem **Strafverfahren** haben Gericht, Staatsanwalt und Kriminalpolizei Zugriff auf diese Daten. Die Anbieter sind unter bestimmten Voraussetzungen verpflichtet diese Daten herauszugeben. Eine Auskunft über als Vorratsdaten gespeicherte Daten ist grundsätzlich nur unter den Voraussetzungen des § 135 Abs 2a Strafprozessordnung (StPO) zulässig. Drei Fallgruppen sind hier zu unterscheiden: (i) Die Auskunft ist zulässig, wenn der Inhaber der technischen Einrichtung, die Ursprung oder Ziel einer Übertragung von Nachrichten war oder sein wird, der Auskunft ausdrücklich zustimmt und wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als sechs Monaten bedroht ist, gefördert werden kann. (ii) Ebenfalls zulässig ist eine Auskunft, wenn zu erwarten ist, dass dadurch die Aufklärung einer vorsätzlich begangenen Straftat, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist, gefördert werden kann und anzunehmen ist, dass dadurch Daten des Beschuldigten ermittelt werden können. (iii) Dritte Möglichkeit der Beauskunftung ist unter der

[58] *Zankl,* IT Update 4.0 – Aktuelle Entwicklungen, ecolex 2012, 122 (123); *Tichy/Paulitsch,* Jagd auf die Gehackten, Der Standard 2011/40/15.

Voraussetzung, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer mit mehr als einem Jahr Freiheitsstrafe bedrohten Vorsatztat dringend verdächtig ist, ermittelt werden kann. Als formelle Voraussetzung ist die Anordnung der Staatsanwaltschaft aufgrund einer gerichtlichen Bewilligung notwendig.

Allerdings kann die Staatsanwaltschaft zur Aufklärung jeder Straftat ohne richterliche Bewilligung Stammdaten und Kennung von Teilnehmern hinter bestimmten IP-Adressen oder E-Mail-Adressen erfragen, auch wenn diese als Vorratsdaten gespeichert werden (§ 76a Abs 2 StPO). Handelt es sich lediglich um Stammdaten, so kann die Kriminalpolizei auch von sich aus tätig werden (§ 76a Abs 1 StPO). Diese Möglichkeit der Beauskunftung ohne richterliche Bewilligung wird in der Literatur kritisiert.[59]

Auch die **Sicherheitspolizei** kann im Rahmen der ersten allgemeinen Hilfeleistung und der Gefahrenabwehr Auskunft über die Stammdaten des Benutzers einer IP-Adresse verlangen, selbst dann, wenn deren Ermittlung die Verarbeitung von Vorratsdaten voraussetzt (§ 53 Abs 3a Sicherheitspolizeigesetz).

Are there laws or regulations obliging an internet service provider to register users prior to providing services?

Zwischen Diensteanbieter (Provider) und Nutzer sindlaut Bestimmungen des ECG Vereinbarungen über die Übermittlung oder Speicherung von Informationen abzuschließen.

Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

Nein.Die Möglichkeit einen Beschuldigten, gegen den ein Ermittlungsverfahren durchgeführt wird, zwingen zu können von ihm verwendete Passwörter zu verraten, würde dem Verbot des Zwangs zur Selbstbelastung widersprechen.

G. Internationalisierung

1. Internationales Strafrecht

Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to entering data from abroad?

Österreichische Gerichtsbarkeit ist jedenfalls dann gegeben, wenn der Täter entweder im Inland handelt oder der Erfolg im Inland eingetreten ist (Inlandstat, §§ 62 iVm 67 StGB). Ein Erfolg im Inland ist dann eingetreten, wenn sich tatsächliche Erscheinungen in der Außenwelt merkbar verändern. Gibt der Täter also bspw Daten im Ausland in das Internet ein, so wäre österreichische Gerichtsbarkeit gegeben, wenn bspw dadurch in Österreich ein Vermögensschaden einträte. Das bloße Abrufen von Informationen im Internet wird von der überwiegenden Meinung noch nicht als Erfolgseintritt gesehen.[60]Handelt es sich um eine Inlandstat, so ist keine „doppelte Strafbarkeit" erforderlich.

Für schwere Verstöße gegen das Verbot pornographischer Darstellungen Minderjähriger (§ 207a Abs 1 und 2)[61] im Ausland enthält § 64 Abs 1 Z 4a StGB einen Anknüpfungspunkt für österreichische Gerichtsbarkeit. Voraussetzung

---

[59]*Feiler/Stahov,* Die Einführung der Vorratsdatenspeicherung in Österreich, Medien und Recht 2011, 111 (114); *Metzler,* Pflicht zur Vorratsdatenspeicherung in Kraft – und bald schon Rechtsgeschichte? Zeitschrift für Energie- und Technikrecht 2012, 106 (107 f).

[60]*Reindl-Krauskopf,* Computerstrafrecht 131 f; siehe ausführlich *Höpfel/U. Kathrein* in Höpfel/Ratz (Hrsg), WK² § 67 Rz 13a mwN.

[61]Nicht erfasst sind Fälle des Besitzes kinderpornographischen Materials oder des wissentlichen Zugriffs darauf im Internet.

dafür ist, dass (i) der Täter oder das Opfer Österreicher ist oder seinen gewöhnlichen Aufenthalt im Inland hat, (ii) durch die Tat sonstige österreichische Interessen verletzt worden sind *oder* (iii) der Täter zur Zeit der Tat Ausländer war, sich in Österreich aufhält und nicht ausgeliefert werden kann.

Handelt es sich um ein Medieninhaltsdelikt, also um Straftaten, die durch den Inhalt eines Mediums[62] begangen werden und in einer an einen größeren Personenkreis gerichtete Mitteilung oder Darbietung bestehen, so sind die besonderen strafrechtlichen Bestimmungen des Mediengesetzes, wie § 51 über den Geltungsbereich, zu beachten. § 51 Mediengesetz bietet eigene Regeln für die Anknüpfung inländischer Gerichtsbarkeit Medien betreffend, die ihren Sitz im Ausland haben. Verbreitet der Täter zB nationalsozialistische Propagandaschriften über ein Medium wie zB eine Internet-Website, welcheihren Sitz im Ausland hat, so ist österreichische Gerichtsbarkeit gegeben, wenn folgende Voraussetzungen kumulativ vorliegen: (i) die Abrufbarkeit des Mediums im Inland, (ii) ein besonderer Bezug zu österreichischen Interessen und (iii) die Verletzung bestimmter Rechtsgüter wie die Ehre, der wirtschaftliche Ruf, die Privat- und Geheimsphäre, die sexuelle Integrität und Selbstbestimmung und die Sicherheit des Staates und der öffentliche Frieden.

2. Der Einfluss internationaler Instrumente auf das österreichische Strafrecht

To what extent has your country's criminal law in the area of ICT and internet been influenced by international legal instruments?

Das österreichische Strafrecht wurde im Bereich des Computerstrafrechts ab dem Jahr 2000 wesentlich von internationalen und europäischen Vorgaben beeinflusst. In das Kernstrafrecht wurden mit dem Strafrechtsänderungsgesetz **(StRÄG) 2002**[63]folgende Tatbestände in Umsetzung der Cybercrime-Konvention des Europarats vom 23. 11. 2001 neu eingeführt: Hacking (§ 118a), Missbräuchliches Abfangen von Daten (§ 119a), Missbrauch von Tonaufnahme- oder Abhörgeräten (§ 120 Abs 2a), Störung der Funktionsfähigkeit eines Computersystems(§ 126b), Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c) undDatenfälschung (§ 225a). Des Weiteren wurden entsprechende Anpassungen an die Cybercrime-Konvention durchgeführt (bei§§ 119 und 148a). Eine zweite wesentliche Novelle erfolgte mit dem **StRÄG 2004**[64], mit dem insbesondere der Rahmenbeschluss des Rates zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln vom 28. 5. 2001 ins österreichische Recht umgesetzt wurde (§§ 241a-g StGB) sowie § 207a StGB den Erfordernissen verschiedener internationaler und europäischer Instrumente (wie zB der Cybercrime-Konvention) angepasst wurde. **2008**[65] wurden die Vorgaben des Rahmenbeschlusses über Angriffe auf Informationssysteme in das österreichische Recht implementiert und Änderungen bei bestehenden Delikten (§§ 118a, 126a und b StGB) vorgenommen.**2011**[66] erfolgte die Implementierung von§ 208a („Grooming")und § 215a Abs 2a StGB in das österreichische Recht in Umsetzung des Übereinkommens des Europarates zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch (SEV-Nr. 201).Die Inhaltsdelikte terroristische Handlungen betreffend wurden ebenfalls**2011**[67] in Umsetzung des Übereinkommens des Europarats zur Verhütung von Terrorismus (ETS

[62]Zum Begriff des Mediums iSd Mediengesetzes vergleiche ausführlich *Rami* in Höpfel/Ratz (Hrsg), WK²MedienG § 1 Rz 13.
[63]BGBl I 2002/134.
[64]BGBl I 2004/15.
[65]BGBl I 2007/109.
[66]BGBl I 2011/130.
[67]BGBl I 2011/103.

Nr. 196)sowie des Rahmenbeschlusses 2008/919/JI zur Terrorismusbekämpfung[68] in das österreichische Recht übernommen. Was Nebengesetze betrifft, wurde bspw 2000 das Datenschutzgesetz und das Zugangskontrollgesetz sowie 2001 das E-Commerce-Gesetz in Umsetzung europarechtlicher Vorgaben geschaffen.

3. Teilnahme an Expertengruppen

Does your country participate in discussions about the harmonization of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

Exemplarisch werden folgende Teilnahmen Österreichs an einschlägigen Expertengruppen genannt: Österreich war Mitglied der"U.N. Open-endedintergovernmental expert grouptoconduct a comprehensivestudyoftheproblemofcybercrime", die von 17.-21. Januar 2011 in Wien tagte. Des Weiteren nehmen österreichische Vertreter des Bundeskanzleramts und der verschiedenen Ministerien regelmäßig an den jährlich stattfindenden„Octopus Interface-Konferenzen" der CooperationagainstCybercrime des Europarats teil.

H. Künftige Entwicklungen

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

Rechtliche Debatten beinhalten regelmäßig eine Kritik an den oftmals sehr komplizierten Formulierungen der Computerstraftatbestände sowie an den überdurchschnittlich hohen Vorsatzanforderungen, insbesondere was den erweiterten Vorsatz betrifft. Dies führt dazu, dass bspw der Hackingparagraph aufgrund von Beweisschwierigkeiten praktisch unanwendbar ist.[69] Dies zeigen auch die extrem niedrigen Verurteilungszahlen computerspezifische Delikte betreffend.

Immer wieder wird auch die Einführung einer Online-Durchsuchung – also das Ausspionieren fremder Computersysteme mit Hilfe heimlich installierter Software – als Überwachungsmethode im Strafprozessrecht diskutiert. Die Einführung einer solchen Überwachungsmethode wird aufgrund potentieller schwerwiegender Grundrechtseingriffe – möglicherweise auch in Rechte am Strafverfahren Unbeteiligter – sehr kritisch gesehen.[70] Bestimmungen dazu existieren in Österreich daher derzeit nicht.

[68] Rahmenbeschlusses 2008/919/JI zur Änderung des Rahmenbeschlusses 2002/475/JI zur Terrorismusbekämpfung, ABl. Nr. L 330 vom 9.12.2008.
[69]Siehe zB *Salimi,* ÖJZ 2012, 998 (1000 f).
[70]Siehe zB *Venier,* Die Online-Durchsuchung. Oder: Die Freiheit der Gedanken, AnwBl 2009, 480 (480 ff).