Prof. Dr. Dr. h.c. mult. Ulrich Sieber
Max-Planck-Institut für ausländisches
und internationales Strafrecht, Freiburg i.Br.

Kurzpräsentation des strafrechtlichen Gutachtens „Straftaten und Strafverfolgung im Internet“

auf dem 69. DJT in München am 19.9.2012

I.

Es ist mir eine besondere Freude, heute im September 2012, auf dem 69. DJT das strafrechtliche Gutachten über „Straftaten und Strafverfolgung im Internet“ vorstellen zu können. Vor genau 40 Jahren, im Herbst 1972, begann ich in Freiburg meine Dissertation über „Computerkriminalität und Strafrecht“. Mein Doktorvater, Prof. Klaus Tiedemann, war damals skeptisch, ob der Gegenstand dieser Dissertation überhaupt existierte. Die beiden einzigen Aufsätze zum Thema diskutierten darüber, ob es sich bei dieser neuen Kriminalität um „Dichtung oder Wahrheit“ handele.

Heute ist unbestritten, dass Computer- und insbesondere Internetkriminalität eine fundamentale Herausforderung der Informationsgesellschaft ist. Die Verletzlichkeit von Wirtschaft, Verwaltung, Militär und privaten PCs durch Hackingangriffe, Viren, Botnetze und die sich abzeichnenden Gefahren eines Cyberwar sind offensichtlich. Die schlimmsten Bilder mit Kinderpornografie finden sich in verborgenen und abgeschotteten Foren des Internet – dem sog. Darknet – , in denen eine Mitgliedschaft die Begehung von Straftaten voraussetzt, was die Ermittlungsbehörden ausschließt. Urheberrechtsverletzungen schädigen die Software-, Musik- und Filmindustrie in gravierendem Ausmaß. Datensammlungen im Internet und soziale Netzwerke realisieren inzwischen Orwell’sche Visionen.

Die Hilflosigkeit der Nationalstaaten gegenüber diesen Entwicklungen wird bei den sog. Botnetzen deutlich, wenn Ermittlungsbehörden Millionen von mit Schadsoftware infizierten Rechner feststellen, die von Unbekannten gesteuert und für illegale Zwecke missbraucht werden. Ratlosigkeit herrscht auch bei dezentralisierten Diensten wie dem Cloud-Computing, wenn niemand weiß, in welchem Staat die durch technische Vorgaben der Rechnerauslastung weltweit verschobenen Daten gerade gespeichert sind. In diesen Situationen ist unklar, wo überhaupt Rechtshilfe

beantragt werden könnte, die im Übrigen in vielen Fällen auch schon an der Verschlüsselung der gesuchten Daten scheitern würde. Weitere Durchsetzungsprobleme zeigten sich im deutschen Datenschutzrecht, als die deutsche Verbraucherschutzministerin 2010 in ihrer Not mit der Rückgabe ihres Facebookaccounts drohte.. Diese wenigen Beispiele machen deutlich: Straftaten und Strafverfolgung im Internet führen heute zu existentiellen Problemen. Internetkriminalität gefährdet nicht nur den Fortschritt der modernen Informations- und Netzwerkgesellschaft, sondern auch die Durchsetzungsfähigkeit des Nationalstaates in der globalen Weltgesellschaft. Geeignete rechtliche Maßnahmen sind daher unverzichtbar.

In den 1970er und 1980er Jahren war Deutschland bei der Entwicklung des Computerstrafrechts zusammen mit den USA und Canada national und international führend. Dies beruhte vor allem darauf, dass Wissenschaftler und Praktiker in der Kommission zur Bekämpfung der Wirtschaftskriminalität zusammenarbeiteten und teilweise auch in der OECD und im Europarat federführend waren. Auch in den 1990er Jahren gingen von Deutschland – etwa für die Providerhaftung – noch bedeutende Anstöße aus. Wichtige deutsche Fälle wie Inkassoprogramm, KGB-Hacking und CompuServe, an denen ich gutachtlich beteiligt war, fanden weltweit Beachtung.

Inzwischen hat Deutschland seine Vorbildfunktion für ausländische Rechtsordnungen und internationale Vorgaben verloren. Dies hat vielfältige Gründe:

- Es mangelt allgemein an seriösen kriminologischen Studien zu den einschlägigen Phänomenen und ihren Verfolgungsproblemen.
- Der Mut zu einer umfassenden Reform fehlt. Die Gesetzgebung beschränkt sich vielmehr auf kleinere Reparaturen, die eng an bisherige Gesetze angelehnt werden, welche jedoch für körperliche Gegenstände entwickelt wurden.
- Damit fehlt eine systematische Berücksichtigung der immateriellen Charakteristika von Daten und Informationen. Das Gleiche gilt für andere dogmatische Grundlagenfragen im Informationsstrafrecht wie Globalisierung oder den Problembereich Privatisierung, Verpflichtung Privater, staatlich-private Koregulierung und Geltung von Grundrechten für Private
- Häufig sind die Gesetze auch nicht ausreichend technikneutral formuliert und unnötig kompliziert.

- Einzelne Probleme sind noch überhaupt nicht behandelt. Selbst die zehn Jahre alte Cybercrime-Konvention des Europarats ist heute nicht vollständig umgesetzt.

Mein schriftliches Gutachten für den 69. Deutschen Juristentag beschreibt deswegen die einschlägigen Phänomene und Ermittlungsprobleme, zeigt die grundlegende Dogmatik immaterieller Güter im globalen Cyberspace, skizziert die internationalen Vorgaben und analysiert das geltende Recht. Auf dieser Grundlage erfolgt dann ein umfassender Überblick zum Reformbedarf.

Aus Zeitgründen kann ich die einschlägigen Phänomene, Verfolgungsprobleme und anderen Grundlagen der Internetkriminalität nicht darstellen, welche die Reformforderungen anschaulich machen und belegen würden. Ich beschränke mich daher auf die wichtigsten Ergebnisse für die Reform, die in die Resolutionen des DJT eingehen sollten.

Diese Reformforderungen betreffen das materielle Strafrecht, das Strafprozessrecht, das Gefahrenvorsorgerecht sowie das internationale Koordinations- und Kooperationsrecht.

II.

A. Zum materiellen Recht

1. Die im Wesentlichen seit 1986 im StGB geregelten und für das Internet zentralen **Strafbestimmungen zum Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit von informationstechnischen Systemen** (insbes. §§ 202a, 202b, 202c, 303a, 303b StGB) sollten zusammengefasst und den Vorgaben der Cybercrime-Konvention des Europarats besser angepasst werden.
2. Zur Verfolgung von Cyberterrorismus, organisierter Computerkriminalität und großflächigen Angriffen gegen eine Vielzahl von Computersystemen benötigen diese zentralen Tatbestände vor allem **strafschärfende Qualifikationen**, die durch eine Aufnahme in den Katalog des § 100a Abs. 2 StPO auch eine **Telekommunikationsüberwachung** ermöglichen.
3. Die – vom BVerfG nur notdürftig reparierten – **Vorfelddelikte gegen Schadsoftware** zur Begehung von Hacking, Computerbetrug und Computersabotage in den §§ 202c, 263 Abs. 3, 303a Abs. 3 sollten in einem einzigen Tatbestand mit zwei – konzeptionell unterschiedlichen – Alternativen verbunden werden. Absatz 1 der neuen Bestimmung sollte

Computerprogramme sowie Web-Seiten erfassen, die neben rechts*widrigen* auch recht*mäßigen* Zwecken dienen können. Der Besitz und das Zugänglichmachen solcher Dual-use-Schadsoftware sollten allerdings nur bestraft werden, wenn der Täter die Absicht hat, dass damit ein entsprechendes Delikt begangen wird.

4. Absatz 2 dieses Vorfeldtatbestands sollte dagegen **Passwörter, Zugangssicherungen und Berechtigungsdaten** erfassen, deren Besitz und deren Zugänglichmachung auch ohne entsprechende deliktische Absicht bestraft werden kann, soweit es nicht um ein rechtmäßiges berufliches Verhalten geht.

   Dieser neu konzipierte Absatz 2 erfüllt gleichzeitig auch den berechtigten Kern der aktuellen Forderung nach einer allgemeinen Kriminalisierung der Datenhehlerei. Die hierüber hinausgehende Forderung nach einem allgemeinen **Datenhehlereitatbestand** ist demgegenüber problematisch, weil Informationen im Gegensatz zu den körperlichen Tatobjekten der Hehlerei keinen exklusiven Eigentumsschutz genießen. Sie sind darüber hinaus auch ohne Entziehung gegenüber dem Eigentümer beliebig oft kopierbar. Ein allgemeiner Tatbestand der „Datenhehlerei“ wäre auch im Hinblick auf den Kreis der Vortaten problematisch (vor allem wenn dieser – wie teilweise vorgeschlagen - alle Daten erfassen würde, „die ein anderer ausspäht oder sonst rechtswidrig erlangt“ hat). Er würde auch zu massiven Strafbarkeitsrisiken der Presse und der sog. „Whistleblowing-Plattformen führen, wenn diese irgendwie „bemakelte“ Informationen veröffentlichen. Im Übrigen wird eine „Hehlerei“ von wichtigen anderen Daten – wie Geschäftsgeheimnissen und personenbezogenen Daten – bereits von § 17 UWG bzw. § 44 BDSG strafrechtlich erfasst.
5. Notwendig ist sodann eine Erweiterung des **strafrechtlich geschützten Berufsgeheimnisses** zum Schutz anvertrauter Computerdaten. Diese Bestimmung hat insbesondere für das Cloud-Computing Bedeutung.
6. Für das **Datenschutzrecht** sollte eine allgemeine Strafbestimmung im StGB loziert werden, damit schwere Verstöße unabhängig vom uneinheitlich geregelten Strafschutz in den bereichsspezifischen Vorschriften einheitlich erfasst werden können. Dies kann in der Praxis auch das notwendige Problembewusstsein für diese Delikte schaffen.
7. Für das Datenschutzstrafrecht und andere Deliktsbereiche ist weiter die Entwicklung eines – event. verwaltungsrechtlichen - **spezifischen**

Sanktionsregimes zu prüfen, das auch gegen international agierende Unternehmen im globalen Cyberspace greift.

8. Die Durchsetzung des **Urheberstrafrechts** sollte zur Schonung der Strafverfolgungsressourcen und zur Umsetzung des Verhältnismäßigkeitsprinzips auf gravierende Fälle beschränkt werden. Als Kompensation sollte die zivilrechtliche Rechtsdurchsetzung vor allem im Bereich der Auskunftsansprüche verbessert werden.
9. Im Hinblick auf die Verbreitung illegaler Inhalte sollte der – an körperlichen Datenträgern orientierte – **Schriftenbegriff des § 11 Abs. 3** StGB durch den allgemeineren Begriff der Medien ersetzt werden, der auch gestreamte Inhalte erfasst und dadurch die entsprechenden (uneinheitlichen) Erweiterungen des Schriftenbegriffs im Besonderen Teil des StGB überflüssig macht.
10. Das im StGB, im Jugendschutzgesetz und im Mediendienstestaatsvertrag unübersichtlich und unsystematisch geregelte **Pornografiestrafrecht** sollte auf eine knappe systematische Regelung reduziert werden.

B. Zum Strafprozessrecht

Im Strafprozessrecht müssen vor allem die Eingriffsbefugnisse den neuen Herausforderungen und Ermittlungsmöglichkeiten der digitalen Welt angepasst werden. Dies bedeutet vor allem:

1. Die Überwachung verschlüsselter Telekommunikation erfordert heute in vielen Fällen eine **Quelldatentelekommunikationsüberwachung**, d.h. ein Abhören der Daten an den noch unverschlüsselten Schnittstellen der Endgeräten. Dies muss gesetzlich geregelt werden. Denn § 100a StPO entspricht nicht den Vorgaben des BVerfG nach rechtlichen und technischen Begrenzungen. Das Gesetz oder die Gesetzesbegründung müssen auch eine Reihe spezieller Fragen klären. Dies gilt insbesondere für die Abgrenzung der Quellen-TKÜ von der Online-Durchsuchung, und zwar sowohl bezüglich der erfassbaren Daten im Vorfeld des eigentlichen Kommunikationsprozesses als auch für die Anwendbarkeit der Vorschrift auf eine Kommunikation mit den eigenen Datenbeständen beim Cloud-Computing. Wann liegt hier noch Quellen-TKÜ und wann schon bei eine Online-Durchsuchung vor?
2. Eine hierüber hinausgehende **Online-Durchsuchung** zu repressiven Zwecken kann vor allem für Fälle diskutiert werden, in denen sowohl präventive als auch repressive Ziele verfolgt werden. Dabei kommt auch eine Regelung in Betracht, die beim Verdacht zurückliegender schwerer Straftaten und

gleichzeitiger schwerer zukünftiger Gefahren unter engsten Voraussetzungen eine bundeseinheitliche Ermächtigung in der StPO schafft.

3. Als mildere Maßnahme gegenüber einer Online-Durchsuchung kann in vielen Fällen auch die **Installation eines Keyloggers** erfolgen, der die Tastatureingaben einer überwachten Person protokolliert und dadurch insbesondere Codes, Passwörter, Verschlüsselungsalgorithmen und ausgelagerte Speicherorte von Daten erfassen kann. Eine entsprechende Regelung müsste jedoch im Hinblick auf die hierfür zulässigen Begleiteingriffe sorgfältig geprüft werden und ähnlich hohe Eingriffsvoraussetzungen wie eine Online-Durchsuchung verlangen.
4. Die **Abgrenzung zwischen der Telekommunikationsüberwachung und der Durchsuchung** sollte – etwa für die Ausleitung von E-Mails beim Provider – dahingehend klargestellt werden, dass die besonders eingriffsintensiven heimlichen und permanenten Maßnahmen nur unter den strengeren Voraussetzungen der Telekommunikationsüberwachung möglich sind.
5. Erhebliche Erleichterungen der Ermittlungsarbeit sollten dadurch ermöglicht werden, dass eine **Neuregelung der strafprozessualen Herausgabepflichten** für Nicht-Beschuldigte auch informatikspezifische Pflichten zur Herausgabe spezifizierter Dateninhalte und Datenformate einschließt, zu denen im Rahmen des Möglichen auch die Verpflichtung zur Entschlüsselung von Daten zählt.
6. Für **Auskunftspflichten** gegenüber dem Staatsanwalt und dem Richter über **Zugriffs- und Entschlüsselungscodes** sollten hingegen strengere Voraussetzungen als für die allgemeinen Auskunftspflichten normiert werden.
7. Der Zugriff auf **Verkehrsdaten** muss nach dem Urteil des BVerfG neu geregelt werden. Für die spezielle Zuordnung von dynamischen IP-Adressen zu ihren Anschlussinhabern sollte dabei ebenso wie für den Zugriff auf Bestandsdaten die Möglichkeit eines automatisierten Auskunftsverfahrens in Echtzeit geschaffen werden.
8. Ein **Quick-Freeze-Verfahren** sollte nicht nur für Verkehrsdaten, sondern – wie von der Cybercrime-Konvention des Europarats gefordert – für alle Datenbestände eingeführt werden. Die Ermittlungsbehörden müssen danach bei der Gefahr des Datenverlusts kurzfristig und ohne richterliche Entscheidung eine Sicherung der Daten verlangen können, die von den Adressaten allerdings erst nach einer richterlichen Entscheidung herauszugeben sind.

C. Zur Gefahrenvorsorge und zur Prävention

1. Die Frage nach einer **allgemeinen Vorratsdatenspeicherung** geht über die Thematik der Internetkriminalität weit hinaus und kann ohne eine umfassendere empirische Erhebung derzeit nicht seriös entschieden werden. Die Frage wurde deswegen im Gutachten auch bewusst nicht beantwortet.
2. Eindeutig erforderlich und für die Aufklärung der Internetkriminalität unverzichtbar ist jedoch die – begrenzte und sehr viel weniger eingriffsintensive – Speicherpflicht der Provider für die **Zuordnung der dynamisch vergebenen IP-Adressen zu den jeweiligen Anschlussinhabern.** Diese Zuordnung ist für die Rückverfolgung und Aufklärung von Straftaten im Internet oft der einzige Anhaltspunkt. Eine weitere Zurückstellung dieser Regelung bis zur Entscheidung über die große Vorratsdatenspeicherung wäre unverantwortlich.
3. Die in der Politik regelmäßig diskutierten **Sperrverfügungen gegen illegale Inhalte s**ind grundsätzlich abzulehnen. Sie lösen die Problematik illegaler Inhalte nicht, sind leicht zu umgehen, schaffen eine missbrauchsanfällige Infrastruktur und gefährden die Informationsfreiheit.

D. Zum Recht der internationalen Koordination und Kooperation

1. Für die Anwendbarkeit des deutschen Strafrechts ist vor allem das **Territorialitätsprinzip** maßgebend, das jedoch im Hinblick auf die Abrufbarkeit illegaler Inhalte von ausländischen Servern umstritten ist. Eine Ausdehnung des deutschen Strafrechts auf die im Ausland abrufbaren Daten sollte dabei nur unter sehr restriktiven Bedingungen erfolgen, wenn entsprechende deutsche Interessen tangiert und in einem Straftatbestand definiert sind.
2. Die internationale Strafverfolgung im globalen Cyberspace erfordert weiter eine verbesserte **Amts- und Rechtshilfe** sowie eine verstärkte **Rechtsharmonisierung**. Die deutsche Bundesregierung sollte hier vor allem die aktuellen Initiativen des Europarats und der Vereinten Nationen unterstützen.
3. Internationale Vereinbarungen sollten vor allem regeln, unter welchen Voraussetzungen eine Beweiserhebung und ein Einfrieren von Daten (Quick Freeze) auf **ausländischen Servern** möglich ist. Dies gilt speziell für die Fälle des Cloud-Computing, bei denen der Speicherort von der technischen

Auslastung internationaler Computersysteme abhängt und schnell wechseln kann, sodass der Empfängerstaat eines Rechtshilfegesuchs kaum mehr bestimmt werden kann.

4. Dabei ist auch die Schaffung von **internationalen und supranationalen Strafverfolgungsbehörden** zu prüfen, die weiterreichende transnationale Ermittlungsbefugnisse haben. Ausgangspunkt dieser Institutionen sollte entsprechend Art. 35 der Cybercrime Konvention eine engere Kooperation im 24/7-Kontaktstellennetzwerk sein. Konzeptionell können auch die in Europa für Eurojust und die Europäische Staatsanwaltschaft entwickelten Modelle hilfreich sein.

III.

Die notwendigen Maßnahmen ließen sich weiter fortsetzen. Aus Zeitgründen verweise ich jedoch insoweit auf das schriftliche Gutachten und komme zum Fazit und Abschluss:

Der Überblick über die Vielzahl der notwendigen Reformmaßnahmen hat deutlich gemacht, dass der frühere Vorbildcharakter des deutschen Computerstrafrechts seit einem Jahrzehnt verloren gegangen ist: Dem materiellen Strafrecht mangelt es an Dogmatik und Systematik, die Strafverfolgungsbehörden haben kein gutes Ermittlungsinstrumentarium, der Schutz der Bürgerrechte ist suboptimal und häufig fehlt es auch an Rechtssicherheit.

Dies ist nicht primär als Vorwurf an den Gesetzgeber gemeint. Denn der technische Wandel, die Komplexität und damit auch die Verfallszeit von Gesetzen in diesem Bereich sind extrem hoch. Erforderlich ist jedoch ein neuer systematischer Reformansatz mit einer Vielzahl von miteinander zusammenhängenden Maßnahmen. Die Komplexität dieser Maßnahmen erfordert eine **neue interdisziplinäre Reformkommission** nach dem Beispiel der früheren Sachverständigenkommission zur Bekämpfung der Wirtschaftskriminalität. Der 69. DJT sollte daher nicht nur die zentralen Punkte und die Richtung dieser Reform aufzeigen, sondern auch eine entsprechende Weiterführung empfehlen. Ein solcher Ansatz kann dann auch wieder wichtige Impulse für die notwendigen Initiativen auf europäischer und weltweiter Ebene geben.