Anhang B

Recht im Internet

Das Vordringen der Informations- und Kommunikationstechnik in fast alle Lebensbereiche hat neue IT-Delikte hervorgebracht und die Computerkriminalität insgesamt vielfältiger und gefährlicher gemacht. Mit der Verbreitung der weltweiten Netze sind Veränderungen der Täter- und Opferprofile einhergegangen: Computerdelikte können heute von jedermann vom Wohnzimmersessel aus begangen werden und jeder kann Opfer werden. Die elektronische Datenverarbeitung ist mit der Telekommunikation zusammengewachsen, so dass die Delikte zunehmend über Telekommunikationsnetze, auch vom Ausland aus, begangen werden und neue Formen angenommen haben. /Pohl 2000/

In kaum einem anderen Bereich zwischenmenschlicher Kommunikation gibt es so viele Verstöße gegen geltendes Recht wie im Internet: Beleidigungen, Verleumdungen, Boykotte, Namens- und Markenrechtsverletzungen, Verstöße gegen das Urheberrecht usw. sind an der Tagesordnung. Mit der wachsenden Bedeutung der Kommunikation in und über Netze wird offensichtlich, dass rechtliche Regelungen unumgänglich sind. Wo immer mehr Menschen im und mit dem Netz Geld verdienen wollen, verstärkt sich der Handlungsbedarf, im zwar nicht »rechtsfreien«, aber bisher fast »rechtsfolgenfreien« Raum rechtsverbindliche und auch in der Praxis durchführbare Orientierungshilfen zur Verfügung zu stellen.

Die neuen Kommunikationsmöglichkeiten bringen dabei eine ganz neue Dimension von Rechtsverstößen mit sich. Das hängt zum einen mit der nie dagewesenen weltweiten Relevanz von Handlungen zusammen, die es jedem einfachen Benutzer einer Mailbox ermöglicht, in einem anderen Teil der Welt für Unruhe zu sorgen, ohne dass er sich der Verantwortung bewusst ist, die mit solchen Befugnissen normalerweise verbunden ist.

B.1 Aktuelle Formen des Delikts »Computerkriminalität«

Bei den neuen Rechtsverstößen im Internet handelt es sich nicht um Delikte, die vor der Vernetzung unbekannt waren, sondern um altbekannte Rechtsverletzungen, die sich in neuem Gewand präsentieren. Gesetzgeber und Justiz stehen ihnen daher nicht hilflos gegenüber, sondern sie müssen altbewährtes Recht den neuen Dimensionen anpassen. Die häufigsten Missbräuche wie Persönlichkeitsrechtsverletzungen und vor allem Wirtschaftsdelikte sind ja keine gänzlich neuen Delikte, sondern aktuelle Formen von Verstößen, die seit jeher geahndet werden und spätestens seit Erfindung der EDV die Rechtsprechung beschäftigt haben.

B.1.1 Persönlichkeitsrechtsverletzungen

Das Persönlichkeitsrecht des Bürgers ist gesetzlich geschützt und kann durch Sammlung, Speicherung, Weitergabe oder Verknüpfung personenbezogener Daten verletzt werden. In heutigen Statistiken spielen Persönlichkeitsrechtsverletzungen nur eine geringe Rolle. Allerdings kann sich dies durch die neuen Möglichkeiten im Internet schnell ändern: Delikte wie die Benutzung unrichtiger Daten (zum Beispiel falsche Adressangabe bei E-Mail), die unbefugte Erlangung von Daten, die unbefugte Sammlung, Speicherung, Weitergabe oder Verwendung personenbezogener Daten und der Verstoß gegen die Formalvorschriften des Datenschutzrechts finden hier einen neuen, fruchtbaren Nährboden.

Elektronischen Nachrichten fehlt so etwas wie ein »digitaler Briefumschlag«. Mit entsprechendem technischem Know-how können Filter in die Transportserver (MTAs) eingebaut werden, die den Datenfluss analysieren und bestimmte E-Mails herausfischen können. Auf diese Weise können zum Beispiel die E-Mails an einen bestimmten Empfänger abgefangen, auf ein anderes Rechnersystem umgeleitet und dort eingesehen werden.

Ein Beispiel besonders unverfrorener und vor allem professioneller Beschaffung von Daten lieferte 1996 ein Unbekannter beim US-amerikanischen Internet-Provider Prodigy: Eingeloggten Mitgliedern wurde während des Surfens die Aufforderung zugestellt, sich umgehend bei ihrem Provider zu melden. Unter der angegebenen Telefonnummer meldete sich eine Voicebox, die mit dem Hinweis auf Probleme bei der letzten Beitragsrechnung um den Namen, die Adresse, die Kreditkartennummer, Telefonnummer und den Geburtstag bat. Diese Auskünfte wurden von etlichen Benutzern geliefert, die erst Wochen später bei der nächsten Abrechnung merkten, dass man sie hereingelegt hatte.

B.1.2 Wirtschaftsdelikte

Das Internet hat mit seinem rasanten Wachstum auch die Möglichkeiten von Wirtschaftsdelikten aller Art enorm gesteigert. Computermanipulationen, Sabotage und Erpressung, Hacking, Spionage, Softwarediebstahl und andere Formen der Produktpiraterie breiten sich schneller aus, als Politik und Gesetzgebung ihnen mit entsprechenden Gesetzen, Verboten oder Strafen Einhalt gebieten könnten.

Computermanipulationen

Zu den klassischen Computermanipulationen zählen Abrechnungsmanipulationen wie Gehalts- und Rechnungszahlungen von Industrieunternehmen, Bilanzmanipulationen und Kontostandsmanipulationen bei Banken. Die derzeit noch vorherrschende Sorglosigkeit der Organisationen lädt Hacker geradezu ein, sich an ihren Rechnersystemen zu versuchen.

Seit einigen Jahren sind Kartenmissbräuche das häufigste Computerdelikt. Geschichten von findigen Tüftlern, die wiederaufladbare Telefonkarten konstruiert

oder Kreditkarten gefälscht haben, liest man immer wieder in der Presse. Neue Möglichkeiten des Missbrauchs bieten elektronische Zahlungsmittel. Für diese Systeme gewinnt die Sicherung durch Chipkarten-Technologie an Bedeutung.

Im Internet soll sich jetzt der elektronische Geldverkehr bewähren, der mit Electronic Sales, Cybermoney und Electronic Banking auf dem Vormarsch ist und nicht nur für Banken und Geschäfte im Internet, sondern auch für kriminelle Aktivitäten reichlich neue Perspektiven bietet.

Während das Telefonnetz früher allenfalls manipuliert wurde, um die eigene Telefonrechnung zu verfälschen, hat inzwischen eine qualitative Veränderung der Manipulationen im Telefonnetz stattgefunden. Seit unzureichend geschützte und nicht zu diesem Zweck entwickelte Telefonnetze in unvorsichtiger Weise zur Abrechnung von Dienstleistungen eingesetzt werden, finden auch zunehmend finanzielle Manipulationen mit dem Ergebnis der Überweisung von Geldern statt.

Computersabotage und -erpressung

Viren- und Wurmprogramme, die vor allem über raubkopierte Software oder in Netzwerken verbreitet werden, verursachen massenhaft Schäden. Im Internet bietet sich die neue Möglichkeit, im Hintergrund von Programmen, vom Benutzer unbemerkt, eine Art Zeitbombe zu installieren, die nach einer bestimmten Zeit Programme zerstört oder die Festplatte gründlich »aufräumt«.

Die Abhängigkeit der Informationsgesellschaft von Rechnersystemen macht Computererpressung zu einer gefährlichen Angriffsform. Mit der Drohung, Rechnersysteme und Datenbestände unbrauchbar zu machen, lassen sich Organisationen erpressen, die sich nicht ausreichend abgesichert haben.

Hacker

Beim klassischen Computerhacking stand vor allem die Freude an der Überwindung technischer Sicherheitsmaßnahmen im Vordergrund, die das angegriffene Unternehmen schädigte und bei der Spätschäden drohten, wenn die erlangten Kenntnisse zur Begehung von Spionage- und Sabotagehandlungen genutzt wurden. Rechtlich waren die Geheimnissphäre und die Integrität des betroffenen Rechnersystems beeinträchtigt.

Im Telefonnetz gibt es massenhaft Missbräuche durch Phreaker in Telefonleitungen, Anrufbeantwortern und Voice-Boxen, zum Beispiel das Mithören von Gesprächen und die Nummern von Telefonberechtigungskarten. Durch das digitale ISDN-Netz und die Verbindung von Telefon- und Computertechnik sind neue Möglichkeiten des Missbrauchs entstanden.

So erlaubt der neue Dienst »leistungsfähiger Messaging Service für Netware-LANs« computergenerierte Telefonanrufe, die dazu missbraucht werden können, gezielt Telefonterror zu betreiben: mit entsprechender Botschaft und per Knopf-

druck eingestellter Stimme (beispielsweise Flüstern) kann man ein Telefon zu einer beliebigen Uhrzeit klingeln lassen und am anderen Ende der Leitung Angst und Schrecken verbreiten.

Wirtschaftsspionage

Schon die klassische Wirtschaftsspionage versprach hohe Gewinne, die heute durch den Reiz großer Datenmengen auf kleinstem Raum, schnell und einfach zu kopieren, um ein Vielfaches gewachsen sind. Tatobjekte sind Programme, Forschungs- und Rüstungsdaten, Daten des kaufmännischen Rechnungswesens sowie Kundenadressen. Die Täter sind meist jugendliche Hacker, konkurrierende Organisationen und zunehmend auch Nachrichtendienste.

Zur Spionage zählt auch das Abhören von Telefongesprächen. Autotelefone, Richtfunksender und Satellitenverbindungen sind bei unverschlüsselter Kommunikation leichte Angriffsziele.

Softwarediebstahl und andere Formen der Produktpiraterie

Die unbefugte Kopie und Nutzung fremder Computerprogramme betraf früher vor allem Individualsoftware, während heute die rechtswidrige Kopie von massenhaft vertriebener Standardsoftware dominiert. Datenbanken und andere Datensammlungen sowie die unbefugte Nutzung von Multimedia-Produkten und ähnlichem erfreuen sich zunehmender Beliebtheit. Wenn Pay-TV-Sender ihren auf Verschlüsselung beruhenden Bildsignalton ändern, vergehen immer nur wenige Tage, bis der elektronische Nachschlüssel auf einschlägigen Internetseiten auftaucht. Software-, Musik-, Video-, und Multimediapiraterie werden durch die Verbreitung von Geräten zum Abspielen und Herstellen von CDs und DVDs erleichtert.

B.1.3 Sonstige Delikte

Die Verbreitung von gewaltverherrlichenden, rassistischen oder pornografischen Informationen sowie der zunehmende Einsatz von Rechnersystemen bei der organisierten Kriminalität und die Gefahr möglicher Manipulationen in Kernkraftwerken, Rüstungssystemen usw. sind die stärksten Argumente von Befürwortern einer »Cyberpolizei«. Computermissbrauch ist zu einer globalen Bedrohung geworden und die Sicherheit moderner Rechnersysteme hat für die heutige Informationsgesellschaft zentrale Bedeutung gewonnen.

B.2 Rechtsfragen

Der Gesetzgeber in Deutschland hat auf die neuen Kriminalitätsformen in vier Wellen computerspezifischer Reformen reagiert: Persönlichkeitsschutz, Wirtschaftsstrafrecht und der Schutz des geistigen Eigentums wurden in verschiedenen Reformwellen in den 70er und 80er Jahren erfaßt, wobei unter anderem der zivilrechtliche Urheberrechtsschutz, das Urheberstrafrecht und der Rechtsschutz

von Topografien sowie die allgemeinen Regelungen zur Produktpiraterie den neuen Anforderungen angepaßt wurden. Die entsprechenden Reformgesetze umfassen öffentlich-rechtliche und zivilrechtliche Maßnahmen mit Schwerpunkt im Strafrecht.

In Deutschland bereits gültige Bestimmungen, die im Internet den gesetzlichen Rahmen bilden, sind im Einzelnen:

- das Gesetz über das Urheberrecht und verwandte Schutzrechte,
- der Staatsvertrag über Bildschirmtext,
- das Gesetz über Fernmeldeanlagen (FAG),
- das Telekommunikationsgesetz (TKG), die Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen,
- die Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost/Telekom,
- das Gesetz über die Verbreitung jugendgefährdender Schriften (GjS),
- das Strafgesetzbuch (StBG) und
- das Grundgesetz (GG).

In den meisten westlichen Staaten war die Reaktion ähnlich. Internationale Organisationen wie OECD, Europarat, EU, WIPO, WTO und AIDP begleiteten die nationalen Reformmaßnahmen. Der Druck der Industrie förderte die Rechtsvereinheitlichung, wodurch es zu raschen Lösungen kam, die aber ad hoc und isoliert waren und denen keine grundsätzlichen Überlegungen zur Rolle des Strafrechts in der Informationsgesellschaft zugrunde lagen.

B.3 Paradigmenwechsel und Perspektiven

Der Wandel von der Industrie- zur Informationsgesellschaft hat Folgen für das Rechtssystem und die aus der entstehenden Risikogesellschaft resultierenden Veränderungen des Strafrechts.

Dieser Wandel (»zweite industrielle Revolution«) bedeutet vor allem eine Verlagerung menschlicher Geistestätigkeit auf Maschinen. Neben körperlichen Dingen gewinnen zunehmend unkörperliche Werte wie elektronisches Geld, Urheberrechte, Geschäftsgeheimnisse und sonstiges Know-how an Bedeutung. Information ist ein neuer Wert, der auch Machtfaktor und Gefährdungspotential bedeutet.

Der gesellschaftliche Paradigmenwechsel hat das Strafrecht bereits erreicht, aber es fehlt eine allgemeine Theorie für den Schutz von Informationen, die zu der dritten Grundgröße neben Materie und Energie geworden sind. Information ist ein neues wirtschaftliches, kulturelles und politisches Gut, das aber auch neue Probleme schafft. Die moderne Informationstechnik steigert den Wert von Information: Information wird zu einem aktiven Faktor, der in automatischen Datenverarbeitungssystemen ohne weiteres menschliches Zutun Veränderungen

vornimmt, und in manchen Bereichen ersetzen informationstechnische Systeme menschliche Entscheidungen.

Bei der rechtlichen Beurteilung materieller und immaterieller Güter gibt es einige Unterschiede zu beachten: Während Eigentum oder Besitz an materiellen Gütern geschützt werden können, handelt es sich beim immateriellen Gut Information um ein öffentliches Gut, das nicht durch Ausschließlichkeitskriterien geschützt werden kann. Das grundlegende Prinzip der Informationsfreiheit und des freien Informationsflusses ist eine wesentliche Vorausssetzung für ein freies wirtschaftliches und politisches System.

Außerdem betrifft der Schutz von Information nicht nur die wirtschaftlichen Interessen ihres Besitzers, sondern auch die Interessen derjenigen, die von ihrem Inhalt betroffen sind. Das bedeutet rechtlich eine neue Anforderung an den Persönlichkeitsrechtsschutz im IT-Bereich.

Zum dritten gewinnen die Zugangsrechte zu Informationen für den privaten und den öffentlichen Bereich an Bedeutung (Access to Information Rights), zum Beispiel bezüglich des Datenschutzrechtes und für Strafverfolgungsbehörden. Aus diesen Unterschieden ergibt sich, dass Rechtsregeln für Informationen nicht auf dem Wege einer Analogie aus Vorschriften über materielle Gegenstände entwickelt werden können, sondern einer eigenständigen Grundlage und Theorie bedürfen.

Die Entwicklung der Technikgesellschaft und des Technikrechts in der postindustriellen Informationsgesellschaft wird auch unter dem Stichwort »Risikogesellschaft« diskutiert. Damit sind insbesondere die Technikgefahren der Chemie, der Kernenergie, der Gentechnik und anderer Anlagen mit schädlichem Einwirkungspotential auf den Menschen und die Umwelt gemeint. Bei Betrachtung der neuen Risiken muss berücksichtigt werden, dass sie oft vergesellschaftet sind und nicht mehr auf einen Urheber zurückgeführt werden können, vor allem aber, dass sie schwerwiegende Folgen haben können, die nach Ort, Zeit und Kreis der Betroffenen nicht eingrenzbar sind. Gleichzeitig werden Komplexität und Entwicklungsgeschwindigkeit der gesellschaftlichen und technischen Veränderungen immer größer.

Rechtlich ergibt sich aus der Betrachtung der Risiken die Forderung nach einer besseren gesellschaftlichen Kriminalitätsprophylaxe, von der die Informationstechnik als Teil der Risikogesellschaft ebenfalls betroffen ist. Zur Bekämpfung der Computerkriminalität sind vor allem außerstrafrechtliche Maßnahmen gefordert: technische Sicherheitsstandards mit Zugriffskontrollsystemen, Aufklärung der betroffenen Benutzer und geeignete zivilrechtliche und öffentlich-rechtliche Rahmenbedingungen. Das Strafrecht muss an die neuen Risiken angepasst werden. Eine Voraussetzung für rechtliche Regelungen in diesem Bereich ist ein strukturelles Denken: Statt bei zufälligen technischen Veränderungen anzusetzen, müssen Funktionen beschrieben werden, die auch in Zukunft der veränderten Technik standhalten können.

Das bedeutet vor allem, dass nationale Grenzen ihre Bedeutung verlieren und eine internationale Harmonisierung des Rechts stattfinden muss. Bei der Nutzung internationaler Telekommunikationsnetze wie dem Internet können Daten in Sekundenbruchteilen über internationale Netze übertragen werden, ohne dass eine Kontrolle möglich ist. Mit Hilfe von Rechnersystemen können Straftaten begangen werden, deren Konsequenzen im Ausland eintreten.

Unterschiedliche nationale Gesetze würden dagegen zu »Data Havens« oder »Computer Crime Havens« führen, die nationale Beschränkungen des freien Informationsflusses zur Folge hätten. Zudem wären nationale Barrieren wirkungslos, da Informationen über internationale Netze auch in verschlüsselter Form ins Ausland übertragen werden können. Nationale Beschränkungen und Überwachungsmaßnahmen würden Persönlichkeitsrechte der Bürger und Geschäftsgeheimnisse von Organisationen gefährden sowie die wirtschaftliche Entwicklung eines internationalen Informationsmarktes behindern. Daher ist die internationale Harmonisierung des Informationsrechts durch EU, Europarat, OECD, UN, WIPO, TWTO und AIDP zu begrüßen, wenngleich noch eine Verstärkung von Kontakten und verbesserte Zusammenarbeit zwischen den einzelnen Staaten erforderlich ist.

1997 haben die Justiz- und Innenminister der G-8-Länder einen Plan ausgearbeitet, um mit internationaler Kooperation die wachsende IT-Kriminalität zu bekämpfen. US-Generalstaatsanwältin Janet Reno äußerte, Informations-technologie habe eine neue grenzüberschreitende »Frontier« der Kriminalität eröffnet. Nötig sei, den Cyberkriminellen nicht länger hinterherzuhinken, sondern ihnen einen Schritt voraus zu sein. Der Plan sieht unter anderem vor, dass in jedem Land eine ausreichende Zahl von Spezialisten zur Bekämpfung der IT-Kriminalität angestellt werden, dass die Staaten enger zusammenarbeiten und Täter, beispielsweise bei Angriffen auf Netzwerke, schnelle identifiziert werden sollen, dass ein Straftäter auch in dem Land zur Rechenschaft gezogen werden kann, in das er geflohen ist, wenn eine Auslieferung nicht möglich ist, und dass entsprechende Gesetze für eine leichtere Strafverfolgung geschaffen werden müssen.

Ende Januar 2001 legte die Europäische Kommission einen Forderungskatalog zur Bekämpfung der Computerkriminalität vor. Die FAZ berichtete am 31.1.2001 in dem Beitrag »Programm gegen Computerkriminalität – Brüssel im Zwiespalt zwischen Sicherheit und Grundrechtssicherung«:

»Die Europäische Kommission hat am Dienstag einen Forderungskatalog zur Bekämpfung der Computerkriminalität vorgelegt. Zur Vorbeugung und zur Bekämpfung müsse die Sicherheit der Informationsinfrastruktur verstärkt und dafür Sorge getragen werden, daß die Behörden in der Europäischen Union über geeignete Mittel verfügten. Dabei müßten aber die Grundrechte der Bürger gewahrt bleiben, heißt es.

Ein auch von den Regierungen der EU-Mitgliedstaaten gefordertes, abgestimmtes Handeln sei notwendig, weil man mit Hilfe der Computersysteme jederzeit von jedem Ort der

Welt aus illegale Handlungen begehen könne, heißt es in der Kommissionsmitteilung. Die Zahl der aufgedeckten und gemeldeten Übergriffe verschleiert nach Ansicht der Kommission das wahre Ausmaß des wachsenden Problems.

Nach den ersten, vor rund drei Jahren eingeleiteten Vorhaben zur Bekämpfung des wachsenden Mißbrauchs der neuen Informations- und Kommunikationstechniken fordert die Kommission jetzt weitere Schritte, zum Beispiel die zügige Verabschiedung eines gemeinschaftlichen Rechtsinstruments. Dies soll den EU-Mitgliedstaaten erlauben, mit wirksamen Sanktionen beispielsweise gegen Kinderpornographie vorzugehen. Längerfristig will die Kommission Gesetzesvorschläge zur weiteren Angleichung der materiellen Strafrechtsvorschriften auf dem Feld der sogenannten High-Tech-Kriminalität vorlegen, heißt es in der Mitteilung. Die Erklärung der »Cyberkriminalität« zur Straftat böte einen besseren Opferschutz und erleichtere die grenzüberschreitende Zusammenarbeit der Behörden. Mit der von der Kommission empfohlenen Angleichung des Rechts auf europäischer Ebene fiele die Computerkriminalität unter das Gemeinschaftsrecht. Damit würden gemeinschaftliche Zwangsmaßnahmen möglich, heißt es in der Mitteilung. Die E-Partner sollten sich auf eine wirkungsvollere Politik zur Bekämpfung der Computerkriminalität verständigen. Damit will sich die Gemeinschaft mit ihren Plänen positiv von einem geplanten Abkommen des Europarates abheben, das lediglich Mindestvorschriften enthalten soll.

Die Kommission will darauf hinwirken, daß auf nationaler Ebene in allen EU-Ländern spezialisierte Polizeidienste eingerichtet werden. In diesem Zusammenhang will sie auch europäische Schulungsprogramme für Mitarbeiter der Strafverfolgungsbehörden und Veranstaltungen zum Thema Informationssicherheit fördern. Zur Stärkung der Zusammenarbeit will die Kommission sämtliche mit dem Thema befaßten Stellen in einem »EU-Forum« zusammenführen. Am 7. März 2001 findet in Brüssel eine öffentliche Anhörung dazu statt.«

B.4 Zusammenfassung

Das Zusammenwachsen von Datenverarbeitungs- und Datenübertragungstechnik hat die Computerkriminalität vielfältiger und gefährlicher gemacht. Die Möglichkeiten und Gefahren, die sich schon heute und in Zukunft verstärkt im Internet ergeben, sind derzeit kaum abzuschätzen. Zentralen Einfluss auf die Zukunft haben aus rechtlicher Sicht vor allem drei grundsätzliche soziale Veränderungen in unserer Gesellschaft: Die Entstehung der Informationsgesellschaft mit ihren neuen strafrechtlichen Rechtsgütern, die Veränderung der Risikogesellschaft, in der außerstrafrechtlichen Maßnahmen größere Bedeutung zukommt als strafrechtlichen und strafprozessualen Maßnahmen, und das Zusammenwachsen der Bürger in einer Informationsgesellschaft, in der sich die neuen Herausforderungen nur durch gemeinsame internationale Anstrengungen bewältigen lassen.