Irini E. Vassilaki

Materielles Strafrecht, Strafprozessrecht, Rechtsinformatik und Informationsgesellschaft

1. Problemstellung

»In ihrer weitesten Bedeutung sind Gesetze die notwendigen Bezüge, wie sie sich aus der Natur der Sache ergeben« (Montesquieu, 1. Buch, 1. Kapitel). Dieser Aphorismus von Montesquieu pointiert, dass nicht nur die äußeren Bedingungen menschlicher Gesellschaften, wie etwa das Klima oder geographische Gegebenheiten, sondern auch soziale Strukturen, wie etwa Klassenverhältnisse oder wirtschaftliche Aktivitäten, in einem komplizierten Wechselspiel »die Natur der Sache« ausmachen und den »esprit général«, den »Zeitgeist« bilden, der die Gesetze einer Gesellschaft durchbringt. Demnach beruht die Natur der Sache auf natürlichen, wirtschaftlichen und kulturellen Gegebenheiten, an welche die Rechtsordnung anknüpfen kann und muss. (Über das Werk von Montesquieu und seine rechtsphilosophische Bedeutung vgl. nur Coing, S. 184, 190; Strömholm, S. 190 ff.; Zippelius, § 7 I.) Sie weist nämlich gewisse Strukturen auf, die gewertet und eingeordnet werden, so dass die Erkenntnis gewonnen wird, ob und gegebenenfalls wie die Rechtsordnung einzugreifen hat.

Die Suche nach der Natur des Sache des 21. Jahrhunderts führt nunmehr unausweichlich zu den Anwendungen der Informationstechnik. Ihre Relevanz und Einfluss auf die Gesellschaft, die auch als Informationsgesellschaft bezeichnet wird, kann als Axiom in dieser Stelle dahingestellt bleiben. (Über den Einfluss der Informationstechnik auf die Gesellschaft vgl. nur Lange, Tauss/Kollbeck, Tinnefeld/Phillips/Heil, Weizenbaum). Es sind aber kaum Syllogismen verarbeitet worden, wie die Strafrechtswissenschaft auf diese neuen informationellen Strukturen agiert. Diese Aufgabe habe ich im folgenden Beitrag als Ziel gesetzt. Ich werde untersuchen, ob die Informationstechnik ein soziales, kriminologisch relevantes Ordnungsproblem für die Gesellschaft darstellt (unter 2). Die Ergebnisse werde ich bei den einschlägigen Responsen des Straf- und Strafprozessrechts anwenden (unter 3 und 4). Hinzu werde ich die Frage ansprechen, ob und wie die Rechtsinformatik der Strafrechtsfortbildung verhilft (unter 5) und die Ausführungen mit einem Ausblick abschließen (unter 6).

2. Der kriminologische Wertgesichtspunkt

Dass die Information eine dritte »Grundgröße« neben Materie und Energie darstellt (Wiener zitiert nach Steinbuch, S. 581.), hat Norbert Wiener bei der Fundierung der Wissenschaft der Kybernetik schon in den fünfziger Jahren pointiert. Im Anschluss daran hat die Verarbeitung und Übermittlung der

Information von computergestützten Systemen in den achtziger Jahren dazu geleitet, die Information auch als Gefahrenpotential zu nominieren, im Sinne von unrichtiger, unbefugt gesteuerter, fehlender und rechtsgutgefährdender Information. (Dazu etwa Bertrand, S. 400 ff.; Bing, S. 12 ff.; Bull; Sieber, NJW 1989, S. 2570 f.; Zimmerli).

Ob diese Betrachtung am Anfang des 21. Jahrhunderts Gültigkeit für das Strafrecht hat, bleibt offen. Voraussetzung für die Beantwortung der einschlägigen Frage ist die kriminologische Untersuchung des Missbrauchs von Multimedia und vom Internet, die – wie der Computer der achtziger Jahre – heute die Information übertragen. Als Erkenntnismittel wurden Strafakten als auch Täter- und Opferbefragung herangezogen.

2.1 Erscheinungsformen des Missbrauchs des Internets

Aus der Verwertung der Erkenntnisquellen lässt sich ableiten, dass der Missbrauch des Internet zwei Hauptgruppen bildet: Erstens Aktivitäten, die Informationen mit rechtswidrigem Inhalt verbreiten und zweitens solche, die die Rechte dritter Personen an der Information verletzen. (Eine Übersicht über die Risiken der Computernetzwerke in: Dornsreif/Klein, S. 226 ff.). Eine Zuordnung nach Delikttypen innerhalb dieser Gruppen führt zu folgenden Ergebnissen:

2.1.1 Verbreitung von Informationen mit rechtswidrigem Inhalt

Mittels des Internets lassen sich Informationen mit rechtswidrigem Inhalt unterschiedlicher Art ausbreiten. Am häufigsten findet man aber Informationen, deren Inhalt in engem Zusammenhang mit drei Deliktgruppen steht.

1. **Delikte gegen die sexuelle Selbstbestimmung**
   Hier ist die Verbreitung von pornographischen Bildern einzuordnen, indem die Täter ihre Opfer – meistens Kinder – via Daten-Highways aussuchen und ihre Angebote ohne Verfolgungsrisiko aus der Ferne machen (vgl. etwa Horb, S. 53). Auch die sexuelle Belästigung am Arbeitsplatz, die unter besonderen Umständen als Beleidigung betrachtet werden kann, ist unter diesem Delikttypus einzusortieren. Das Opfer ist mittels Manipulationen von Daten gezwungen, z.B. pornographische Bilder am Arbeitsplatz anzuschauen oder die Zusendung sexistischen und pornographischen Materials an seiner Mailbox auf sich zu nehmen. (vgl. dazu Möhn, CHIIP 1995 (Heft 1), S. 60 ff.).
2. **Delikte gegen die öffentliche Ordnung**
   Neben den sexuell gerichteten Kriminellen wird das Internet auch von extremistischen politischen Gruppen missbraucht: Das Datennetz wird einerseits von extremistischen Kreisen benutzt, um ihre Botschaften

unzensiert zu verbreiten (Pack, S. 52.), während andererseits Informationen, die terroristischer Aktivitäten unterstützen, wie z. B. Anleitungen zum Bombenbau oder zum Mischen von Nitroglyzerin, öffentlich im Rahmen der »rechtmäßigen« Nutzung des Systems angeboten werden.

3. **Fälschung von Hypertexten**
   Die Verbreitung von Texten und Bildern via Datennetzen bietet Kriminellen die Möglichkeit, die Inhalte von Internetseiten zu manipulieren. (P. Klimsa, S. 188 f.). Den Informationen, die dort enthalten sind, wird durch Bearbeitungsprogramme, etwa Viren, ein völlig neuer Inhalt gegeben oder sie werden zerstört. So sind etwa die Originalinhalte der Homepage der CIA und des US-Justizministeriums durch Hakenkreuze, nacktes Fleisch und Anti-Zensur-Parolen ersetzt (siehe Luckhardt, S. 235) oder Rechner durch Viren (z. B. durch den »I love you«-Virus), die durch E-Mail verbreitet worden sind, abgestürzt.

2.2. Verletzung von Rechten Dritter an der Information

Bei der Aufarbeitung der zweiten Hauptgruppe des Missbrauchs des Internets fällt auf, dass die Rechtsgüter, die von den entsprechenden Handlungen verletzt werden, meistens nicht von dem StGB geschützt werden. Vielmehr handelt es sich um Rechtsgüter, die von Normen des Nebenstrafrechts geschützt werden.

1. **Verletzung urheberrechtlicher Vorschriften**
   Das Angebot von Raubkopien, etwa von Programmen oder Musik-CDs, wird heute durch das Netz gemacht und diese werden durch die Verwendung des Internet kopiert und übertragen. Hinzu wird den Piraten die Möglichkeit gegeben, für bestimmte Zeit Zugriff auf Mailboxen zu haben, die die allerneueste Software enthalten. Damit ist die Anonymität sowohl des Kunden als auch des Vertreibers gewährt, die gefährlichen Beweisobjekte in Form von Disketten entfallen und die strafrechtlichen Tatbestände des Urhebergesetzes sind erfüllt (vgl. Bär, S. 440). Diese Tatsache führt dazu, dass das Raubkopieren über das Internet zu einem »Kavaliersdelikt« gemacht wurde, so dass in fast jedem privaten Computer Raubkopien zu finden sind.
2. **Verletzung datenschutzrechtlicher Vorschriften**
   Trotz der hauptsächlichen Anonymität der Nutzung eines Datennetzes ist die Gefährdung des Rechts auf informationelle Selbstbestimmung möglich. E-Mail-Adressen, Verbindungsdaten z.B. Zeitpunkt und Dauer einer Verbindung, Entgeltdaten, die für Abrechungszwecke verarbeitet werden, Bestandsdaten wie Namen oder Anschriften von Netzbenutzern können als personenbezogene Daten in Erscheinung kommen, deren Sammlung Kommunikations- oder Nutzungsprofile herstellen lassen. Weiterhin verletzt das Abhören der übertragenen Informationen als Inhaltsdaten die Vertraulichkeit der Kommunikation und leitet zu der

Anwendung von datenschutzstrafrechtlichen Normen (s. dazu Eckhardt, S. 197 ff.).

2.3 Zwischenergebnis: Ende des 20. Jahrhunderts: Information als Gefahrenpotential

Aus den Vorangegangenem kann gefolgert werden, dass auch mit dem Einsatz von Multimedia und des Internets die Aussage aufrechterhalten bleibt, dass die Information ein Gefahrenpotential darstellt. Diese These ist aber nicht als eine rechtlich relevante Naturtatsache nach der Radbruchschen Lehre zu bewerten (Siehe Radbruch, S. 10 ff., wo er den Stoff, der das Recht zu formen hat, in drei Gruppen gliedert: in die Gruppe der rechtlich relevanten Naturtatsachen, die Gruppe der sozialen Vorformen der Rechtsverhältnisse und die Gruppe des bestehenden Rechts. Dass die Information per se, um den Aphorismus von Norbert Wiener zu Ende zu denken, in den meisten Fällen eine neutrale Größe ist, stellt eine rechtsunerhebliche Seinsgegebenheit dar. Nur unter Bezug auf einen bestimmten Gesichtspunkt, dass nämlich die Information mittels der Informationstechnik verarbeitet und übertragen wird, wird diese zum Gefahrenpotential pervertiert, das für das Recht Relevanz hat. Denn – um Stratenwerth zu zitieren – »erst die spezielle Blickrichtung hebt das Wesen der Sache aus der Masse vorfindbarer Fakten heraus.« (Stratenwerth, Die Natur der Sache, S. 27).

3. Der strafrechtliche Wertegesichtspunkt

Mit der Feststellung, dass die Information ein Gefahrenpotential in Form der Internet-Kriminalität darstellt, ist aber noch nicht gesagt worden, wie das Strafrecht solche Sachverhalte bewertet und – wenn notwendig – ordnend eingreift. Die Ansätze dafür bietet die Rechtsprechung beim Judizieren von internetspezifischen Fällen.

3.1 Problemkreis: »Anwendbarkeit des deutschen Strafrechts«

Der BGH hat sich in seinem Beschluss vom 12.12.2000 mit der Anwendbarkeit des deutschen Strafrechts bei der Bestrafung der Internetkriminalität auseinandergesetzt.

Der Angeklagte, ein australischer Staatsbürger, hat von ihm verfasste Äußerungen, die den Tatbestand der Volksverhetzung nach § 130 StGB erfüllten, auf einem australischen Server in das Internet gestellt, die Internetnutzern in Deutschland zugänglich waren. Das Gericht entschied für die Anwendung des deutschen Strafrechts und dabei wie folgend argumentiert: »Wenn für die Anwendung deutschen Strafrechts die Auslegung des § 9 StGB erfolgen muss,

so ist das Merkmal ›zum Tatbestand gehörender Erfolg‹ nicht ausgehend von der Begriffsbildung der allgemeinen Tatbestandslehre zu ermitteln. Der Erfolgseintritt ist in enger Beziehung zum konkreten Straftatbestand zu sehen.« Demnach interpretierte der Senat den einschlägigen Tatbestand § 130 Abs. 1, 3 StGB, wobei das deutsche Strafrecht uneingeschränkt zur Anwendung gelangt. Denn nach Ansicht des Gerichts sei der nach § 9 StGB erforderliche Erfolg des konkret abstrakten Gefährdungsdelikts der Volksverhetzung in Deutschland eingetreten (s. dazu BGH, CR 2001, 262 ff. m. Anm. Vassilaki).

Unklar und vom BGH nicht konkretisiert ist allerdings, welche die Kernaussage des Ausdrucks »zum Tatbestand gehörender Erfolg« sein kann, bzw. was die Konsequenz ist, wenn dieser Erfolg – was auch immer ihn ausmacht – eintritt. Auf diese Frage kann es nur eine Antwort geben: Wenn der tatbestandsmäßige Erfolg eintritt, wird das geschützte Rechtsgut beeinträchtigt, d.h. gemäß dem einschlägigen Tatbestand entweder verletzt oder gefährdet. Wenn nunmehr der Parameter »Eintritt des tatbestandsmäßigen Erfolges« eng mit dem Parameter »Rechtsgutbeeinträchtigung« verbunden ist, lassen sich aus einer Betrachtung des letzteren Ansätze zur Konkretisierung des ersten gewinnen. So erhält der Begriff »tatbestandsmäßiger Erfolg« i. S. von § 9 StGB Konturen.

Das mittels eines Straftatbestandes geschützte Rechtsgut kann durch die Vornahme von Handlungen in zweifacher Hinsicht betroffen werden: Einerseits kann es unmittelbar beeinträchtigt werden, indem das Rechtsgut verletzt wird, wie z.B. durch die Verbreitung von Viren, die den ordnungsgemäßen Betrieb einer EDV-Anlage verhindern und so das Rechtsgut »Eigentum«. Andererseits kann das inkriminierte Verhalten mittelbar zu einer Beeinträchtigung führen, wovon immer dann auszugehen ist, wenn nicht sicher ist, ob es zu einer tatsächlichen Schädigung kommen wird, so z. B. das Verbreiten unvollständiger Informationen über Wertpapiere via Internet, was nach § 264 a StGB das Allgemeininteresse an der Funktionsfähigkeit des Kapitalmarktes negativ beeinträchtigt. Bei den Erfolgsdelikten wird somit die Rechtsgutbeeinträchtigung »festgestellt«, während bei den Gefährdungsdelikten eine solche »prognostiziert« wird.

Für eine solche »Prognoseentscheidung« ist im Bereich der Gefährdungsdelikte der Schwerpunkt auf das inkriminierte Verhalten zu legen und zu fragen, ob dieses Verhalten geeignet ist, zu einer Beeinträchtigung des geschützten Rechtsgutes zu führen. Die Feststellung der Geeignetheit soll nach einer ex-ante-Bewertung des zur Prüfung anstehenden Verhaltens abstrahiert vom Einzelfall geschehen. Es muss nämlich gefragt werden, ob das konkrete Verhalten gemäß dem vom Täter vorgestellten Verlauf zur Beeinträchtigung des geschützten Rechtsgutes führt. Wenn diese Frage positiv beantwortet werden kann, liegt eine Gefährdung des Rechtsgutes vor und der zum Tatbestand gehörende, aber in diesem nicht beschriebene Erfolg ist eingetreten, so dass die Anwendung des deutschen Strafrechts gem. § 9 I StGB in Betracht kommt.

3.2 Problemkreis: Garantenstellung

Das AG Tiergarten hatte über einen Fall zu entscheiden, in dem die Angeklagte durch das Einfügen eines Links in ihrer Homepage den Zugriff auf die Zeitschrift »Radikal« ermöglichte, deren Verbreitung in Deutschland verboten ist. Im Heft 154 der Zeitschrift »Radikal« konnte man zwei Artikel lesen, die zu Sabotageakten gegen die Deutsche Bahn aufforderten und unter dem Gesichtspunkt des § 316b Abs. 1, der die Störung öffentlicher Betriebe bestraft, und § 126 Abs. 1 Nr. 7 StGB, der die Störung des öffentlichen Friedens durch Androhung von Straftaten bestraft, von strafrechtlicher Bedeutung waren. Für das Gericht war die Tatsache von Bedeutung, dass zum Zeitpunkt des Installierens des Links, nämlich im April 1996, die entsprechende Ausgabe der Zeitschrift noch nicht existierte. Erst zu einem späteren Zeitpunkt, nämlich im Juni 1996, sind die rechtswidrigen Artikel eingespeist worden. Demzufolge verneinte das Amtsgericht die Absicht der Angeklagten, Beihilfe zur Anleitung zu Straftaten zu leisten und sprach sie frei. Es sind jedoch keine Ausführungen zu finden, die die Kardinalfrage betreffen, nämlich ob grundsätzlich jeder, der einen Link in seiner Homepage einbaut, verpflichtet ist, den Inhalt der von ihm verwiesenen Web-Seite vorher zu kontrollieren. Gleichwohl hat das Gericht die Möglichkeit einer Strafbarkeit unter dem Gesichtspunkt der Garantenpflicht aus Ingerenz in Betracht gezogen (s. AG Tiergarten., CR 1998, 111 m. Anm. Vassilaki). Das Gericht hat erkannt, dass die Unterlassungsproblematik eine wichtige Rolle bei der Bestrafung des Missbrauches von Internet spielen wird. Dass es keine eindeutige Aussage dazu geliefert hat, ist teilweise auf den komplizierten dogmatischen Aufbau der Unterlassungsdelikte zurückzuführen. Gleichwohl ist eine Garantenstellung aus Ingerenz abzulehnen, denn diese würde bedeuten, dass, wie die h. M. als Voraussetzung für die Ingerenz verlangt, das Herstellen des Links ein objektiv pflichtwidriges Verhalten darstellt. Diese Konsequenz wäre aber weder rechtlich noch rechtspolitisch haltbar. Vielmehr ist die Frage zu stellen, ob die Schaltung bzw. Aufrechterhaltung eines Links die Begründung einer Garantenpflicht zur Folge hat, weil damit der Linkprovider die Herrschaft über einen Gefahrenbereich übernimmt. Da die Antwort umfangreiche Ausführungen verlangt, wird an dieser Stelle nur ansatzweise diese Problematik erörtert werden.

Für das Bestehen einer Garantenstellung des Linkanbieters wegen der Herrschaft über einen Gefahrenbereich könnte der Entstehungsgrund dieser Garantenpflicht sprechen. Wollen die Menschen via Internet kommunizieren, können sie dieses nur, wenn sie erwarten können, dass jeder, der die neuen Medien benutzt, seinen Einflussbereich im Netz in einer Weise gestaltet, dass von diesem keine unvorhersehbaren Gefahren für die Rechtsgüter Dritter oder der Allgemeinheit ausgehen. Demzufolge ist der Urheber einer Homepage ein Inhaltsanbieter, der den rechtlichen Einfluss, die Herrschafts- bzw. Verfügungsgewalt über die Homepage hat. Damit ist er verpflichtet, diese zu kontrollieren, so dass sie keine rechtswidrigen Informationen enthält oder auf keine rechtswidrigen Inhalte weiterverweist. Unter diesem Gesichtspunkt

kann eine Rechtspflicht zur Kontrolle begründet werden, deren Zumutbarkeit für den Garanten gesondert zu prüfen ist (Ausführlich dazu Vassilaki, CR 1999, 85 ff.).

3.3 Problemkreis: Schriftenbegriff (§ 11 Abs. 3 StGB)

OLG Nürnberg hat sich in einem Beschluss v. 23.6.1998 mit der Problematik des Schriftenbegriffs beschäftigt. Der Senat hatte über die öffentliche Beschimpfung eines christlichen Bekenntnisses nach § 166 StGB zu entscheiden, weil eine Firma über ihre Internet-Homepage ein T-Shirt anbot, auf dem ein an das Kreuz genageltes Schwein abgebildet war. Nach der Begründung fallen die Datenträger der Homepage unter den Schriftenbegriff des § 11 III StGB. Denn Daten, die über das Internet abgerufen werden können, werden durch Speichermedien wie Festplatten bereitgestellt, so dass eine Verkörperung vorliegt, die für den Schriftenbegriff des § 11 III StGB notwendig ist. Unerheblich ist dabei, dass die Wahrnehmung solcher Daten nur durch den Einsatz von technischen Mitteln möglich ist.

Damit steht fest, dass die auf Datenspeichern festgehaltenen Informationen eine Schrift gem. § 11 III StGB darstellen. Das OLG Nürnberg hat allerdings die Frage offengelassen, ob solche Informationen unter dem Begriff der »Darstellung« des § 11 III StGB subsumiert werden können. Obwohl das Zögern des Senats aufgrund der Unklarheiten, die die Technik oft verursacht, verständlich ist, bleibt das Gericht der Strafrechtswissenschaft eine Antwort schuldig. Diese kann jedoch aus der Argumentation anderer Gerichte abgeleitet werden. Denn die Auslegung des § 11 III StGB lässt es zu, die gespeicherten Informationen als »Darstellungen«, die den Oberbegriff der Vorschrift bilden, zu betrachten (Ausführlich dazu Vassilaki, MMR 1999, 528 f.).

3.4 Zwischenergebnis: Materielles Strafrecht + Internet = »Law in action«

Die kurze Darlegung dieser internetspezifischen Urteile weist deutlich darauf hin, dass im konkreten Zeitpunkt in diesem Bereich grundsätzlich Lösungen durch die Anwendung des allgemeinen Teils des Strafrechts gesucht werden. Die Auslegung der Vorschriften des Besonderen Teils erfolgt in der Regel ohne Schwierigkeiten. Bei der Internet-Kriminalität ist daher nicht die Verhaltensregelung bzw. -bestrafung, sondern die Verhaltenseinordnung problematisch. Das strafrechtlich relevante Verhalten wird nach den allgemeinen Voraussetzungen der strafbaren Handlung geprüft. Die Gegebenheiten der Informationsgesellschaft werden in die Grundprinzipien des Strafrechts gekleidet. Diese Feststellung ergibt sich von den Ansätzen der Rechtsprechung, die sich um die Formung von Grundsatzlinien bemüht, die eine Richtschnur für die Beantwortung von Fragen der Internet-Kriminalität bilden sollen.

Dieses Vorgehen stellt freilich nichts anderes als die Reaktion des Rechts

gegenüber neuen Phänomenen in seiner Eigenschaft als »law in action« dar. Denn das Recht ist nicht bloß ein normatives Sinngefüge, sondern es hat auch eine faktische Seite. Diese Seite nimmt die neuen Strukturen der Informationsgesellschaft wahr und versucht den Anwendungsbereich des Rechts auch auf diese Neuheiten zu erweitern. In diesem Sinne verhilft der Missbrauch des Internet der strafrechtlichen Entwicklung. Neuer Regelungen durch den Gesetzgeber bedarf es nicht. Vielmehr ist die Strafrechtswissenschaft herausgefordert, die Dogmatik des Allgemeinen Teils auf die neuen Fragen anzuwenden. Auf diese Weise wird die Strafrechtswissenschaft das Strafrecht aus geschriebenem Recht (law in the books) zum lebenden Recht (law in action) des 21. Jahrhunderts überleiten.(Über das Recht als »law in action« vgl. Esser, S. 19 ff.; Rehbinder, § 1 2; Pound, S. 44 (1910), S. 12 ff.; Zippelius, ..., S. 16 f.; ders..., Rechtsphilosophie, § 4 III.).

4. Der strafprozessuale Wertgesichtspunkt

Im Gegensatz zu der internetspezifischen Rechtsprechung, die sich mit Fragen des materiellen Strafrechts beschäftigt, karg sind die Ausführungen, die strafprozessuale Themen betreffen. Gleichwohl mannigfaltig und kompliziert sind die Probleme, die während der Strafverfolgung der Internet-Kriminalität hervorgerufen werden. Im Folgenden sollen nur die wichtigsten davon erläutert werden.

4.1 Problemkreis: Durchsuchung

In einem Beschluss vom 3. 8. 1995 betrachtete der BGH die Durchsuchung und Durchsicht von Datenträgern als Maßnahmen, die den Anforderungen der §§ 102 ff. StPO gerecht werden (siehe dazu BGH, CR 1996, S. 36 ff. m. Anm. Bär). Damit ist zuzustimmen. Der Richter hat die Ausführungen einer älteren Entscheidung des Gerichts fortgeführt, die die Frage der Anwendung des § 110 StPO bejahend beantwortet hat (siehe dazu BGH, CR 1988, S. 142 f.). Damit macht es keinen Unterschied, wenn das für das Strafverfahren von Bedeutung gewonnenes Beweismaterial in elektronischen Informationsträgern gespeichert ist . Anders ist aber die Sachlage, wenn die Durchsuchung den Zugriff auf Daten bedeutet, die via Netzwerk aufgerufen werden sollen. In diesem Fall ist zu differenzieren: Wenn die Durchsuchungsanordnung den Zugriff auf Daten innerhalb eines lokalen Netzwerkes erfasst, z. B. die internen Online-Verbindungen eines Betriebs, entstehen aus der »Vergeistigung« der Durchsuchung keine Probleme. Dieses Vorgehen ist mit dem Fall zu vergleichen, in dem die Durchsuchung ein ganzes Haus betrifft und diese in jedem Zimmer durchgeführt wird.

Anders ist aber die Konstellation zu betrachten, in der die Beweismittel durch Zugriff auf Daten gewonnen werden müssen, ohne dass vorher der

Standort des Servers, in dem die Informationen gespeichert sind, bekannt ist. Eine solche Durchsuchung von Kommunikationseinrichtungen verstößt gegen strafprozessuale Normen und Prinzipien. Sie überschreitet zunächst das Ausmaß der Durchsuchungsanordnung, die, wenn es sich um die Durchsuchung »anderer Räume« handelt, genau bezeichnet werden muss (über die Bezeichnung des Ausmaßes der Durchsuchungsanordnung vgl. etwa BVerfGE 20, 162 [227]; 42, 212 [21]; 44, 353 [371]; BVerfG, NStZ 1992, S. 91.).

Die für die Rechtmäßigkeit der Maßnahme notwendige Angabe, dass die Durchsuchung sich in Datenbestände innerhalb Deutschlands erstreckt, würde dem Gebot der Verhältnismäßigkeit unterlaufen (Bär,1996, S. 229 f.).

Hinzu kommt die Gefahr, die Grenzen zwischen Durchsuchung und Telekommunikationsüberwachung verwischen zu lassen, was die folgende Bemerkung erleuchtet: Da die durch die Durchsuchung Beweismittel »ex tunc« während diese mittels der Telekommunikationsüberwachung »ex nunc« gewonnen werden sollen, ermöglicht die Schnelligkeit der Datenfernverarbeitung und -übertragung solche Differenzierungen nur in wenigen Fällen. Denn es ist oft schwierig festzustellen, welche Daten gespeichert waren, bevor die Ausführung der Durchsuchung angefangen hat und welche Daten während der Durchführung dazu kommen (Über die Unterschiede zwischen Durchsuchung und Kommunikationsüberwachung vgl. detalliert: Council of Europe, PC-PC (93) 27).

Nicht zuletzt sind die aus der Durchsuchung im Internet abgeleiteten Probleme des internationalen Strafrechts zu erörtern. Der Zugriff auf Datenbestände im Netz kann schnell den deutschen Hoheitsbereich verlassen und die Hoheitsgewalt fremder Staaten gefährden. Diese vom Europarat genannte »direct penetration« (Über die Problematik der »direct penetration« siehe Council of Europe, Recommendation No. R (89), 9 S. 66 ff.) unterläuft das Rechtshilfeabkommen und führt zur unverwertbaren Beschaffung von Beweismitteln.

Demzufolge kann eine Durchsuchung angeordnet und ausgeführt werden nur wenn der Zielrechner, in dem die gesuchten Beweismittel gespeichert sind, bekannt ist. Für die entsprechende Suche sind §§ 100g, h StPO von Bedeutung, die durch das »Gesetz zur Änderung der StPO« v. 20.12.2001 in die StPO eingefügt worden sind. Diese stehen nunmehr als Rechtsgrundlage für den Zugriff auf Verbindungsdaten zur Verfügung. Danach sind die TK-Anbieter verpflichtet, etwa die beteiligten Rufnummern einer Kommunikation den Untersuchungsbehörden mitzuteilen, die zu einem Zentralrechner führen können, der danach untersucht wird (Bizer, S. 237.).

4.2 Problemkreis: Beschlagnahme

Die Unkörperlichkeit von Daten bringt besondere Probleme hervor, wenn sie beschlagnahmt werden sollen. Gleichwohl besteht Klarheit darüber, wenn sie in Datenträgern gespeichert sind. In diesem Fall werden die externen Speicher-

medien als »Gegenstände« nach § 94 StPO sichergestellt. Weil dagegen einzelne Daten nicht verkörperte Objekte darstellen, scheiden als Beschlagnahmeobjekte aus. Das gleiche gilt für Informationen, die via Netz am Bildschirm zu sehen sind, die freilich wegen ihrer Vergänglichkeit nicht unter § 94 StPO subsumiert werden können.

Für unkörperliche Informationen kommt die gem. § 94 StPO Sicherstellung »in anderer Weise« in Betracht. Diese ist notwendig, wenn Gegenstände, wie etwa Grundstücke oder Räume, nicht in Verwahrung genommen werden können oder aus Zwecken genauerer Untersuchung, an Ort und Stelle, wenn auch nur vorübergehend, verbleiben müssen (vgl. dazu Kleinknecht/Meyer-Goßner, § 94 Rn. 16; KK-Laufhütte, § 94 Rn. 15; LK-Schäfer, § 94, Rn. 33). Dabei sei aber bemerkt, dass ein Herrschaftsverhältnis der Strafverfolgungsbehörde begründet werden soll. Es muss nämlich eine amtliche Handlung vorliegen, die in geeigneter Weise erkennbar zum Ausdruck bringt, dass die Sache der freien Verfügung des Inhabers entzogen und der amtlichen Obhut unterstellt wird. Demzufolge dürfen die in einem Zentralcomputer und für ein Strafverfahren von Bedeutung gespeicherten Daten nicht mehr vom Beschuldigten verwendet werden. Dieses wird in der Regel mittels Sperrung der entsprechenden Datenbestände erreichbar sein, was darüber hinaus die weitere Benutzung von Hard- und Software seitens des Beschuldigten ermöglicht. Danach kann ein Herunterladen der einschlägigen Daten von der Festplatte auf Datenträger und deren Inverwahrungnahme gem. § 94 Abs. 1 StPO für das weitere Strafverfahren erfolgen. Gleichwohl reicht das einfache Downloading der in Betracht kommenden Daten ohne Einwirkung auf die Anlage, in der die Informationen gespeichert sind, nicht. Denn in diesem Fall wird – entsprechend der vom BGH gestellten Anforderungen (siehe dazu BGHSt 3, S. 400; 15, S. 150; ähnlich auch RGSt 18, S. 71 ff.) – keine staatliche Herrschaftsgewalt auf die original gespeicherten Informationen begründet (Anders aber Bär, 1996, S. 745, der das bloße Kopieren beweisrelevanter Informationen und deren Inverwahrungnahme unter dem Begriff »Sicherstellung auf anderer Weise« subsumiert).

Demzufolge ist die Beschlagnahme von für ein Strafverfahren beweisrelevanten Daten in den Fällen beschränkt, in denen zugleich die Datenträger mit beschlagnahmt werden. Gespeicherte Informationen werden dagegen gem. § 94 I StPO »in anderer Weise sichergestellt«, wenn es technisch möglich ist, sie innerhalb einer Computeranlage zu sperren.

4.3 Problemkreis: Kommunikationsüberwachung

Dass die neuen Formen der Kommunikation innerhalb der Informationsgesellschaft auch Unklarheiten hinsichtlich ihrer Überwachung hervorruft, benötigt keine besondere Erläuterung. Demnach liegt es der Sache nahe, dass der Gesetzgeber Änderungen in die einschlägigen Normen durchgeführt hat.

Mit dem BegleitG zum TKG ist das in §§ 100a und 100b StPO verankerte Wort »Fernmeldeverkehr« von dem Begriff »Telekommunikation« ersetzt wor-

den. Damit werden die Überwachungsvorschriften, wie die Gesetzesbegründung betont, den neuen Informationstechnologien und der Terminologie des TKG angepasst (siehe BT-Druck. 369/97, S. 45, 46). Den Begriff der Telekommunikation liefert nunmehr § 3 Nr. 16 TKG, der darunter den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art, Bildern oder Tönen mittels Telekommunikationsanlagen subsumiert. Dabei ist unerheblich, wie die TKG-Gesetzesbegründung hervorhebt, welche Art die Nachrichten sind (z. B. menschliche Sprache oder Rundfunkprogramme) (siehe BT-Druck. 13/3609, S. 37).

Daraus folgt, dass die Zwangsmaßnahme der Überwachung eine Wende erfährt. Ab sofort kann sie in jeglicher Art von Nachrichten eingesetzt werden, unabhängig davon, ob es um einen Kommunikationsvorgang zwischen Menschen oder zwischen Menschen und Computern geht. Das Fernmeldegeheimnis wird damit zu einem Kommunikationsgeheimnis umgewandelt. Dieses aber enthält nicht unbedingt einen sozialen Bezugspunkt im Sinne eines zwischenmenschlichen Informationsaustausches. Nunmehr reicht für die Begründung eines überwachungsgeeigneten Vorganges der Zugang zu Informationsquellen, die mittels technischer Vorgänge Nachrichten übermitteln.

Die Veränderung des Charakters des Fernmeldegeheimnisses wird mehr einleuchtend, wenn man den veränderten § 100b Abs. 3 S. 1 StPO liest. Demnach hat jeder geschäftsmäßige Erbringer von Telekommunikationsdiensten die Überwachung zu ermöglichen. Wen diese Norm betrifft, bestimmt § 3 Nr. 5 TKG. Diese Vorschrift erfasst nämlich alle, die das nachhaltige Angebot von Telekommunikation, einschließlich des Angebots von Übertragungswesen für Dritte mit oder ohne Gewinnerzielungsabsicht, bereitstellen. Die daraus abgeleiteten Konsequenzen liegen auf der Hand. Als Telekommunikationserbringer wird jeder nominiert, der mit einiger Nachhaltigkeit Router und Server im Internet betreibt (Bär, 1998, S. 436; Grundermann, S. 51), den Betreiber von Mailboxen eingeschlossen (Siehe den Beschluß von BGH, der sich mit der Überwachung von Mailboxen auseinandersetzte, BGH, CR 1996, S. 488 ff.; NStZ 1997, S. 247 f.; StV 1997, S. 396 f.; vgl. auch die Anmerkungen von Bär, CR 1996, S. 490 f.; Bizer, DuD 1996, S. 627; Kudlich, JuS 1988, S. 209 ff.; Palm/Roy, NJW 1997, S. 1904 f.). Die Überwachung erstreckt sich über die öffentlichen Fernmeldenetze hinaus und erfasst nunmehr auch die geschlossenen Benutzergruppen (Corporate Networks), was, wie in der Gesetzesbegründung ausdrücklich artikuliert ist , ein Ziel der Veränderung war.

Die vorangegangenen Ausführungen rufen die Frage hervor, ob die Neufassung der Überwachungsvorschriften den Anforderungen des Verhältnismäßigkeitsgrundsatzes entspricht. Dabei sind nicht nur Bedenken wegen der Aushöhlung oder besser der Verabschiedung von der Garantie des Fernmeldegeheimnisses anzumelden. Vielmehr ist auch die Beeinträchtigung des Art. 14 Abs. 1 GG der Telekommunikationsanbieter vor Augen zu halten, die mittels der TKÜV v. 23.1.2002 erfahren haben, welche Maßnahmen sie ergreifen müssen, um staatliche Überwachungen zu ermöglichen (Pernice, DuD 2002, 207 ff).

4.4 Strafprozessrecht + Multimedia = Juristisches Neuland

Die ausgewählten Problemkreise haben darauf hingewiesen, dass – im Gegensatz zum materiellen Strafrecht – das Strafprozessrecht die aus der Entwicklung der Informationstechnik hergeleiteten rechtlichen Fragen nicht beantworten kann. Diese Feststellung ist auf die Tatsache zurückzuführen, dass die strafprozessualen Regelungen an der Sammlung vom Beweismaterial orientiert sind, die aus körperlichen Objekten zu gewinnen ist. Die Immaterialisierung der Information entspricht somit den Prämissen der strafverfahrensrechtlichen Normen nicht.

Demzufolge ist eine Erneuerung des Strafverfahrens erforderlich, die die einschlägigen Rechtslücken abschließen soll. Dabei ist freilich Vorsicht gefragt. Denn das Strafverfahren muss als angewandtes Verfassungsrecht (Über das Strafverfahrensrecht als angewandtes Verfassungsrecht vgl. Roxin, 2) auch grundrechtsschutzorientiert sein. Wie aber aus den ersten Änderungen zu entnehmen ist, nach denen das Fernmeldegeheimnis zu einem Telekommunikationsgeheimnis unter Vorbehalt gewandelt wird, besteht die Gefahr, aus solchen gesetzgeberischen Operationen Eingriffsmaßnahmen zu entstehen, die die Grundrechte in Frage stellen. Dadurch würde der Weg vorbereitet, innerhalb der Informationsgesellschaft den »gläsernen Menschen« zu schaffen.

5. Die Position der Rechtsinformatik

Dass auch die mathematische Methodik der Informationstechnik die gesamte Rechtswissenschaft beeinflussen wird, ist schon seit den 70er Jahren propagiert worden (Für die ältere Literatur vgl. nur Fiedler, Haft, Philipps, Simitis, Suhr). Unabhängig davon, ob man über »Juristische Informatik«, »Computers and the law«, »Rechtskybernetik«, »informatique juridique« oder »Rechtsinformatik« spricht, erfassen diese Begriffe »die Lehre von den Möglichkeiten, Voraussetzungen und Folgen der EDV im Recht« (Steinmüller, S. 30). Diese Definition enthält drei Hauptfelder, die das Verhältnis der Informationstechnik mit der Rechtswissenschaft bestimmen: Es handelt sich dabei um das Ansetzen der Informationstechnik für a) die Gewinnung von juristischen Informationen, b) die Optimierung der juristischen Ausbildung und last but not least c) die Automatisierung der Rechtsgewinnung.

5.1 Juristische Informationssysteme

Als die einfachste Aufgabe der Rechtsinformatik erscheint die Gewinnung von juristischen Informationen mit Hilfe der Informationstechnik. Der Aufbau von juristischen Off- und Online Datenbanken – an dieser Stelle sei nur das System JURIS erwähnt – die Möglichkeit, über Internet Zugang zu verschiedenen juristischen Bibliotheken im ganzen Globus zu erlangen, die Gelegenheit,

durch das Netz elektronische juristische Presse zu studieren, bieten nur ein paar Beispiele dafür, welche Vorteile gegenüber den herkömmlichen Informations-Einrichtungen die Informationstechnik dem Juristen anbietet.

5.2 Juristische Lehrtechnologie

Auch wenn die Verwendung der Informationstechnologie beim deutschen juristischen Studium nicht besonders verbreitet ist, haben einschlägige Projekte der Universitäten Berlin, Hannover, Heidelberg, Münster, München, Passau, Saarbrücken, Tübingen und Würzburg gezeigt, dass multimediales Lernen und Lehren in ein paar Jahren unentbehrliches Instrumentarium der juristischen Ausbildung sein wird. Es sind dabei dialogfähige Programme gefragt, die etwa mit Begriffsbäumen dem Lernenden helfen, Tatbestände besser zu verstehen. Die Selbständigkeit der Erarbeitung je nach dem individuellen Verständnis des Studenten, die unterschiedlichen Alternativen und das enorme Angebot an Literatur und Rechtsprechung in Verbindung mit der Möglichkeit der Bewertung der Antworten und der Hilfestellung der Lernsoftware bieten eine zusätzliche – wohlbemerkt – juristische Ausbildungsmöglichkeit (Über die Anwendungen von juristischen Lernprogrammen vgl. etwa Brehm, PC-Fallbeispiel Zwangsvollstreckung: Fiedler/Oppenhorts; Haft/Müller-Krumbhaar, S. 556 ff.; Philipps, S. 103 ff.; Ring, S. 64. Denn die Erfahrung mit den Lernprogrammen hat auf eine Tatsache hingewiesen: Sie können neben und nicht statt der klassischen juristischen Basis-Ausbildung angeboten werden.).

5.3 Juristische Rechtsfindung

Die Herausforderung der Rechtsinformatik liegt darin, die Informationstechnik zu verwenden, um eine automatisierte Rechtsanwendung zu gewinnen. Gefragt wird dabei, die Formalisierung von Rechtsanwendungsmodellen der Methodenlehre, so dass die Subsumtion automatisch folgt. Es sind bis jetzt zwei Systeme, die ansatzweise eine solche Umsetzung erreicht haben. Das erste ist das Expertensystem Lex, das ein Forschungsprojekt der IBM Deutschland und der Universität Tübingen § 142 StGB verarbeitet hat. Es verwendet »Wenn-dann-Regeln« und beinhaltet Auslegungsalgorithmen, die auf Wortinterpretation basieren. (Über das Expertensystem-Lex siehe ausführlich, Sulz). Das an der Universität München erstellte Neuronale Netz erarbeitet dagegen ein System zum Schmerzensgeldanspruch nach § 847 BGB. Das Netz besteht aus kleinen Einheiten, die sog. Neuronen, die mit der geeigneten technischen Unterstützung die Eigenschaft besitzen, sich trainieren zu lassen. Das System enthält höchstrichterliche Rechtsprechung, die den Schmerzensgeldanspruch betrifft. Diese wird vom System als Muster verwendet und mit einem Vergleichsalgorithmus auf den gestellten Sachverhalt übertragen, so

dass eine automatisierte Entscheidung getroffen werden kann. Rechtsmethodisch wird nämlich die aristotelische Topik verwendet, indem der Topoikatalog und unterschiedliche Gesichtspunkte des Sachverhaltes von den Neuronen bewertet werden. (Ausführliche Beschreibung des Münchener Neuronalen Netzes siehe in: Ring, S. 123 ff.; dazu vgl. auch Philipps/Brass/Emmerich.).

5.4 Rechtsinformatik: Die Konvergenz der Informationstechnik und der Rechtstheorie

Die synoptische Darstellung der Arbeitsfelder der Rechtsinformatik weisen darauf hin, dass diese eine Herausforderung für die gesamte Rechtswissenschaft darstellt. Insbesondere werden rechtstheoretische Ansätze gesucht und überarbeitet, die geeignet sind, einer formalisierten Sprache übersetzt zu werden. Ob dabei die Informationstechnik als Subsumtionshilfe oder als selbstständiges Entscheidungsautomat verwendet wird, ist eine Frage, die nicht nur von dem Willen der Juristen abhängig ist, sondern auch von der Fähigkeit der Informatiker die komplizierten Methoden der Rechtsfindung zu juristisch tauglich mathematischen Algorithmen umzuwandeln.

6. Ausblick

Die vorangegangene Untersuchung hat dargelegt, dass Verhaltensformen der Informationsgesellschaft unterschiedliche Fragen in einem weiten Bereich der Strafrechtswissenschaft hervorrufen. Dass für die Antworten in einigen Fällen die klassische Strafrechtsdogmatik eingesetzt werden muss, während in anderen Fällen das Einschreiten des Gesetzgebers gefragt ist, ist die natürliche Reaktion des Rechts gegenüber neuen gesellschaftlichen Phänomenen. Denn – um die Ausführungen von Platon leicht zu verändern – mittels des Rechts werden die Elemente bekannt, die notwendig für das Zusammenleben in einer konkreten Gesellschaft sind. (Platon, 875a). Und es sieht so aus, als dass die Informationstechnik – in welcher Form auch immer – sich als ein wichtiger Teil der Gesellschaft des 21. Jahrhunderts entwickelt.

Literatur

Bär, W.: Polizeilicher Zugriff auf kriminelle Mailboxen, CR 1995, S. 489 – 495.
Bär, W.: Durchsuchungen im EDV-Bereich, CR 1995, S. 227 – 236.
Bär, W.: Rechtsprechung zum Strafrecht, BGH »Durchsuchung« einer Mailbox, CR 1996, S. 490 – 500.
Bär, W.: EDV-Beweissicherung im Strafverfahresrecht: Änderungen durch das BegleitG zum TKG, CR 1998, S. 434 - 440;
Bertrand, P.: Il était une fois ... le droits de l´informatique, Expertises 1987.
Bing, J.: in: International Computer Law Adviser Bd. 1 (1987), S. 12 – 16.

Bizer, J.: Verpflichtung zur Herausgabe von TK-Verbindungsdaten an den Staatsanwalt, DuD 2002, 237.
Bull, P.: Datenschutz oder die Angst vor dem Computer, München 1984.
Coing, H. : Grundzüge der Rechtsphilosophie, 5. Auflage, Berlin 1993
Council of Europe, PC-PC (93) 27, Strasbourg1993.
Dornsreif, M./Klein, C.: Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke, DuD 2002, S. 226 – 230.
Eckhardt, J.: Neue Regelungen der TK-Überwachung, DuD 2002, S.197 – 201.
Esser, J.: Grundsatz und Norm, 4. Auflage, Tübingen 1990.
Fiedler, H.: Forschungaufgaben der Juristischen Informatik, in: A. Kaufmann (Hrsg.), Münchner Ringvorlesung EDV und Recht, München 1987, S. 229 – 235.
Grundermann P.: Das neue TKG-Begleitgesetz, KuR 1998, S. 48 – 53.
Haft F.: Elektronische Datenverarbeitung im Recht, München 1970.
Horb P.: Spiegel Special 1995 (Heft 3), S. 53.
Karlsruher Kommentar zur Strafprozessordnung, Pfeiffer G. (Hrsg.), 4. Auflage 1999.
Kleinknecht T./Meyer-Goßner L., Strafprozessordnung, 46. Auflage 2001.
Klimsa W.: Multimedia, Anwendungen, Tools und Techniken, München 1995.
Kudlich H.: Der heimliche Zugriff auf Daten in einer Mailbox: ein Fall der Überwachung des Fernmeldeverkehrs? JuS 1998, S. 209 – 215.
Leipziger Kommentar, Großkommentar, Jähnke B./Laufhütte H./Odersky W. (Hrsg.), 11. Auflage 1992.
Luckhardt T.: c´t 1997, (Heft 4), S. 235.
Montesquieu C-L: Vom Geist der Gesetze,Stuttgart 1994.
Pack D.: CHIP 1995 (Heft 10), S. 52.
Palm T./Roy G.: Der BGH unf der Zugriff auf Mailboxen, NJW 1997, S. 1904 – 1908.
Pernice I-M.: Die Telekommunikations-Überwachungsverordnung, DuD 2002, S. 207 – 211.
Philipps L./Brass C./Emmerich H: A Neural Network to Identify Legal Procedents München 1990.
Philipps L.: Testaufgaben in der Rechtswissenschaft, München 1978;
Platon, Nomoi, Buch IX, 875a Athen 1988.
Radbruch G.: Einführung in die Rechtswissenschaft, Stuttgart 1980.
Rehbinder M.: Rechtssoziologie 3. Auflage, Berlin 1993.
Ring S.: Computergestützte Rechtsfindungssysteme, Köln 1994.
Roxin C.: Strafverfahrensrecht, 25. Auflage 1998.
Sieber U.: Informationsrecht und Recht der Informationstechnik, NJW 1989, S. 2570 – 2581.
Simitis U., Rechtliche Anwendungsmöglichkeiten Kybernetischer Systeme, Frankfurt 1966
Steinbuch, GRUR 1987, S. 581
Strömholm S.: Kurze Geschichte der abendländischen Rechtsphilosophie, Göttingen 1991.
Suhr A., Der Computer als juristischer Gesprächspartner, München 1970.

Sulz J.: LEX1-Prototyp eines computergestützten juristischen Expertensystems auf natürlichsprachlicher Basis, in: Haft F./Lehmann H.: Das LEX-Projekt. Entwicklung eines Expertensystems, Tübingen 1989 S. 77 – 114.
Tinnefeld M-T./Phillips L./Heil S.: Informationsgesellschaft und Rechtskultur in Europa Baden-Baden 1998.
Vassilaki I.: Strafrechtliche Verantwortlichkeit durch Einrichten und Aufrechterhalten von elektronischen Verweisen (Hyperlinks). Die Anwendbarkeit der allgemeinen Strafrechtsdogmatik auf neuen Verhaltensformen; in: CR 1999, S. 85 – 93.
Vassilaki I.: Der Einfluß der Informations- und Telekommunikationstechnik auf die Strafrechtsfortbildung im Jahre 1998 - Rechtsprechungsübersicht über kommunikationsrechtliche, computer- und internetspezifische Entscheidungen der Strafgerichte - in: Multimedia und Recht 1999, S. 525 – 533.
Weizenbaum J.: Die Macht der Computer und die Ohnmacht der Vernunft, Frankfurt.A.M. 1994.
Weizenbaum J.: Wer erfindet Computermythen? Freiburg 1994.
Zimmerli W.: (Hrsg.), Herausforderungen der Gesellschaft durch den technischen
Wandel, München 1989.
Zippelius R.: Das Wesen des Rechts, Eine Einführung in die Rechtsphilosophie, 5. Auflage, München 1997.
Zippelius R.: Rechtsphilosophie, 3. Auflage, München 1994.