BÜNDNIS 90
DIE GRÜNEN
Bundestagsfraktion

lang & schlüssig

14 40
SEPT. 2001

Eine Information der Bundestagsfraktion Bündnis 90/ Die Grünen

Cybercrime und Bürgerrechte

Impressum

Herausgeberin	Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin www.gruene-fraktion.de
Verantwortlich	Grietje Bettin MdB medienpolitische Sprecherin Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin Fon: 030 / 227 75051 Fax: 030 / 227 76051 eMail: grietje.bettin@bundestag.de www.grietje-bettin.de
Redaktion	Peter Schaar
Bezug	Bündnis 90/Die Grünen Bundestagsfraktion Info-Dienst Platz der Republik 1 11011 Berlin Fax: 030 / 227 56566 eMail: public@gruene-fraktion.de
Schutzgebühr	DM 3,---
Redaktionsschluss	September 2001

Inhalt

1 Formen der “Internet-Kriminalität” 3
1.1 Unzulässige Inhalte 3
1.2 Hacking 5
1.3 Andere Missbräuche des Internet 6

2 Schützenswerte Freiheitsrechte im Netz 6
2.1 Informations- und Meinungsfreiheit 6
2.2 Recht auf informationelle Selbstbestimmung/Fernmeldegeheimnis 6

3 Derzeitige Rechtslage 7
3.1 Auswertung veröffentlichter Informationen 7
3.2 Strafverfolgung 8
3.3 Heimliches Eindringen in Mailboxen und andere geschützte Bereiche des Internet 10
3.4 Öffentlichkeitsfahndung im Internet 11
3.5 Polizeirecht 11
3.6 Nachrichtendienste 13

4 Zusätzliche Strafnormen und Befugnissen für Sicherheitsbehörden? 13
4.1 Forderungen aus Sicherheitsbehörden 13
4.2 Datenverschlüsselung - Kryptodebatte 15
4.3 Internationale Initiativen 15
4.3.1 G8-Initiative 16
4.3.2 Cyber Crime Convention 16
4.3.3 EU-Initiative “sicheres Internet” 18
4.4 Telekommunikations-Überwachungsverordnung (TKÜV) 18

5 Schlussfolgerungen 19
5.1 Ausstattung von Strafverfolgungsbehörden verbessern 19
5.2 Verantwortung von Diensteanbietern stärken 20
5.3 Datenschutz ausbauen und modernisieren 20
5.4 Selbstschutz und Nettiquette 20

Cybercrime und Bürgerrechte

Angesichts der Berichte über unzulässige Inhalte des Internet (insb. Kinderpornografie und rechtsextreme Propaganda) und über andere Missbrauchsfälle (insb. Hacking, Computer-Betrug) stellt sich die Frage, wie der “Internet-Kriminalität” wirksam begegnet werden kann. Die in diesem Zusammenhang vorgeschlagenen Maßnahmen müssen den jeweiligen Gefährdungen angemessen sein und dürfen nicht zu unverhältnismäßigen Eingriffen in die Kommunikationsfreiheit und den Datenschutz führen. Manche der öffentlich diskutierten Maßnahmen entsprechen nicht diesen Anforderungen. Im folgenden sollen die wichtigsten Formen von Missbrauch und die Befugnisse der Sicherheitsbehörden dargestellt werden. Auf dieser Basis werden die öffentlich diskutierten Maßnahmen und Rechtsänderungen hinsichtlich ihrer Wirksamkeit und Verfassungsmäßigkeit untersucht. Schließlich werden eigene Vorschläge für den Umgang mit der “Internet-Kriminalität” entwickelt.

1 Formen der “Internet-Kriminalität”

Das Internet kann für eine Vielzahl von Straftaten missbraucht werden. Dabei handelt es sich zum einen um typische Computerdelikte, also die mit “Hacking” umschriebenen Sachverhalte (Ausspähen, Verfälschung und Löschung von Daten und destruktive Eingriffe in fremde Datenverarbeitungssysteme) und Computerbetrug. Hinzu kommen Verstöße gegen das Datenschutzrecht, etwa die unzulässige Verarbeitung und Nutzung personenbezogener Daten.

Schließlich können Computernetze auch als Tatwerkzeuge für eine Vielzahl anderer unerlaubter Handlungen - von der Beleidigung bis zur Geldwäsche - verwendet werden. Von besonderer Bedeutung und öffentlicher Beachtung sind Delikte, bei denen unerlaubte Inhalte ins Netz gestellt werden, etwa rechtsextremistische Propaganda oder pornografische Abbildungen.

1.1 Unzulässige Inhalte

Die durch Art. 5 Abs. 1 GG gewährleistete Informations- und Meinungsfreiheit (siehe hierzu Abschnitt 2.1) wird durch Gesetze begrenzt. Hinzuweisen ist in erster Linie auf die so genannten "Äußerungsdelikte" im Strafgesetzbuch. Hierzu gehören z.B. die Volksverhetzung und die Verbreitung von Pornografie. Bei diesen Straftaten stellt sich nicht nur die Frage der Verantwortlichkeit des Urhebers, sondern auch diejenige nach der Verantwortlichkeit des Internet Providers, der die Inhalte zugänglich gemacht hat.

Eine besondere Problematik stellt in diesem Zusammenhang die unterschiedliche Bewertung pornografischer Darstellungen in den nationalen Rechtsordnungen dar. So sind in etlichen Ländern pornografische Darstellungen – anders als bei uns - weitgehend straffrei. Lediglich hinsichtlich des Verbots der Kinderpornografie gibt es einen weitgehenden internationalen Konsens. Ähnlich ist die Situation bei extremistischer Propaganda. So ist es in den USA durchaus zulässig, rechtsradikale Propaganda öffentlich zu verbreiten. Dem entsprechend sind auch Angebote, die die so genannte “Auschwitzlüge” verbreiten, im Hinblick auf die hohe Wertschätzung der Meinungsfreiheit (erster Verfassungszusatz) nach US-Recht straffrei.

Die Anwendbarkeit des deutschen Strafrechts geht von dem Prinzip des "Erfolgsortes" aus. Entscheidend ist dementsprechend nicht, an welchem Ort ein strafbarer Inhalt ins Netz gestellt wird, sondern ob dieser Inhalt im Inland abrufbar ist. Dies hat zu der Frage

geführt, ob auch Zugangsvermittler, also insbesondere Internet Access-Provider, für die Inhalte, die im Internet bereitgestellt werden und die aus Deutschland abgerufen werden können, verantwortlich sind. Das erste “CompuServe-Urteil” des Amtsgerichts München (AG München, Urteil v. 28.5.1998, NStV 1998, S. 518) hatte die Verantwortlichkeit des Zugangsvermittlers bejaht. Die Entscheidung ist jedoch mit Urteil des Landgerichts München (LG München I, Urteil v. 17.11.1999, CR 2000. S. 17) zurückgenommen worden. Dabei wurde zu Recht darauf verwiesen, dass nach dem Teledienstegesetz Zugangsvermittler zum Internet nur sehr eingeschränkt für fremde Inhalte verantwortlich zu machen sind. Insbesondere ist es ihnen nicht zuzumuten, die im Internet verfügbaren Inhalte lückenlos zu überwachen.

Fraglich ist hingegen, wie mit jenen unerlaubten Inhalten zu verfahren ist, von denen Zugangsvermittler Kenntnis erhalten haben. Prinzipiell während sie technisch dazu in der Lage, durch Installation von Filtern den Zugriff von Nutzern auf diese Inhalte zu unterbinden. Das Bundeskriminalamt hat verschiedentlich den Versuch unternommen, ein derartiges Verhalten von Internet Providern zu verlangen, teils durch Strafandrohung, teils durch Überzeugungsarbeit.

Gegen die generelle Installation von derartigen Filtern spricht, dass es keine bekannten Methoden gibt, mit denen sich unzulässige Inhalte vollständig und sicher blockieren ließen. Zwar könnten die Adressen bestimmter Internet-Seiten (Uniform Ressource Locator – URL) oder Rechneradressen (Domain-Namen oder IP-Nummern) gesperrt werden. Während die Sperrung einzelner Seiten durch die Urheber der unerlaubten Inhalte leicht umgangen werden kann, indem die Ressourcen umbenannt werden, würde die Sperrung auf der Basis von Rechneradressen oder Domainnamen zur Folge haben, dass auch die auf den gesperrten Rechnern bereit gehaltenen – nach deutschem Recht aber zulässigen – Inhalte für r die Nutzer nicht mehr zugänglich wären. Dies würde im allgemeinen eine unverhältnismäßige Beschränkung der Informationsfreiheit (Art. 5 Abs. 1 Grundgesetz) darstellen.

Im Hinblick auf diese Schwierigkeiten sollten sich die Maßnahmen zur Blockierung des Zugangs auf die auch quantitativ verhältnismäßig geringe Anzahl von kinderpornografischen Darstellungen konzentrieren, die weltweit unzulässig sind und insofern auch durch internationale Zusammenarbeit der Strafverfolgungsbehörden unterbunden werden könnten. Dagegen wäre der Versuch zur Unterbindung des Zugriffs auf einfache Pornografie und extremistische Propaganda, die in vielen Ländern strafrechtlich nicht sanktioniert wird, nicht erfolgversprechend.

Im Bereich der **Pornografie** ist strafrechtlich zu unterscheiden zwischen der Verbreitung "einfacher pornografischer Schriften" (§ 184 Absätze 1 und 2 StGB) und so genannter "harter Pornografie" (§ 184 Absätze 3 bis 5 StGB). Während der Gesetzgeber bei der "einfachen Pornografie" vor allem den Zugang von Jugendlichen zu bestimmten Inhalten verhindern will, geht es bei der "harten" Pornografie darum, generell die Darstellung von Gewalttätigkeiten, des sexuellen Missbrauchs von Kindern oder sexueller Handlungen von Menschen mit Tieren zu unterbinden. Im Hinblick auf derartige Darstellungen ist jede Form der "Verbreitung" strafbar.

Als besonders schwerwiegende und menschenverachtende Form der Pornografie wird die Darstellung sexueller Handlungen von bzw. mit Kindern angesehen. Dieser Tatsache hat der Gesetzgeber dadurch Rechnung getragen, dass er gem. § 184 Abs. 5 Satz 2 StGB bereits den "Besitz" von Kinderpornografie unter Strafe stellt.

Das deutsche Strafrecht enthält eine ganze Reihe von Verbotstatbeständen, die durch **extremistische Propaganda** erfüllt werden können. Hierzu gehören die Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB), die Verwendung von Kennzeichen verfassungswidriger Organisationen (§ 86a StGB), die Volksverhetzung (§ 130 StGB) und die Gewaltdarstellung (§ 131 StGB).

Strafbar ist auch der öffentliche Aufruf zu Straftaten (§ 111 StGB). Entsprechendes gilt gem. § 116 Ordnungswidrigkeitengesetz (OwiG) für den Aufruf zu Handlungen, die mit einer Geldbuße bedroht werden. Zudem ist die Verbreitung von Schriften untersagt, die geeignet sind als Anleitung zu bestimmten rechtswidrigen Taten zu dienen und nach ihrem Gehalt dazu bestimmt sind, die Bereitschaft anderer zur Begehung einer solchen Tat zu fördern (§ 130a StGB).

Im Hinblick auf diese Vorschriften gehen rechtsextremistische Organisationen zunehmend dazu über, die entsprechenden Internetangebote auf ausländischen Servern ins Internet einzuspeisen. Dies ändert jedoch nichts an der Strafbarkeit der entsprechenden Aktivitäten nach deutschem Recht (s.o.).

Hinzuweisen ist schließlich auf Verstöße gegen das **Urheberrecht**, wenn geschützte Werke (insb. Software, Musik, Filme) unberechtigt über das Internet bereitgestellt werden.

1.2 Hacking

Durch das Internet ergeben sich neue Möglichkeiten zum Hacking, d. h. zum unbefugten Eindringen in Computersysteme und zum Missbrauch der gespeicherten Daten.

Das Internet weist strukturelle Sicherheitsmängel (unverschlüsselte Kommunikation, keine gesicherte Authentifizierung) auf, die Hacking sehr leicht machen. So können Informationen nicht nur bei Sender und Empfänger, sondern auch auf dem gesamten Übertragungsweg (insb. in Netzknoten) abgehört und unbemerkt manipuliert werden, sofern keine zusätzlichen Sicherheitsmaßnahmen getroffen wurden. Von besonderer Tragweite ist es, wenn Daten ausspioniert werden, die den Zugang zu geschützten Computersystemen ermöglichen, etwa Passwörter und Nutzerkennungen. Diese Daten können von den Tätern dazu verwendet werden, in diese Systeme unberechtigt einzudringen und weiteren Schaden anzurichten. Zum anderen erleichtern Dienste-anbieter und Systembetreiber das Hacking, die diesen Schwachstellen und den daraus resultierenden Risiken nicht Rechnung tragen.

Bereits vor einigen Jahren wurden verschiedene Computerdelikte unter Strafe gestellt. Strafbar ist demnach das Ausspähen von Daten (Datenspionage - § 202a StGB), rechts-widrige Verfälschung und Löschung von Daten (Datenveränderung - § 303a StGB) und destruktive Eingriffe in fremde Datenverarbeitungssysteme, (Computersabotage - § 303b StGB) und Computerbetrug (§ 263a StGB).

Bei der Computerspionage und -Sabotage handelt es sich häufig um Delikte, bei denen die Privatsphäre der Betroffenen z. T. erheblich beeinträchtigt wird, insbesondere, wenn es sich um Daten handelt, die besonders schutzwürdig sind, etwa um medizinische Angaben. Ferner entstehen teilweise erhebliche wirtschaftliche Nachteile, etwa wenn Kreditkartennummern, Bankverbindungsdaten usw. ausspioniert und missbraucht werden.

1.3 Andere Missbräuche des Internet

Wie bereits weiter oben erwähnt, können Computer und Netze zu einer Vielzahl unterschiedlicher Straftaten missbraucht werden. So können kriminelle Taten verabredet und ihre Ausführung durch Internet-Dienste organisiert werden. Besonders schwerwiegend sind dabei Delikte, die dem Bereich der "organisierten Kriminalität" zuzurechnen sind, etwa der internationale Waffen- und Rauschgifthandel.

Zu den typischen Internet-Straftaten gehören auch Verstöße gegen das Datenschutzrecht. Das Datenschutzrecht schützt das Recht auf informationelle Selbstbestimmung (s. 2.2). Typische Datenschutzverstöße im Internet sind zum einen die unzulässige Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Internet-Nutzerinnen und Nutzern. Zum anderen handelt es sich um unzulässige Veröffentlichungen mit personenbezogenen Inhalten.

2 Schützenswerte Freiheitsrechte im Netz

Die Auseinandersetzung mit der Internet-Kriminalität darf nicht den Blick davor verstellen, dass das Netz eine Vielzahl von sinnvollen Nutzungs- und Entfaltungsmöglichkeiten in sich birgt. Die durch die Verfassung garantierten Grundrechte müssen deshalb auch im virtuellen Raum gewährleistet werden.

2.1 Informations- und Meinungsfreiheit

Das Internet ist sowohl ein Medium zur Äußerung von Meinungen als auch ein wirksames Instrument zur Erlangung von Informationen und trägt insofern in zunehmenden Maße zur öffentlichen Meinungsbildung bei, die durch das Grundrecht nach Art. 5 Abs. 1 GG gewährleistet wird. Art. 5 schützt sowohl den Anbieter als auch die Nutzer von Informationen (hierzu gehören sowohl Meinungen als auch Werturteile und Nachrichten aller Art).

Die Maßnahmen zur Unterbindung bestimmter Inhalte im Netz bzw. des Zugriffs auf sie greifen in dieses Grundrecht ein. Sie müssen deshalb sorgfältig abgewogen werden. Dabei ist zu berücksichtigen, dass die Sperrung des Zugriffs auf bestimmte strafbare Inhalte möglicherweise dazu führt, dass auch auf legale Informationen nicht mehr zugegriffen werden kann.

Datenschutzrechtliche Vorgaben, insbesondere zur Absicherung der Vertraulichkeit der Kommunikation und die restriktive Handhabung der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten über die Inanspruchnahme des Internet (Nutzungsdaten) sichern den freien Meinungsbildungsprozess ab, der durch Art. 5 Abs. 1 GG geschützt wird. Nur wenn die Informationsgewinnung und Meinungsbildung auch im Internet weitestgehend frei von Beobachtung und Kontrolle geschieht, wird der Einzelne die Möglichkeiten der neuen Dienste auch in Anspruch nehmen.

2.2 Recht auf informationelle Selbstbestimmung/Fernmeldegeheimnis

Das "Recht auf informationelle Selbstbestimmung" ist ein Grundrecht, obwohl es nicht explizit im Grundgesetz erwähnt wird. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65,1,1 = NJW 1984, 419) den Datenschutz zum ersten Mal im Sinne eines Grundrechts verwendet:

> "Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig."

Das allgemeine Persönlichkeitsrecht bildet die verfassungsrechtliche Grundlage des Rechts auf informationelle Selbstbestimmung. Nach dem Urteil des Bundesverfassungsgerichts

> "wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 i. V. m. Art. 1 Absatz 1 Grundgesetz umfasst."

Das Recht auf informationelle Selbstbestimmung umfasst sämtliche personenbezogenen Daten unabhängig von ihrer Sensibilität, weil es angesichts der Möglichkeiten der modernen Datenverarbeitung "kein belangloses Datum mehr" gibt. Entscheidend sind allein die Nutzbarkeit und Verwendungsmöglichkeit der Daten. Dieser Befund des Volkszählungsurteils ist angesichts der Verknüpfungs- und Auswertungsmöglichkeiten, die sich gerade durch das Internet ergeben, heute aktueller denn je.

Eng verwandt mit dem Grundrecht auf informationelle Selbstbestimmung ist das Fernmeldegeheimnis (Art. 10 GG). Dieses schützt nicht allein die Inhalte, sondern auch die "näheren Umstände" der Kommunikation. Dem entsprechend steht auch die Tatsache, zwischen welchen Internetteilnehmern E-Mails ausgetauscht wurden oder auf welche Inhalte bzw. URL zugegriffen wurde, unter dem Schutz des Grundrechts auf Fernmeldegeheimnis.

Maßnahmen zur Bekämpfung der Computer- und Netzkriminalität, bei denen Kommunikationsinhalte überwacht oder das Nutzungsverhalten registriert und ausgewertet wird, greifen in das Recht auf informationelle Selbstbestimmung und in das Fernmeldegeheimnis ein. Sie bedürfen - da es sich um Beschränkungen von Grundrechten handelt - einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entsprechen (Gesetzesvorbehalt).

3 Derzeitige Rechtslage

Im folgenden wird dargestellt, welche Befugnisse Sicherheitsbehörden nach derzeitigem Recht zur Bekämpfung von Internet-Kriminalität haben.

3.1 Auswertung veröffentlichter Informationen

Grundsätzlich haben die Sicherheitsbehörden zwar das Recht, ebenso wie alle anderen Nutzer im Netz zu surfen, ohne dass diesen Maßnahmen Eingriffsqualität zukommt. Fragwürdig ist jedoch, ob sie dabei gezielt nach Daten bestimmter Personen recherchieren dürfen. Dabei ist zu beachten, dass viele Informationen mit Personenbezug unzulässigerweise durch Dritte im Internet veröffentlicht werden, etwa in der Absicht, den Betroffenen zu schädigen (etwa gefälschte Kontaktanzeigen oder Selbstbezichtigungen). Die Verwendung dieser unzulässig veröffentlichten personenbezogenen Daten durch Sicherheitsbehörden ohne besondere gesetzliche Befugnis ist nicht zulässig. Zu beachten ist ferner, dass Veröffentlichungen im Internet eine andere Qualität besitzen als Veröffentlichungen in herkömmlicher Form. Alle Angaben, die irgendwann im Internet veröffentlicht wurden, sind auf Dauer recherchierbar. Das BVerfG hat klargestellt, dass

insbesondere die dauerhafte und wiederholte Verwendung von nicht mehr aktuellen Informationen in besonderem Maße das Persönlichkeitsrecht der Betroffenen beeinträchtigt. Die Verwendung von personenbezogenen Daten, die bereits vor langer Zeit im Internet veröffentlicht wurden, durch Sicherheitsbehörden ist deshalb besonders fragwürdig.

Zudem können bereits durch die Verknüpfung und Auswertung der vielfältigen im Internet verfügbaren Informationen sehr aussagekräftige Persönlichkeitsbilder entstehen, die wirtschaftliche Umstände, sexuelle Orientierungen, persönliche Interessen und politische Meinungen des Betroffenen umfassen.

Zusammenfassend lässt sich deshalb feststellen, dass Sicherheitsbehörden zwar im Internet surfen, jedoch nicht beliebig und ohne Zweckbegrenzung veröffentlichte personenbezogene Daten erheben, verarbeiten oder nutzen dürfen. Jede gezielte personenbezogene Recherche im Internet bedarf der gesetzlichen Erlaubnis. Keine Eingriffsqualität haben jedoch solche Recherchen, mit denen Lagebilder oder sonstige allgemeine Einschätzungen ohne direkten Personenbezug gewonnen werden sollen, und zwar auch dann, wenn bei dieser Gelegenheit, quasi als Beiwerk, der Behörde auch personenbezogene Daten zur Kenntnis gelangen. Die Nutzung dieser Zufallsfunde bedarf wiederum einer gesetzlichen Ermächtigung.

3.2 Strafverfolgung

Strafrechtliche Ermittlungen können von der Polizei oder Staatsanwaltschaft und von anderen zur Strafverfolgung befugten Behörden innerhalb ihres begrenzten Wirkungsbereichs (z. B. Finanzamt, Zollfahndungsstelle) durchgeführt werden. Die Ermittlungen werden von Amts wegen oder auf Strafanzeige angestellt, sobald die Strafermittlungsbehörden Kenntnis von einem Verdacht einer Straftat erhalten haben (Anfangsverdacht - § 152 StPO).

Im Hinblick auf die Verarbeitung personenbezogener Daten bei Ermittlungshandlungen im Internet ist zu unterscheiden zwischen Kundendateien, Bestands-, Verbindungs-, Nutzungs- und Inhaltsdaten.

§ 90 Abs.1 TKG verpflichtet Telekommunikationsanbieter zur Führung von Kundendateien. Gem. § 90 Abs. 2 TKG müssen die Diensteanbieter die **Kundendateien** zum Abruf durch die Regulierungsbehörde für Telekommunikation und Post in einem automatisierten Verfahren bereit stellen. Die Regulierungsbehörde leitet diese Daten an Gerichte, Staatsanwaltschaften und andere Justizbehörden sowie sonstige Strafverfolgungsbehörden, an die Polizeien des Bundes und der Länder, an Gefahrenabwehrbehörden, Zollfahndungsämter sowie das Zollkriminalamt und schließlich an die Verfassungsschutzbehörde des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst weiter. Der auf diese Weise entstehende komplexe Informationsverbund zwischen Telekommunikations- und Sicherheitsbehörden stößt auf erhebliche datenschutzrechtliche Bedenken, insbes. weil die Betroffenen weder den Verdacht auf eine Straftat, noch Gefahren für die öffentliche Sicherheit oder gar für nachrichtendienstliche Schutzgüter hervorgerufen haben.

Anbieter von Internet-Diensten unterliegen im Regelfall nicht den Verpflichtungen aus § 90 TKG, soweit sie keine Telekommunikationsdienste anbieten und wenn kein festes Vertragsverhältnis zwischen ihnen und den Nutzern besteht und sie somit auch gar nicht in der Lage wären, die entsprechenden Daten bereit zu stellen.

§ 89 Abs. 6 TKG verpflichtet die Anbieter von Telekommunikationsdiensten dazu, ihre **Bestandsdaten**[1] im Einzelfall auf Ersuchen an die für die Verfolgung von Straftaten oder Ordnungswidrigkeiten und zur Abwehr von Gefahren zuständigen Stellen (also Staatsanwaltschaften, Bußgeldbehörden und Polizeien), die Verfassungsschutzbehörden, den Bundesnachrichtendienst, den militärischen Abschirmdienst sowie das Zollkriminalamt zu übermitteln. Die Übermittlungen sind zulässig, soweit sie zur Aufgabenerfüllung der genannten Stellen erforderlich sind. Die Tatsache einer Auskunft an die genannten Stellen darf dem Kunden oder Dritten nicht mitgeteilt werden. § 89 Abs. 6 TKG ist im Regelfall ebenfalls nicht auf Diensteanbieter im Internet anwendbar. Dabei ist allerdings zu beachten, dass das Angebot von E-Mail-Diensten der Telekommunikation zuzurechnen ist und entsprechende Auskunftsverpflichtungen auslöst.

Die Bestandsdaten gehören nicht zu den gem. § 97 StPO von Beschlagnahme ausgeschlossenen Gegenständen. Allerdings könnte in den Fällen ein **Beschlagnahmehindernis** vorliegen, in denen sich die Beschlagnahme auf Dienste bezieht, die von Personen mit einem Zeugnisverweigerungsrecht gem. § 53 StPO angeboten werden, also von Geistlichen in ihrer Eigenschaft als Seelsorger, Rechtsanwälten, Ärzten, Zahnärzten, Psychotherapeuten, Apothekern, Hebammen, Mitarbeitern anerkannter Beratungsstellen, Mitgliedern von Parlamenten; ferner von Journalisten bzw. berufsmäßigen Mitarbeitern von Verlagen und Rundfunkanstalten, soweit sich die Beschlagnahme auf Daten von Personen beziehen soll, die zu redaktionellen Publikationen beigetragen haben und deren Identität durch die Beschlagnahme offenbart würde.

Verbindungsdaten[2] unterliegen als nähere Umstände der Telekommunikation dem Fernmeldegeheimnis. Nach § 12 Fernmeldeanlagengesetz (FAG) kann aufgrund richterlicher Anordnungen in Strafermittlungsverfahren Auskunft über die Telekommunikation verlangt werden, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und dass die Auskunft für die Untersuchung Bedeutung hat. Der Auskunftsanspruch bezieht sich ausschließlich auf Kommunikationsvorgänge in der Vergangenheit.

Im Unterschied zu den Vorschriften zur Überwachung der Telekommunikationsinhalte gem. § 100a StPO (s.u.) lässt § 12 FAG den Zugriff auf Informationen über die Telekommunikation des Beschuldigten ohne Beschränkung auf einen Straftatenkatalog zu, wodurch u.E. das Fernmeldegeheimnis in unverhältnismäßiger Weise beschränkt wird.

Auch die **Nutzungsdaten** im Internet unterliegen dem Fernmeldegeheimnis, da die Tele- und Mediendienste auf der Basis von Telekommunikationsdiensten abgewickelt werden. Die Aussagekraft der Nutzungsdaten ist dabei teilweise größer als die der Verbindungsdaten, denn sie offenbaren nicht nur "nähere Umstände der Kommunikation", sondern auch Inhalte. Dies ist insbesondere dann der Fall, wenn Suchanfragen und andere Inhalte von Eingaben in Web-Formulare als Bestandteile einer URL übertragen und gespeichert werden (so führt eine Anfrage nach den Suchbegriffen "Datenschutz und Internet" zu der

---

[1] Bei den Bestandsdaten handelt es sich um Angaben, die für die Vertragsgestaltung und -abwicklung bei Telekommunikations-, Tele- und Mediendiensten erforderlich sind, also z.B. die Namen der Anschlussinhaber.

[2] Verbindungsdaten bezeichnen alle Angaben, die bei dem Aufbau und bei der Abwicklung von Telekommunikationsverbindungen anfallen, also z.B. die angerufene Telefonnummer und den Zeitpunkt der Verbindung.

URL "http://www.altavista.com/sites/search/web?q=Datenschutz+und+Internet&kl=XX&search=Search"). Selbst eine URL, die derartige Erweiterungen nicht enthält, kann erhebliche Aussagekraft hinsichtlich des Inhalts entfalten, denn sie identifiziert nicht nur den Diensteanbieter, auf dessen Angebot ein Nutzer zugegriffen hat, sondern sie spezifiziert darüber hinaus die Web-Seite, der das Interesse des Nutzers galt, also z. B. einen bestimmten Artikel in einer elektronischen Zeitschrift. Diensteanbieter dürfen Nutzungsdaten nur nach Maßgabe von Bestimmungen, die das Fernmeldegeheimnis einschränken, an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung weitergeben. Da sich die Befugnis gem. § 12 FAG ausschließlich auf Verbindungsdaten bezieht, kann eine Auskunftspflicht über Nutzungsdaten an Strafverfolgungsbehörden allenfalls bezüglich solcher Nutzungsdaten erfolgen, die lediglich die Tatsache und den Zeitpunkt einer Nutzung betreffen, nicht jedoch die Inhalte der Kommunikation offenbaren würden. Auskünfte über Nutzungsdaten mit Inhaltsbezug dürfen nur dann auf diese Vorschrift gestützt werden, wenn eine Straftat vorliegt, die eine Überwachung des Inhalts der Telekommunikation erlauben würde. Der Straftatenkatalog aus § 100a StPO muss für die Beurteilung herangezogen werden, ob diese Voraussetzungen vorliegen.

Die Überwachung von **Kommunikationsinhalten** stellt den weitest gehenden Eingriff in das Fernmeldegeheimnis dar. Nach § 100a StPO darf die Überwachung und Aufzeichnung der Telekommunikation angeordnet werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine schwere Katalogstraftat begangen hat und wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Der Straftatenkatalog ist – trotz Kritik der Datenschutzbeauftragten – vom Gesetzgeber wiederholt ausgeweitet worden. Er umfasst neben Kapitalverbrechen inzwischen auch Straftaten gegen die öffentliche Ordnung (§§ 129-130 StGB), Bandendiebstahl und bestimmte Verstöße gegen das Asylverfahrens- und das Ausländergesetz. § 100b StPO regelt das Verfahren der Überwachung. Danach darf die Überwachung und Aufzeichnung der Telekommunikation nur durch den Richter angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch von der Staatsanwaltschaft getroffen werden. Die Anordnung muss schriftlich ergehen. Sie muss Namen und Anschrift des Betroffenen, gegen den sie sich richtet, und die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten. In ihr sind Art, Umfang und Dauer der Maßnahmen zu bestimmen. Die Anordnung ist auf höchstens drei Monate zu befristen. Ferner enthält § 39 Außenwirtschaftsgesetz (AWG) eine entsprechende Befugnis für das Zollkriminalinstitut zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz.

3.3 Heimliches Eindringen in Mailboxen und andere geschützte Bereiche des Internet

Eine spezielle Form der Überwachung von Kommunikationsinhalten stellt das "**staatliche Hacking**" dar, bei dem eine Strafverfolgungsbehörde sich heimlich Zugang zu Informationen verschafft, die auf geschützten Computersystemen (etwa Mailboxen) abgelegt sind. Nach der Rechtsprechung des BGH stellt ein derartiger Zugriff ebenfalls eine Telekommunikationsüberwachung dar, die eine Anordnung gem. §§100a,b StPO bedarf. Das Eindringen in Mail-Systeme kann nicht auf die strafprozessualen Befugnisse der Beschlagnahme von Gegenständen oder zur Durchsuchung von Räumen (§§ 94ff, 102ff StPO) gestützt werden, vor allem weil der Zugriff anders als bei den vorgenannten Maßnahmen im Regelfall geheim ist und auch die zukünftige Kommunikation umfasst.

Schließlich haben Strafverfolgungsbehörden unter bestimmten Umständen die Befugnis, **verdeckte Ermittler** im Internet einzusetzen. Bei diesen handelt es sich um Vollzugsbeamte, die auf Dauer unter veränderter Identität ("Legende") operieren. Der Einsatz verdeckter Ermittler nach Polizeirecht ist nur zulässig, soweit dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist oder wenn Tatsachen die Annahme rechtfertigen, dass Straftaten von erheblicher Bedeutung in der Form organisierter Kriminalität begangen werden sollen und der Einsatz zur vorbeugende Bekämpfung dieser Straftaten erforderlich ist. Zur Strafverfolgung dürfen verdeckte Ermittler eingesetzt werden, wenn die Aufklärung von Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Bezogen auf das Internet kommt der Einsatz verdeckter Ermittler insbesondere dann in Frage, wenn die Strafermittlungsbehörden unter falscher Identität Zugriff auf geschützte Daten nehmen wollen, z.B. unter Verwendung von Passwörtern, die unter der Legende beschafft wurden, z.B. um auf Mailboxen einer terroristischen Szene zuzugreifen, die nur bestimmten bevorrechtigten Gruppenmitgliedern zugänglich sind. Im Rahmen der Strafverfolgung können verdeckte Ermittler gem. § 110a f. StPO eingesetzt werden, wenn eine Katalogstraftat gem. § 100a StPO vorliegt. Dementsprechend kommt etwa zur Verfolgung von Urheberrechtsverletzungen der Einsatz verdeckter Ermittler nicht in Betracht.

3.4 Öffentlichkeitsfahndung im Internet

Das Internet wird von Strafverfolgungsbehörden als Medium der Öffentlichkeitsfahndung eingesetzt. Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets in das Recht des Betroffenen auf informationelle Selbstbestimmung eingegriffen. Besonders schwerwiegend ist der Eingriff in den Fällen, in denen zunächst nach einem Verdächtigen gefahndet wird, bei dem sich später dessen Unschuld herausstellt. Der mit der Veröffentlichung eines Fahndungsaufrufs verbundene Schaden ist in diesen Fällen praktisch nicht mehr rückgängig zu machen.

Bei der Anwendung der neuen Vorschriften zur Öffentlichkeitsfahndung (§§ 131, 131a, 131b StPO) muss der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets auch bei der Auswahl des Mediums berücksichtigt werden. Da jede Internet-Fahndung weltweit verfügbar ist und somit das informationelle Selbstbestimmungsrecht der Betroffenen in besonderer Weise beeinträchtigt, kommen hierfür nur solche Straftaten in Betracht, bei denen eine Veröffentlichung in regionalen Medien nicht ausreicht. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

Schließlich ist darauf hinzuweisen, dass wegen der allgemeinen Sicherheitsschwächen des Internet Möglichkeiten zur Fälschung und zur Veränderung von Inhalten von öffentlichen Fahndungsausschreibungen möglich sind, womit weitere Risiken für den Datenschutz entstehen.

3.5 Polizeirecht

Zur Aufdeckung von Straftaten im Internet wurde 1999 beim **Bundeskriminalamt** eine bundesweite Zentralstelle für anlassunabhängige Recherchen im Internet eingesetzt. Ihre Aufgabe besteht insbesondere darin, die Verbreitung von Kinderpornografie, Anleitungen zu extremistischen Handlungen, Kreditkartenbetrug und Hehlerei in Datennetzen aufzuspüren. Vom 1. Januar bis zum 10. Oktober 2000 hat die Internet-Zentralstelle des

BKA in 1015 Fällen aufgrund eines Anfangsverdachts Anzeigen erstellt und an die zuständigen in- und ausländischen Dienststellen weitergeleitet. Dabei handelte es sich um 881 Fälle von Kinderpornografie, 6 Staatsschutzdelikte, 14 Delikte nach dem Betäubungsmittelgesetz, 31 Delikte nach dem Arzneimittelgesetz, 10 Urheberschutzdelikte, 43 Fälle von Tierpornografie, 12 Fälle des sexuellen Missbrauchs von Kindern und 18 sonstige Delikte.[3]

Das Bundesinnenministerium hat dem Bundesamt für die Sicherheit in der Informationstechnik (BSI) den Auftrag erteilt, eine spezielle Meta-Suchmaschine zu entwickeln, um schneller kriminelle Inhalte und Anbieter herauszufinden. Mit dieser Suchmaschine soll zum einen auf bestehende Suchdienste kommerzieller Anbieter (z. B. AltaVista, Yahoo oder Lycos) zugegriffen werden, die ohnehin das Internet systematisch absuchen. Zum anderen soll die Suchmaschine bestimmte Teile des Internets, in denen regelmäßig kriminelle Sachverhalte vermutet werden, automatisch durchsuchen. Dieses Internet-Ermittlungstool (**INTERMiT**) wurde inzwischen auch der Öffentlichkeit vorgestellt.

Mit der Software **PERKEO** (Programm zur Erkennung relevanter kinderpornografischer eindeutiger Objekte) verfügen die deutschen Fahnder über ein Werkzeug, mit dem Bilddateien, die auf Servern gehalten werden, durch Vergleich mit bekanntem Referenzmaterial ausgewertet werden können.

Unstrittig ist, dass der heimliche oder zwangsweise Zugriff von Polizei- und sonstigen Sicherheitsbehörden auf Daten im Internet, die besonders gegen Zugriffe Dritter geschützt sind (z. B. durch Passwörter oder durch Verschlüsselung), nur zulässig ist, wenn eine spezielle Ermächtigungsgrundlage hierfür eine Befugnis enthält (s. hierzu 3.2). Gleiches gilt auch für den Fall, dass unter Verwendung fremder Passwörter auf eine Mailbox zugegriffen wird (s. hierzu 3.3).

Die gezielte Recherche im Internet ohne Vorliegen eines Anfangsverdachts kann zur Gefahrenabwehr und zur Erforschung von Straftaten erfolgen. Für die Gefahrenabwehr müssen die Normen des Polizeirechts der Länder und das Gesetz über das Bundeskriminalamt (BKAG) herangezogen werden. Dagegen fällt die Erforschung von Straftaten in den Bereich repressiven Handelns, das im wesentlichen einer Ermächtigung im Strafprozessrecht bedarf.

Die Datenverarbeitungsvorschriften im Polizeirecht beziehen sich auf die Vorbereitung für die Hilfeleistung und das Handeln in Gefahrenfällen (Gefahrenabwehr im engeren Sinne) und zur Verhütung von Straftaten sowie zur Vorsorge für die Verfolgung zukünftiger Straftaten (vorbeugende Bekämpfung von Straftaten). Das Polizeirecht gestattet es der Polizei generell, personenbezogene Daten aus allgemein zugänglichen Quellen zu erheben, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist. Soweit die Polizei im Rahmen dieser Aufgaben offen im Internet “Streife geht”, also auch öffentlich zugängliche Informationen auswertet, bestehen hiergegen deshalb keine datenschutzrechtlichen Bedenken.

Problematischer ist das verdeckte Ermitteln in (etwa durch Passwörter) geschützten Bereichen des Internet. Es ist klärungsbedürftig, ob derartige Ermittlungshandlungen auf die Bestimmungen des Polizei- und des Strafprozessrechts zum Einsatz verdeckter Ermittler gestützt werden können. Fraglich ist, ob auch der Abgleich von Daten mit Suchmaschinen im Internet eine Rasterfahndung darstellt, die nur unter sehr restriktiven

[3] BfD 18. TB, 105.

Vorgaben zulässig ist. Solange sich die Suche auf öffentlich zugängliche Angaben beschränkt, ist dies zu verneinen. Anders verhält es sich, wenn für den polizeilichen Abgleich neben den im Internet öffentlich verfügbaren Daten auch Datenbestände herangezogen werden, die der Polizei auf Grund besonderer Befugnisse zur Verfügung stehen (etwa das INPOL-System).

3.6 Nachrichtendienste

Das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz - G 10) erlaubt Überwachungsmaßnahmen durch Nachrichtendienste. Danach dürfen die Verfassungsschutzbehörden, der militärische Abschirmdienst und der Bundesnachrichtendienst zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes die Telekommunikation überwachen und aufzeichnen. Der Eingriff ist nur zulässig, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine im G10-Gesetz aufgeführte schwerwiegende politische Straftat plant, begeht oder begangen hat und wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Daneben erlaubt das G10-Gesetz die verdachtsunabhängige Telekommunikationsüberwachung durch den BND, um die Gefahr eines bewaffneten Angriffs, der Begehung internationaler terroristischer Anschläge und weitere im Gesetz genannte schwere Straftaten rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. Die vom BND hierbei verwendeten Suchbegriffe dürfen keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Fernmeldeanschlüsse führen.

Das G10-Gesetz ist im Frühjahr 2001 - als Folge eines Urteils des Bundesverfassungsgerichts zur Zulässigkeit der strategischen Kontrolle (BVerfGE 100, 313) - novelliert worden. Dabei wurde bei allen unumgänglichen Kompromissen eine Verbesserung der parlamentarischen Kontrolle der Überwachungsmaßnahmen erreicht.

4 Zusätzliche Strafnormen und Befugnissen für Sicherheitsbehörden?

Angesichts verschiedener spektakulärer Vorfälle, die sich in den letzten Jahren ereignet haben (insb. Virenattacken, Austausch von Kinderpornografie), wird wiederholt die Forderung nach einer Ausweitung der Befugnisse der Sicherheitsbehörden und nach zusätzlichen Strafnormen laut. Um es vorweg zu nehmen: Aus unserer Sicht reichen die Strafvorschriften und die Befugnisse von Strafverfolgungsbehörden und von Nachrichtendiensten aus. Wichtig sind hingegen der Abbau des vielfach feststellbaren Vollzugsdefizits, mehr Verantwortungsbewusstsein der Diensteanbieter und der Ausbau des Selbstschutzes der Internet-Nutzerinnen und –Nutzer.

4.1 Forderungen aus Sicherheitsbehörden

Die Innenminister des Bundes und der Länder haben auf ihrer Konferenz am 24.11.2000 gefordert, für Zwecke der Strafverfolgung "den Providern und Betreibern von Servern eine Protokollierungspflicht hinsichtlich der IP-Adresse und des Nutzungszeitraums sowie eine angemessene Aufbewahrungszeit der Daten" vorzuschreiben und die CDU fordert in ihren Sicherheitsleitlinien die Festlegung genereller Mindestfristen für die Speicherung von

Daten (**Vorratsdatenspeicherung**). Derartige Vorgaben wären verfassungswidrig, da das Bundesverfassungsgericht wiederholt festgestellt hat, dass die Speicherung personenbezogener Daten nicht zu einer Rundumbeobachtung der Bürger führen darf. Das wäre aber im Bereich der Internetnutzung der Fall. Ein Gebot zur Vorratsdatenspeicherung würde den durch das Fernmeldegeheimnis und die Datenschutzbestimmungen des über Tele- und Mediendiensterechts gewährleisteten Schutz in unvertretbarer Weise abbauen. Es widerspräche auch dem neuen Bundesdatenschutzgesetz, das die Entwicklung und den Einsatz von technischen Verfahren fordert, die mit einem Minimum an personenbezogener Datenverarbeitung betrieben werden können (Datenvermeidung).

Die Forderungen nach Vorratsdatenhaltung im Internet sind vergleichbar mit einer Verpflichtung der Post, sämtliche Absender- und Empfängerangaben im Briefverkehr für Zwecke einer möglichen späteren Strafverfolgung zu speichern und für den Zugriff der Sicherheitsbehörden bereitzuhalten. Deshalb ist - wie die meisten Datenschutzbeauftragten in einer gemeinsamen Erklärung festgestellt haben - der Versuch, das Internet für Zwecke der Strafverfolgung in ein Fahndungsnetz zu verwandeln, ungeeignet und unangemessen. Zudem hatte sogar die alte (CDU/CSU-FDP-) Bundesregierung vor einigen Jahren entsprechende Forderungen der Sicherheitsbehörden nach Mindestspeicherfristen mit Verweis auf die Grenzen, die durch die Verfassung gezogen werden, zurückgewiesen. Die bestehenden Befugnisse der Strafverfolgungsbehörden gewährleisten unseres Erachtens schon jetzt eine effektive Strafverfolgung im Internet, denn Providern können ohne weiteres IP-Nummern ab dem Zeitpunkt des Vorliegens eines entsprechenden richterlichen Beschlusses, oder bei Gefahr in Verzug einer staatsanwaltlichen Anordnung, vorhalten - eine obligatorische Vorratsspeicherung ist deshalb auch nicht erforderlich.

Das Vorhaben der Innenministerkonferenz würde zu einem **unverhältnismäßigen Eingriff** in das Recht auf informationelle Selbstbestimmung von Millionen rechtstreuer Internetnutzer führen, die keineswegs alle potenzielle Straftäter sind. Das gesamte Vorhaben wäre zudem zur Verfolgung von schweren Straftaten untauglich, weil Straftäter ohne größere technische Schwierigkeiten auf Provider in anderen Ländern ausweichen könnten.

Immer wieder wird auch die Forderung nach einer **Ausweitung von Überwachungsbefugnissen** gestellt. So hat die CDU in ihren sicherheitspolitischen Leitlinien vom Juni 2001 gefordert, die Netzbetreiber gesetzlich dazu zu verpflichten, rund um die Uhr Überwachungsschaltungen vorzunehmen und Verbindungsdaten zur Aufklärung schwerer Straftaten oder Abwehr erheblicher Gefahren zur Verfügung zu stellen. Bereits heute müssen die Unternehmen, die Telekommunikationsdienstleistungen erbringen, Vorkehrungen treffen, um die Überwachung im Einzelfall zu ermöglichen. Die gesetzlichen Regelungen reichen deshalb unseres Erachtens aus.

Besonders problematisch ist die von der CDU erhobene Forderung nach Befugnissen für die Polizei zur **Durchsuchung von Computern und Netzen** ohne Hinzuziehung von Staatsanwälten oder Richtern. Im Hinblick auf die große Bedeutung von Computernetzwerken und die Sensibilität der in jenem gespeicherten Daten wäre eine derartige pauschale Ermächtigung für die Polizei verfassungswidrig. Zudem gibt es - wie oben aufgezeigt - bereits jetzt weit gehende Möglichkeiten der Strafverfolgungsbehörden zur Aufklärung von schweren Straftaten. Hierzu gehören auch Befugnisse zur Durchsuchung und Beschlagnahme von Computersystemen.

4.2 Datenverschlüsselung - Kryptodebatte

In der Vergangenheit ist intensiv über die Frage diskutiert worden, inwieweit die Möglichkeiten zur Verschlüsselung gesetzlich beschränkt oder verboten werden sollen, um eine missbräuchliche Nutzung des Internet zu kriminellen Zwecken zu verhindern. Im Vordergrund steht dabei die Befürchtung, dass die gesetzlichen Befugnisse zur Überwachung des Telekommunikationsverkehrs leer laufen könnten, wenn sich Kriminelle starker Verschlüsselungsverfahren bedienen. Als mögliche Maßnahmen wurden neben einem generellen Verbot der verschlüsselten Kommunikation Vorgaben zur Verwendung "schwacher" Verschlüsselung durch Begrenzung der Schlüssellänge und das Gebot zur Hinterlegung von Schlüsseln bei staatlichen Stellen diskutiert. Diese Maßnahmen würden jedoch dem mit Verschlüsselung angestrebten Schutzzweck – einer sicheren und beweisbaren Kommunikation im Internet - widersprechen und zudem ins Leere stoßen, weil

- sie leicht umgangen werden können, insbesondere dann, wenn die notwendigen Fachkenntnisse und finanziellen Mittel zur Verfügung stehen (z. B. in Kreisen des organisierten Verbrechens),
- sie kaum kontrollierbar sind, weder aus technischer noch aus finanzieller Sicht,
- sie anderen staatlichen und wirtschaftlichen Interessen an der Sicherung von Daten gegen Risiken der Vertraulichkeit, Integrität (Unversehrtheit) und Zurechenbarkeit (Authentizität) bei der Übertragung und Speicherung zuwiderlaufen,
- sich bei den dann eventuell realisierten Stichprobenkontrollen die unbefugte Kenntnisnahme übermittelter oder gespeicherter Daten nicht verhindern lässt.

Aus diesen Gründen haben sich Datenschutzkontrollinstitutionen auch auf internationaler Ebene für verbesserte Möglichkeiten zur Verschlüsselung von Daten ausgesprochen.

Die Debatte um ein Verschlüsselungsverbot wurde in Deutschland vorläufig beendet durch die von der Bundesregierung beschlossenen Eckpunkte der Kryptopolitik vom 2. Juni 1999. Darin erklärt die Bundesregierung, dass sie nicht beabsichtige, die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken. Sie sehe in der Anwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen. Die Bundesregierung werde deshalb die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützten. Dazu zähle insbesondere die Förderung des Sicherheitsbewusstseins bei den Bürgern, der Wirtschaft und der Verwaltung. Die Bundesregierung strebe an, das Vertrauen der Nutzer in die Sicherheit der Verschlüsselung zu stärken. Sie halte aus Gründen der Sicherheit von Staat, Wirtschaft und Gesellschaft die Fähigkeit deutscher Hersteller zur Entwicklung und Herstellung von sicheren und leistungsfähigen Verschlüsselungsprodukten für unverzichtbar. Sie werde Maßnahmen ergreifen, um die internationale Wettbewerbsfähigkeit dieses Sektors zu stärken. Wir begrüßen diese Position der Bundesregierung.

4.3 Internationale Initiativen

Computerstraftaten machen nicht an den Ländergrenzen halt. Sie können grundsätzlich von jedem Ort der Welt aus verübt werden. Allgemein besteht Einigkeit darüber, dass sowohl auf nationaler als auch auf internationaler Ebene wirksame Maßnahmen zur Bekämpfung der Computerkriminalität ergriffen werden müssen. Obwohl bestimmte

Delikte, die über das Internet begangen werden, nach nationalem Recht auch dann strafbar sind, wenn dabei ausschließlich im Ausland belegene Ressourcen verwendet werden, ist nach den Grundsätzen des Strafprozessrechts das Übergreifen der Strafverfolgungstätigkeit eines Staates auf das Gebiet eines anderen grundsätzlich unzulässig.

Vor allem bei den strafrechtlichen Bestimmungen über das Hacking, den Schutz von Geschäftsgeheimnissen und bezogen auf illegale Inhalte weisen die nationalen Rechtsordnungen weltweit nach wie vor große Unterschiede auf. Beträchtliche Differenzen bestehen auch hinsichtlich der Befugnisse der Strafverfolgungsbehörden, bei der gerichtlichen Zuständigkeit in Strafsachen und bei der Verantwortlichkeit von Vermittlern und Anbietern von Online-Inhalten.

Auf internationaler Ebene werden deshalb verstärkt Bemühungen unternommen, um die Sicherheit im Internet zu erhöhen und einheitliche Vorgaben für die Strafverfolgung im Internet zu treffen.

4.3.1 G8-Initiative

Im Dezember 1997 billigten die Justiz- und Innenminister der weltweit bedeutendsten Industrienationen (G8) einen 10-Punkte-Aktionsplan, der im Mai 1998 auf dem Gipfeltreffen der G8 in Birmingham angenommen wurde und zur Zeit umgesetzt wird .[4] Vorgesehen sind vor allem die folgenden Maßnahmen:

- Einrichtung nationaler, auf die Bekämpfung der Computerkriminalität spezialisierter Polizeidienststellen;
- Verbesserung der Zusammenarbeit zwischen den Strafverfolgungsbehörden, der Industrie, den Verbraucherorganisationen und den Datenschutzbehörden;
- Förderung von geeigneten Initiativen der Industrie bzw. von Bürgergruppen, beispielsweise zur Entwicklung von Sicherheitsprodukten.
- Verbesserung der gesetzlichen Möglichkeiten, um die transnationale Rechtsdurchsetzung zu verbessern und die Lokalisierung und Identifizierung von High-Tech-Tätern sicherzustellen. Hierzu gehören auch Maßnahmen, die datenschutzrechtlich problematisch sind, wie z.B. die obligatorische Speicherung von Verbindungsdaten.

Die G8-Länder haben ein jederzeit erreichbares Informationsnetz der Strafverfolgungsbehörden eingerichtet. Dieses Informationsnetz soll nicht auf die G8-Staaten begrenzt bleiben. Hauptaufgabe des Informationsnetzes ist die Beantwortung dringender Ersuchen um Kooperation in Fällen, in denen elektronische Beweismittel eine Rolle spielen. Die nationalen Anlaufstellen sollten auf direktem Wege zusammenarbeiten und so die bestehenden Rechtshilfestrukturen und Kommunikationskanäle sinnvoll ergänzen.

4.3.2 Cyber Crime Convention

Es ist zu erwarten, dass der Europarat noch im Jahr 2001 eine Konvention über die Datennetzkriminalität (Cyber Crime Convention) billigt. Die Tragweite der Konvention kommt darin zum Ausdruck, dass sie sich nicht nur an die Mitglieder des Europarates richtet, sondern auch diejenigen Länder einschließt, die aufgrund ihrer technologischen und wirtschaftlichen Fähigkeiten das Internet prägen, insbesondere die Vereinigten

[4] http://ue.eu.int/ejn/index.htm).

Staaten und Japan. Die Konvention enthält Anforderungen zur Gestaltung des materiellen Strafrechts, insbesondere zur Strafbarkeit des Besitzes von Kinderpornografie und der illegalen Verbreitung kopiergeschützten Materials. Auch die Ausweitung der Strafbarkeit auf bestimmte bislang legale Handlungen ist vorgesehen: So soll bereits der Besitz von "Hacker-Tools", d.h. von Programmen, die sich zum unbefugten Eindringen in Computersysteme eignen, unter Strafe gestellt werden, soweit die Absicht der missbräuchlichen Verwendung besteht. Im Hinblick darauf, dass Programme, die der Überprüfung der Computersicherheit dienen, häufig auch für Angriffe benutzt werden können, ist das vorgesehene Verbot von "Hacker-Tools" untauglich und würde möglicherweise dazu führen, dass wegen der Strafbarkeit des Besitzes notwendige Sicherheitsüberprüfungen von Computern und Netzen unterbleiben.

Ferner werden die Staaten zur Harmonisierung ihres Strafprozessrechts verpflichtet, um die Gewinnung und Sicherung von Beweismitteln zu erleichtern. Die Konvention enthält unter anderem Vorgaben zur vorsorglichen Speicherung und Offenbarung von Bestands-, Verbindungs- und Nutzungsdaten und zur Einrichtung von Schnittstellen zur Überwachung von Kommunikationsinhalten. Dabei ist nicht deutlich, unter welchen Voraussetzungen und für welchen Zeitraum die Daten auf Vorrat gespeichert werden sollen. Diese Vorgaben sind in Hinblick auf die Unbestimmtheit der Anwendungsbereiche und mangelnder datenschutzrechtlicher Garantien datenschutzrechtlich problematisch. Zudem würde die Verpflichtung der Provider zur Bereithaltung von Überwachungsschnittstellen, über die sich die Sicherheitsbehörden rund um die Uhr in Echtzeit in denen Kommunikationsverkehr einschalten können, erhebliche zusätzliche Sicherheitsrisiken mit sich bringen.

Ferner enthält die Konvention Vorgaben zur internationalen Kooperation für Ermittlungen im Zusammenhang mit computerbezogenen Straftaten und zur Sammlung von Beweisen in elektronischer Form. Die meisten Verpflichtungen zur gegenseitigen Unterstützung, die in diesem Kapitel aufgeführt sind, betreffen nicht nur die Computernetzkriminalität im engeren Sinne. Die Verpflichtungen umfassen die Gewinnung, Recherche und vorsorgliche Speicherung von Daten, die auf Computern gespeichert werden einschließlich der Verbindungs- und Nutzungsdaten. Dieses Kapitel enthält gleichfalls die Vorgaben zur Überwachung von E-Mail und Telefax und zum grenzüberschreitenden Zugriff auf diese Daten. Insbesondere diesen Vorgaben mangelt es an datenschutzrechtlicher Substanz und normativer Klarheit.

Die datenschutzrechtliche Kritik an der Konvention richtet sich vor allem gegen Vorgaben zur vorsorglichen Speicherung von Nutzungsdaten, insbesondere Kennungen und IP-Adressen. Auch die Bestimmungen zum jederzeitigen grenzüberschreitenden Zugriff von Ermittlungsbehörden auf Computerdaten lassen befürchten, dass hiermit erneut die Frage nach der Zulässigkeit von bzw. des Zugriffs auf verschlüsselte Kommunikation (s. hierzu 4.2) aufgeworfen wird.

Leider enthält die Konvention keine Ansätze zur Harmonisierung des Datenschutzes und des Fernmeldegeheimnisses auf hohem Niveau. Sie nimmt nicht einmal auf die Datenschutz-Konvention des Europarats Bezug. Vielmehr wird es den Staaten überlassen, die entsprechenden Datenverarbeitungs- und Überwachungsmöglichkeiten national zu regeln. Zwar sind die Mitgliedstaaten des Europarates verpflichtet, die Grundrechte ihrer Bürger zu schützen. Dies gilt jedoch nicht für weitere Staaten, die dem Europarat nicht angehören und die ebenfalls eingeladen sind, der Konvention beizutreten. Es ist deshalb zu befürchten, dass auf Grund der Konvention personenbezogene Daten von Internet-Nutzern auch in Länder übermittelt werden müssen, in denen kein angemessenes Niveau

des Datenschutzes und der Fernmeldegeheimnisses gewährleistet sind und in denen keine hinreichenden verfahrensmäßigen Garantien bei Eingriffen in das Fernmeldegeheimnis bestehen.

Bündnis 90/Die Grünen werden sich dafür einsetzen, dass durch Änderungen an der Konvention den Datenschutzbedenken Rechnung getragen wird und dabei insbesondere jegliche Verpflichtung zur Vorratsdatenspeicherung entfällt und die Übermittlungen in andere Länder an verfassungsrechtliche, insbesondere datenschutzrechtliche Garantien gebunden werden.

4.3.3 EU-Initiative "sicheres Internet"

Im Juni 2000 billigte der Europäische Rat den umfassenden "eEurope"-Aktionsplan und forderte seine Durchführung bis 2002. Der Aktionsplan befasst sich schwerpunktmäßig mit der Sicherheit von Netzen und der Bekämpfung der Computernetzkriminalität. In einem im Januar 2001 vorgelegten ersten Bericht formuliert die EU-Kommission das kurzfristige Ziel, ein Rechtsinstrument der EU zu schaffen, das wirksame Sanktionen der Mitgliedstaaten gegen die Kinderpornografie im Internet gewährleistet. Langfristig plant die Kommission Legislativvorschläge zur weiteren Angleichung der materiellen Strafrechtsvorschriften für den Bereich der High-Tech-Kriminalität.

Die Kommission kündigte zudem an, dass sie die Strafverfolgungsbehörden, die Anbieter von Internet-Diensten, die Telekommunikationsbetreiber, Bürgerrechtsorganisationen, die Vertreter der Verbraucher und der Datenschutzbehörden sowie andere interessierte Parteien in einem eigens eingerichteten EU-Forum zusammenzubringen will, um ihr gegenseitiges Verständnis und die Zusammenarbeit auf EU-Ebene zu fördern. Ziel des Forums soll es auch sein, das öffentliche Bewusstsein für die Gefährdung durch über das Internet begangene Straftaten zu schärfen, optimale Sicherheitsbedingungen zu schaffen, Instrumente und Verfahren für eine wirksame Bekämpfung der Computerkriminalität aufzuzeigen und die Weiterentwicklung von Frühwarnsystemen und Mechanismen der Krisenbewältigung anzuregen.

Wir begrüßen es, dass hier - anders als bei der Cyber Crime Convention des Europarats - eine breite öffentliche Diskussion angestoßen wurde. Bündnis 90/Die Grünen werden sich an den Beratungen des Aktionsplans auf nationaler und internationaler Ebene beteiligen.

4.4 Telekommunikations-Überwachungsverordnung (TKÜV)

§ 88 TKG verpflichtet die Betreiber von Telekommunikationsanlagen auf eigene Kosten zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation. Die Ausgestaltung der Überwachungsverpflichtung soll durch Rechtsverordnung erfolgen.

Die technische Umsetzung von Überwachungsmaßnahmen ist bislang in der Fernmeldeverkehr-Überwachungs-Verordnung (FÜV) geregelt. Da es sich bei den von Diensteanbietern im Internet betriebenen Einrichtungen üblicher Weise nicht um für den öffentlichen Verkehr bestimmten Fernmeldeanlagen handelt, sind die Vorgaben der FÜV nicht auf diese anwendbar. Das Bundeswirtschaftsministerium hat im Frühjahr 2001 den Referentenentwurf einer Telekommunikationsüberwachungsverordnung (TKÜV) vorgelegt. Die TKÜV soll auch geschlossene Benutzungsgruppen und sonstige geschäftsmäßige Telekommunikationsdienste umfassen, die nicht für die Öffentlichkeit bestimmt sind.

In dem TKÜV-Entwurf wird unterschieden zwischen Betreibern von Telekommunikationsanlagen oder Teilen von Telekommunikationsanlagen, mittels derer Telekommunikations-

dienstleistungen für die Öffentlichkeit erbracht werden und sonstigen Betreibern, die gesetzlich verpflichtet sind, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.

Während die erste Gruppe dazu verpflichtet ist, die technischen Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und vorbereitende organisatorische Vorkehrungen für die Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung der Telekommunikation zu treffen, soll die zweite Gruppe von diesen Verpflichtungen befreit werden, muss jedoch gleichwohl die Überwachung im Einzelfall ebenfalls ermöglichen.

Im Hinblick auf die Tragweite der zusätzlichen Verpflichtungen zur Gewährleistung einer Internet-Überwachung stehen wir dem TKÜV-Entwurf kritisch gegenüber. Unsere Kritik wird von den wesentlichen Berufsverbänden der Informatiker und der Internet-Wirtschaft und von Datenschutzbeauftragten geteilt. Wir erwarten von der Bundesregierung, dass sie der Kritik Rechnung trägt und vor einer erneuten Ausweitung von Überwachungsmaßnahmen zunächst eine Bewertung der bisherigen Befugnisse vornimmt (Evaluation).

5 Schlussfolgerungen

Wie im realen Leben gibt es im virtuellen Raum des Internet auch Schattenseiten. Gleichwohl beachtet die überwiegende Zahl der Angebote den legalen Rahmen und auch die aller meisten Nutzerinnen und Nutzer des Internet verhalten sich rechtskonform. Angesichts des hohen Wertes der Meinungsfreiheit und des Rechts auf informationelle Selbstbestimmung sollte die freie Kommunikation im Internet deshalb so wenig wie möglich beschränkt werden. Zensur und allgegenwärtige Überwachung sind der Tod jeder freien Kommunikation.

Das Internet ist kein rechtsfreier Raum. Sowohl das Straf- als auch das Zivilrecht und die Datenschutzvorschriften gelten auch im Netz. Durch die vor einigen Jahren eingeführten Vorschriften des Computerstrafrechts (insbesondere zum Computerbetrug und zur Computersabotage) und durch die Erstreckung der Straf-Ermittlungsbefugnisse (insbesondere der Telekommunikationsüberwachung zur Aufklärung besonders schwerer Straftaten) auf alle elektronischen Dienste besteht in Deutschland ein ausreichender Rechtsrahmen gegen den Missbrauch von Computernetzen. Zudem wären im Hinblick auf die Internationalität des Netzes zusätzliche nationale Rechtsvorschriften, die darauf abzielen, in Deutschland verbotene (aber in anderen Ländern erlaubte) Inhalte von Deutschlands Surferinnen und Surfern fernzuhalten, von vornherein zum Scheitern verurteilt.

Bündnis 90/Die Grünen sehen deshalb keine Notwendigkeit zum Ausbau der Ermittlungsbefugnisse und der Strafnormen.

5.1 Ausstattung von Strafverfolgungsbehörden verbessern

Eine wirksame Bekämpfung der Computer- und Netzkriminalität scheitert nicht an unzureichenden Strafnormen und Befugnissen, sondern einen der unzureichenden Ausstattung und Qualifikation von Ermittlungsbehörden. Deshalb begrüßen wir die Bemühungen von Bund und Ländern, dieses Defizit auszugleichen. Insbesondere im Bereich der Qualifikation von Polizeibeamten und Staatsanwälten besteht dringender Handlungsbedarf, damit Kinderpornografie und Betrugsdelikte im Internet wirksam bekämpft werden können.

5.2 Verantwortung von Diensteanbietern stärken

Eine Vielzahl von Missbrauchsfällen und Computerdelikten wird erst dadurch möglich, dass die Diensteanbieter keine oder unzureichende Schutzmaßnahmen treffen. Immer noch wird der überwiegende Teil der Internet-Kommunikation unverschlüsselt abgewickelt und bietet deshalb vielfältige Angriffsmöglichkeiten. Viel zu wenige Diensteanbietern machen von der Möglichkeit Gebrauch, die Authentizität ihrer Angebote durch digitale Zertifikate nachzuweisen.

Bündnis 90/Die Grünen halten es angesichts dieser Defizite für erforderlich, den Einsatz von verschlüsselten Kommunikationstechniken voranzubringen, etwa indem die Haftungsregelungen bei Missbräuchen aufgrund unzureichenden technischen Schutzes verändert werden. Ferner treten wir dafür ein, dass die Sicherheit und Vertrauenswürdigkeit von Internet-Angeboten durch unabhängige Gutachter überprüft und zertifiziert werden können. Im Hinblick auf verabscheuungswürdige Inhalte, insbesondere der Kinderpornografie, verlangen wir von den Providern, dass sie durch geeignete Maßnahmen die Verbreitung verhindern.

5.3 Datenschutz ausbauen und modernisieren

Internet-Ökonomie und E-Government werden nur dann den in sie gesetzten Erwartungen gerecht, wenn die Bürgerinnen und Bürgern darauf vertrauen können, dass mit ihren persönlichen Daten verantwortungsbewusst umgegangen wird. Deshalb setzen sich Bündnis 90/Die Grünen für eine umfassende Modernisierung des Datenschutzrechts ein. Mit der ersten Stufe der Novellierung des Bundesdatenschutzgesetzes, die im Mai 2001 in Kraft getreten ist, ist ein wichtiger erster Schritt erfolgt. Dabei wird es nicht bleiben.

Wir setzen uns dafür ein, dass noch in diesem Jahr die Novelle des Teledienstedaten-schutzgesetzes in Kraft tritt, das gerade im Hinblick auf die Möglichkeiten zur Missbrauchsverhinderung und -Aufklärung deutliche Verbesserungen enthält. Wir begrüßen es schließlich, dass im Auftrag der rot-grünen Bundesregierung und der sie tragenden Bundestagsfraktionen durch namhafte Wissenschaftler ein Gutachten erarbeitet wurde, das die Wege zu einem zukunftsweisenden neuen Datenschutzrecht aufzeigt. Wir erwarten von der Bundesregierung, dass sie diese Vorschläge zügig aufgreift und die notwendigen Schritte zu ihrer Umsetzung ergreift.

Ein Kernbestandteil eines modernen Datenschutzrechts im Zeitalter der Internet-Ökonomie stellen Ansätze dar, durch die datenschutzfreundliches Verhalten von Unternehmen belohnt wird. Im Zentrum derartiger Überlegungen steht das Datenschutz-Audit, d. h. die Möglichkeit zur unabhängige Begutachtung der Datenschutzpolitik von Unternehmen mit der Berechtigung, die Prüfsiegel in ihren Internetangeboten als Qualitätsnachweise zu verwenden. Deshalb erwarten wir von der Bundesregierung, dass noch in dieser Legislaturperiode ein Datenschutz-Audit-Gesetz verabschiedet wird.

5.4 Selbstschutz und „Netiquette“

Alle staatlichen Anstrengungen zur Verhinderung von Missbrauch werden leer laufen, wenn sich die Nutzer lediglich als Konsumenten von Internet-Diensten verstehen und sich nicht als Netzbürgerinnen und Netzbürger verhalten. Das Internet stellt insofern eine gewaltige Herausforderung an unser Bildungs- und Gesellschaftssystem dar. In der Frühphase des Internet gab es allgemein beachtete Grundsätze, die einem Missbrauch des Netzes entgegenwirkten, die so genannte "Netiquette". Im Zuge der Kommerzialisierung des Netzes und der Entwicklung immer neuer Nutzungsformen ist die Bindungswirkung

derartiger freiwilliger Verhaltensregelungen leider verloren gegangen. Wir setzen uns dafür ein, die Debatte um die Selbstregulierung und den Selbstschutz im Netz wieder aufzunehmen.

Dabei kommt Verbraucherverbänden, Bürgernetzvereinen und anderen nichtkommerziellen Organisationen besondere Bedeutung zu. Wir setzen uns dafür ein, Bestrebungen zu unterstützen und zu fördern, die eine "elektronische Basisdemokratie" voranbringen. Bedeutsam sind auch Initiativen wie das Projekt "E-Demokratie" der Bundestagsfraktionen von Bündnis 90/Die Grünen und der SPD, mit denen eine möglichst breite elektronische Beteiligung an Gesetzgebungsvorhaben sichergestellt werden soll (http://www.modernes-datenrecht.de).

Schließlich müssen die Internet-Nutzerinnen und -Nutzer Möglichkeiten bekommen, sich durch einfache technische Mittel wirksam gegen Missbräuche zu schützen. Hierzu gehört sowohl die Verfügbarkeit kostenloser Software zur Verschlüsselung als auch anderer Selbstschutz-Software (Virenscanner, Webwasher, Firewalls etc.). Wir werden uns weiterhin dafür einsetzen, entsprechende Projekte zu fördern und durch Aufklärungs- und Öffentlichkeitsarbeit das Bewusstsein und die Kenntnisse über die Gefahren und Chancen des Netzes zu verbessern.