

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

FDP-Bundestagsfraktion

Eckpunkte zur Verbesserung der Kriminalitätsbekämpfung im Internet:

Freiheit und Sicherheit im Internet bewahren

- Stand: 9. November 2010 -

1	<u>Gliederung</u>	
2		
3	0. Ausgangslage	2
4		
5	I. Allgemeine Maßnahmen zur Kriminalitätsbekämpfung	4
6	1. Aufstockung der Ermittlungskapazitäten.....	4
7	2. Bündelung von IT-Kompetenz in der Justiz.....	4
8	3. Flankierung durch internationale Kooperationen.....	4
9	4. Einsatz spezialisierter Suchtechnologie.....	5
10	5. Nutzung der Erkenntnisse aus der Missbrauchsbekämpfung bei Bankkundendaten.....	6
11	6. Nutzung von Verfahren zum schnellen Einfrieren von Verkehrsdaten (Quick Freeze).....	7
12	7. Bekämpfung illegal ferngesteuerter Rechnernetze.....	9
13	8. Wappnung gegen Cyber-Angriffe auf Behörden und kritische Infrastrukturen.....	10
14	9. Vermeidung unverhältnismäßiger Online-Durchsuchungen.....	11
15	10. Einhaltung rechtsstaatlicher Maßstäbe bei Überwachungsmaßnahmen.....	11
16	11. Unterlassung der Quellen-Telekommunikationsüberwachung.....	12
17		
18	II. Spezielle Maßnahmen zur Bekämpfung von Darstellungen von	
19	Kindesmissbrauch im Netz	13
20	1. Löschung krimineller Netzinhalte statt bloßer Zugangerschwerung	13
21	2. Ausweitung von Ermittlungen in schwer zugängliche Bereichen des Internet.....	14
22	3. Verdachtsgestützte Überprüfung der Zahlungsströme im Online-Bereich	15
23	4. Präzisierung der Privilegierung in § 184b Abs. 5 StGB	16
24	5. Überprüfung der Strafandrohung in § 184b Abs. 4 StGB.....	16
25		
26	III. Bekämpfung von Datenschutzverstößen	16
27		

1 0. Ausgangslage

2
3 Im digitalen Raum des Internets ist ein neuer umfassender Verkehr entstanden:
4 Menschen kommunizieren miteinander, Menschen treiben Handel miteinander,
5 Menschen entwickeln gänzlich neue Produkte und Dienstleistungen. Dabei
6 verlieren bestimmte Hürden an Bedeutung, die vor der Digitalisierung noch
7 wesentlich waren wie etwa Entfernungen oder Staatsgrenzen. Das ist
8 grundsätzlich von Vorteil, weil es die Verständigung der Menschen untereinander,
9 ihre Kreativität und Produktivität steigert. Der digitale Raum ist in erster Linie eine
10 Chance, keine Gefahrenzone. Wie in jedem Zusammenleben von Menschen
11 kann es hier aber auch zu Rechtsverstößen kommen. Es ist selbstverständlich,
12 dass Kriminalität auch im Internet und in weiteren Bereichen neuer Medien
13 konsequent bekämpft werden muss. In gleicher Weise wie Recht und Gesetz
14 auch im Internet gelten, muss der Staat die Grenzen unserer Verfassung auch im
15 Internet einhalten.

16
17 Straftaten wie die Verbreitung und der Besitz von Darstellungen des Missbrauchs
18 von Kindern sind schreckliche und widerwärtige Verbrechen, die der Rechtsstaat
19 verhindern und mit aller Kraft bekämpfen muss. Das Verbrechen geschieht dabei
20 nicht erst im Internet; der Missbrauch und das unerträgliche Leiden der Kinder
21 finden zuvor in der realen Welt statt. Daher muss ein umfassender Ansatz zur
22 Bekämpfung des Missbrauchs von Kindern gewählt werden, wie ihn die FDP-
23 Bundestagsfraktion in ihrem Positionspapier „Kindesmissbrauch wirksam
24 bekämpfen“ vom Mai 2010 einfordert. So bedarf es für Sexualstraftäter u.a. der
25 Einführung einer Begutachtungspflicht sowie der Einschränkung des
26 Strafbefehlsverfahrens. Dadurch wird auch dem Opferschutz stärker Rechnung
27 getragen. Notwendig ist zudem der Ausbau der psychotherapeutischen
28 Behandlung auch schon im Vorfeld von Straftaten etwa durch Projekte wie „Kein
29 Täter werden“.

30 Auch andere Delikte wie Betrugsstraftaten müssen im Internet konsequent
31 verfolgt werden. Die Zahlungssicherheit im Netz ist unerlässlich, um Vertrauen in
32 Internetangebote zu gewährleisten. Das Abgreifen von Bankdaten oder der
33 Missbrauch von Kreditkartendaten sind daher wirksam zu bekämpfen.

1 Von herausragender Bedeutung für die digitale Welt ist der Datenschutz. Ein
2 effektiver Schutz persönlicher Daten ist zugleich Opferschutz. Wenn
3 Datenmissbrauch verhindert wird, nimmt dies vielen Straftaten mit fremden Daten
4 die Grundlage. Datenschutzdelikte sind keine Kavaliersdelikte. Es bedarf daher
5 einer strikten Durchsetzung des Datenschutzrechts und der konsequenten
6 Verfolgung und Abwehr von Datenmissbrauch.

7 Bei der Durchsetzung des Rechts im Internet stehen die Behörden vor neuen
8 Herausforderungen. Daher muss auch der Einsatz neuer Instrumente der
9 Strafverfolgung und Gefahrenabwehr diskutiert werden. Für uns Liberale sind in
10 dieser Diskussion folgende Aspekte von besonderer Bedeutung:

- 11
- 12 • Freiheit und Eigentum der Bürger zu schützen, betrachten Liberale als
13 vornehme Aufgabe. Sicherheit und Freiheit wollen wir in einen vernünftigen
14 Ausgleich bringen – im digitalen wie auch im nicht-digitalen Raum.
- 15 • Sämtliche Maßnahmen zum Schutz der Sicherheit, die in Freiheit eingreifen,
16 müssen erforderlich, geeignet und verhältnismäßig sein. Wir wollen effektive
17 und messbare Sicherheit, nicht bloß suggerierte Sicherheit. Es darf nie mehr
18 Freiheit geopfert werden, als auch effektive Sicherheit geschaffen wird.
- 19 • Kriminalitätsbekämpfung im Internet betrifft in hohem Maße den Umgang mit
20 personenbezogenen Daten in großer Menge. Neue Technologien und
21 fortschreitende Digitalisierung ermöglichen im Zusammenspiel mit der Vielzahl
22 der zur Verfügung stehenden Daten eine früher nicht vorstellbare Erfassung
23 praktisch aller Aktivitäten der Bürgerinnen und Bürger. Es gehört zur
24 verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die
25 Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und
26 registriert werden darf. Dies gilt auch, soweit heute die technischen
27 Möglichkeiten bestehen, um private Sachverhalte zu erfassen, die in der nicht-
28 digitalen Welt sich der Kenntnisnahme durch Dritte weitgehend entziehen. Bei
29 der Abwägung zwischen dem Nutzen einer Datenerhebung oder –speicherung
30 einerseits und dem Recht auf Privatheit andererseits ist daher stets zu
31 berücksichtigen, dass der einzelne Eingriff für sich gesehen zwar klein
32 erscheinen mag, aber die Summe aller Daten, die mittlerweile erhoben
33 werden, und die Möglichkeiten zu ihrer Verknüpfung bereits die Gefahr eines
34 Überwachungsstaates in sich bergen. Schon deshalb muss bereits die
35 Notwendigkeit der Datenerhebung regelmäßig nachgewiesen werden.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34

Um auch im Internet Sicherheit durch effektive Kriminalitätsbekämpfung zu gewährleisten, zugleich aber unsere Freiheit zu bewahren, schlagen wir folgende Maßnahmen vor:

I. Allgemeine Maßnahmen zur Kriminalitätsbekämpfung

1. Aufstockung der Ermittlungskapazitäten

Sowohl beim Bundeskriminalamt als auch bei den Polizeien der Länder muss die personelle und technische Ausstattung in den Dezernaten verbessert werden, die mit Ermittlungen im Internet befasst sein, insbesondere im Bereich der Straftaten gegen die sexuelle Selbstbestimmung. Neben einer guten technischen Ausstattung und einer ausreichenden Zahl von Ermittlerinnen und Ermittlern sind Qualifizierungsmaßnahmen erforderlich, um Straftaten im Internet besser aufklären zu können.

2. Bündelung von IT-Kompetenz in der Justiz

Die Bundesländer sollen die Errichtung von Schwerpunktdezernaten bei den Staatsanwaltschaften für den Bereich der Kriminalität im Internet prüfen, um die Fachkompetenz zur Ermittlung von Straftaten zu bündeln, die unter Nutzung des Internet begangen werden. Erfahrungen mit den in mehreren Bundesländern eingerichteten zentralen Zuständigkeiten für Wirtschaftsstrafsachen können hierzu gute Beispiele liefern.

3. Flankierung durch internationale Kooperationen

Im Rahmen der bi- und multilateralen Zusammenarbeit mit anderen Staaten, in denen grundlegende Probleme hinsichtlich der Gefahrenabwehr und Strafverfolgung im Bereich der Internetkriminalität – insbesondere im Bereich der Straftaten gegen die sexuelle Selbstbestimmung – festgestellt werden, soll Hilfe durch Technik und Kompetenzvermittlung angeboten werden. Erforderlichenfalls ist auf bi- und multilaterale Abkommen zur Zusammenarbeit hinzuwirken. In Staaten, in denen entsprechende Technik und Ausbildung vorhanden ist, ist auf die politische Priorisierung der Aufgabe hinzuwirken.

1 Wir schlagen parallel eine multilaterale Regelung mit folgenden Hauptanliegen
2 vor:

3
4 • Eine für die Staaten verbindliche Vereinbarung, was unter dem Begriff
5 "Kinderpornografische Inhalte" verstanden wird und dass die Herstellung,
6 Verbreitung oder das Zugänglichmachen dieser Inhalte unter Strafe gestellt wird.
7 Zwar gibt es einen internationalen Konsens, dass die Verbreitung solcher Inhalte
8 grundsätzlich strafbar ist. Allerdings gibt es große Unterschiede etwa bei den
9 einschlägigen Altersgrenzen der dargestellten Personen.

10
11 • Jeder Staat benennt eine zentrale Stelle zur Koordination der Strafverfolgung im
12 Bereich Kinderpornographie. Er stattet zudem die jeweiligen
13 Strafverfolgungsbehörden mit den notwendigen Personal- und Arbeitsmitteln für
14 eine effektive Verfolgung der Täter aus.

15
16 • Jeder Staat erlaubt den Polizeibehörden aller Vertragsländer ausdrücklich,
17 formlose Hinweise an seine inländischen Hosting-Provider zu verschicken, wenn
18 auf deren Servern kinderpornografische Inhalte zu finden sind.
19 Zugleich werden Polizeibehörden verpflichtet, kinderpornografische Inhalte
20 unverzüglich an die Hosting-Provider zu melden.

21
22 • Die Hosting-Provider werden verpflichtet, Meldungen von den für sie
23 zuständigen Polizeibehörden unverzüglich nachzugehen, vorhandene Beweise zu
24 sichern, kinderpornografische Inhalte dem öffentlichen Zugriff zu entziehen
25 ("Löschung") und die lokale Zentralstelle nach Ziff. 2 über die Löschung und
26 Beweissicherung zu informieren.

27 28 **4. Einsatz spezialisierter Suchtechnologie**

29 Ermittlungsarbeit ist hoheitliche Aufgabe. Das gilt auch für Ermittlungen mittels
30 spezialisierter Suchtechnologie für kriminelle Inhalte im Internet. Deshalb ist es
31 einerseits richtig, dass wir die Möglichkeiten zur effektiven Strafverfolgung nutzen.
32 Zum anderen darf dies aber kein Anlass sein, um hoheitliche Ermittlungsarbeit zu
33 privatisieren oder Private zu ihr zu zwingen.

1 Notwendig ist der Einsatz spezialisierter Technologien bei den
2 Ermittlungsbehörden zur Auffindung krimineller Inhalte. Die Ermittlungsbehörden
3 sollen in Wahrnehmung ihrer hoheitlichen Aufgaben eigene spezialisierte
4 Suchmaschinen mit auf die Ermittlungsziele optimierten Algorithmen in ihren
5 Rechenzentren verwenden, die das Auffinden von kriminellen Inhalten effektiv
6 ermöglichen. Hierzu wird ein Technologietransfer aus Wirtschaft und
7 Wissenschaft zu den Ermittlungsbehörden erforderlich werden.
8 Ermittlungsbehörden in Bund und Ländern können in einem Kompetenzzentrum
9 zusammenarbeiten, um Sachkenntnis und erfolgversprechende Lösungen
10 auszutauschen.

11 Sofern bei privaten Suchmaschinenbetreibern ohnehin konkrete Erkenntnisse
12 über Anbieter und Speicherorte krimineller Inhalte vorliegen, sollten diese mit den
13 Ermittlungsbehörden regelmäßig ausgetauscht werden. Insbesondere kommen
14 hierbei Erkenntnisse in Betracht, die Suchmaschinenbetreiber erlangen, wenn sie
15 bestimmte Suchergebnisse wegen des Verdachts auf kriminelle Inhalte
16 unterdrücken.

17 Wir lehnen es dagegen ab, dass Ermittlungsbehörden mit Suchmaschinen-
18 betreibern Ermittlungsvereinbarungen abschließen oder dass Ermittlungs-
19 behörden private Suchmaschinenbetreiber zu Ermittlungen verpflichten können.
20 Eine Einbindung von Unternehmen als Hilfspersonen der Ermittlungsbehörden ist
21 auch dann abzulehnen, wenn nur bestimmte technische Identifikationsmerkmale
22 von Dateien mit rechtswidrigen Inhalten zur Verfügung gestellt werden sollen.
23 Bereits die Weitergabe solcher technischer Identifikationsmerkmale illegaler
24 Dateien kann Ermittlungserfolge gefährden und birgt die erhebliche Gefahr
25 weiterer Verbreitung. Ermittlungsanordnungen nach der Strafprozessordnung
26 bleiben unbenommen.

27

28 **5. Nutzung der Erkenntnisse aus der Missbrauchsbekämpfung bei** 29 **Bankkundendaten**

30 Im Bereich internetbasierter Bankgeschäfte und dem Online-Handel stellen
31 sogenannte Identitätsdiebstähle oder sogenannte „Phishing“-Angriffe, bei denen
32 mittels gefälschter Internetseiten und betrügerischer Emails Passwörter
33 abgefangen werden, weiterhin ein Problem dar. Dabei erschleichen Kriminelle die
34 Zugangsdaten zu Online-Banking-Kunden, indem sie beispielsweise Bankportale
35 vortäuschen, auf denen die Kunden dann ihre Zugangs- und Transaktionsdaten

1 eingeben sollen. Diese Daten werden dann für betrügerische Transaktionen
2 benutzt.

3 Der Gesetzgeber stellte 2007 das Vorbereiten des Ausspähens und Abfangens
4 von Daten unter Strafe (§ 202c StGB), wobei jedoch der Versuch noch nicht
5 erfasst wird. Es ist zu prüfen, ob hier gesetzliche Lücke zu schließen sind.

6 Die Erkenntnisse insbesondere der Kreditwirtschaft, die große Bemühungen zu
7 schnellen Reaktionen auf kriminelle Handlungen in diesem Bereich vornimmt und
8 damit bereits beachtliche Ergebnisse vorweisen kann, sollen im Erfahrungsaustausch mit den Ermittlungsbehörden auch für andere Bereiche der Online-Kriminalität genutzt werden. So haben Forscher der Universität Cambridge in einer Studie (*The Impact of Incentives on Notice and Take-down*, Tyler Moore and Richard Clayton, 2008) aufgezeigt, dass Banken es im Durchschnitt innerhalb von vier bis acht Stunden schaffen, zur Kenntnis gelangte „Phishing Websites“ weltweit löschen zu lassen. Insbesondere für die Kriminalitätsbekämpfung im Bereich der Darstellungen von Kindesmissbrauch sind Erkenntnisse wertvoll, wie sich die Geschwindigkeit bei der Abschaltung krimineller Internetseiten mit ausländischem Server-Standort erhöhen lässt.

19 **6. Nutzung von Verfahren zum schnellen Einfrieren von Verkehrsdaten** 20 **(Quick Freeze)**

21 Der Rechtsgrundsatz, dass grundrechtsrelevante Maßnahmen im Rahmen der
22 Strafverfolgung oder der Gefahrenabwehr nur unter der Voraussetzung erfolgen,
23 dass ein ausreichender Verdacht oder Anlass für diese Maßnahme gegeben ist,
24 muss auch im digitalen Raum gelten. Wir lehnen daher die verdachts- und
25 anlassunabhängige Speicherung personenbezogener Daten auf Vorrat ab. Wir
26 setzen uns vielmehr für die Möglichkeit ein, Verbindungsdaten zu puffern und für
27 die Strafverfolgung und Gefahrenabwehr zu verwerten, wenn ein ausreichender
28 Verdacht bzw. Anlass existiert. Für das sogenannte Quick-Freeze-Verfahren ist
29 eine gesetzliche Grundlage zu schaffen. In Fällen, in denen Polizei und
30 Staatsanwaltschaft Ermittlungen im Internet führen, soll es möglich sein, die
31 Telekommunikationsprovider zu verpflichten, für einen bestimmten Zeitraum
32 bestimmte und nach klaren Kriterien eng begrenzte Telekommunikations-
33 verbindungsdaten mit Personenbezug unverseht und kurzfristig zu puffern
34 (schnelles Einfrieren der Daten, „quick freeze“). Der Zugriff auf die so gepufferten
35 Daten (das „Auftauen“) und deren Nutzung steht unter Richtervorbehalt.

1 Damit können in Fällen, in denen im Internet z.B. wegen
2 Missbrauchsdarstellungen, Organisierter Kriminalität, Wirtschaftsdelikten oder
3 Terrorismus ermittelt wird, wichtige Ermittlungsansätze erlangt und genutzt
4 werden, ohne alle Bürgerinnen und Bürger unter einen Generalverdacht zu
5 stellen und anlasslos alle Telekommunikationsverbindungsdaten zu puffern.
6 Quick Freeze ist somit eine verfassungskonforme Alternative zur
7 Vorratsdatenspeicherung.

8 Insbesondere bei Ermittlungen in Foren, Tauschbörsen oder bei bekannten
9 Angeboten im World Wide Web wegen schwerer und schwerster Kriminalität
10 werden schon heute erfolgreich für einen bestimmten Beobachtungs- und
11 Ermittlungszeitraum solche Daten in strafprozessual zulässiger und verfassungs-
12 rechtlich unbedenklicher Weise erhoben (§§ 100 a und g StPO). Um die Daten
13 den hinter den Internetprotokoll-Adressen stehenden Personen zuordnen zu
14 können, ist es notwendig, für den Ermittlungszeitraum auch solche
15 Telekommunikationsverbindungsdaten kurzfristig zu speichern, die ansonsten
16 mangels Veranlassung von den Telekommunikationsanbietern bislang oft nicht
17 mehr gespeichert werden. Eine kurze Speicherdauer ist praxisgerecht, da infolge
18 der überwiegenden Nutzung pauschaler Internetzugangstarife auch die meisten
19 Internetverbindungen mit temporärer Internetprotokolladresse bis zu 24 Stunden
20 lang aufrechterhalten werden. Ein schnelles Ermitteln der Strafverfolgungs-
21 behörden ermöglicht eine hohe Erfolgswahrscheinlichkeit ohne die Notwendigkeit
22 einer Vorratsdatenspeicherung.

23 In der Strafprozessordnung ist der Anwendungsbereich eines Quick-Freeze-
24 Verfahrens für die Strafverfolgung zu eröffnen, wenn ein durch konkrete
25 Tatsachen begründeter Verdacht auf bestimmte schwere Straftaten besteht. Bei
26 der Aufstellung eines hierfür einschlägigen abschließenden Straftatenkatalogs in
27 der Strafprozessordnung sind vor allem die im Internet am häufigsten
28 vorkommenden Straftaten mit hohen Schäden zu erfassen. Die Eingrenzung der
29 relevanten Tatbestände ist anhand der Vorgaben des Bundesverfassungsgerichts
30 vorzunehmen. Es sind dieselben Maßstäbe anzulegen wie bei einer
31 herkömmlichen Telekommunikationsüberwachung.

32 Eine Anordnung mit Wirkung für maximal drei Monate soll durch die
33 Staatsanwaltschaft erfolgen, in Eilfällen für höchstens drei Tage durch das
34 zuständige Polizeipräsidium. Eine Verlängerung um wiederum drei Monate soll
35 möglich sein, wenn der Antragsteller fallbezogen begründen kann, warum die

1 Maßnahme bisher keinen Erfolg gehabt hat, in der Verlängerungsperiode jedoch
2 mit hoher Wahrscheinlichkeit erfolgreich sein wird. So soll einer schematischen
3 „Kettenverlängerung“ vorgebeugt werden.

4 Im Bereich der Gefahrenabwehr kann auf Antrag des Präsidenten der jeweils
5 zuständigen Behörde oder dessen Stellvertreters das Gericht ein Quick-Freeze-
6 Verfahren anordnen, wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr
7 für Leib, Leben oder Freiheit der Person, für den Bestand oder die Sicherheit des
8 Bundes oder eines Landes oder für eine gemeine Gefahr bestehen. Auch hier ist
9 für das „Auftauen“ der Daten ein richterlicher Beschluss erforderlich.

10 Für die Verfolgung beispielsweise von Betrugsstraftaten im Internet sowie für die
11 Gefahrenabwehr im Übrigen wie auch für Ordnungswidrigkeiten bleibt die
12 Möglichkeit der Sicherheitsbehörden zur Abfrage einer hinter einer dynamisch
13 zugewiesenen IP-Adresse stehenden Person gem. § 113 Satz 1, 2. Halbsatz
14 TKG bestehen, sofern den anfragenden Behörden im Einzelfall diese Adresse
15 bereits bekannt ist. Die vom Bundesverfassungsgericht angeregte Klarstellung
16 der Eingrenzung auf Einzelabfragen bereits bekannter IP-Adressen soll in § 113
17 TKG aufgenommen werden.

19 **7. Bekämpfung illegal ferngesteuerter Rechnernetze**

20 Ermöglicht werden muss die effektive Bekämpfung von Rechnernetzen, deren
21 Computer durch Schadsoftware infiziert und ohne Wissen ihrer Besitzer
22 ferngesteuert werden, um z.B. Spam zu versenden oder für Angriffe auf andere
23 Rechnernetze oder andere kriminelle Zwecke missbraucht zu werden
24 (sogenannte Bot-Netze). Insbesondere ist hier auf Aufklärung der Computer-
25 besitzer zu setzen, damit diese ihre Rechner vor Schadsoftware schützen und
26 Fernsteuerungen verhindern können. Zu begrüßen ist die Initiative des Internet-
27 Branchenverbandes eco die Besitzer infizierter Rechner informiert und Hilfe
28 anbietet.

29 Der Datenschutz der Betroffenen ist bei allem zu wahren und eine unverhältnis-
30 mäßige Überwachung des Internetdatenverkehrs zu vermeiden. Vor allem ist es
31 nicht erforderlich, die Opfer eines kriminellen Angriffs auf ihre Rechner polizeilich
32 mittels Vorratsdatenspeicherung zu erfassen. Anti-Bot-Netz-Initiativen wie die des
33 eco-Verbandes erreicht die Betroffenen auch ohne solch unverhältnismäßige
34 Mittel. Ziel muss sein, die Opfer von Schadsoftware in die Lage zu versetzen, die
35 Infektion zu beseitigen. Zudem ist es vordringlich geboten, Tätern auf die Spur zu

1 kommen, welche Schadsoftware verbreiten und Rechnernetze fernsteuern oder
2 solche gegen Geld „vermieten“. Hierzu ist eine intensive Zusammenarbeit mit den
3 Staaten erforderlich, aus denen heraus zahlreiche Bot-Netze gesteuert werden.

4 5 **8. Wappnung gegen Cyber-Angriffe auf Behörden und kritische** 6 **Infrastrukturen**

7 Die Sicherheit kritischer IT-Infrastrukturen der Privatwirtschaft sowie des Staates,
8 insbesondere von Behördennetzen, hat eine große gesamtwirtschaftliche und
9 gesellschaftliche Bedeutung. IT-Infrastrukturen sind inzwischen mindestens
10 ebenso wichtige Lebensadern unserer Gesellschaft wie Straßen oder
11 Elektrizitätsversorgung.

12 Angriffe von Kriminellen oder fremden Staaten auf IT-Netze zum Zwecke der
13 Spionage oder mit dem Ziel der Zerstörung oder Manipulation wichtiger
14 Infrastrukturen müssen effektiv abgewehrt werden können. Daher ist es für
15 staatliche IT-Infrastrukturen mindestens so wichtig wie für Unternehmen,
16 Sicherungsmechanismen gegen Angriffe zu etablieren.

17 Mit dem BSI-Gesetz wurde in der vergangenen Legislaturperiode die Aufgabe der
18 Sicherung der staatlichen Netze des Bundes dem Bundesamt für Sicherheit in der
19 Informationstechnik (BSI) übertragen. Im Koalitionsvertrag wird bekräftigt, dass
20 das BSI diese Aufgabe übernehmen und für die IT-Sicherheit des Bundes
21 verantwortlich sein soll. Hierbei muss jedoch stets beachtet werden, dass die
22 Abwehrmaßnahmen verhältnismäßig sein müssen.

23 Wie es auch in Unternehmen selbstverständlich ist, durch geeignete Programme
24 und Filter nach Schadsoftware in der elektronischen Kommunikation zu suchen
25 und verdächtige Daten auszusondern, muss auch in der Verwaltung des Bundes
26 mittels Schutzprogrammen die IT-Sicherheit gewährleistet werden. Nicht
27 erforderlich ist jedoch, die Kommunikation mit Behörden so weitgehend zu
28 überwachen, dass durch das BSI auch von solchen Inhalten Kenntnis genommen
29 werden kann, die wegen ihres Bezuges zum Kernbereich privater Lebens-
30 gestaltung grundgesetzlich absolut geschützt sind. Im Sinne des Koalitions-
31 vertrages, nach dem eine generelle Überwachung des Internetdatenverkehrs
32 abgelehnt wird, sind die Vorschriften des § 5 BSI auf ihre Verhältnismäßigkeit
33 hin zu überprüfen und alsbald eine Evaluierung durch einen unabhängigen
34 Sachverständigen vorzunehmen

1 **9. Vermeidung unverhältnismäßiger Online-Durchsuchungen**

2 Das allgemeine Persönlichkeitsrecht wird bei länger andauernder Überwachung
3 besonders intensiv verletzt. Längere Überwachungen eines Computers bergen
4 die Gefahr, dass die Persönlichkeit des betroffenen Besitzers in einer Weise
5 ausgeforscht wird, die ein umfassendes Persönlichkeitsprofil ermöglicht. Der
6 Staat würde so Einblick auch in intimste Lebensumstände des Betroffenen
7 bekommen, was die Grenze des verfassungsrechtlich Zulässigen überschritte.

8 Wenngleich das Bundesverfassungsgericht mit seiner Entscheidung vom Februar
9 2008 heimliche Onlinedurchsuchungen unter bestimmten strengen Voraus-
10 setzungen für verfassungsrechtlich möglich gehalten hat, bleibt die Maßnahme
11 solange unverhältnismäßig, wie ein überzeugender Nachweis der Notwendigkeit
12 eines derart schwerwiegenden Grundrechtseingriffs nicht erbracht ist. Die FDP-
13 Bundestagsfraktion hat die Möglichkeit zur heimlichen Online-Durchsuchung
14 bereits im BKA-Gesetz abgelehnt. Eine etwaige Ausweitung des Instruments auf
15 andere Bereiche kommt für uns nicht in Frage.

16 Beachtlich ist dagegen bei den bestehenden Beschlagnahmeregelnungen für
17 Computer, dass diese bei Ermittlungen vor allem deshalb oft ins Leere laufen,
18 weil die Sicherheitsbehörden nicht über ausreichend Personal mit speziellem
19 technischem Sachverstand verfügen, um beschlagnahmte Medien auswerten zu
20 können. Durch Online-Durchsuchungen erhobene Daten sind zudem aufgrund
21 der zur Durchführung der Maßnahme erforderlichen Manipulation der Zielrechner
22 als Beweismittel ungeeignet. Eine Verwendung im Strafverfahren als Beweismittel
23 kommt nicht in Frage, weil Zweifel an der Authentizität der Daten nie ganz
24 ausgeräumt werden können. Dieser Zustand ist unhaltbar.

25 Es ist inakzeptabel, dass heimlich auf Computer zugegriffen wird, statt die
26 personelle und sächliche Ausstattung der Sicherheitsbehörden so zu gestalten,
27 dass von den bestehenden Befugnissen auch effektiv Gebrauch gemacht werden
28 kann. Ebenso scheint der Bedarf nach einer solchen Maßnahme sehr fraglich,
29 nachdem diese bis jetzt noch nie angewendet wurde. Bund und Länder müssen
30 ihre Sicherheitsbehörden so ausstatten, dass Medien, die beschlagnahmt
31 wurden, auch ausgewertet und für die Ermittlungen genutzt werden können.

32 **10. Einhaltung rechtsstaatlicher Maßstäbe bei Überwachungsmaßnahmen**

33 Es kann nicht bezweifelt werden, dass im Rahmen der Verhältnismäßigkeit und
34 innerhalb der strikten verfassungsrechtlichen Grenzen die Telekommunikations-
35

1 überwachung ein sinnvolles und notwendiges Instrument sowohl im Bereich der
2 Strafverfolgung als auch im Bereich der Gefahrenabwehr und der
3 nachrichtendienstlichen Tätigkeit ist. Neue Kommunikationsformen erfordern
4 neue technische Lösungen, um im gegebenen rechtlichen Rahmen
5 Telekommunikation zu überwachen. Neue Technologien zur Telekommunika-
6 tionsüberwachung dürfen jedoch nicht zu einer Aufweichung der
7 verfassungsrechtlichen Grenzen genutzt werden. Dies gilt insbesondere für die
8 Überwachung von Internet-Telefonie und anderer neuer Telekommunikations-
9 formen.

11. Unterlassung der Quellen-Telekommunikationsüberwachung

12 Die FDP-Bundestagsfraktion lehnt die sogenannte Quellen-Telekommunikations-
13 überwachung (Quellen-TKÜ) ab. Bei dieser Maßnahme dringen Behörden in
14 einen Computer ein, infizieren ihn mit einer Software, die dann an die
15 entsprechende Behörde Daten noch vor einer eventuellen Verschlüsselung
16 versendet. Zur Quellen-TKÜ hat das Bundesverfassungsgericht in seiner
17 Entscheidung zur heimlichen Onlinedurchsuchungen ausgeführt, dass „mit der
18 Infiltration die entscheidende Hürde genommen ist, um das System insgesamt
19 auszuspähen“. Die Quellen-TKÜ bedient sich prinzipiell der gleichen Technik wie
20 die heimliche Onlinedurchsuchung. Zwar soll das aufgespielte Überwachungs-
21 programm auf Daten laufender Telekommunikationsvorgänge beschränkt sein;
22 dies kann jedoch nicht garantiert werden. Es werden vielmehr unzulässigerweise
23 regelmäßig auch Daten erfasst, die noch nicht oder nicht mehr Gegenstand
24 laufender Telekommunikationsvorgänge sind. Schon aus diesem Grunde ist eine
25 solche Maßnahme unverhältnismäßig.

26 Stattdessen müssen andere technische Mittel gefunden werden, um neue
27 Kommunikationsformen in den elektronischen Medien zu überwachen, ohne
28 dabei in die Rechner der Betroffenen einzugreifen. Hierzu soll im vor kurzer Zeit
29 eingerichteten Kompetenzzentrum TKÜ beim Bundesverwaltungsamt an neuen
30 Lösungen gearbeitet werden.

II. Spezielle Maßnahmen zur Bekämpfung von Darstellungen von Kindesmissbrauch im Netz

1. Löschung krimineller Netzinhalte statt bloßer Zugängerschwerung

Kriminelle Inhalte im Internet müssen bekämpft und nicht versteckt werden. Netzsperrern leisten keinen Beitrag, um kriminelle Inhalte im Internet und insbesondere Darstellungen sexuellen Missbrauch von Kindern zu bekämpfen. Denn der weit überwiegende Teil des kriminellen kinderpornographischen Materials befindet sich gerade nicht im World Wide Web, in dem Netzsperrern eingesetzt werden sollen, sondern in anderen Internetdiensten, auf die Netzsperrern keinen Einfluss haben. Zudem können Netzsperrern gerade von denen, die nach solchem Material suchen, sehr leicht umgangen werden. Netzsperrern sind darüber hinaus gefährlich, denn sie weisen auf Fundstellen für bestimmte Inhalte geradezu hin und dienen somit gleichsam als „Gelbe Seiten“ für diejenigen, die auf der Suche nach diesen Inhalten sind. Sie können damit sogar noch zur Verbreitung der Inhalte beitragen, statt diese zu begrenzen. Dies geschah beispielsweise bei der Veröffentlichung der Sperrlisten in Finnland und Dänemark. Täter werden durch Sperrern zwar gewarnt, aber Opfer werden nicht geschützt, da die Inhalte online bleiben. Netzsperrern schaden auch, indem sie Ressourcen binden, die effektiver eingesetzt werden können. Sperrern fördern eine Mentalität des Wegsehens, denn sie wiegen die Gesellschaft in der falschen Sicherheit, dass das für viele nicht mehr leicht auffindbare, nicht mehr vorhanden sind.

Zur nachhaltigen Bekämpfung von Missbrauchsdarstellungen im Internet und zugleich zum Schutz konkreter und potentieller Opfer ist stattdessen das konsequente Löschen der Inhalte und vor allem die intensive Verfolgung der Täter notwendig. Es muss dazu eine enge internationale Zusammenarbeit stattfinden. Einerseits muss weltweit durch die zuständigen Behörden in den Staaten, in denen die Inhalte ins Internet gelangen, gegen die Täter vorgegangen werden. Andererseits muss schnell und konsequent die Löschung von Missbrauchsdarstellungen im Netz vorangetrieben werden.

Die Zusammenarbeit mit den Host-Providern ist hierbei von großer Bedeutung, damit kriminelles Material schnell von den Servern entfernt werden kann. Die Zusammenarbeit mit den Internetbeschwerdestellen und ihren internationalen Partnern und Netzwerken wie INHOPE ist unerlässlich und muss seitens der

1 deutschen Polizeibehörden noch verbessert werden. Um diese Zusammenarbeit
2 weiter zu optimieren, müssen klare Prozesse definiert werden. Ebenso ist die
3 Erfassung der Löscherfolge mit eindeutigen Verfahren zu regeln.

4 5 **2. Ausweitung von Ermittlungen in schwer zugängliche Bereichen des** 6 **Internet**

7 Der überwiegende Teil krimineller Inhalte und die Dokumentationen schwerer
8 Missbrauchstaten befinden sich nicht im leicht zugänglichen World Wide Web,
9 sondern in Foren, Tauschbörsen und geschlossenen Benutzergruppen.

10 Hier ist eine massive Ausweitung der Ermittlungsbemühungen daher unerlässlich.
11 Eine Konzentration auf frei zugängliche Seiten hieße, nur an der Spitze des
12 Eisbergs zu ermitteln. Für diese Ermittlungszwecke ist ein Modell von Online-
13 Streifen auszubauen, damit Konsumenten krimineller Inhalte noch möglichst
14 während der Tat dingfest gemacht werden können.

15 Bei geschützten oder verschlüsselten Foren, in denen auch Maßnahmen
16 herkömmlicher Telekommunikationsüberwachung nicht zum Ziel führen, ist der
17 Einsatz von verdeckten Ermittlern und nicht offiziell ermittelnden Polizeibeamten
18 (auf dienstliche Weisung ermittelnde Polizeibeamter, die ihre Identität nach außen
19 nicht preisgeben, ohne dabei verdeckte Ermittler zu sein) zu erwägen. Dafür
20 muss der Gesetzgeber keine neuen Ermittlungsbefugnisse schaffen: Der Einsatz
21 von verdeckten Ermittlern (§ 110a Abs. 1 Nr. 3 StPO) ist hier schon nach heutiger
22 Rechtslage zulässig. Denn bei Tauschringen und geschlossenen Foren ist eine
23 gewerbsmäßige oder zumindest eine gewohnheitsmäßige Nutzung in der Regel
24 anzunehmen. Der Einsatz von nicht offiziell ermittelnden Polizeibeamten ist
25 sinnvoll und zulässig in Bereichen, in denen eine auf Dauer angelegte Legende
26 oder veränderte Identität von Personen nicht erforderlich ist, wie zum Beispiel in
27 Chatforen. Die ermittelnden Beamten machen sich auch nicht strafbar, weil schon
28 der Tatbestand nicht gegeben ist. Jedenfalls aber wären sowohl verdeckte
29 Ermittler, als auch nicht offiziell ermittelnde Polizeibeamte nach § 184 b Abs. 5
30 StGB strafrechtlich privilegiert. Beide handeln in Erfüllung ihrer dienstlichen
31 Pflichten. Ein wohlabgewogener Einsatz von verdeckten Ermittlern und nicht
32 offiziell ermittelnden Polizeibeamten macht grundrechtlich bedenkliche ungezielte
33 Massenüberwachungen und verfassungswidrige Online-Durchsuchungen bzw.
34 Quellen-Telekommunikationsüberwachungen auch ermittlungstaktisch überflüs-
35 sig.

1 Dazu ist es nicht nötig, neue Privilegierungen § 184b Abs. 5 StGB einzuführen.
2 Die Begehung sogenannter millieubedingter Straftaten ist im deutschen Recht
3 insgesamt nicht zulässig. Dabei soll es bleiben.
4

5 **3. Verdachtsgestützte Überprüfung der Zahlungsströme im Online-Bereich**

6 In Zusammenarbeit mit der Kreditkartenwirtschaft sind Methoden zu entwickeln,
7 mit denen inländische Kunden ausländischer Anbieter von Missbrauchsdarstel-
8 lungen aufgespürt werden können. Insbesondere die Zahlungsströme über das
9 Internet stehen dabei im Fokus.

10 Anhand mehrerer Kriterien ist die Fahndung möglichst gezielt auszugestalten.
11 Große Teile der Bevölkerung zunächst abstrakt zu verdächtigen und damit
12 Fehlermittlungen gegen Unschuldige in großer Zahl zu riskieren, darf dagegen
13 kein Regelfall werden. Das Überschreiten der Grenze vom Anfangsverdacht zum
14 Generalverdacht ist zu vermeiden.

15 Ist der Strafverfolgungsbehörde eine Internetseite bekannt, die den Zugang zu
16 kinderpornographischen Inhalten vermittelt, ist es nach der höchstrichterlichen
17 Rechtsprechung auf der Ermächtigungsgrundlage des § 161a StPO zulässig,
18 eine Abfrage von Kreditkartendaten durchzuführen. Dies ist zielführend, da der
19 Zugang zu Internetseiten mit kinderpornographischen Inhalten meist gegen
20 Zahlung eines bestimmten Betrages erfolgt, der regelmäßig über eine Kreditkarte
21 abgerechnet wird. Die Kreditkartenabrechnung weist den Zahlungsempfänger
22 und den Zahlungsbetrag aus. Mittels dieser Eckdaten kann ein maschineller
23 Abgleich bei Kreditkarteninstituten erfolgen. Mit der durchgeführten Abfrage der
24 Kreditkartendaten kann gezielt nach Personen gesucht werden, die eine genau
25 bezeichnete, nach dem jeweiligen Ermittlungsstand mit hinreichender
26 Wahrscheinlichkeit strafbare Handlung vorgenommen haben. Kreditkartenin-
27 haber, zu denen keine solche Abbuchung gespeichert ist, werden dagegen nicht
28 als „Treffer“ angezeigt. Durch eine erweiterte Plausibilitätsprüfung ist
29 sicherzustellen, dass nicht Opfer von Kartendatendiebstählen (Phishing-Opfer)
30 Ermittlungen ausgesetzt werden. Das Ergebnis der Nichttreffer wird weder
31 gespeichert noch an die Strafverfolgungsbehörde übermittelt.

32 Eine Anmeldung verdeckter Ermittler bei kommerziellen Internetanbietern der
33 Darstellungen von Kindesmissbrauch zur Bestimmung des Zahlungsempfängers
34 wird nur in engen Grenzen zulässig sein. Die Begehung szenetypischer Straftaten
35 durch verdeckte Ermittler ist abzulehnen.

1 Mittels dieses Ermittlungsansatzes lassen sich unter Wahrung des Verhältnis-
2 mäßigkeitsgrundsatzes sowohl Konsumenten und Anbieter von Darstellungen
3 des Kindesmissbrauchs identifizieren als auch potentielle Konsumenten und
4 Anbieter abschrecken.

6 **4. Präzisierung der Privilegierung in § 184b Abs. 5 StGB**

7 Im Rahmen der Zusammenarbeit mit dem Bundeskriminalamt ist es regelmäßig
8 notwendig, dass Mitarbeiter von Internet-Beschwerdestellen die Netzadressen
9 oder sonstige elektronische Fundstellen der Ihnen bekanntgewordenen Angebote
10 mit Missbrauchsdarstellungen an die Behörde weitergeben. Zur Absicherung
11 dieser Praxis ist es erforderlich, die notwendigen Handlungen rechtssicher unter
12 die Privilegierung aus § 184b Absatz 5 StGB einordnen zu können. Nach dieser
13 Vorschrift bleibt die Besitzverschaffung von Darstellungen von Kindesmissbrauch
14 straflos, solange sie ausschließlich der Erfüllung rechtmäßiger dienstlicher oder
15 beruflicher Pflichten dienen.

17 **5. Überprüfung der Strafandrohung in § 184b Abs. 4 StGB**

18 Die Strafdrohung für den Besitz und die Besitzverschaffung von Missbrauchs-
19 darstellungen in § 184b Absatz 4 StGB ist auf ihre Abschreckungswirkung hin zu
20 überprüfen. Wertungswidersprüche zu anderen Delikten müssen vermieden
21 werden. Mit der Strafandrohung einer Freiheitsstrafe von maximal zwei Jahren
22 hat das Delikt immer noch den Charakter eines „Kavaliersdelikts“, obwohl die
23 Konsumenten von Missbrauchsdarstellungen an Kindern die entscheidenden
24 Anreize für die Herstellung von Missbrauchsdarstellungen setzen und damit für
25 die Zunahme von Missbrauchshandlungen zu diesem Zweck sorgen. Eine
26 Erhöhung des Strafrahmens kann der mittelbaren Förderung sexuellen Miss-
27 brauchs entgegenwirken.

29 **III. Bekämpfung von Datenschutzverstößen**

31 Datenschutz gewinnt im Informationszeitalter erheblich an Bedeutung.
32 Datenschutz ist kein Täterschutz. Vielmehr müssen Datenschutzverstöße mit der
33 angemessenen Härte des Gesetzes geahndet werden. Notwendig ist ein
34 modernes und technikneutrales Datenschutzrecht, das die illegale Verwendung
35 von Daten erschwert und angemessen sanktioniert.

1 Insbesondere im Bereich des Internets und der elektronischen Datenverarbeitung
2 brauchen wir ein starkes Sanktionsregime, um Datenmissbrauch zu bekämpfen.
3 Zur Bekämpfung von Kriminalität im Internet gehört als elementarer Bestandteil
4 eine Stärkung des Datenschutzes, da dieser auch kriminalpräventive Wirkung
5 entwickelt. Datenmissbrauch und Datendiebstahl bilden für viele Straftaten erst
6 die Grundlage. Ein strikter Datenschutz führt zu weniger Kriminalität. Datenschutz
7 ist Schutz der Menschen vor Straftaten.