An die
Abgeordneten der FDP-Fraktion des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

10. Juni 2011

Intelligente Strategien für ein sicheres Netz – IP-Vorratsdatenspeicherung stoppen!

Sehr geehrte Damen und Herren,
sehr geehrte Abgeordnete des Deutschen Bundestages,

die FDP betrachtet sich als Partei der Grundrechte und des Rechtsstaats. Eine freiheitliche Politik muss sicherstellen, dass Straftaten wirksam verfolgt werden – im Internet wie in der realen Welt. Gleichzeitig muss liberale Politik die Meinungs- und Pressefreiheit sowie die persönlichen, sozialen, kulturellen und wirtschaftlichen Entfaltungsmöglichkeiten in unserer Informationsgesellschaft berücksichtigen.

Der Gesetzentwurf des Bundesjustizministeriums, auf dessen Grundlage ein Kompromiss mit der Union in Sachen Vorratsdatenspeicherung erarbeitet werden soll, enthält einerseits den Vorschlag einer schnellen anlassbezogenen Sicherung von Telekommunikations-Verkehrsdaten, wenn diese voraussichtlich zur Aufklärung des konkreten Verdachts einer Straftat benötigt werden („Quick Freeze“). Andererseits wird dann aber vorgeschlagen, Internet-Zugangsanbieter zu verpflichten, flächendeckend und ohne Anlass für die Dauer von sieben Tagen auf Vorrat zu speichern, wer wann unter welcher IP-Adresse mit dem Internet verbunden war. Solche Protokolle sollen es Staatsbeamten ermöglichen, schon bei dem Verdacht einer Bagatellstraftat die Identität des Nutzers einer IP-Adresse ohne richterliche Anordnung offenlegen zu lassen, voraussichtlich aber auch schon präventiv sowie für geheimdienstliche Ermittlungen (§ 113 TKG). Alleine die Deutsche Telekom AG musste 2010 täglich über 50 Staatsanfragen nach der Identität des Nutzers einer IP-Adressen beantworten.

1. IP-Vorratsdatenspeicherung schafft den gläsernen Internetnutzer

Bei der Information, wer wann unter welcher IP-Adresse mit dem Internet verbunden war, handelt es sich um Telekommunikations-Verkehrsdaten, die – nicht anders als Telefon-Verbindungsdaten – dem Schutz des Fernmeldegeheimnisses unterliegen. Eine kompetente Netzpolitik begreift IP-Adressen nicht als „Telefonnummer“ oder „Kfz-Kennzeichen des Internets“. Mit dem Telefon oder dem Pkw lesen wir keine Zeitung, recherchieren wir keine Informationen, schauen uns keine Produkte an und veröffentlichen wir keine Kommentare. Normalerweise schreibt niemand mit, von welchen Rufnummern er angerufen oder von welchen Pkws er aufgesucht wird. Genau diese minuziöse Verhaltensprotokollierung wird aber im Internet praktiziert. Insofern trifft die Annahme des Bundesverfassungsgerichts, das Telemediengesetz verhindere grundsätzlich die Rekonstruierbarkeit der Internetnutzung, in der Praxis bei den meisten deutschen und bei fast allen internationalen Internetdiensten nicht zu.

Eine identifizierte IP-Adresse ermöglicht zwar für sich genommen noch keinen unmittelbaren Rückschluss auf Gesprächspartner. In Verbindung mit Internet-Nutzungsdaten, die staatliche Stellen ohne richterliche Anordnung bei Internetanbietern wie Google anfordern können (§ 15 Abs. 5 S. 4 TMG), lässt sich mit einer identifizierten IP-Adresse aber sogar der Inhalt der Telekommunikation einer Person nachvollziehen, also wer wonach im Internet gesucht, sich wofür interessiert und welchen Beitrag veröffentlicht hat. Information und Meinungsäußerung ohne Furcht vor Nachteilen werden durch eine IP-Vorratsdatenspeicherung unmöglich. Ist ein Pseudonym (Benutzerkonto) über die IP-Adresse des Nutzers erst einmal identifiziert, ermöglichen Nutzungsdaten des Anbieters oft die Rückverfolgung jedes Klicks und jeder Eingabe des Inhabers über Tage, Wochen oder Monate hinweg. Daneben wird in die meisten E-Mails die IP-Adresse des Absenders aufgenommen, ohne dass man einfach eine Unterdrückung dieser „Rufnummernübermittlung“ wählen könnte. Durch eine IP-Vorratsdatenspeicherung werden Meinungsäußerungen per E-Mail ohne Furcht vor Nachteilen unmöglich. Schließlich ermöglichen es IP-Adressen gerade beim mobilen Internetzugang, Bewegungsprofile zu erstellen, weil aus der jeweiligen IP-Adresse der ungefähre Standort des Nutzers ermittelt werden kann.

Derzeit speichern nur einzelne Internet-Zugangsanbieter die Zuordnung von IP-Adressen einige Tage lang auf Vorrat. Die Zulässigkeit dieser Praxis ist Gegenstand laufender Gerichtsverfahren und bereits von mehreren Gerichten rechtskräftig verneint worden. Jedenfalls kann man sich derzeit vor einem Bekanntwerden sensibler Informationen über die eigene Internetnutzung durch Inanspruchnahme eines nicht auf Vorrat speichernden Internet-Zugangsanbieters (z. B. Freenet, Hansenet) schützen. Im Fall einer allgemeinen Zwangsspeicherfrist wäre dies nicht mehr möglich. Datenschutz durch marktwirtschaftlichen Wettbewerb ist eine liberale Lösung, die ein Speicherzwang auslöschen würde.

Eine allgemeine IP-Vorratsdatenspeicherung träfe junge Menschen und zukünftige Generationen, deren privater und beruflicher Alltag sich zu einem immer größeren Teil im Internet abspielt, in ungleich gewaltigerem Ausmaß als internetfernere Generationen. Sie ermöglichte es Staatsbeamten, einen bislang ungeahnten Teil unseres Privat- und Berufslebens aufzudecken. In

den Worten des Bundesverfassungsgerichts: Es handelte sich um einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Die anlasslose Speicherung von Internet-Verbindungsdaten ist „geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann“, nämlich in allen Bereichen, in denen das Internet zum Einsatz kommt.

2. Strafverfolgung funktioniert ohne Vorratsdatenspeicherung

Der von dem Bundesjustizministerium erarbeitete Vorschlag einer flächendeckenden Internet-Verbindungsdatenspeicherung, der auch für viele FDP-Abgeordnete völlig überraschend kam, basiert auf einem Bericht des Bundeskriminalamts, wonach im vergangenen Jahr 830 von 983 (84,4%) durch das BKA angeforderte Auskünfte über die Identität des hinter einer IP-Adresse stehenden Anschlussinhabers nicht erteilt worden seien, weil Internet-Zugangsanbieter nach dem Urteil des Bundesverfassungsgerichts keine Verbindungsdaten mehr speicherten.

Diese Zahl des Bundeskriminalamts wirft mehr Fragen auf als sie beantwortet: Inwieweit beruhten erfolglose Anfragen auf Verzögerungen seitens des Bundeskriminalamts bei der Anforderung von Auskünften? Waren Anfragen des Bundeskriminalamts zu Zeiten der Vorratsdatenspeicherung nicht ebenso häufig erfolglos? Wie häufig wurden Ermittlungsverfahren trotz erfolgreicher Datenabfrage folgenlos eingestellt und sind erteilte Auskünfte mithin im Ergebnis ohne Nutzen? Diese und sieben weitere Fragen richtete der Arbeitskreis Vorratsdatenspeicherung an Bundeskriminalamt und Bundesinnenministerium – nicht eine Frage wurde beantwortet. Ohne Antworten auf die genannten Fragen können relevante Schlüsse aus den Zahlen des Bundeskriminalamts nicht gezogen werden.

Die Angaben des Bundeskriminalamts sind nicht aussagekräftig. So betrafen 147 der ergebnislosen Auskunftsersuchen des BKA Internetverbindungen, die im Zeitpunkt der Anfrage (25.05.2010) länger als sechs Monate zurück lagen (Zeitstempel: 29.05.2009-11.09.2009) und deswegen selbst im Fall einer sechsmonatigen Vorratsdatenspeicherung ergebnislos geblieben wären. Dr. Michael Kilchling vom Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat die BKA-Zahlen mit den Worten kommentiert: „Für eine seriöse wissenschaftliche Stellungnahme fehlt jede Basis“.

Die BKA-Zahlen betreffen nur einen sehr kleinen und nicht repräsentativen Ausschnitt aus der Kriminalitätswirklichkeit. 74,4% der in die BKA-Zahlen eingeflossenen, erfolglosen Anfragen zu IP-Adressen galten der Verfolgung der Verbreitung, des Erwerbs oder des Besitzes kinder- und jugendpornografischer Schriften, weil sich die Recherchestelle ZaRD des BKA schwerpunktmäßig damit befasst. Nur 3% der insgesamt an staatliche Stellen erteilten Auskünfte werden aber zur Strafverfolgung wegen pornografischer Schriften erteilt. Nicht mehr als 5.200 von 5.933.278 im Jahr 2010 polizeilich registrierten Straftaten betrafen die Verbreitung pornografischer Schriften im Internet, also weniger als 0,1% aller bekannten Straftaten. Die FDP darf vor dem Totschlagargument „Kinderpornografie“ nicht kapitulieren, sondern ist den 51 Mio. Internetnutzern in Deutschland eine sachliche Auseinandersetzung mit diesem Thema schuldig.

Der Vorschlag einer flächendeckenden Vorratsspeicherung von Internet-Verbindungsdaten lässt die Eigenheiten des Internets völlig außer Acht. Aus einer Untersuchung des Max-Planck-Instituts im Auftrag des Bundesjustizministeriums ist bekannt, dass 72% der Ermittlungsverfahren mit erfolgreicher Verbindungsdatenabfrage gleichwohl eingestellt wurden. Bei IP-Adressen ist selbst im Fall einer Vorratsdatenspeicherung eine Identifizierung des Täters häufig nicht möglich. In vielen Fällen verwenden Straftäter Internet-Cafés, offene Internetzugänge (WLAN), Anonymisierungsdienste, öffentliche Telefone, unregistrierte Handykarten usw., so etwa die mutmaßliche Düsseldorfer Qaida-Zelle. Laut einer Umfrage nutzen schon 12,8% der Internetnutzer einen Anonymisierungsdienst, weitere 33,6% beabsichtigten dies in Zukunft. Ein Anonymisierungsdienst ersetzt die IP-Adresse des Kunden durch eine andere, nicht rückverfolgbare IP-Adresse. Solche Dienste werden für ein geringes monatliches Pauschalentgelt in Deutschland, Europa und weltweit legal angeboten. Eine seriöse Rechtspolitik setzt auf Strafverfolgungsmaßnahmen, die einen ernsthaften Beitrag zur Aufklärung von Straftaten leisten. Damit muss eine Vorratsdatenspeicherung bei Internet-Zugangsanbietern, die auf vielfältige Weise schon mit geringem Aufwand umgangen werden kann, ausscheiden.

Eine moderne und zukunftsfähige Internetpolitik setzt Internetnutzer keinen Überwachungsmaßnahmen aus, die bei vergleichbaren Tätigkeiten außerhalb des Internet unbekannt sind. Wer außerhalb des Internets Bücher liest, fernsieht oder CDs tauscht, hinterlässt keine identifizierbaren Spuren. Es gibt keinen Grund, weshalb dies im Internet anders sein sollte. Es ist nicht zu rechtfertigen, dass Anrufe mit unterdrückter Rufnummernanzeige bei Telefon-Flatrates ebenso spurenlos möglich bleiben sollen wie postalische Meinungsäußerungen ohne Absender und mündliche Äußerungen gegenüber Unbekannten, dass einzig im Internet aber potenziell jede E-Mail und jeder Kommentar anhand einer auf Vorrat gespeicherten IP-Adresse identifizierbar bleiben soll.

Im Internet begangene Straftaten werden auch ohne Vorratsspeicherung von Internet-Zugangsdaten deutlich häufiger aufgeklärt als außerhalb des Internet begangene Straftaten. Die Kriminalstatistik für das Jahr 2010, also im Wesentlichen nach dem Ende der Vorratsdatenspeicherung, belegt: Im Jahr 2010 wurden auch ohne Vorratsdaten fast drei von vier Internetdelikten aufgeklärt (71%). Damit waren im Internet begangene Straftaten auch ohne Vorratsdatenspeicherung deutlich häufiger aufzuklären als außerhalb des Internet begangene Straftaten (55%). Auch die Verbreitung von „Kinderpornografie“ wurde nach dem Ende der Vorratsdatenspeicherung deutlich häufiger aufgeklärt (79%) als außerhalb des Internet begangene Straftaten. Vor diesem Hintergrund besteht keinerlei Rechtfertigung für ein Anonymitätsverbot gerade im Internet.

Dass die Speicherung nur der Daten von Verdächtigen eine wirksame Verfolgung auch von Internetdelikten ermöglicht, zeigt die Praxis vieler Staaten weltweit. Sicherlich will niemand ernsthaft behaupten, dass in Staaten wie Österreich, Schweden oder Kanada das Internet ein rechtsfreier Raum sei, weil Internet-Verbindungsdaten dort wie in Deutschland mit Verbindungsende zu löschen sind.

Umgekehrt droht eine IP-Vorratsdatenspeicherung die Strafverfolgung im Internet massiv zu beeinträchtigen. Schon die Einführung der letzten Internet-Vorratsdatenspeicherung im Jahr 2009 führte dazu, dass 46,4% aller Internetnutzer Anonymisierungsdienste nutzten oder nutzen wollten und 24,6% öffentliche Internet-Cafés. Im Ergebnis war trotz sechsmonatiger IP-Vorratsdatenspeicherung nur ein geringerer Teil der registrierten Internetdelikte (75,7%) aufzuklären als noch im Vorjahr ohne IP-Vorratsdatenspeicherung (79,8%)! Eine IP-Vorratsdatenspeicherung fördert Vermeidungsverhalten, welches die Verhinderung und Verfolgung selbst schwerer Straftaten erschwert. Denn Vermeidungsmaßnahmen können zugleich verdachtsabhängige Telekommunikationsüberwachungsmaßnahmen vereiteln, wie sie ohne Vorratsdatenspeicherung noch möglich sind. Dadurch entfaltet eine Vorratsdatenspeicherung auf Gefahrenabwehr und Strafverfolgung kontraproduktive Wirkungen und verkehrt den erhofften Nutzen der Maßnahme in sein Gegenteil.

3. IP-Vorratsdatenspeicherung ist schädlich für Deutschland

Auf der anderen Seite hätte eine verdachtslose Vorratsspeicherung von Internet-Verbindungsdaten massive Nachteile für Bürger, aber auch für Unternehmen, Ärzte, Rechtsanwälte, Psychologen, Beratungsstellen und viele mehr zur Folge: Im Zuge einer IP-Vorratsdatenspeicherung würden ohne jeden Verdacht einer Straftat Informationen gesammelt, die die Rückverfolgung praktisch jeden Klicks und jeder Eingabe im Internet von über 80 Millionen Bundesbürgerinnen und Bundesbürgern ermöglichen würden. Dies würde Datenpannen und -missbrauch begünstigen. Eine IP-Vorratsdatenspeicherung würde daneben das permanente Risiko schaffen, unschuldig einer Straftat verdächtigt, einer Wohnungsdurchsuchung oder Vernehmung unterzogen oder abgemahnt zu werden, denn Verbindungsdaten lassen nur auf den Inhaber eines Anschlusses rückschließen und nicht auf dessen Benutzer.

Diese Risiken würden eine enorme Abschreckungswirkung entfalten und eine unbefangene Internetnutzung in sensiblen Situationen vereiteln (z.B. anonyme Information von Journalisten per E-Mail, anonyme Meinungsäußerung im Internet, vertraulicher Austausch von Geschäftsgeheimnissen, vertrauliche Koordinierung politischer Proteste, psychologische, medizinische und juristische Beratung und Selbsthilfegruppen von Menschen in besonderen Situationen wie Notlagen und Krankheiten). Eine IP-Vorratsdatenspeicherung würde den Schutz journalistischer Quellen untergraben und damit die Pressefreiheit im Kern beschädigen. Sie würde auch Anwalts-, Arzt-, Seelsorge-, Beratungs- und andere Berufsgeheimnisse aushöhlen. Wenn gefährliche oder gefährdete Menschen nicht mehr ohne Furcht vor Nachteilen Hilfe suchen können, verhindert dies eine sinnvolle Prävention und kann sogar Leib und Leben Unschuldiger gefährden. Insgesamt stehen grundlegende Funktionsbedingungen unseres freiheitlichen demokratischen Gemeinwesens auf dem Spiel.

Jede massenhafte Erfassung des Informations- und Kommunikationsverhalten vollkommen Unschuldiger verstößt gegen die EU-Grundrechtecharta und die Europäische Menschenrechtskonvention. Der EU-Gerichtshof, der Europäische Gerichtshof für Menschenrechte und der Rumänische Verfassungsgerichtshof haben flächendeckende Veröffentlichungen,

Erfassungen oder Aufzeichnungen persönlicher Daten bereits als unverhältnismäßig verworfen. Das Bundesverfassungsgericht hat in seiner Entscheidung zur Vorratsdatenspeicherung nur das Grundgesetz angewandt, nicht aber die ebenfalls zu beachtende EU-Grundrechtecharta und die Europäische Menschenrechtskonvention geprüft.

Der Vorschlag einer Vorratsspeicherung von IP-Adressen lässt auch vollkommen die technische Entwicklung außer Acht. Mit der ab Ende 2011 geplanten Umstellung des Internets auf das neue Adress-System „IPv6“ droht die individuelle Verfolgbarkeit jedes unserer Online-Schritte über lange Zeiträume hinweg. Denn die neuen Internet-Adressen verändern sich fast nie – im Gegensatz zu der derzeitigen, veränderlichen Nummernzuteilung. Mit einer einzigen polizeilichen Abfrage der IP-Adresszuordnung und nachfolgenden Anfragen an die privaten Anbieter nach Logdateien kann künftig auf Monate hinaus ein Online-Leben nachvollzogen werden. Aus Gründen des Datenschutzes ist es dringend geboten, weiterhin eine häufig wechselnde Vergabe vorzuschreiben. Der Vorschlag einer Vorratsdatenspeicherung geht genau in die falsche Richtung.

Besonders Sorgen macht uns, dass die FDP im Bereich des Internetzugangs erstmals eine Abkehr von dem rechtsstaatlichen Grundsatz der Verdachtsabhängigkeit von Ermittlungsmaßnahmen und einen Einstieg in die Logik einer vorsorglichen Massenerfassung Unschuldiger ins Blaue hinein vollziehen würde, indem sie eine flächendeckende Informationssammlung über Verhalten der gesamten Bevölkerung erstmals als notwendig und verhältnismäßig anerkennen würde. Ist dieser Damm einmal gebrochen und ein Präzedenzfall geschaffen, dann könnte die FDP dem unersättlichen Hunger von Sicherheitsideologen nach immer weiteren potenziell nützlichen Informationen über die gesamte Bevölkerung (z. B. Telefonverbindungsdaten und -standortdaten bei Flatrates, Reisedaten, Büchereidaten, Bestelldaten, Internet-Nutzungsdaten) zukünftig keinen grundsätzlichen Einwand mehr entgegen setzen.

Eine IP-Vorratsdatenspeicherung unter Beachtung der verfassungsrechtlichen Vorgaben würde die über 6.000 betroffenen Telekommunikationsunternehmen und deren Kunden schon wegen der hohen Sicherheitsanforderungen Millionen von Euro kosten. Dies zöge Preiserhöhungen nach sich, führte zur Einstellung von Angeboten und belastete mittelbar auch die Verbraucher. Um Kosten zu vermeiden, bestünde die Gefahr, dass die Anbieter einfach auf der Grundlage des § 100 TKG ohne Sicherheitsvorkehrungen auf Vorrat speichern würden, um die Daten auch für eigene Zwecke und zur millionenfachen Auskunfterteilung an Private (§ 101a UrhG) verwenden zu können. Ungelöst ist auch die Frage, wie für die vom Bundesverfassungsgericht angesprochenen, auf besondere Vertraulichkeit angewiesenen Verbindungen im Internetbereich ein grundsätzliches Übermittlungsverbot vorgesehen werden soll. Internetanbieter können nicht wissen, ob eine Internetverbindung der anonymen Kontaktaufnahme zu Beratungsstellen oder Journalisten gedient hat.

Dementsprechend ist der Vorstoß des Bundesjustizministeriums unter anderem bei dem Arbeitskreis Vorratsdatenspeicherung, dem Deutschen Journalistenverband, dem Chaos Computer Club, der Neuen Richtervereinigung, dem LSVD und dem Verband der deutschen Internetwirtschaft (eco) auf Ablehnung gestoßen.

4. Sexuellem Kindesmissbrauch wirksam begegnen

Dem Bundesjustizministerium zufolge soll eine Rückverfolgbarkeit jeder Internetnutzung „insbesondere zum Vorgehen gegen Kinderpornografie“ geschaffen werden. Das Ziel, Kinder zu schützen und sowohl ihren Missbrauch als auch dessen Dokumentation zu verhindern, stellen wir keineswegs in Frage. Alle hierzu geeigneten, erforderlichen und angemessenen Mittel, die nicht mehr schaden als sie nutzen, müssen eingesetzt werden. Gerade wegen der hohen Bedeutung der Rechte von Kindern und der Abscheulichkeit ihres Missbrauchs aber dürfen dringend benötigte Ressourcen nicht für wirkungslose oder gar kontraproduktive Maßnahmen verschleudert werden. Sexuell missbrauchte Kinder dürfen nicht politisch ein zweites Mal für Vorhaben missbraucht werden, die in Wahrheit keinen Beitrag zum Kinderschutz leisten. Nach unserer Überzeugung ist genau dies bei einer generellen und pauschalen Vorratsspeicherung der Identität vollkommen unverdächtiger Internetnutzer der Fall.

▶ IP-Vorratsdatenspeicherung ist ungeeignet zum Schutz von Kindern

Eine Vorratsspeicherung der IP-Adressen Unverdächtiger ist zum Schutz von Kindern denkbar ungeeignet, wie an vielen Stellen offengelegt und von Experten aus den unterschiedlichsten Bereichen mehrfach bestätigt worden ist. Eine Vorratsdatenspeicherung hatte weder in Deutschland noch hat sie im Ausland irgend einen messbaren Einfluss auf die körperliche und seelische Unversehrtheit missbrauchter Kinder.

Zunächst einmal geht die strafrechtliche Verfolgung von „Kinderpornografie“ von vornherein an dem größten Teil des Problems sexuellen Kindesmissbrauchs vorbei. Der Anteil von Kinderpornografiedelikten an allen polizeilich bekannten Delikten gegen die sexuelle Selbstbestimmung ist mit 7% gering. Nur ausnahmsweise kann Opfern sexuellen Kindesmissbrauchs durch Ermittlungen wegen kinderpornografischer Darstellungen geholfen werden. Laut Kriminalstatistik werden nicht mehr als 1% der polizeilich registrierten Fälle von Kindesmissbrauch überhaupt fotografisch dokumentiert, meist von Familienmitgliedern oder nahen Verwandten. Den Hauptteil der Straftaten im Bereich des sexuellen Missbrauchs begehen nicht Pädophile, die sich für Darstellungen sexuellen Kindesmissbrauchs interessieren können, sondern Täter, die sich an ihrem Opfer als Ersatz für Sexualkontakt mit Erwachsenen vergehen. Überdies werden 90% aller Fälle von Kindesmissbrauch und sogar 98% der Fälle familiären Missbrauchs von Kindern der Polizei nie bekannt. Im Dunkelfeld kann Strafverfolgung von vornherein nicht weiter helfen. Es kommt hinzu, dass Kindesmissbrauch nicht identisch ist mit Strafbarkeit. Vernachlässigung und nicht-sexuelle Misshandlung kann ebenso schwerwiegende Folgen für Kinder haben, auch wo sie nicht strafbar ist.

In der Medienwirkungsforschung und sonstigen Wissenschaft ist umstritten, ob die Verfügbarkeit von Darstellungen sexuellen Missbrauchs das Risiko eigener Übergriffe der Konsumenten erhöht. Nach Angaben des renommierten Berliner Krankenhauses Charité kann nach gegenwärtigem Stand der Forschung nicht abschließend beurteilt werden, inwiefern der Konsum kinderpornografischer Materialien den Wunsch nach Realisierung eines tatsächlich direkten sexuellen Kontaktes mit einem Kind und dessen Umsetzung verstärkt. Der Klinik zufolge ist Pädophilie fester Bestandteil

der Persönlichkeit von geschätzt 200.000 Menschen in Deutschland und nicht „wegzutherapieren“. Therapieziel der Charité ist vielmehr, dass die pädophile Neigung der Betroffenen nur noch in deren Fantasie ausgelebt wird – dies kann um der Sicherheit von Kindern willen nicht verboten oder geächtet werden. In der Praxis soll es nach der Aufhebung oder Lockerung von Kinderpornografieverboten in Tschechien, Dänemark und Japan zu einem Rückgang der Kindesmissbrauchsfälle gekommen sein. Die faktisch erhöhte Verfügbarkeit von Darstellungen sexuellen Missbrauchs durch das Internet in Deutschland ist ebenfalls mit einem Rückgang der registrierten Fälle von Kindesmissbrauch einher gegangen. 2010 registrierte die Polizei die zweitniedrigste Zahl von Kindesmissbrauchsfällen seit 1987. Die Häufigkeit solcher Fälle geht bereits seit den 1950er Jahren deutlich zurück.

Noch zweifelhafter ist, ob der Versuch einer Intensivierung der schon heute wirksamen strafrechtlichen Verfolgung des Austauschs kinderpornografischer Darstellungen den Schutz von Kindern vor sexuellen Übergriffen erhöhen kann. Jedenfalls ist nicht belegt oder auch nur plausibel, dass gerade eine IP-Vorratsdatenspeicherung auch nur ein Kind vor sexuellem Missbrauch schützen könnte. Weder aus Deutschland noch aus einem anderen Staat der Welt ist bekannt, dass die Zahl von Missbrauchsfällen nach Einführung einer Vorratsdatenspeicherung stärker zurückgegangen wäre. Bei den ausführlichen Diskussionen des Runden Tisches der Bundesregierung zu sexuellem Kindesmissbrauch ist eine Vorratsdatenspeicherung zu Recht von keiner Arbeitsgruppe empfohlen worden.

Wir sind zwar der Meinung, dass der Staat zum Schutz von Kindern für ein ernsthaftes Entdeckungsrisiko sorgen muss, um potenzielle Täter von entsprechenden Straftaten abzuschrecken. Werden auch ohne Vorratsdatenspeicherung die meisten Fälle sexuellen Kindesmissbrauchs und des Austauschs von „Kinderpornografie“ aufgeklärt, ist diese Abschreckungswirkung aber ausgeschöpft. Es gibt keinen Beleg dafür und ist kriminologisch unwahrscheinlich, dass eine – unterstellt – um einige Prozentpunkte höhere Aufklärungsquote die Entscheidung potenzieller Täter für oder gegen einen Kindesmissbrauch beeinflussen könnte. Tatsächlich ist eine höhere Aufklärungsquote nicht zu erwarten. Die Berliner Charité hat festgestellt, dass Konsumenten von „Kinderpornografie“ im Umgang mit Computern geübt sind. Geübte Computernutzer können eine IP-Vorratsspeicherung bei ihrem Internet-Zugangsanbieter aber jederzeit durch Zwischenschaltung eines in- oder ausländischen Anonymisierungsdienstes ausschalten, weshalb eine IP-Vorratsspeicherung gerade in diesem Bereich aussichtslos ist. Nach Einführung einer sechsmonatigen IP-Vorratsdatenspeicherung in Deutschland zum 01.01.2009 ist die Aufklärungsquote im Bereich der Verbreitung pornografischer Schriften über das Internet sogar von zuvor 87,5% auf 83,8% gefallen.

▶ **Anonyme Internetnutzung schützt Kinder**

Anonyme Internetnutzung ist nicht Ursache sexuellen Missbrauchs, sondern wichtige Voraussetzung für dessen Bewältigung. Gerade für Missbrauchsbetroffene ist es häufig hilfreich, im Schutz der Anonymität ohne Angst vor Bloßstellung relativ frei über den erlittenen Missbrauch sprechen und sich austauschen zu können. Eine unterschiedslose IP-Vorratsdatenspeicherung würde Opfern und potenziellen Opfern sexuellen Missbrauchs massiv schaden, indem sie

tausenden von Opfern und auch Tätern den Zugang zu anonymen Beratungs-, Selbsthilfe- und Therapieangeboten verschließen würde. Gerade im Bereich des sexuellen Missbrauchs sind Opfer und Täter meist nur im Schutz absoluter Anonymität bereit, sich zu informieren und Hilfe anzunehmen, da sie andernfalls soziale Ächtung oder – bei Tätern – strafrechtliche Verfolgung befürchten. Beispielsweise bietet die Berliner Charité nicht justizbekannten, hilfesuchenden Pädophilen die Möglichkeit einer vollkommen anonymen Therapie, um (weitere) Übergriffe zu verhindern. Therapiewillige können sich unter anderem per Internet informieren und per E-Mail anonym melden. Eine Rückverfolgbarkeit jedes Interessenten anhand der IP-Adresse würde die Therapie potenzieller Täter und damit den Schutz deren potenzieller Opfer auf das Spiel setzen. Eine Einschränkung der Möglichkeiten anonymer Hilfe vertieft das Leiden von Opfern und führt, wo die Therapie von Tätern vereitelt wird, zu weiterem Kindesmissbrauch. Es ist unverantwortlich, den Wunsch von Strafverfolgern nach Überführung möglichst noch des letzten Delinquenten über den Schutz und das Wohl von Kindern zu stellen.

Auch der Strafverfolgung selbst würde eine IP-Vorratsdatenspeicherung schaden: Nicht ohne Grund ermöglichen die meisten Internet-Beschwerdestellen in Europa anonyme Anzeigen kinderpornografischer Inhalte. Wer auf solche Inhalte stößt, ist wegen des Risikos sozialer Ächtung oder strafrechtlicher Verfolgung meist nur im Schutz absoluter Anonymität bereit, dies zu melden. Die Anonymität als zentrale Voraussetzung von Anzeigen kinderpornografischer Darstellungen im Internet entfiele durch eine IP-Vorratsdatenspeicherung.

▶ **Wirksamer Kinderschutz: Retten statt Mitschreiben!**

Der richtige Weg, um sexuellem Missbrauch und dessen Dokumentation wirksam entgegen zu treten, ist nach unserer Überzeugung die Förderung von Präventionsmaßnahmen und -projekten, deren Wirksamkeit wissenschaftlich belegt ist. Der Fokus sollte dabei auf Maßnahmen gegen Missbrauch gelegt werden, der vor Ort im eigenen Umfeld der Zielgruppe geschieht. Sexueller Missbrauch findet in Schulen, in Kindergärten, in Kinderheimen, in Internaten, in Sportvereinen, in Jugendvereinen und in den Familien der Opfer statt, so dass dort zuerst angesetzt werden muss. Angebote einer qualifizierten Therapie sowie eine angemessene Entschädigung der Opfer sexuellen Missbrauchs müssen selbstverständlich sein.

Daneben sind anonyme Beratungs- und Therapieangebote für potentielle Täter im Vorfeld sexueller Übergriffe ein wirksames Mittel zum Kinderschutz. Es ist ein Skandal, dass etwa die Berliner Charité gegenwärtig nur der Hälfte der Pädophilen, die sich freiwillig einer anonymen Therapie unterziehen möchten, einen Platz anbieten kann, dass Krankenkassen diese Behandlung nicht zahlen und dass das Therapieangebot in zwei Jahren mangels Finanzierung ganz auslaufen muss. Dass sich das politische und finanzielle gesellschaftliche Engagement bisher nahezu ausschließlich auf rechtsbekannte und rechtskräftig verurteilte Sexualstraftäter, also auf Täter aus dem Hellfeld richtet, ist ein Fehler. Klinische Erfahrungen zeigen, dass rechtskräftig verurteilte Sexualstraftäter für therapeutische Angebote oft nur noch schwer zugänglich sind, da sie ihr Innenleben aus Angst vor rechtlichen Nachteilen im Strafvollzug vor Therapeuten abschirmen.

Kontraproduktiv ist auch das gegenwärtige Klima einer Verteufelung der als solchen unheilbaren Pädophilie, weil dies die Betroffenen von einer Therapie mit dem Ziel eines gefahrlosen Lebens mit ihrer Neigung abhält.

Werden neue Darstellungen sexuellen Missbrauchs aufgefunden, so muss die Identifikation der abgebildeten Opfer an erster Stelle stehen. Daneben sollten die Anstrengungen zur Löschung kinderpornografischen Materials verstärkt werden. Im Zeitalter des Internet ist dazu nur eine internationale Zusammenarbeit aussichtsreich. Die grenzüberschreitende Löschung von Darstellungen sexuellen Missbrauchs bereitet derzeit offensichtlich Probleme. Ziel einer internationalen Zusammenarbeit muss es daher sein, sich völkerrechtlich darauf zu verständigen, die Verbreitung von Inhalten, die den universellen Menschenrechten widersprechen, allgemein zu unterbinden. Insbesondere erscheint ein internationales Abkommen zur grenzüberschreitenden Löschung von Darstellungen sexuellen Kindesmissbrauchs sinnvoll. Selbst das 2000 von der UN erarbeitete Fakultativprotokoll zum Übereinkommen über die Rechte des Kindes betreffend den Verkauf von Kindern, Kinderprostitution und Kinderpornografie ist gegenwärtig aber von vielen europäischen Staaten noch nicht ratifiziert worden.

An diesen Problemen muss gearbeitet werden, anstatt eine untaugliche und grundrechtswidrige Vorratsspeicherung der Identität zu 99,6% vollkommen unverdächtiger Internetnutzer voranzutreiben, die das Risiko von Kindesmissbrauch sogar erhöhen könnte. Zu Recht spielt eine Vorratsdatenspeicherung bei der ausführlichen Expertendiskussion am Runden Tisch der Bundesregierung zu sexuellem Kindesmissbrauch keine Rolle. Ständige Forderungen nach einer Vorratsdatenspeicherung lenken von den eigentlichen Defiziten bei dem Schutz von Kindern ab, die sich nicht durch plakative Forderungen und für den Staat kostenlose Paragrafen beseitigen lassen. Die Forderung einer Vorratsdatenspeicherung verringert den Antrieb für wirksames Handeln und schadet damit dem Kinderschutz.

Insbesondere vor dem Hintergrund der Debatte um Internetsperren erschüttert uns, dass nun ein FDP-geführtes Ministerium mit demselben Totschlagargument „Kinderpornografie“ erneut einen massenhaften Grundrechtseingriff rechtfertigen will. Inzwischen ist man sich einig, dass das Löschen von Missbrauchsdarstellungen häufiger als erwartet zum Erfolg führt und Sperren deshalb verzichtbar sind. Auch die Aufklärung des Austauschs kinderpornografischer Darstellungen über das Internet ist nach dem Ende der Vorratsdatenspeicherung in den meisten Fällen erfolgreich. Befürchtungen eines weitgehend „rechtsfreien Raums Internet“ haben sich nicht bestätigt. Die Politik muss daher auf das von den Bürgern abgelehnte Mittel einer massenhaften Vorratsspeicherung der Identität vollkommen unverdächtiger Internetnutzer verzichten.

5. Internetkriminalität – Intelligente Strategien für ein sicheres Netz

Bei 97,9% der im Internet begangenen Straftaten und 99,9% der insgesamt in Deutschland registrierten Kriminalität handelt es sich nicht um den Austausch kinderpornografischer Darstellungen. Auch jenseits von „Kinderpornografie“ kann die Politik viel tun, um den Schutz vor Kriminalität im Internet zu optimieren. Einige Lösungsansätze existieren bereits, viele neue können erarbeitet werden. Eine IP-Vorratsdatenspeicherung ist allerdings keiner davon: weder für die zu schützenden Internetnutzer noch für unsere Informationsgesellschaft insgesamt.

Dies unterstreicht auch die 2010 eingesetzte Enquete-Kommission „Internet und digitale Gesellschaft“ des Deutschen Bundestages. Diese wurde nicht zuletzt wegen schlechter netzpolitischer Erfahrungen zu den Zeiten der Großen Koalition im Bund einberufen, um in Zukunft Fehlentscheidungen zu vermeiden. Die Regelung zur Vorratsdatenspeicherung, die vom Bundesverfassungsgericht als verfassungswidrig eingestuft wurde, das Zugangserschwerungsgesetz („Netzsperren“), das inzwischen allgemein als nicht zielführend angesehen wird und als Hauptgrund für das Erstarken der Piratenpartei gedeutet werden kann, und auch die Online-Durchsuchung („Bundestrojaner“), die ebenfalls von Karlsruhe einkassiert worden ist, sind Negativbeispiele der Vergangenheit. Die FDP-Bundestagsfraktion hat es nun in der Hand, ob diese unselige Liste erweitert werden muss.

▶ Wie ein besseres Vorgehen gegen Netzkriminalität jetzt schon möglich ist

Es gibt bereits gute Beispiele für modernen Schutz vor Internetkriminalität. Eine Schlüsselrolle spielt hierbei die Prävention, denn 82% aller polizeilich registrierten Internetdelikte sind Betrugsdelikte zulasten von Personen, die sich haben täuschen lassen. Hinzu kommt zunehmend Daten- und Identitätsdiebstahl unter Ausnutzung ungesicherter IT-Systeme (z.B. Trojaner) oder der Sorglosigkeit von Nutzern (z.B. Phishing) zur Vorbereitung von Betrug und anderer Straftaten.

Leicht verständliche Tipps und Anleitungen zum Schutz vor Netzkriminalität und zur Sicherung des eigenen Computers sind bereits entwickelt und veröffentlicht worden. Sie erreichen aber bislang nur sehr wenige Menschen. Wir könnten uns vorstellen, kurze Verhaltensempfehlungen für Erwachsene und Jugendliche als „Beipackzettel“ jedem neu verkauften Computer und Smartphone beizulegen.

Software zur Gewährleistung der Sicherheit des eigenen Computers ist bereits entwickelt und veröffentlicht worden. Sie aufzufinden, zu installieren und in Stand zu halten überfordert aber viele Menschen. Sinnvoll erschiene uns eine Hotline, die kostenfreie Beratung bei der Absicherung der eigenen Computer und bei der Beseitigung von Schadprogrammen anbietet. Wir könnten uns auch vorstellen, Hersteller und Anbieter kommerzieller Internetdienste zu verpflichten, gebrauchsfertige Geräte zur Internetnutzung sowie öffentliche Internetdienste so voreinzustellen und in Stand zu halten, dass die Vertraulichkeit, Verfügbarkeit und Unversehrtheit des Systems und der darauf gespeicherten Nutzerdaten dauerhaft nach den anerkannten Regeln der Technik gewährleistet ist (z.B. automatische Sicherheitspatches, Firewall, Schadprogrammerkennung). Der Nutzer muss allerdings stets die volle Kontrolle über Vorkehrungen zu seinem Schutz behalten und diese auch abschalten können.

Bestehende Datenschutzgesetze enthalten wichtige Vorgaben, die die Verfügbarkeit persönlicher Daten für Straftaten reduzieren und dadurch Identitätsdiebstahl und sonstigen Datenmissbrauch verhüten können. Leider läuft die Durchsetzung dieser Vorgaben im Internet weitgehend leer. Wir hielten es für sinnvoll, wenn Wettbewerber, Verbraucherzentralen und Datenschutzverbände das Recht gegeben würde, Datenschutzverstöße kommerzieller Anbieter von Internetdiensten abzumahnen. Auch sollte der Verlust persönlicher Daten durch kommerzielle Anbieter von Internetdiensten einen Anspruch der Betroffenen auf pauschale Entschädigung nach sich ziehen (z.B. 200 Euro pro Person). Schließlich sollte unterbunden werden, dass kommerzielle informationstechnische Produkte zur Verarbeitung personenbezogener Daten so vertrieben werden, dass der Verwender in der Voreinstellung „automatisch“ gegen deutsches Datenschutzrecht verstößt („privacy by design“).

Die Aufklärung von Internetkriminalität gelingt bereits jetzt in den meisten Fällen. Gleichwohl bestehen vielfältige Möglichkeiten für eine effizientere Strafverfolgung im Netz: Die Einrichtung leistungsfähiger Spezialdienststellen der Polizei und von Schwerpunktstaatsanwaltschaften zur Verfolgung von Computerkriminalität erscheint sinnvoll. Gefordert werden auch besonders qualifizierte Polizeibeamte und Staatsanwälte für diese Aufgaben, die Entwicklung eines Berufsbildes „Computerkriminalist“, die Entwicklung standardisierter Sachbearbeitungsverfahren auf nationaler und die Entwicklung von Standards für IT-Forensik auf internationaler Ebene.

Laut periodischem Sicherheitsbericht ist bei ca. 80% der Ermittlungen wegen Internetdelikten ein Zugriff auf im Ausland vorhandene Informationen notwendig. Sinnvoller als jede nationale Maßnahme erschiene es daher, in rechtsstaatlichem Rahmen und nicht nur auf dem Papier eine unverzügliche, schnelle Sicherung im Ausland gespeicherter Computer- und Verkehrsdaten für nachfolgende Übermittlungsersuchen zu ermöglichen. Solange die Möglichkeiten des gegenwärtigen Rechtsrahmens aus personellen, organisatorischen und finanziellen Gründen nicht annähernd ausgeschöpft sind, darf es keinen Masseneingriff in die Rechte Unschuldiger geben.

Befähigung ist besser als Überwachung, Dialoge vermeiden Paragrafen, informationelle Selbstbestimmung braucht keine Totalprotokollierung. Sich mutig für neue Wege zu öffnen ist der beste Schritt nach vorne, um sich von nicht-funktionalen Wunschvorstellungen zu verabschieden und chancenorientiert das Internet als Zukunft unserer Gesellschaft zu begreifen. Internetnutzer und Strafverfolger, die ernst genommen werden, werden selbstgewählte Sicherheitsvorkehrungen und Verbesserungen mit hoher Akzeptanz aufnehmen. Damit ist die eigentliche Absicht, einen gesellschaftlich getragenen Diskurs über die Information und Kommunikation der Zukunft zu eröffnen, konstruktiv angegangen. Der Schutz von Internetnutzern bekommt endlich die stabile Basis, die den Forderungen nach totaler Rückverfolgbarkeit abhanden gekommen ist.

▶ Medienkompetenzland Deutschland

Medienkompetenz ist der Schlüssel zu Partizipation an der digitalen Gesellschaft und verlangt heute mehr als Medienwissen, Medienkritik und gestaltende Medienproduktion. Die neue Dimension der zu stärkenden Medienkompetenz ist die verantwortungsvolle Mitwirkung an der

gesellschaftlichen Entwicklung mittels Medien. Dazu gehört auch das Verständnis und Kommunizieren bewährter Maßnahmen zum Schutz vor und zur Verfolgung von Internetdelikten.

Es gilt, eine Offensive für aufgeklärte Internetnutzung zu starten. Ziel muss hierbei vorrangig die Qualifizierung von Lehrenden, Pädagogen und (politischen) Entscheidern sein. Nur so kann schon den Ursachen von Kriminalität entgegengewirkt werden. Es ist ratsam, auf eine breite Beteiligung zu setzen und die bereits von Bund und Ländern geförderten Einrichtungen in die Pflicht zur Mitentwicklung von Konzepten und Inhalten zu nehmen. Dazu sollten Best-Practice-Beispiele aus der bisherigen medienpädagogischen Arbeit aufgegriffen werden. Ein runder Tisch „Medienkompetenz“, der sich auch online transparent abbildet, trägt die besten Ideen für das Medienkompetenzland zusammen. Die geförderten, erfahrenen Institutionen sollten federführend diesen Prozess moderieren. Ergebnis wird ein inhaltlicher Fahrplan sein, der das „Netzpferdchen“ zum Galopp bringen wird und Deutschland mit seiner Bildungsoffensive für ein sicheres digitales Zeitalter verdient herausstellt.

Strafverfolgungsinteressen dürfen nicht zur Chancen-Bremse im Internet werden. Eine einseitig an Gefährdungsszenarien ausgerichtete Politik verhindert eine Verbesserung der Möglichkeiten und zementiert Risiken.

6. Gemeinsam für ein freies und sicheres Netz

Die Idee einer Rückverfolgbarkeit jeder Internetnutzung „insbesondere zum Vorgehen gegen Kinderpornografie“ zeigt, dass über Sinnhaftigkeit und Erfolgsaussichten des Vorhabens nicht transparent mit Internetnutzern als Betroffenen gesprochen worden ist. Das Eckpunktepapier des Bundesjustizministeriums vom Januar 2011 und der Gesetzentwurf vom Juni 2011 sind in einer intransparenten Weise zustande gekommen. Das Ministerium hat bis heute nicht zu einer Anhörung von Vertretern der Betroffenen in Beruf und Gesellschaft eingeladen. Von Anfang an waren wenige (oder gar keine) Personen aus dem Netzpolitik- oder Informatikspektrum beteiligt. Doch das ist elementar, bevor Politik so grundlegend in eine Technikentwicklung eingreift. Entscheidungen dürfen nicht ohne frühestmögliche Beteiligung derjenigen gefällt werden, die sie betreffen.

Von europäischen Verfassungsgerichten und auf EU-Ebene wird die Erforderlichkeit und Verhältnismäßigkeit einer systematischen Vorratsdatenspeicherung zurzeit neu diskutiert. Nach Nichtigerklärungen in Rumänien, Deutschland und Tschechien bestehen gute Aussichten, dass auch der Europäische Gerichtshof 2012 die EU-Richtlinie zur Vorratsdatenspeicherung für unvereinbar mit der Grundrechtecharta und ungültig erklären wird. Eine vorauseilende Teilumsetzung der Richtlinie in Deutschland wäre verfehlt. Sie beseitigte das Risiko eines mit Sanktionen verbundenen EU-Vertragsverletzungsverfahrens gegen Deutschland nicht. Ohnehin ist die Festsetzung von Sanktionen nicht vor Ablauf eines Jahres zu erwarten. Es ist vollkommen offen, ob und in welcher Form die EU-Richtlinie zur Vorratdatenspeicherung zu diesem Zeitpunkt noch existieren wird. Vor allem hat die Bundesregierung die Möglichkeit, aus wichtigen Gründen des Grundrechtsschutzes eine Befreiung von der Pflicht zur Umsetzung der EU-Richtlinie zur

Vorratsdatenspeicherung zu beantragen und dies nötigenfalls einzuklagen (Art. 114 Abs. 4 AEUV). Dadurch kann eine Verurteilung wegen Vertragsverletzung auf absehbare Zeit ausgeschlossen werden.

Bislang ist die FDP zutreffend ihrem inneren Kompass gefolgt und hat jede anlasslose und massenhafte Aufzeichnung von Telefon- oder Internetverbindungen „auf Vorrat“ kategorisch abgelehnt. Ein erfreulich klarer Beschluss der FDP aus dem vergangenen Jahr betont zum Thema „Vorgehen gegen Internetkriminalität“, es dürfe

> „nicht vom Grundsatz abgerückt werden, der für den Rechtsstaat konstitutiv ist, dass mit staatlicher Überwachung und Verfolgung nur derjenige rechnen muss, gegen den ein Verdacht vorliegt. Eine anlasslose Überwachung aller Bürgerinnen und Bürger unabhängig von einem Verdacht wie durch die Vorratsdatenspeicherung widerspricht diesem Grundsatz.“

„Die anlass- und verdachtsunabhängige Vorratsdatenspeicherung hat die FDP von Anfang an abgelehnt“, heißt es auch im Wahlprogramm der FDP aus dem Jahr 2009, auf dessen Grundlage 14,6% der Wählerinnen und Wähler ihre Stimme der FDP gegeben haben. In Umsetzung dieses Auftrags hat die FDP-Bundestagsfraktion am 9.11.2010 beschlossen:

> „Der Rechtsgrundsatz, dass grundrechtsrelevante Maßnahmen im Rahmen der Strafverfolgung oder der Gefahrenabwehr nur unter der Voraussetzung erfolgen, dass ein ausreichender Verdacht oder Anlass für diese Maßnahme gegeben ist, muss auch im digitalen Raum gelten. Wir lehnen daher die verdachts- und anlassunabhängige Speicherung personenbezogener Daten auf Vorrat ab.“

Noch 2011 erklärte der damalige Bundesvorsitzende Dr. Guido Westerwelle:

> „Wir sollten nicht ohne Anlass die Telefon- und Internetverbindungsdaten aller Bürger speichern.“

Würden Sie nunmehr doch einer Erfassung sämtlicher Internetverbindungen Deutschlands auf Vorrat ohne jeden Verdacht und Anlass zustimmen, würden Sie den eigenen Grundsätzen der FDP zuwider handeln und das Vertrauen der Netzgemeinde endgültig verlieren.

Wie funktionierende Wege zu einem freien und sicheren Internet aussehen, haben wir oben aufzeigt. Wir – und auch viele weitere Sachverständige – wollen gerne die politischen Prozesse begleiten, so dass kurz- und mittelfristig gute, funktionierende und sinnvolle gesetzliche Regelungen entstehen können und langfristig Medienpädagogik, Präventionsarbeit und Technikgestaltung Weg und Ziel zugleich bilden können. Bis diese Prozesse zu Ergebnissen führen, ist die derzeitig gültige Rechtslage eindeutig die bessere Alternative.

Wir bitten Sie, die klare Linie der FDP beizubehalten und jede anlasslose Vorratsspeicherung von Internet-Verbindungsdaten strikt abzulehnen. Die Freiheit und Sicherheit von 51 Mio. Internetnutzern in Deutschland darf für die FDP als „Bürgerrechtspartei“ nicht verhandelbar sein. Einen „Kompromiss“ mit der Union zulasten der Gesamtheit der Internetnutzer Deutschlands auszuhandeln, ist weder sachlich sinnvoll noch politisch klug. Eine IP-Vorratsdatenspeicherung würde weit mehr Schaden anrichten als nutzen.

Mit den besten Grüßen,

Christian Bahls
1. Vorsitzender MOGiS e. V. – Eine Stimme für Betroffene

Markus Beckedahl
Vorstand der Digitalen Gesellschaft e. V. und Mitglied der Enquête-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages

Dr. Patrick Breyer
Arbeitskreis Vorratsdatenspeicherung

Joerg Heidrich
Rechtsanwalt und Fachanwalt für IT-Recht

Michael Konken
Vorsitzender des Deutschen Journalisten-Verbands e. V.

Constanze Kurz
Sprecherin des Chaos Computer Club e. V. und Mitglied der Enquête-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages

Ulrike Maercks-Franzen
Bundesgeschäftsführerin der Deutschen Journalistinnen- und Journalisten-Union dju in ver.di

Annette Mühlberg
Vorstandsmitglied der europäischen Internetnutzerorganisation der Internet Corporation for Assigned Names and Numbers (ICANN) und Mitglied der Enquête-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages

Andy Müller-Maguhn
Chaos Computer Club e. V.

Christine Nordmann
Vorstandsmitglied und Sprecherin der Neuen Richtervereinigung e. V.

Anne Roth
Bloggerin

Prof. Dr. Volkmar Sigusch
Direktor em., Institut für Sexualwissenschaft im Klinikum der Goethe-Universität Frankfurt/Main

Thomas Stadler
Fachanwalt für IT-Recht

Udo Vetter
Fachanwalt für Strafrecht und Lehrbeauftragter für Medienrecht an der Fachhochschule Düsseldorf