# Sicherheit geht vor Sammelwut - Vorratsspeicherung gefährdet Menschenleben

## 1 Einführung

### 1.1 Traditionelle Vertraulichkeit von Gesprächen

Wenn wir miteinander sprechen oder einander Briefe schreiben, können wir sicher sein, dass unsere privaten und geschäftlichen Kontakte vertraulich bleiben. Niemand fertigt Aufzeichnungen darüber an, und wir müssen niemandem Rechenschaft darüber ablegen, mit wem wir gesprochen haben, wo wir gewesen sind oder was wir gelesen haben. Nicht anders ist dies seit jeher bei Telefongesprächen und Internetverbindungen gewesen: Telefongespräche wurden bis in die 80er Jahre analog vermittelt. Aufzeichnungen darüber wurden nur auf richterliche Anordnung erstellt. Mit der Einführung digitaler Vermittlungstechnik wurde dann erstmals die elektronische Erfassung jedes Telefongesprächs möglich. Die Telekommunikationsgesellschaften durften aber nur die zur Abrechnung erforderlichen Informationen erfassen. Kunden konnten die verkürzte Erfassung der gewählten Rufnummern und die Löschung aller Aufzeichnungen mit Rechnungsversand verlangen. Durch Nutzung von Pauschaltarifen konnten sie die Erfassung ihrer Verbindungen insgesamt verhindern. Im Verdachtsfall konnten die zuständigen Behörden Abrechnungsdaten einsehen und zukünftige Verbindungen aufzeichnen lassen.

### 1.2 Einführung einer Vorratsdatenspeicherung zum 01.01.2008

Trotz verbreiteter Proteste von Bürgern und Experten wurde zum 01.01.2008 erstmals die verdachtsunabhängige Erfassung und sechsmonatige Speicherung sämtlicher Telefon- und Handyverbindungen in Deutschland eingeführt. Bei jedem Handytelefonat und jeder versandten oder eingegangenen SMS wurde der Standort des Handynutzers erfasst. Zum 01.01.2009 musste dann auch jede Internetverbindung erfasst werden. In Verbindung mit anderen Daten konnte sechs Monate lang festgestellt werden, was wann über unseren Internetanschluss getan wurde.

### 1.3 Ende der Vorratsdatenspeicherung am 04.03.2010

34.000 Bürgerinnen und Bürger reichten gegen das Gesetz zur Vorratsdatenspeicherung Verfassungsbeschwerde ein. Am 04.03.2010 erklärte das Bundesverfassungsgericht die Vorschriften zur Vorratsdatenspeicherung für

verfassungswidrig und hob sie auf. Seither gilt wieder die bewährte Regel, dass unsere Verbindungen nur ausnahmsweise erfasst werden dürfen, wenn dies zur Rechnungsstellung nötig ist.

### 1.4 Kampagne zur Wiedereinführung

Im Oktober 2010 wurde bekannt, dass CDU und CSU eine "öffentliche Kampagne" eingeleitet haben, um die FDP zu einem neuen Gesetz zur Erfassung aller Verbindungsdaten zu bewegen. Die FDP hat eine solche Vorratsdatenspeicherung immer wieder als unverhältnismäßig abgelehnt; Bundesjustizministerin Leutheusser-Schnarrenberger war dagegen sogar vor das Bundesverfassungsgericht gezogen. Bundesinnenminister de Maizière (CDU) und der Präsident des nachgeordneten Bundeskriminalamts wollen nun aber am 08.10.2010 "anhand möglichst spektakulärer Fälle" belegen, dass es wegen der aktuell fehlenden Speicherpflicht "blinde Flecken in der Verbrechensbekämpfung" gebe. Das Bundeskriminalamt hat dazu einen Bericht über die Auswirkungen des Endes der Vorratsdatenspeicherung am 04.03.2010 erstellt.

Der Arbeitskreis Vorratsdatenspeicherung als Zusammenschluss von Bürgerrechtlern, Datenschützern und Internetnutzern legt mit diesem Bericht eine eigene Expertise über die Forderung nach Erfassung aller Verbindungen vor.

## 2 Vorratsdatenspeicherung gefährdet den Schutz von Kindern und Menschenleben

Eine Erfassung sämtlicher Telefongespräche und Verbindungen hat schwerwiegende unerwünschte Nebenwirkungen auf unser Leben und auf unsere Gesellschaft:

### 2.1 Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet den Schutz von Kindern und kann Menschenleben kosten

Das Leben und die Gesundheit potenzieller Opfer von Gewalttaten kann in vielen Fällen nur durch anonyme Beratung geschützt werden (z.B. Telefonseelsorge, Hotlines). Viele Täter sind nur im Schutz der Anonymität bereit, sich helfen zu lassen, wobei sie vielfach von geplanten Gewalttaten abgebracht oder von der Notwendigkeit einer Behandlung überzeugt werden können. Viele Opfer können sich nur im Rahmen anonymer Beratung entschließen, Täter anzuzeigen. Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet die Bereitschaft von Tätern und Opfern zur Inanspruchnahme von Beratung und gefährdet damit Menschenleben.

Beispiel 1: Im Jahr 2007 konnte ein bei der Telefonseelsorge in Bayern tätiger Pfarrer einen Jugendlichen überzeugen, einen geplanten Amoklauf in seiner Schule zu unterlassen. Wäre der Anruf rückverfolgbar gewesen, hätte der Jugendliche wohl nie über sein Vorhaben gesprochen.

Beispiel 2: Im Jahr 2010 erwägt ein betrogener Ehemann, seine Ehefrau oder ihren Liebhaber zu töten. Die Telefonseelsorge kann ihn davon abbringen. Wäre der Anruf rückverfolgbar gewesen, hätte der Mann wohl nie über sein Dilemma gesprochen.

Beispiel 3: Eine akut krebskranke Patientin vermeidet wegen der Vorratsdatenspeicherung, sich per Telefon oder E-Mail nach einer Behandlungsmöglichkeit für ihre Tumorerkrankung zu erkundigen und vereinbart stattdessen einen persönlichen Gesprächstermin in einem Berliner Klinikum. Das Abwarten verzögert den Behandlungsbeginn. In der Zwischenzeit wächst der Tumor weiter, die Prognose der Patientin verschlechtert sich.

Eine repräsentative Umfrage unter 1.002 Bundesbürgern am 27./28. Mai 2008 ergab, dass mehr als die Hälfte der Deutschen wegen der Vorratsdatenspeicherung davon absehen würden, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten. Dies betrifft über 40 Mio. Menschen in Deutschland.

## 2.2 Eine Erfassung sämtlicher Telefongespräche und Verbindungen begünstigt Korruption

Korruption und andere öffentliche Missstände werden oftmals erst dann wirksam aufgeklärt und angegangen, wenn die Medien darüber öffentlich berichten. Wer Journalisten von solchen Fällen als Insider berichtet, riskiert aber oftmals seine Anstellung oder muss sogar mit einem Strafverfahren wegen Geheimnisverrats rechnen. Wichtige Missstände und Skandale melden Informanten der Presse daher nur im Schutze absoluter Vertraulichkeit. Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet die Bereitschaft von Informanten, mit Journalisten zu sprechen, und begünstigt damit Korruption und andere Missstände im Verborgenen.

Beispiel 1: Der Journalist Philipp Kunze (Name geändert) aus Nordrhein-Westfalen befasst sich im Rahmen seiner Arbeit unter anderem mit Menschenrechtsverletzungen der EU-Grenzagentur Frontex. Bereits kurz nach Inkrafttreten der Vorratsdatenspeicherung lehnen zwei Kontaktpersonen den Informationsaustausch via E-Mail ab.

Beispiel 2: Die Drehbuchautorin Maria Urner (Name geändert) aus Bayern recherchierte den Wismut-Skandal, in dessen Rahmen ca. 2.800 ehemaligen Uranerz-Bergmänner der DDR durch Radioaktivität in den Stollen Krebserkrankungen bekamen und nun keine Unfallrente erhalten. Nach dem 1.1.2008 bekommt Frau Urner bei telefonischen Recherchen, besonders in der ehemaligen DDR, nur noch zögerlich oder gar keine Auskünfte zu dem Thema mehr.

Beispiel 3: Der Sportjournalist Florian Schröder (Name geändert) aus Hamburg ist nach Inkrafttreten der Vorratsdatenspeicherung damit konfrontiert, dass viele Informanten nicht nur Fragen am Telefon oder per E-Mails ablehnten, sondern auch direkte Gespräche und Treffen. Für seine Arbeit etwa beim Thema Doping sind die Auswirkungen katastrophal.

In einer Umfrage unter 1.489 deutschen Journalisten aus dem Jahr 2008 erklärte jeder vierzehnte Journalist, das Bewusstsein, dass Kommunikationsdaten auf Vorrat gespeichert werden, habe sich bereits negativ auf die Kommunikation mit seinen Informanten ausgewirkt. Damit beeinträchtigte die Vorratsdatenspeicherung die Arbeit von hochgerechnet mindestens 3.000 Journalisten in Deutschland.

## 2.3 Eine Erfassung sämtlicher Telefongespräche und Verbindungen gefährdet die Wissenschaft

Wissenschaftliche Forschung setzt in vielen Bereichen die Bereitschaft von Menschen voraus, anonym über ihre Persönlichkeit und ihr Leben Auskunft zu geben. Werden alle Kontakte erfasst, können Forschungsprojekte an der fehlenden Bereitschaft zur Mitwirkung an Umfragen scheitern.

Beispiel: Leon Schulz (Name geändert) arbeitet in der universitären Onlineforschung an einem Lehrstuhl für Persönlichkeitspsychologie. Für seine psychologischen Studien über die menschliche Persönlichkeit sind oft sehr intime Fragen nötig. Diese Fragen werden von den Versuchsteilnehmern nach Inkrafttreten der Vorratsdatenspeicherung nicht mehr beantwortet, wodurch die Forschung im Bereich Psychologie sehr leidet.

## 2.4 Eine Erfassung sämtlicher Telefongespräche und Verbindungen setzt Arbeitsplätze aufs Spiel

Geschäftsbeziehungen und Vertragsverhandlungen sind oft äußerst vertraulich. Eine Erfassung telefonischer oder elektronischer Kontakte schafft das Risiko, dass Geschäftsgeheimnisse bekannt werden (z.B. durch Wirtschaftsspionage), was großen Schaden nach sich ziehen kann. Deswegen verzichten

Wirtschaftsunternehmen teilweise lieber ganz auf Kontakte als das Risiko unbefugter Offenlegung einzugehen. Dadurch können Unternehmen Aufträge verlieren, was Arbeitsplätze kosten kann.

> Beispiel: Hans Grunwald aus Bayern arbeitet in der Industrieproduktion. Sein Unternehmen, in dem acht Mitarbeiter tätig sind, fertigt für potenzielle Kunden aus ganz Europa Prototypen, wofür technische Zeichnungen oder sonstige sicherheitsrelevante Beschreibungen der Geschäftspartner benötigt werden. Nach Inkrafttreten der Vorratsdatenspeicherung weigern sich mehrere Kunden, die erforderlichen Unterlagen per Email oder Telefax zu versenden. Dadurch verliert das Unternehmen einen Großkunden und muss zwei Arbeitnehmer entlassen.

## 2.5 Eine Erfassung sämtlicher Telefongespräche und Verbindungen lässt politische Kritiker abtauchen

Die Vorbereitung spektakulärer Protestaktionen gegen Gentechnik, gegen Atomenergie usw. bedarf oft absoluter Vertraulichkeit. Viele Menschen sind nicht zu einem Engagement in politisch kritischen Gruppen bereit, wenn sie damit rechnen müssen, in das Raster des Verfassungsschutzes zu geraten.

> Beispiel 1: Patrick Schuhmacher (Name geändert) engagiert sich antifaschistisch und befürchtet mit Inkrafttreten der Vorratsdatenspeicherung, dass seine Daten besonders geprüft werden. Auf Telefongespräche und Internetkorrespondenz, die nicht unbedingt notwendig sind, verzichtet er daher.
>
> Beispiel 2: Katharina Gärtner aus Baden-Württemberg ist in einer Attac-Gruppe aktiv. Seit Inkrafttreten der Vorratsdatenspeicherung wirken die Diskussionsbeitrage im Internetforum der Gruppe wie zensiert, die Diskussionsteilnehmer trauen sich nicht mehr, ihre Meinung zu äußern.

## 2.6 Eine Erfassung sämtlicher Telefongespräche und Verbindungen verhindert die Ermittlung von Straftätern

Eine verdachtsunabhängige Erfassung jedes Telefonats und jeder Verbindung gräbt sich in das Bewusstsein Unschuldiger wie Schuldiger ein. Eine Vorratsdatenspeicherung erhöht daher die Entwicklung und Nutzung anderer Kommunikationskanäle. Viele Menschen gehen dazu über, Gespräche nicht mehr telefonisch zu führen, wechselnde Handys zu benutzen oder mit ausländischen Anonymisierungsdiensten im Internet zu surfen. Dies verschließt den Ermittlern selbst im Fall eines konkreten Verdachts die Möglichkeit einer Überwachung und Aufklärung schwerster Straftaten.

Beispiel: Ein anonymer Nutzer kündigt im Polizisten-Forum Copzone einen Amoklauf an und bedroht dabei eine Arbeitsvermittlerin massiv. Weil er einen internationalen Anonymisierungsdienst nutzt, ist eine Identifizierung nicht möglich. Stattdessen wird versehentlich der Betreiber des Dienstes verhaftet.

In einer infas-Umfrage aus dem Jahr 2009 erklärten schon 12,8% der Befragten, einen Anonymisierungsdienst einzusetzen, 6,4%, sie seien zu einem Provider ohne Vorratsdatenspeicherung gewechselt, und 5,1%, dass sie Internet-Cafés benutzten. Eine jederzeitige Rückverfolgbarkeit durch Vorratsdatenspeicherung dürfte diese Entwicklung erheblich beschleunigen.

## 2.7 Eine Erfassung sämtlicher Telefongespräche und Verbindungen führt zur Verfolgung Unschuldiger

Verbindungsdaten können die Ermittlung eines Anschlussinhabers ermöglichen, geben aber nicht an, wer das entsprechende Telefon oder Handy oder den Internetanschluss konkret genutzt hat. Durch Verbindungsdaten geraten daher viele Menschen zu Unrecht in einen falschen Verdacht, z.B. wegen eines Zahlendrehers, wegen eines verkauften Handys, wegen eines offenen Internetzugangs. Dies zieht immer wieder Überwachungsmaßnahmen, Hausdurchsuchungen oder sogar Festnahmen Unschuldiger nach sich und hat schon das Leben von Menschen ruiniert.

Beispiel 1: Die Wohnung eines deutschen Professors wurde durchsucht und seine Computer beschlagnahmt, weil er Kinderpornografie über das Internet verbreitet haben soll. Tatsächlich hatte sein Internet-Zugangsanbieter der Polizei eine falsche Auskunft erteilt.

Beispiel 2: Im Dezember 2008 stürmte das Spezialeinsatzkommando (SEK) die Wohnung eines 38jährigen Mannes in Recklinghausen. Die Polizei hatte von einer Amokdrohung erfahren. Erst später stellte sich heraus, dass ein Nachbar die Drohung über das offene Funknetz des Mannes versandt hatte.

## 2.8 Eine Erfassung sämtlicher Telefongespräche und Verbindungen führt zum Bekanntwerden vertraulichster Beziehungen

Beinahe wöchentlich werden immer neue Fälle von Missbrauch, Verkauf, Verlust, Veröffentlichung von und Zugang zu persönlicher Daten bekannt. Heutzutage sind nur nicht erfasste Daten sichere Daten. Eine Erfassung sämtlicher Telefongespräche und Verbindungen führt dazu, dass weit mehr Menschen unter dem Missbrauch, dem Verkauf, dem Verlust, der Veröffentlichung von und dem missbräuchlichen Zugang zu ihren vertraulichen Kontakten und Aufenthaltsorten leiden als sonst.

Beispiel 1: Die Deutsche Telekom AG kontrolliert über einen Zeitraum von insgesamt anderthalb Jahren die Telefonverbindungen von Journalisten sowie von Arbeitnehmer-Aufsichtsräten, Managern und Betriebsräten des Unternehmens. Da keine Vorratsdatenspeicherung erfolgt, sind die Verbindungen von Menschen mit Pauschaltarifen vor missbräuchlicher Aufdeckung ihrer Kontakte geschützt.

Beispiel 2: Im Jahr 2006 verkaufte ein Mitarbeiter von T-Mobile die Daten der 17 Mio. Kunden des Mobilfunkunternehmens. Darunter befinden sich Privatanschriften und -nummern vieler Prominenter aus Kultur und Gesellschaft sowie eine erstaunliche Anzahl geheimer Nummern und Privatadressen von bekannten Politikern, Ministern, Ex-Bundespräsidenten, Wirtschaftsführern, Milliardären und Glaubensvertretern, für die eine Verbreitung ihrer Kontaktdaten in kriminellen Kreisen eine Bedrohung ihrer Sicherheit darstellt (etwa von Charlotte Knobloch, Präsidentin des Zentralrats der Juden). Das Bundeskriminalamt erstellt eine Gefährdungsanalyse, um Betroffene schützen zu können. Zur Aufklärung des Datenlecks verletzte T-Mobile erneut das Fernmeldegeheimnis und überprüfte illegal auf eigene Faust Verbindungsdaten.

## 3 Eine Erfassung sämtlicher Telefongespräche und Verbindungen verbessert die Ermittlung von Straftätern nicht

Der vom Bundeskriminalamt veröffentlichten Polizeilichen Kriminalstatistik zufolge hat die Erfassung aller Internetverbindungen im Jahr 2009 weder von Straftaten abgeschreckt, noch den Anteil der aufgeklärten Straftaten erhöht. Obwohl im Internetbereich Verbindungsdaten teilweise der einzige Ermittlungsansatz sind, konnte ohne Vorratsdatenspeicherung sogar eine höhere Aufklärungsrate erzielt werden.

Im Jahr 2008, in dem Internet-Einwahlen und E-Mails von den Anbietern allenfalls kurzfristig protokolliert wurden, wurden danach 167.451 Internet-Straftaten registriert, die zu 79,8% aufgeklärt werden konnten. Im Jahr 2009, in dem alle Internet-Einwahlen und E-Mails für sechs Monate protokolliert wurden, registrierte die Polizei demgegenüber 206.909 begangene Internet-Straftaten, und ihre Aufklärung gelang nur zu 75,7%.

Internetdelikte wurden ohne Vorratsdatenspeicherung weit häufiger aufgeklärt (79,8%) als sonstige Straftaten (54,8%). Das gilt übrigens auch für die Verbreitung von Kinderpornografie im Internet (87,5%). Von einem rechtsfreien Raum kann keine Rede sein. Andere Staaten auf der ganzen Welt (z.B. Österreich, Griechenland, Schweden, Rumänien, Norwegen, Australien, Kanada, Japan) ermitteln schon immer erfolgreich ohne Vorratsdatenspeicherung.

### 3.1 Die Zahlen des Bundeskriminalamts belegen keinen Bedarf

Der aktuell diskutierte Bericht des Bundeskriminalamt über die Auswirkungen des Endes der Vorratsdatenspeicherung belegt keinen Bedarf nach einer neuerlichen Erfassung sämtlicher Telefongespräche und Verbindungen.

Dem Bericht des Bundeskriminalamts zufolge forderte das Bundeskriminalamt im Zeitraum vom 2. März bis zum 16. Juni 2010 von Telekommunikationsanbietern Auskunft über 701 Anschlüsse. Zu 422 dieser Anschlüsse sei keine Auskunft erteilt worden (374 Internet-Anschlüsse und 48 Telefonfestnetz- und Mobilfunkanschlüsse).

Aus den folgenden Gründen belegt dies keine "blinde Flecken in der Verbrechensbekämpfung":

1. Wären im Fall einer Vorratsdatenspeicherung nicht ebenso viele Auskünfte unterblieben? Das Bundeskriminalamt liefert keine Vergleichswerte für die Zeit, als in Deutschland alle Verbindungen auf Vorrat erfasst wurden (2009). Deswegen belegen die Zahlen nicht, dass gegenwärtig weniger Auskünfte erteilt würden. Das Bundeskriminalamt liefert auch keine Vergleichswerte für die Zeit vor Einführung der Vorratsdatenspeicherung. Deswegen belegen die Zahlen nicht, dass gegenwärtig weniger Auskünfte erteilt würden als seit jeher.
2. Wäre im Fall der Auskunfterteilung eine Identifizierung möglich gewesen? Das Bundeskriminalamt beantwortet diese Frage nicht. Deshalb kann nicht davon ausgegangen werden, dass Auskünfte zur Identifizierung der Täter geführt hätten. In vielen Fällen verwenden Straftäter Internet-Cafés, offene Internetzugänge (WLAN), Anonymisierungsdienste, öffentliche Telefone, unregistrierte Handykarten usw. Eine Auskunft über den Anschlussinhaber ermöglicht eine Identifizierung des Nutzers in diesen Fällen nicht.
3. Wäre es im Fall der Auskunfterteilung zur Verurteilung des Verdächtigen gekommen? Das Bundeskriminalamt beantwortet diese Frage nicht. Deshalb kann nicht davon ausgegangen werden, dass Auskünfte letztlich zur Verurteilung von Straftätern geführt hätten. Nach einer Untersuchung des Max-Planck-Instituts im Auftrag des Bundesjustizministeriums kam es in 72% der Verfahren mit erfolgreicher Verbindungsdatenabfrage gleichwohl zu keiner Verurteilung.
4. Hat das Bundeskriminalamt Auskünfte eingeholt, obwohl es von vornherein wusste, dass bei dem Anbieter keine Verbindungen (mehr) verzeichnet sind? Das Bundeskriminalamt beantwortet diese Frage nicht. Deshalb kann nicht ausgeschlossen werden, dass das Bundeskriminalamt die Zahl erfolgloser Auskunftsersuchen durch erkennbar aussichtslose Anfragen in die Höhe getrieben hat. Dem Bundeskriminalamt liegt eine

Liste vor, wie lange welches Unternehmen Verbindungsdaten aufbewahrt. Finden dennoch erkennbar aussichtslose Anfragen statt, so ist die Zahl der erfolglosen Anfragen manipuliert und wertlos. Auch im Fall einer Vorratsdatenspeicherung hätten so viele ergebnislose Anfragen vorgenommen werden können.

5. In wie vielen Fällen konnte das Bundeskriminalamt physisch anwesende Täter oder Absender von Briefen nicht identifizieren? Ohne eine Antwort auf diese Frage muss davon ausgegangen werden, dass physisch anwesende Täter oder Absender von Briefen seltener identifizierbare Spuren hinterlassen als Täter von Telefon- oder Internetdelikten. Es ist nicht einzusehen, warum Telefon und Internet gläserner sein sollten als persönliche Kontakte und die Post. Tatsächlich werden Internetdelikte auch ohne Vorratsdatenspeicherung zu 80% aufgeklärt, während sonstige Straftaten nur zu 55% aufgeklärt werden. Während vier Fünftel aller im Internet begangenen Straftaten aufgeklärt werden, bleibt etwa jeder zweite Raub unaufgeklärt.

Laut Bundeskriminalamt konnten Straftaten bei 49 Anschlüssen "nicht", bei 133 Anschlüssen nur "unvollständig" und bei 211 Anschlüssen nur "wesentlich erschwert oder erst zu einem späteren Zeitpunkt" aufgeklärt werden, nachdem keine Aufzeichnungen über frühere Verbindungen verfügbar waren.

Aus den folgenden Gründen belegt dies keine "blinde Flecken in der Verbrechensbekämpfung":

1. Selbst nach den Angaben des Bundeskriminalamts konnten 74% der Straftaten auch ohne Vorratsdatenspeicherung aufgeklärt werden (701-49-133=519 von 701 Taten). Diese Aufklärungsquote übersteigt die durchschnittliche Aufklärungsquote von 55% bei weitem und belegt keinerlei Handlungsbedarf.
2. Umgekehrt belief sich die Aufklärungsquote auch während der verdachtslosen Vorratsdatenspeicherung im Jahr 2009 auf 75,7% bei Internetdelikten und 55% bei sonstigen Delikten. Mit Vorratsdatenspeicherung wurde also auch keine signifikant höhere Aufklärungsrate erzielt. Vor diesem Hintergrund belegen die Zahlen des Bundeskriminalamts keinen Bedarf nach einer Erfassung sämtlicher Verbindungsdaten.

## 3.2 Die Fallberichte des Bundeskriminalamts belegen keinen Bedarf

Die vom Bundeskriminalamt im Einzelnen geschilderten Straftaten belegen ebensowenig "blinde Flecken in der Verbrechensbekämpfung":

### 3.2.1 Fall 1 ("Komplott der Terrororganisation Hamas")

*Im Zusammenhang mit der Ermordung eines Funktionärs der paramiliärischen Terrororganisation Hamas in Dubai im Januar 2010 lief ein Ermittlungsverfahren gegen einen Beschuldigten in Deutschland wegen des Verdachts geheimdienstlicher Agententätigkeit. Über einen Mobilfunkanschluss wurden Gespräche des Komplotts rückwirkend noch mehrere Monate abgerechnet. Dadurch wollte das BKA Kontaktpersonen identifizieren und Ansätze für weitere Ermittlungen gewinnen.*

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Hamas-Mitglieder werden geschickt genug sein, um nur mit Handys zu telefonieren, die nicht auf ihren Namen registriert sind. Deswegen belegt der Fall nicht, dass eine Erfassung sämtlicher Verbindungen weiter geführt hätte.

### 3.2.2 Fall 2 ("Wer verlinkte das Terror-Video?")

*In einem Internetforum wurde am 12. April 2010 eine Videoverlautbarung einer terroristischen Vereinigung über verschiedene Links zur Verfügung gestellt. Einer davon stammte von einer unbekannten Person, deren E-Mail-Adresse einen Tag zuvor registriert worden war. Das BKA fragte am 20. April bei der Deutschen Telekom Kundendaten zu der IP-Adresse (Computeradresse im Internet) für den Registrierungstag (11. April) ab. Der Konzern teilte daraufhin mit, dass die Speicherfrist von sieben Tagen bereits abgelaufen sei und verwies auf das Verfassungsgerichtsurteil. Fazit des BKA: Aufklärung unmöglich.*

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Es kann nicht ernsthaft angenommen werden, dass ein Terrorvideo vom Heimanschluss eines Unterstützers verlinkt wird. Wahrscheinlich hätten Verbindungsspuren nur zu einem Internetcafé oder einem offenen Internetzugang (WLAN) geführt und damit nichts zu der Ermittlung beigetragen.

### 3.2.3 Fall 3 ("Terrordrohung gegen Schulen")

*Ein Unbekannter versandte seit Dezember 2009 über ein Briefzentrum mehr als 100 Briefe, in denen er Sprengstoffanschläge androhte. Adressaten waren Schulen, Universitäten und Bürger. Falls sie eine gewisse Geldsumme nicht zahlten, sollten sie getroffen werden. Der Täter kontaktierte per E-Mail am 22. April eine Geschädigte über deren Profil bei „studiVZ“. Zwar bekam das BKA von*

*dem Netzwerk die IP-Adresse des Absenders und fand den dahinter stehenden Anbieter Vodafone. Doch der teilte mit, dass er solche Daten nicht speichere. Fazit des BKA: Aufklärung unmöglich.*

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Es kann nicht ernsthaft angenommen werden, dass der Urheber von 100 Bombendrohungen eine Vodafone-Internetkarte nutzt, die auf seinen Namen registriert ist. Sinnvollerweise wird "studiVZ" eine Fangschaltung einrichten: Wenn sich der Täter wieder anmeldet, wird seine Kennung der Polizei übermittelt. Während der bestehenden Internetverbindung kann Vodafone die Anschlussdaten auch ohne Vorratsdatenspeicherung feststellen.

### 3.2.4 Fall 4 ("Mafiamord in Leverkusen")

*Ein italienischer Staatsbürger wurde am 15. Januar 2010 in Leverkusen ermordet. Als der 43-jährige noch lebte, hatte er sich unangemeldet in Köln aufgehalten. Das BKA erfuhr von italienischen Behörden, dass das Mordopfer der Mafia nahe gestanden haben soll. Dem BKA gelang es, den möglichen Tatort und vier Verdächtige zu ermitteln. Für ein Ermittlungsverfahren wäre laut des BKA jedoch die Auswertung von Telefondaten erforderlich gewesen. Aber einen solchen Antrag lehnte die Staatsanwaltschaft Köln ab. Fazit des BKA: Die Aufklärung des Mordes sei zumindest "wesentlich erschwert".*

Offensichtlich konnte der Fall auch auf anderem Wege aufgeklärt werden. Im Übrigen steht in den Sternen, ob Verbindungsdaten weiter geführt hätten. In Mafiakreisen liegt dies fern.

### 3.2.5 Fall 5 ("Polizistenmord")

*In Brandenburg wurde am 23. November 2009 der Mord an dem 46-jährigen Polizeihauptkommissar Steffen M. bekannt. Der oder die Täter flüchteten mit dem Auto des Opfers. Dieses wurde laut BKA abgestellt und eine andere „Beförderungsmöglichkeit“ per Handy angefordert. Am 18. Februar erging beim Amtsgericht Cottbus ein Beschluss, dass die Daten abgefragt werden dürfen. D2 Vodafone teilte dem BKA daraufhin am 9. März 2010 mit, dass für das betreffende Handy am 7. März keine Verkehrsdaten mehr vorliegen würden. Fazit des BKA: Aufklärung unmöglich.*

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Wenn der Täter einen Komplizen angerufen hat, wird dieser geschickt genug gewesen sein, mit einem Handy zu telefonieren, das nicht auf seinen Namen registriert war. Deswegen belegt der Fall nicht, dass eine Erfassung sämtlicher Verbindungen weiter geführt hätte.

### 3.2.6 Fall 6 ("Hinweise auf Kindesmissbrauch")

*Das BKA erhielt am 14. Mai 2010 die Meldung über einen Kindesmissbrauch. In einem Internetforum fand sich ein Hinweis vom 6. Mai darüber, dass ein Stiefvater seinen Sohn missbraucht und ihn deswegen sogar teilweise mit Medikamenten ruhig stellt. Der Nutzername war anonym und ausschließlich die IP-Adresse sichtbar. Das BKA forschte noch am 14. Mai nach, bekam aber keine Auskunft. Aus dem Inhalt des Textes konnten keine Hinweise auf die Identität des Nutzers gezogen werden. Fazit des BKA: Aufklärung unmöglich.*

Es ist nicht belegt und liegt fern, dass Verbindungsdaten hier weiter geführt hätten. Es kann nicht ernsthaft angenommen werden, dass der Betroffene über einen auf seinen Namen angemeldeten Anschluss über seine Straftaten berichtet hat. Sinnvollerweise wird der Betreiber des Forums eine Fangschaltung einrichten: Wenn sich der Täter wieder anmeldet, wird seine Kennung der Polizei übermittelt. Während der bestehenden Internetverbindung kann der Internet-Zugangsanbieter die Anschlussdaten auch ohne Vorratsdatenspeicherung feststellen.

Selbst wenn dieser Kindesmissbrauch hätte beendet werden können, hätte eine Vorratsdatenspeicherung den Schutz einer weit größeren Anzahl von Kindern vereitelt: Nicht rückverfolgbare, anonyme Beratung ist zum Schutz unzähliger Kindern und Erwachsener unverzichtbar. Anonymen Telefonberatungsstellen gelingt es immer wieder, Täter von Kindesmissbrauch und Pädophile zu überzeugen, sich in Behandlung zu begeben. Gewalttätige Ehemänner werden überzeugt, sich in Therapie zu begeben. HIV-Infizierte werden überzeugt, andere nicht weiter durch ungeschützten Geschlechtsverkehr mit der lebensbedrohenden Krankheit anzustecken. Die Gesundheit Unschuldiger steht und fällt mit der Verfügbarkeit nicht rückverfolgbarer Beratung.

### 3.2.7 Fall 7 ("Angriff auf digitale Identität")

*Ein Ermittlungsverfahren in Luxemburg ergab nach der Auswertung eines beschlagnahmten Computerservers als Teil eines illegalen Botnetzes, dass dieser zur „Verschleierung der Täterkommunikation“ und zur „Erlangung der digitalen Identität“ von Nutzern diente. Es wurden 218.703 deutsche IP-Adressen, die auf den Server zugriffen, mit „Zeitstempel November 2009“ an das BKA übermittelt. Die Fahnder wollten über die Länderpolizeien die Computerbesitzer in Deutschland informieren. Doch das Auskunftsersuchen wurde weitgehend abgelehnt. Das betraf allein in Nordrhein-Westfalen und Hessen 169.964 IP-Adressen. Fazit des BKA: Aufklärung unmöglich.*

Es ist nicht die Aufgabe der Polizei, Computerbenutzer über eine Infektion ihres Computers zu informieren. Dies ist in erster Linie Aufgabe des Nutzers selbst. In zweiter Linie tun dies die Internet-Zugangsanbieter im Rahmen ihrer Anti-

Botnetz-Initiative, ganz ohne Vorratsdatenspeicherung. In dritter Linie wäre es sinnvoll, die Hersteller gebrauchsfertiger Computersysteme zu verpflichten, Computer nur noch mit vorinstalliertem Virenscanner auszuliefern.

### 3.2.8 Fall 8 ("Kontakte einer radikal-islamischen Untergrundorganisation")

*Das BKA wollte nach Hinweisen von amerikanischen und libanesischen Sicherheitsbehörden Mitglieder der sunnitischen radikal-islamischen Untergrundorganisation Fatah al-Islam in Deutschland aufspüren und identifizieren. Das gelang bei einem Mann, weil er falsche Ausweispapiere hatte und gegen ihn ein libanesischer Haftbefehl vorlag. Nach der Festnahme befindet sich der Mann in Auslieferungshaft. Das BKA konnte aber keine Kontaktpersonen ermitteln. Der Grund: Die Telekommunikationsfirmen gaben Telefon- und Internetverbindungsdaten nicht oder nur unvollständig heraus. Fazit des BKA: „Somit konnte keine vollständige Aufhellung der Szene erfolgen".*

Es ist nicht belegt und liegt fern, dass weitere Verbindungsdaten die "Szene" hier "vollständig erhellt" hätten. Es kann nicht ernsthaft angenommen werden, dass Mitglieder einer Untergrundorganisation über auf ihren eigenen Namen registrierte Telefon- oder Internetanschlüsse miteinander kommunizierten. Wahrscheinlich hätten Verbindungsspuren nur zu einem Internetcafé oder einem offenen Internetzugang (WLAN) geführt und damit nichts zu der Ermittlung beigetragen.

## 4 Die EU verpflichtet Deutschland nicht zur Vorratsdatenspeicherung

Die EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung verpflichtet Deutschland nicht zu einer Erfassung sämtlicher Verbindungen. Die EU-Verträge (Art. 114 Abs. 4 AEUV) erlauben es Deutschland, aus wichtigem Grund von solchen Richtlinien abzuweichen und abweichende Gesetze beizubehalten. Der Schutz Unschuldiger und ihrer Grundrechte ist Bestandteil der öffentlichen Ordnung Deutschlands und rechtfertigt eine Abweichung von der EU-Richtlinie zur Vorratsdatenspeicherung. Die Bundesregierung muss dazu lediglich eine entsprechende Anzeige bei der EU-Kommission machen.

Allerdings überprüft die EU-Kommission derzeit ohnehin, ob die EU-Richtlinie 2006/24/EG verhältnismäßig ist. Sowohl EU-Innenkommissarin Cecilia Malmström wie auch EU-Justizkommissarin Viviane Reding hatten damals gegen die Richtlinie gestimmt. Die EU-weite Vorgabe einer Erfassung aller Verbindungsdaten wird voraussichtlich schon deshalb geändert werden müssen, weil der Verfassungsgerichtshof Rumäniens entschieden hat, dass eine Vorratsdatenspeicherung mit der Europäischen Menschenrechtskonvention generell unvereinbar ist.

Vor einigen Monaten hat der irische High Court in Dublin bereits angekündigt, dem Europäischen Gerichtshof die Frage vorzulegen, ob die EU-Richtlinie zur Speicherung aller Verbindungsdaten gegen die Ende 2009 in Kraft getretene EU-Grundrechtecharta verstößt und unwirksam ist. "Es ist klar, dass Überwachungsmaßnahmen gerechtfertigt sein müssen und in der Regel gezielt erfolgen sollten", heißt es in dem Urteil vom 05.05.2010. Ob die EU-Richtlinie aus dem Jahr 2006 überhaupt Bestand haben wird oder ob sie der Europäische Gerichtshof - wie zuvor die Verfassungsgerichte Rumäniens und Deutschlands - aufheben wird, bleibt abzuwarten.

## 5 Die Strafverfolgung bedarf Verbesserungen ganz anderer Art

Wirklich nützlich zur Verbesserung der Strafverfolgung wären ganz andere Maßnahmen als eine Erfassung aller Verbindungsdaten:

### 5.1 Schnelle Datensicherung, bessere Ausbildung

National und international wäre es hilfreich, wenn in rechtsstaatlichem Rahmen eine unverzügliche, schnelle und möglichst unbürokratische Sicherung ohnehin gespeicherter Computer- und Verkehrsdaten für nachfolgende Übermittlungsersuchen veranlasst werden könnte. Wenn auf der Straße ein Verdächtiger noch am Tatort angetroffen wird, kann er festgehalten und seine Identität festgestellt werden. Ebenso wäre es im Internet wichtig, dass ein Tatverdächtiger während der noch bestehenden Internetverbindung durch seinen Internet-Zugangsanbieter auf Ersuchen der Polizei identifiziert wird und die Daten für ein nachfolgendes Ermittlungsverfahren verfügbar gehalten werden. Zurzeit dauert es viel zu lange, bis eine Strafanzeige zu einem sachkundigen Polizeibeamten gelangt; außerdem existiert dann kein Verfahren, in dem der Polizeibeamte die unverzügliche Identifizierung des Verdächtigen durch den Internet-Zugangsanbieter anordnen kann.

Der Bund deutscher Kriminalbeamter fordert dementsprechend beispielsweise die Einrichtung von leistungsfähigen Spezialdienststellen zur Bekämpfung der Computerkriminalität, die Entwicklung eines Berufsbildes "Computerkriminalist" mit eigenen Aus- und Fortbildungsgängen, die zusätzliche Einstellung von Experten mit abgeschlossenen Studiengängen der Informatik, Mathematik und Betriebswirtschaft und Fortbildung zum Kriminalisten, die Entwicklung standardisierter Sachbearbeitungsverfahren für häufige Arbeitsweisen der Computerkriminalität, die Entwicklung internationaler Standards für IT-Forensik und die Benennung von Schwerpunktstaatsanwaltschaften für Computerkriminalität.

## 5.2 Kriminalprävention durch Datenschutz

Die häufigste Internet-Straftat ist Betrug, der oft durch Verwendung fremder Identitäten oder Zahlungsdaten begangen wird. Zur Verhütung von Identitätsdiebstahl und sonstigem Datenmissbrauch muss die Verfügbarkeit persönlicher Daten für Straftaten reduziert werden.

1. Dazu muss die Erfassung, Aufbewahrung und Weiterstreuung persönlicher Informationen von Internetnutzern reduziert werden:

- Anbietern von Internetdiensten muss untersagt werden, die Bereitstellung von Internetdiensten von der Angabe personenbezogener Daten abhängig zu machen, die zur Bereitstellung des Dienstes nicht erforderlich sind ("Koppelungsverbot")
- Schutz der Nutzer vor unangemessenen Datenverarbeitungs-Einwilligungsklauseln, indem klargestellt wird, dass derartige Klauseln einer gerichtlichen Kontrolle unterliegen
- Verbot der Erstellung von Nutzerprofilen ohne Einwilligung des Nutzers
- Erstreckung des Fernmeldegeheimnisses auf Anbieter von Internetdiensten
- Schaffung von Rechtssicherheit durch Klarstellung, dass der gesetzliche Datenschutz auch für Internet-Protocol-Adressen gilt
- Anbieter kommerzieller Internetdienste müssen persönliche Daten nach dem jeweiligen Stand der Technik schützen
- Anbieter kommerzieller Internetdienste müssen ihre Nutzer über die Dauer der Aufbewahrung ihrer Daten und über die getroffenen technischen Vorkehrungen zum Schutz ihrer Daten informieren

2. Außerdem muss die Durchsetzung der Gesetze zum Schutz persönlicher Informationen im Internet verbessert werden:

- Wettbewerber, Verbraucherzentralen und Datenschutzverbände müssen das Recht erhalten, Datenschutzverstöße kommerzieller Anbieter von Internetdiensten abzumahnen
- Der Verlust persönlicher Daten durch Anbieter von Internetdiensten muss einen Anspruch der Betroffenen auf pauschale Entschädigung nach sich ziehen (z.B. 200 Euro pro Person)
- Privacy by design: Kommerzielle informationstechnische Produkte zur Verarbeitung personenbezogener Daten dürfen nicht so voreingestellt sein, dass der Verwender gegen deutsches Datenschutzrecht verstößt

### 5.3 Kriminalprävention durch Verbraucherschutz

Security by default: Gebrauchsfertige Geräte zur Internetnutzung sowie kommerzielle Internetdienste müssen von ihrem Hersteller bzw. Anbieter so voreingestellt und bereit gestellt werden, dass die Vertraulichkeit, Verfügbarkeit und Unversehrtheit der Nutzerdaten dauerhaft nach den anerkannten Regeln der Technik gewährleistet ist (z.B. automatische Sicherheitspatches, Firewall, Schadprogrammerkennung). Der Nutzer muss dabei stets die volle Kontrolle über Vorkehrungen zu seinem Schutz behalten und diese auch abschalten können.

"Beipackzettel": Gebrauchsfertigen Geräten zur Internetnutzung sollten einfache Hinweise zur Vorbeugung vor häufigen Internetdelikten und zur richtigen Reaktion darauf beigefügt werden.

Opfern von Schadprogrammen sollte kostenfreie Unterstützung bei deren Beseitigung zur Verfügung stehen (z.B. Hotline).

## 6 Ergebnis

Im Ergebnis zeigt sich, dass die gegenwärtig verfügbaren Kommunikationsdaten ganz regelmäßig zur effektiven Aufklärung von Straftaten ausreichen. Die Erfahrung mit einer Vorratsdatenspeicherung in Deutschland zeigt, dass bei Erfassung sämtlicher Verbindungen nicht mehr Straftaten aufgeklärt oder verhindert werden als gegenwärtig; etwas anderes ergibt sich auch nicht aus dem Bericht des Bundeskriminalamts. Selbst wenn in vereinzelten Ermittlungen eine Erfassung aller Verbindungsdaten nützlich wäre, so stünde jedem erhofften Erfolg die Unaufklärbarkeit vieler anderer Straftaten und die Gefährdung von Menschenleben infolge einer Vorratsdatenspeicherung gegenüber.

Insgesamt betrachtet ist eine anlass- und verdachtslose Aufzeichnung jeder Telefon-, Handy-, E-Mail- und Internetverbindung damit für die Strafverfolgung nutzlos und zudem völlig unverhältnismäßig. Wer Straftaten wirklich wirksamer verfolgen will, müsste ganz andere organisatorische und gesetzliche Maßnahmen ergreifen.

09.10.2010