

# POLITIKUM

Heft 1 | 2016

ANALYSEN | KONTROVERSEN | BILDUNG

## BIG DATA

Algorithmen:  
Warum Kontrolle notwendig ist?

## LESEPROBE

Vorratsdatenspeicherung  
contra Datenschutz

Das Ende der Privatheit –  
Facebook, Twitter & Co.

Pro und Contra  
Iran-Atomabkommen

Deutschland: € 12,80, Österreich: € 13,-



WOCHEN  
SCHAU  
VERLAG

# Pro & Contra

## VORRATSDATEN- SPEICHERUNG



**D**ie Vorratsdatenspeicherung kommt nicht aus den Schlagzeilen heraus. Nachdem die EU-Mitgliedstaaten 2006 durch eine EU-Richtlinie zur Vorratsdatenspeicherung verpflichtet wurden, trat in Deutschland 2007 ein erstes Gesetz in Kraft. Nach zahlreichen Verfassungsbeschwerden wurde es 2010 vom Bundesverfassungsgericht in Teilen für nichtig erklärt. Auch Sabine Leutheusser-Schnarrenberger, Bundesjustizministerin von 2009 bis 2013, zählte zu den Kritikern/-innen des Gesetzes. Sie schlug 2011 als Alternative eine anlassbezogene Datenspeicherung vor. Es kam jedoch kein neues Gesetz zustande, sodass die EU-Kommission schließlich ein Vertragsverletzungsverfahren wegen Nichtumsetzung der EU-Richtlinie gegen die Bundesrepublik einleitete. 2014 erklärte allerdings der Europäische Gerichtshof auch die EU-Richtlinie für ungültig, sodass das Vertragsverletzungsverfahren hinfällig wurde.

**I**m Dezember 2015 ist das neue Gesetz zur VDS in Kraft getreten. Damit ist die Diskussion aber nicht beendet. Eine neuerliche Klage ist eingereicht – unter anderem von unserer Autorin.



# Reizthema Vorratsdatenspeicherung – warum wir sie benötigen

von UWE DÖRNHÖFER

## Warum tun sich manche Politiker so schwer mit dem Thema Innere Sicherheit?

„Die SPD hat entschieden, die Freiheit im digitalen Zeitalter abzuschaffen“, so die Grünen-Politikerin Göring-Eckardt am 22. Juni 2015 auf SZ-online zum vorliegenden Gesetzentwurf der Bundesregierung zur Wiedereinführung der Vorratsdatenspeicherung (VDS). Ein Zitat von vielen aus der politischen Diskussion der letzten Jahre. Noch drastischer prophezeien einige Journalisten, selbsternannte „Experten“ oder Netzaktivisten „das Ende des ‚anonymen Internets‘“ oder unterstellen gar, gesetzliche Beschränkungen bei Einführung einer Datenspeicherung würden bewusst durch staatliche Organe unterlaufen, um den Bürger auszuforschen. „Aufmachen, Sie haben meine Katze beleidigt!“, treibt Christian Stöcker die Übertreibung am 27.5.2015 in Spiegel-Online auf die Spitze.

Leider bleiben derartige Falschbehauptungen öffentlich meist unwidersprochen, die treffenden Gegenargumente werden nur in Fachkreisen diskutiert. Zwar wirken einige Argumente der Speicherungsgegner

.....

*Bedeutet Freiheit des Internets auch die Freiheit, anonym Straftaten begehen zu können?*

.....

auf den ersten Blick stichhaltig, u. a. weil sich einige Netzaktivisten auf das Postulat der „Freiheit des Internets“ beziehen. Allerdings ohne dabei zu erklären, was das genau bedeuten soll. Etwa auch die Freiheit, in der Anonymität des Internets Straftaten begehen zu können? Das kann in einem Rechtsstaat nicht gemeint sein! Unabhängig davon verkennen viele Kritiker, dass Vorratsdaten auch den Telefonverkehr betreffen, nicht nur das Internet.

## Pro

Befürwortern der Vorratsdatenspeicherung wird hingegen, wie von Christoph Hickmann in der SZ, „Law and Order-Mentalität“ unterstellt, oft gefolgt von dem Argument, die VDS sei verfassungswidrig, taue nicht zur Bekämpfung bzw. Verhütung von Straftaten, diene nur der Bespitzelung der Bürger oder führe zur weiteren Aushöhlung von Grundrechten. Diese Sichtweise hat sich in den letzten Jahren, insbesondere seit den Urteilen des Bundesverfassungsgerichts von 2008 und 2010 und des Europäischen Gerichtshofs für Menschenrechte im Jahr 2014 in der öffentlichen und veröffentlichten Meinung verfestigt.

Umso erstaunlicher war für viele Beobachter, dass die Bundesregierung sich im Frühjahr 2015 dennoch auf eine neue Gesetzesinitiative einigte, die nun harscher Kritik ausgesetzt ist. Leider geht im Getöse des politischen Tagesgeschäfts die Verteidigung der Speicherung unter. Überzeugungsarbeit in der Sache zu leisten heißt, Zuspitzungen zu vermeiden (auch in Bezug auf die Befürworter, die die Diskussion auf populistische Schlagworte wie Kinderpornografie und Terrorismus reduzieren) sowie das nachzuholen, was zu Beginn der Diskussion nicht ausreichend diskutiert worden ist: Aufklärung über die Speicherinhalte, Transparenz der Argumente der Fachleute!

## Was genau hat das Verfassungsgericht entschieden?

Manche Kritiker der VDS behaupten, das Bundesverfassungsgericht habe diese generell für verfassungswidrig erklärt. Das ist unzutreffend. Das höchste deutsche Gericht verwarf lediglich die gesetzliche Ausgestaltung der VDS aus dem Jahr 2007, die einige Dinge nicht klar genug regelte, z. B. Einzelheiten zur Speicherung, zur Datensicherheit und die unbestimmte Norm, die die Voraussetzungen für die Datenübermittlung betraf. Das Gericht stellte in den Leitsätzen jedoch klar, dass eine sechsmonatige Speicherung nur in der im

Gesetz gefundenen Form und nicht von vornherein verfassungswidrig sei. Sicherlich ist es nicht einfach, die umfassenden Auflagen des Verfassungsgerichts und des EuGH, der zwischenzeitlich ebenfalls urteilte, in einem Gesetz angemessen zu berücksichtigen, unmöglich erscheint es allerdings nicht.

Demnach ist die Einführung von VDS als solche nicht grundgesetzwidrig, sondern in erster Linie eine politische Grundsatzentscheidung, deren rechtliche Umsetzung im Rahmen der Rechtsprechung des Bundesverfassungsgerichts und des EuGH erfolgen muss. In diesem Zusammenhang sei auf andere Entscheidungen des höchsten deutschen Gerichts verwiesen, die das verfassungsrechtliche Gebot einer effektiven Strafverfolgung hervorheben (BverfGE 129, 208 <260> m.w.N.). Insofern sollte klar sein: Wer Vorratsdaten speichern möchte, darf das im Grundsatz tun. Dabei geht es um die Abwägung von Rechtseingriffen. Soweit es Rechtseingriffe im Bereich der Datenspeicherung betrifft, ergibt sich in der öffentlichen Wahrnehmung und Diskussion eine Schiefelage zwischen den „guten“ Daten, die der Privatwirtschaft nützen und die der Bürger freiwillig und nahezu ungezügelt weiterzugeben bereit ist, und den „bösen“ Daten, die der Staat speichert oder – wie im Falle der Vorratsdaten – bei Privatfirmen speichern lassen will.

Ein Teil der Gegner der VDS, wie im Jahr 2010 die damalige Bundesjustizministerin Sabine Leutheuser-Schnarrenberger, schlagen als Alternative das

„Ich mache mir Sorgen, dass die Sicherheitsorgane von Teilen der Bevölkerung als Bedrohung und nicht als Verbündeter zum Schutz ihrer Daten empfunden werden.“

Holger Münch, Präsident des Bundeskriminalamts

sogenannte Quick-Freeze-Verfahren vor. Mit „Quick Freeze“ oder auch „Schockfrost“ wird die sofortige Sicherung aller Verkehrsdaten zur Strafverfolgung bezeichnet. Das „Einfrieren“ der Daten geschieht nach Bekanntwerden einer entsprechend klassifizierten Straftat. Ein Vorteil für die Ermittler sei, aus einem „eingefrorenen“ Datenpool heraus in Ruhe die Daten suchen zu können, die in Verbindung mit der Straftat stehen. Ob die Speicherung einer derart großen und unspezifischen Datenmenge einen geringeren Eingriff als die Einführung von Mindestspeicherfristen darstellt, wird allerdings von Netzpolitikern wie Alvar Freude vom Arbeitskreis Zensur auf ZeitOnline (20.1.2011)

.....  
*Wer Vorratsdaten speichern möchte, darf das im Grundsatz tun*  
 .....

bezweifelt; andere, wie Staatsanwalt Dieter Kochheim, sehen gar einen größeren Rechtseingriff als bei VDS.

Weiter sprechen logisch-kriminalistische Erwägungen gegen diese Möglichkeit. Es kann nur auf die Daten zurückgegriffen werden, die beim „Einfrieren“, also nach Bekanntwerden eines Verbrechens, noch vorhanden sind. Alles, was im Vorfeld einer Straftat geschehen ist, wäre nicht gespeichert, auch für nachträglich bekannt werdende Verbrechen liefe die Regelung ins Leere, beispielsweise Morde, die zunächst als harmlos erscheinender Vermisstenfall bei der Polizei registriert werden.

### Freiwillige Preisgabe höchstpersönlicher Daten

Angesichts der – auch verfassungsrechtlich – erheblichen Aufregung um die Speicherung von Daten ist die Gelassenheit erstaunlich, mit der viele Menschen ihre Daten freiwillig zur Verfügung stellen. In Deutschland sind 100 bis 200 Millionen Kundenkarten im Umlauf, der Marktführer hat 20 Millionen aktive Karten-Nutzer. Demnächst werden automatische Notrufsysteme im Auto zur Pflicht, einzelne Kfz-Versicherungen bieten Rabatte an, wenn Telematik-Dienste zur Überwachung



Bedenkenlose Preisgabe persönlicher Daten über Social Media wie Facebook ...



des Fahrverhaltens im Pkw eingebaut sind. „Wearables“ oder Smartwatches gewinnen an Beliebtheit. Unter anderem zeichnen sie Puls, Schrittzahl, Aktivitäts- und Ruhephasen, Schlafrythmus und – GPS-gestützt – Lauf-, Wander- und Fahrradstrecken auf. Nahezu alle dieser Geräte werden mit dem Internet verbunden, um die Daten an zentraler Stelle zu speichern, teilweise erfolgt das öffentliche Posten der Fitnessaktivitäten in sozialen Netzwerken. Es ist zu prognostizieren, dass die Versicherungswirtschaft Wege suchen und finden wird,

.....

*Warum stößt  
Vorratsdatenspeicherung  
auf Widerstand, wenn die  
Preisgabe so vieler Daten  
freiwillig erfolgt?*

.....

an diese Daten zu gelangen, um die Versicherungsprämien nach dem Fitnesszustand der Nutzer gestalten zu können – ade solidarische Krankenversicherung!

Ein weites Feld im Bereich des Datensammelns sind international tätige amerikanische Großkonzerne, die die Entwicklung des Internets und der sozialen Medien in den letzten Jahren prägen. Es darf bezweifelt werden, ob Außenstehende noch durchschauen, welche Art von Daten diese Firmen unbemerkt vom Nutzer erheben, wie diese miteinander verknüpft werden und welcher Speicherdauer sie unterliegen. Auch die Datenverwendung ist nicht bekannt, kaum jemand liest bzw. versteht die Datenschutzrichtlinien der Unternehmen, bevor er das entsprechende Gerät benutzt. Vielen ist inzwischen bekannt: das Internet vergisst nichts.

Dennoch präsentieren Millionen von Deutschen ihr Privatleben in den sozialen Netzwerken, laden Fotos aus allen Lebensbereichen hoch, übermitteln ihre aktuellen Aufenthaltsorte, teilen mit, womit sie sich gerade beschäftigen oder zeigen der Welt, mit wem sie befreundet, verlobt oder verheiratet sind. Obwohl niemand weiß, was Messenger-Dienste alles auf ihre Server übertragen und speichern, nutzen allein ca. 30 Millionen Menschen in Deutschland den Marktführer, um Nachrichten, Bilder u. a. auszutauschen, Tendenz steigend. Problematisch am Vorgehen der genannten Firmen ist, dass eine datenschutzrechtliche Überprüfung ihrer gespeicherten Daten nicht möglich ist, da sie teilweise nicht deutschem bzw. europäischem Recht

unterliegen. Außerdem stehen Server an nicht bekannten Orten im Ausland, eine vollständige Überprüfung durch den deutschen Datenschutzbeauftragten wäre nicht möglich. Vor diesem Hintergrund sei die Frage erlaubt, warum eine stark begrenzte und klar geregelte VDS auf solchen Widerstand stößt, wenn die Preisgabe von so vielen anderen nicht minder sensiblen Daten gegenüber großen Internetdienstleistern freiwillig und ohne großes Aufheben erfolgt?

**Über die Pflicht,  
die Sicherheit aller Bürger zu schützen**

In einem demokratischen Rechtsstaat besteht der Zweck von Strafverfolgung in erster Linie darin, die (Grund-)Rechte der Bürger zu schützen – Leben, körperliche Unversehrtheit, Freiheit der Person, Eigentum. Polizei und Staatsanwaltschaft kommen dem durch Gefahrenabwehr einerseits und eine effektive Strafverfolgung andererseits nach. Jeder Eingriff der Strafverfolgungsorgane in Grundrechte einzelner Bürger dient allein dem Ziel, die Rechte Dritter oder der Gesamtgesellschaft zu schützen.

Polizeiliches Handeln ist also nie Selbstzweck. Es dient ebenfalls nicht, wie in Diktaturen, dem Zweck des Machterhalts. Deswegen sind z. B. Polizei und Staatsanwaltschaft personell und organisatorisch getrennt. Je stärker der Grundrechtseingriff, desto höher sind die gesetzlichen Hürden für dessen Zulässigkeit. Besonders wichtige Grundrechte können nur aufgrund richterlicher Verfügung eingeschränkt werden. Darüber hinaus sind alle Rechtseingriffe von Polizei und Staatsanwaltschaft von unabhängigen Richtern überprüfbar, umfassende Akteneinsichtsrechte schaffen Transparenz für die von den Maßnahmen Betroffenen. Im Laufe der Jahrzehnte weitete das Bundesverfas-



... oder beim „Sexting“ – beliebt bei Jugendlichen

sungsgericht den Geltungsbereich der Grundrechte aus, reagierte auf neue Entwicklungen, kreierte z. B. im Volkszählungsurteil 1983 das neue Grundrecht der „informationellen Selbstbestimmung“. Nicht zuletzt dadurch werden seit vielen Jahren die Anforderungen für die Anordnung vieler Eingriffsbefugnisse erhöht. Eine Verringerung der Anforderungen ist mir hingegen nur in einem Fall bekannt.

Insofern erscheint die bisweilen vernehmbare Behauptung, die Bundesrepublik entwickle sich zu einem Überwachungsstaat, geradezu absurd. Als einer derjenigen, der seit Jahren täglich mit diesen sensiblen Daten umgeht, empfinde ich einige Kommentare und Unterstellungen persönlich als ehrverletzend. Der Präsident des Bundeskriminalamts, Holger Münch, formuliert es so: „Ich mache mir Sorgen, dass die Sicherheitsorgane von Teilen der Bevölkerung als Bedrohung und nicht als Verbündeter zum Schutz ihrer Daten empfunden werden.“

An dieser Stelle sei darauf verwiesen, dass die VDS zum Zweck der Strafverfolgung gänzlich unabhängig von der Tätigkeit der deutschen und ausländischen Nachrichtendienste zu sehen ist. Wer beides vermischt, versteht entweder den Aufbau der deutschen Sicherheitsarchitektur und die klare Trennung zwischen Polizei und Nachrichtendiensten nicht und sollte daher zu dem komplexen Thema besser schweigen, oder er will bewusst in die Irre führen.

Wenn die Strafverfolgungsorgane nicht in der Lage sind, Straftaten zu verfolgen oder Gefahrenabwehr zu betreiben, beeinträchtigt das die Rechtsposition der Bürger. Die freiheitlich-demokratische Grundordnung der Bundesrepublik, ein Europa offener Grenzen sowie



**Neue Straftatbestände: Datendiebstahl und -fälschung**

endliche Personal- und Sachressourcen bedingen hierbei zwangsläufig Defizite. Diese Defizite werden je nach Gesellschaftsschicht unterschiedlich ausgeglichen. Die Bandbreite reicht von Nichtanzeigen von Straftaten, Selbstjustiz bis hin zu Investitionen zum Schutz privater Rechte. Dennoch sind in Deutschland im Gegensatz zu anderen westlichen Staaten bislang nur wenige „Gated Communities“ entstanden. Anders als in anderen Millionenstädten kann man in Deutschland in der Regel gefahrlos nachts die öffentlichen Verkehrsmittel benutzen.

Lässt das staatliche Engagement jedoch weiter nach oder billigt die Gesellschaft rechtsfreie Räume im Bereich der Inneren Sicherheit, führt das insgesamt zu einer Schlechterstellung der Bürger. Die Unter- und Mittelschicht kann dies kaum oder gar nicht kompensieren, die Oberschicht dagegen viel besser, z. B. durch Privatdetektive, Sicherheitsfirmen und Rechtsanwälte.

.....

*Der Zweck von  
Strafverfolgung besteht vor  
allem darin, die Rechte der  
Bürger zu schützen*

.....

Insofern treffen Strafbarkeitslücken und Vollzugsdefizite vorrangig sozial schlechter gestellte Menschen, umgekehrt dient richtig verstandene Innere Sicherheit der sozialen Gerechtigkeit und der freien Entfaltung der Persönlichkeit. Rechtsstaatlich kontrollierte und legitimierte Innere Sicherheit dient somit auch der sozialen Gerechtigkeit und der freien Entfaltung der Persönlichkeit.

**Welche Daten werden bereits jetzt gespeichert?**

Zur Meinungsbildung bezüglich VDS bedarf es einer ganzheitlichen Betrachtung dessen, um welche Daten es sich dabei handelt, was bereits jetzt aufgrund der Bedürfnisse der Privatwirtschaft gespeichert wird, wie sensibel mit diesen Daten umgegangen wird und schließlich – ganz entscheidend –, in welchem Gesamtkontext des Bereichs „Big Data“ diese Daten zu sehen sind.

Viele Bürger wissen nicht, dass Daten über ihr Nutzungsverhalten bereits seit langer Zeit gespeichert werden (§ 96 Telekommunikationsgesetz), denn die Telekommunikationsanbieter benötigen diese Informationen für eigene Zwecke, z. B. für die Abrechnung,





**WOCHENSCHAU  
VERLAG**

... ein Begriff für politische Bildung



**Gratis-  
Beilage**

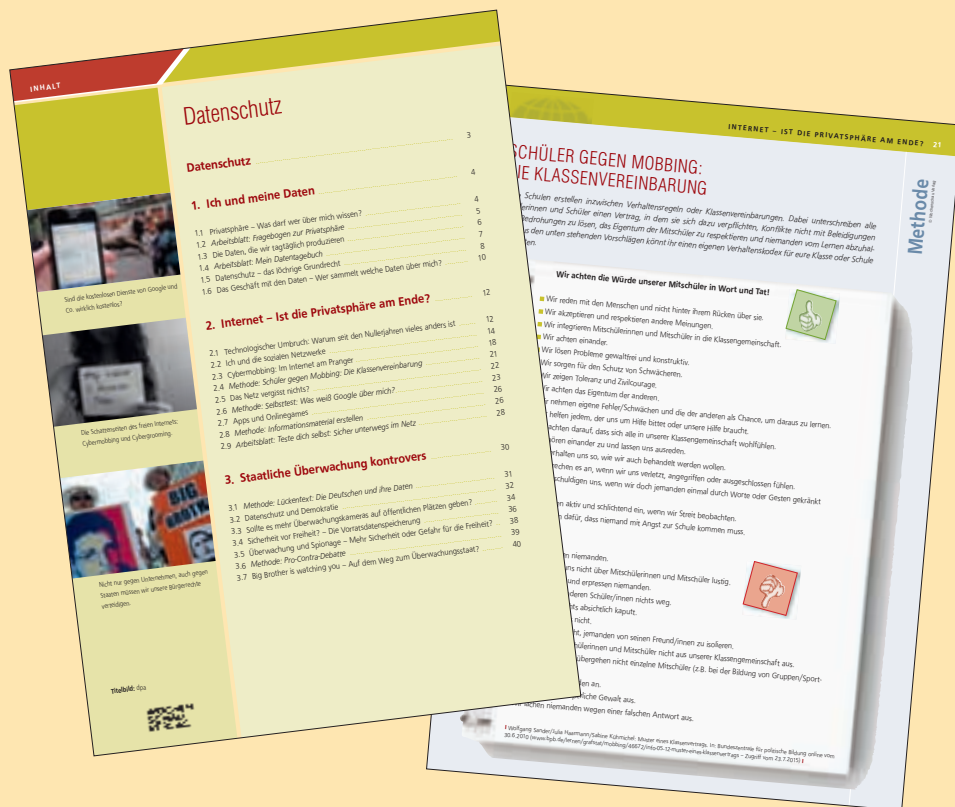
# Datenschutz

Privatsphäre, Datenschutz, Vorratsdatenspeicherung – diese Begriffe mögen Schüler und Schülerinnen als abstrakt und uninteressant empfinden. Doch im Zeitalter von Google, Facebook, Überwachungskameras, Apps und Cybermobbing haben Jugendliche tagtäglich mit ihnen zu tun.

Zielsetzung des Basisheftes, das sich an Schüler der 7. und 8. Jahrgangsstufe richtet, ist die Sensibilisierung für den Umgang mit den eigenen Daten. Das Heft liefert Definitionen und rechtliche Hintergründe, zeigt Widersprüche auf Seiten des Staates auf (Stichworte Datenschutzbeauftragter, Vorratsdatenspeicherung) und bestärkt Jugendliche durch konkrete Arbeitsvorschläge in der Selbstreflexion sowie in der kritischen Auseinandersetzung mit den oben genannten Begriffen.

In der Beilage „Checkheft Datenschutz“ finden Schülerinnen und Schüler konkrete Handlungsempfehlungen und Tipps, wie sie sich und ihre Daten im Internet schützen können.

Sek. I, Best.-Nr. 1315, 48 S. inkl. Checkheft, € 17,10  
Klassensatzpreis ab 10. Expl.: pro Exemplar € 10,20



**JETZT DEN AKTUELLEN NEWSLETTER BESTELLEN: [WWW.WOCHENSCHAU-VERLAG.DE](http://WWW.WOCHENSCHAU-VERLAG.DE)**

Tel. 06196/86065 · [www.wochenschau-verlag.de](http://www.wochenschau-verlag.de) · [info@wochenschau-verlag.de](mailto:info@wochenschau-verlag.de) · [www.facebook.com/wochenschau.verlag](https://www.facebook.com/wochenschau.verlag)

**POLITIKUNTERRICHT**

aus betriebstechnischen Gründen und vor allem zur Auswertung des Nutzerverhaltens. Anbieter von Telefon- und Internetdiensten speichern Zeit und Dauer von Telefonaten, benutzte Telefonnummern, Standort

.....

*Rechtsstaatlich kontrollierte  
innere Sicherheit dient der  
sozialen Gerechtigkeit*

.....

des benutzten Funkmasts bei Handygesprächen und die Kennung von Internetverbindungen (IP-Adressen). Die Speicherfristen betragen je nach Anbieter und Art der Daten zwischen 3 und 180 Tagen (Mahnken 2005).

Zum Zweck der Verhinderung und zur Aufklärung von Straftaten oder zum Schutz wichtiger Rechtsgüter benötigen Polizei und Staatsanwaltschaft die Hilfe privater Institutionen und des Bürgers. Im Fall der Telekommunikations-Daten erfolgt deren Übermittlung an Polizei und Justiz aufgrund der Polizeigesetze der Bundesländer (bei Übermittlung zur Gefahrenabwehr), für die Strafverfolgung ist seit dem Jahr 2001 der §100g der Strafprozessordnung (StPO) einschlägig. Er ersetzte eine alte Vorschrift des analogen Telefonzeitalters aus dem Jahr 1928 (!). Das D-Netz war zu diesem Zeitpunkt bereits

neun Jahre im Betrieb. So lange kann es also dauern, bis der Gesetzgeber auf neue Entwicklungen reagiert.

Aufgrund der Sensibilität dieser Daten dürfen sie nur bei Straftaten von „erheblicher Bedeutung“, z. B. Raub, Tötungsdelikte, Vergewaltigung, gewerbsmäßiger Einbruch, Betäubungsmittelhandel oder eine Straftat, die mittels eines Telekommunikationsmittels begangen wurde, übermittelt werden. Bei Bagatelldelikten wie Beleidigung, Sachbeschädigung oder Ordnungswidrigkeiten greift die Norm nicht. Die Staatsanwaltschaft prüft die rechtlichen Voraussetzungen und beantragt einen Beschluss beim Gericht, nur bei Gefahr im Verzug darf die Staatsanwaltschaft direkt eine Eilanordnung erlassen, die allerdings vom Richter nachträglich überprüft und bestätigt werden muss. Das geschah 2013 in immerhin 12 572 Ermittlungsverfahren. Nicht wenig, aber angesichts einer Gesamtzahl von fast sechs Millionen Straftaten im Jahr auch nicht viel.

Die Schwäche der aktuellen Gesetzgebung, das Dilemma der Strafverfolger zeigen bereits die o. a. Zahlen des Bundesamtes für Justiz. In den 12 572 Ermittlungsverfahren wurden Anfragen zu 20 242 Anschlüssen gestellt, in 3 330 Fällen blieb die Maßnahme ergebnislos, weil die abgefragten Daten ganz oder teilweise nicht (mehr) verfügbar waren. Der Grund hierfür ist, dass die Verkehrsdaten nicht für die Strafverfolger gespeichert



Zunehmende Herausforderung: Bedrohung durch Terroristen





© picture alliance/Cultura RF

**Viele Bürger wissen nicht, dass Daten über ihr Nutzungsverhalten ohnehin gespeichert werden – durch die Telekommunikationsanbieter.**

werden, sondern, wie bereits ausgeführt, ausschließlich für eigene Zwecke der TK-Anbieter. Mit anderen Worten: Was die Firmen nicht oder nicht mehr benötigen, wird gelöscht bzw. gar nicht erhoben. Technische Entwicklungen, Flatrates und Datenschutzbestimmungen führen dazu, dass immer weniger gespeichert wird. Die Vielzahl von TK-Anbietern hat unterschiedlichste Speicherfristen zur Folge, manche speichern bestimmte Daten generell nicht, z. B. IP-Adressen. Für ankommende und abgehende Gespräche bestehen unterschiedliche Fristen. Hinzu kommt, dass Dritten der Einblick in die hochkomplexen technischen Abläufe von modernen TK-Netzen fehlt, der Wahrheitsgehalt einer Nullauskunft kann im Einzelfall von Außenstehenden nicht überprüft werden. Angesichts dieser Betrachtungen stellt sich die Frage, worin der Mehrwert von Vorratsdaten liegt und weshalb diese angesichts der bereits umfangreichen Datensammlungen der Netzbetreiber derart stark kritisiert werden.

### **Was also ist neu an Vorratsdaten?**

VDS bedeutet letztlich, dass die entsprechenden Firmen verpflichtet werden, bestimmte Verkehrsdaten für einen festgelegten Zeitraum zu erheben und zu speichern, also einen „Vorrat“ an Daten anzulegen. Letztlich läuft das auf Ergänzungen zur Speicherung der Verkehrsdaten hinaus, die ohnehin gespeichert werden, insofern trifft der Begriff „Mindestspeicher-

fristen“ (MSF) besser zu als Vorratsdatenspeicherung. Wichtig: Auch diese Daten werden nicht von staatlichen Stellen, sondern ausschließlich von Privatfirmen erhoben und gespeichert und diesen nur unter engen Voraussetzungen zugänglich(er) gemacht.

Im Gegensatz zu den Verkehrsdaten, die weiter im Interesse der betrieblichen Verwendung der Betreiberfirmen gespeichert werden, unterliegen Vorratsdaten einer genauen Zweckbestimmung. Sie dürfen nur unter den unten skizzierten Voraussetzungen an Polizei und Justiz herausgegeben werden. Eine Verwendung für andere Zwecke ist verboten. Die EU-Richtlinie sah Speicherfristen von bis zu zwei Jahren vor, die deutsche Regelung von 2007 sechs Monate. Im nun verkündeten Gesetz sind zehn Wochen für Verbindungsdaten und vier Wochen für ortsbezogene Daten (Funkmasten) vorgesehen. Nicht gespeichert werden hingegen Kommunikationsinhalte wie SMS-Texte oder Sprachaufzeichnungen.

Für Behörden gelten besonders hohe Anforderungen an den Datenschutz und die Datensicherheit, im besonderen Maße betrifft das die Polizei. Deren Einhaltung gewährleisten behördeninterne Datenschutzbeauftragte und die Datenschutzbeauftragten des Bundes und der Länder. Staatsanwaltschaft und Polizei sind direkt den Ministerien unterstellt, diese wiederum unterliegen

.....  
*Vorratsdaten unterliegen  
 einer genauen  
 Zweckbestimmung und  
 strenger Kontrolle*  
 .....

einer parlamentarischen Kontrolle, hinzu kommt die Kontrolle durch Gerichte, betroffene Privatpersonen und die Öffentlichkeit. Polizeibeamte unterliegen weiter einer besonderen Dienstverschwiegenheit, die bei vertraulichen Ermittlungssachverhalten selbst gegenüber anderen Polizeibeamten gilt. Verstöße werden straf- und disziplinarrechtlich konsequent verfolgt. Insofern bestehen keine Zweifel, dass mit erhobenen Vorratsdaten innerhalb der Polizei seriös umgegangen wird, der bisherige Umgang mit anderen sensiblen Daten belegt das. So ist der Zugriff auf andere Datenbestände wie Meldeadresse, Personalausweis, Visa, Führerschein, Kraftfahrzeug, Vorstrafen etc. auf gesetzlicher Grundlage relativ unkompliziert – manchmal per direkter Datenleitung – möglich. Für die Aufrechterhaltung

der Ordnung und Sicherheit ist diese Möglichkeit anerkanntermaßen von zentraler Bedeutung. Unter diesen Aspekten ist unverständlich, weshalb die Speicherung von Vorratsdaten, auf die per se erst einmal niemand Zugriff hat, eine derartige Kontroverse auslöst. Denn der Nutzen der Vorratsdaten wäre enorm.

### Warum wäre die Vorratsdatenspeicherung so nützlich?

Generell muss es Aufgabe des Gesetzgebers sein, die Institutionen des Staates in die Lage zu versetzen, auf neue Entwicklungen zu reagieren. Insbesondere der digitale Wandel stellt dabei eine große Herausforderung dar. Im Bereich der Inneren Sicherheit bedeutet das z. B. die Entstehung neuer Straftatbestände (Computerbetrug, Datendiebstahl, Fälschung beweisheblicher Daten) und im Gegenzug die Ausweitung von Ermittlungskompetenzen wie Mitte der 1990er Jahre durch die Möglichkeit zur Überwachung von Mobiltelefonen. Nach Einführung des D-Netz-Standards war dies nämlich für einige Jahre nicht möglich gewesen. Ein Anbieter warb sogar indirekt mit der „Abhörsicherheit“ seines Netzes. Doch 15 Jahre nach Beginn der digitalen Revolution ist die Anpassung an die neue Wirklichkeit ebenso wenig erfolgt, wie sie notwendig wäre. Gestiegene Anforderungen beim Daten- und Persönlichkeitsschutz seit 2008 mit erweiterten Benachrichtigungs- und Löschungspflichten bei verdeckten Ermittlungsmaßnahmen gehen in die entgegengesetzte Richtung. U. a. müssen Betroffene von Telefonüberwachungen informiert werden, Gespräche mit dem Anwalt und aus dem höchstpersönlichen Lebensbereich sind sofort zu löschen.

Allerdings bestehen mehrere Hindernisse, den konkreten Nutzen von VDS zu begründen. Erstens ist Strafverfolgungsbehörden die Offenlegung von Ermittlungstaktiken grundsätzlich verboten. Zweitens beschränkt sich die Klärung von Straftaten selten auf nur ein einziges Beweismittel, was auch bedeutet, dass niemand allein aufgrund einer Datenspur verurteilt werden wird. Drittens ist es im Einzelfall schwer verifizierbar, wie viel Ermittlungsaufwand gespart wird, wenn durch VDS ein unbekannter Täter ermittelt würde. Ein Beispiel wären DNA-Reihenuntersuchungen nach Tötungsdelikten, die einen erheblichen Grundrechtseingriff für eine Vielzahl von Unbeteiligten bedeuten, Ermittlungsressourcen binden und eventuell obsolet wären, wenn der Täter anhand von TK-Daten ermittelt und dann mittels eines DNA-Vergleichs und weiterer Beweise überführt werden könnte.

Eine hohe Aufklärungsquote wirkt nicht nur präventiv, sondern erhöht auch das Sicherheitsgefühl der Bürger. „Ein Einbruch in eine Wohnung hinterlässt nicht nur materielle, sondern vor allem auch seelische Wunden“, sagte Münchens Polizeipräsident Hubertus Andrä. Er bezog sich auf die im Jahr 2014 sprunghaft angestiegenen Wohnungseinbrüche, die Steigerung in München und Bayern betrug mehr als 25 %. Gemeint ist damit, dass unabhängig vom Sachschaden Einbrüche – teilweise begangen während der Anwesenheit der Bewohner – zur Traumatisierung der Opfer führen

.....

*Nach 15 Jahren digitaler Revolution ist noch keine Anpassung an die neue Wirklichkeit erfolgt*

.....

können. Ziel der meist organisiert vorgehenden Tätergruppen sind nicht nur die Villen der Oberschicht, die entsprechend gut gesichert sind, sondern alle Bürger sind betroffen. Ein wirksamer Bekämpfungsansatz liegt in der Auswertung der Telekommunikationsspuren der Täter, eine effektive VDS wäre hierbei hilfreich.

Neben der Alltagskriminalität ist die Bedrohung durch Terroristen eine der Herausforderungen der Gegenwart, denen sich eine aufgeklärte Gesellschaft in der nahen Zukunft stellen müssen. Der internationale islamistische Terrorismus, aber auch rechter



© picture alliance/Ulrich Baumgarten

Eine hohe Aufklärungsquote würde das Sicherheitsgefühl erhöhen: Beispiel Wohnungseinbrüche

und linker Terror sind reale Bedrohungen unserer Zeit und werden es (leider) auch bleiben.

Modernste Fahndungs- und Ermittlungsmethoden können Terroranschläge erschweren oder gar verhindern, wie das in jüngster Vergangenheit in Deutschland mehrfach der Fall war. Eine vollständige Sicherheit ist angesichts von Terroristen, die zu allem entschlossen sind, natürlich eine Illusion, wie die Anschläge in Frankreich im Januar 2015 zeigen. Dennoch macht gerade dieses Beispiel deutlich, wie wichtig die VDS zur Aufklärung dieser Taten ist. Die Strafverfolger konnten nach dem Anschlag auf „Charlie Hebdo“ anhand der Verbindungs- und Standortdaten die Unterstützer der Terroristen identifizieren und ihren Aufenthaltsort ermitteln, was wahrscheinlich weitere Tötungsdelikte verhindert hat. Auch nach Entdeckung des NSU im Jahr 2011 wären Vorratsdaten hilfreich gewesen, um herauszufinden, wer die Unterstützer des Trios Mundlos, Bönnhardt und Zschäpe gewesen sind. Diese sind nach wie vor nicht alle bekannt.

Angesichts der genannten Bedrohungslagen, auch der Brandanschläge auf Asylbewerberunterkünfte, muss den Politikern jedweder Couleur klar sein, dass die sicherheitspolitischen Versäumnisse schnell bereinigt werden müssen.

### Gesetzgebungsverfahren 2015

Nach langer politischer Diskussion hat der Bundestag im Oktober 2015 ein Gesetz zur Einführung einer Speicherpflicht beschlossen. Die Änderungen zur 2007 beschlossenen Vorratsdatenspeicherung sind vielfältig. Die Übermittlungsbefugnis an die Polizei wurde in einem abschließenden Straftatenkatalog klar geregelt. Doch nicht alles erscheint gelungen, was auf die Notwendigkeit einer Kompromissfindung innerhalb der Großen Koalition zurückzuführen sein dürfte. Bloße Verkehrsdaten werden unnötigerweise stärker geschützt als die Aufzeichnung des gesprochenen Wortes (§ 100a StPO). Die Befugnisse dürften zudem nicht ausreichend sein, um im Bereich schwerer Einzeldelikte und gewerbsmäßig begangener typischer Delikte der Organisierten Kriminalität oder bei Cyber-

crime-Straftaten die erhofften Ermittlungserfolge zu erzielen. Auch die Regelungen zu den Standortdaten und die Beschränkungen bei der elektronischen Post sind unzureichend und bedürfen der Überarbeitung. Im

Klartext: Der Straftatenkatalog für die Verwendung

von Vorratsdaten ist enger als der für die

Telefon- oder Wohnraumüberwachung!

Überspitzt formuliert: Einbrecher,

Räuber und Enkeltrickbetrüger darf

man zwar abhören, wenn man

ihre Telefonnummer kennt. Aber

auf Vorratsdaten zugreifen, um

diese Nummer zu ermitteln, ist

nicht erlaubt.

Kriminelle Kreise und ihre juristi-

schen Berater werden erst mal auf-

atmen, weil sie die Lücken weiterhin

nutzen können, bis das Thema wieder

auf die politische Agenda kommt.

Dann wird auch über die Schließung

weiterer Ermittlungslücken wie die

zunehmende Datenverschlüsselung

in kriminellen Netzwerken zu dis-

kutieren sein.

Dennoch: ein kleiner Schritt

in die richtige Richtung ist getan.

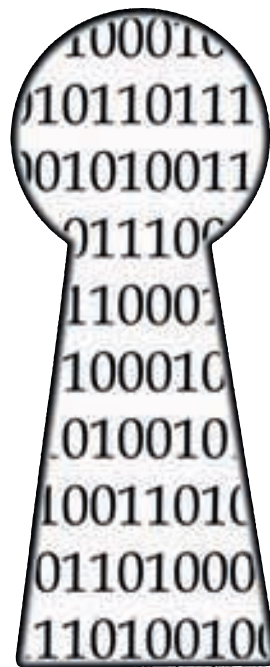
Ein rechtspolitisches Versäumnis

seit dem Verfassungsgerichtsurteil

von 2010 ist geheilt, wichtige Ermitt-

lungs- und Fahndungslücken lassen sich ungeachtet

der skizzierten Mängel schließen.



© dpa

### LITERATUR

Mahnken, Eva 2005: Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten. BKA November.



**Uwe Dörnhöfer**, Erster Kriminalhauptkommissar, ist Leiter der Ermittlungsgruppe Enkeltrick beim Dezernat für Organisierte Kriminalität des Polizeipräsidiums München.