POLITIKUM

Heft 1 | 2016

ANALYSEN | KONTROVERSEN | BILDUNG

BIG DATA

Algorithmen:
Warum Kontrolle notwendig ist

...forschung?

Vorratsdatenspeicherung
contra Datenschutz

Das Ende der Privatheit –
Facebook, Twitter & Co.

Pro und Contra
Iran-Atomabkommen

LESEPROBE

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

WOCHEN SCHAU VERLAG

Vierteljahreszeitschrift | 2. Jahrgang | Frühling 2016

POLITIKUM

EDITORIAL

Was kommt da bloß auf uns zu? Eine Bedrohung, größer als die Atombombe, wie Robert Shiller vermutet, einer der schärfsten Kritiker des Internets? Oder sind die Deutschen in einem für sie typischen Kulturpessimismus und paralysiert durch ungerechtfertigte Zukunftsängste gerade dabei, ihren Wohlstand aufs Spiel zu setzen, wie Christian Illek warnt, Personalvorstand bei der Telekom? Die öffentliche Debatte über das Internet und seinen großen Bruder „Big Data“ hat erheblich an Dynamik und Schärfe zugenommen, seitdem Edward Snowden enthüllt hat, welche Möglichkeiten in Big Data stecken, zum Segen und zum Fluch der Menschen.

Wie aus Datenströmen Macht wird: Sirenenserver (ab Seite 9)

Ungewissheit hat natürlich Unsicherheit zur Folge. Propheten des Untergangs wie des Heils haben Hochkonjunktur. Wie so oft dürfte die Wahrheit nahe der Mitte liegen. Das Internet wird die Arbeitswelt verändern, aber nicht das Oberste nach unten kehren. Die Vorratsdatenspeicherung wird die Persönlichkeitsrechte der Bürger betreffen, aber deren Freiheit nicht zerstören. Das Internet wird viele Bereiche des Lebens bereichern.

Jenseits davon verändert die Erzeugung und die Analyse von Massendaten unser Bild von der Wirklichkeit, unsere Wahrnehmung der Welt. Dieser Vorgang ist ein eminent politischer, der größte Achtsamkeit verdient und der politischen und rechtlichen Bearbeitung bedarf. Wir brauchen mehr Governance der Algorithmenwelt, damit uns Big Data nicht aus dem Ruder läuft! (Klaus Mainzer)

So wie sich unser Bild der Welt und auf die Welt ändert, verändern sich die Wissenschaften, die sich mit deren Vermessung und Erfassung beschäftigen. Themen, Fragestellungen, Theorien und Methoden werden sich erheblich wandeln. Von all dem handelt diese Ausgabe von POLITIKUM und von einigem mehr.

S. Schieren

Stefan Schieren

Seite 4

Schwerpunkt
Die Macht der Algorithmen
Vermehrt nehmen Algorithmen Entscheidungen vor, die früher von Menschen getroffen wurden. Dadurch verändern sich die Machtverhältnisse grundlegend, und die Frage der Verantwortung stellt sich neu.

Seite 14

Schwerpunkt
Algorithmen und Big Data als Politikum
Big Data droht uns politisch und gesellschaftlich aus dem Ruder zu laufen, wenn für die allgegenwärtigen Algorithmen keine neue Governance gefunden wird.

„Weil die Digitalisierung mit dem Neoliberalismus einherging, wurde viel zu lange auf eine demokratische Regulierung verzichtet."
Heiko Maas, Bundesminister der Justiz und für Verbraucherschutz

Seite 20

Schwerpunkt
Das Politische der Großdatenforschung
Die Möglichkeiten von Big Data lassen eine neue Informationswissenschaft entstehen, die ihre theoretischen und methodischen Grundlagen erst noch entwickeln muss. Denn die Methoden der analogen Welt können nicht einfach auf die Welt der sozialen Medien übertragen werden.

Seite 32

Schwerpunkt
Die vierte industrielle (R)evolution
Das „Internet der Dinge" wird die Arbeitswelt nicht auf einen Schlag revolutionieren. Es wird sie aber unaufhaltsam verändern. Damit das verträglich geschieht, bedarf es der gesellschaftlichen und rechtlichen Gestaltung.

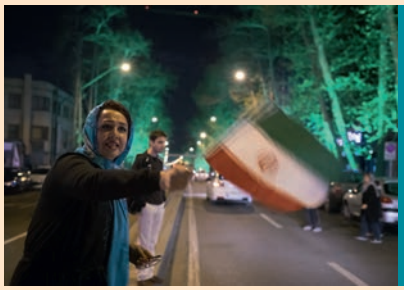
Seite 43

Interview
Muss es neue gesetzliche Regelungen für die digitale Welt geben? Und welche Rolle spielt die EU dabei? Ein Gespräch mit **Jan Philipp Albrecht**, dem innen- und justizpolitischen Sprecher der Grünenfraktion im Europäischen Parlament.


Seite 48

Pro & Contra
Vorratsdatenspeicherung

Auch nach Verabschiedung des neuen Gesetzes im Herbst 2015 ist die Diskussion um Vorratsdaten und Datenschutz nicht beendet. Ob Nutzen oder Schaden überwiegen, ist bei Befürwortern und Gegnern höchst umstritten.


Seite 64

Forum
Atomabkommen mit dem Iran

War das Abkommen ein historischer Durchbruch oder ein epochaler Fehler? Die Meinungen dazu gehen weit auseinander, und die Deutlichkeit der Positionen signalisiert: Bedeutendes ist in jedem Fall geschehen.


Seite 74

Filmbesprechung
Citizenfour

Der Film von Laura Poitras über die Snowden-Affäre in der Kritik.

Pro & Contra

Die 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.

Im 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

Pro

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.

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, tauge 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 Schieflage 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 Leutheusser-Schnarrenberger, schlagen als Alternative das

Bedenkenlose Preisgabe persönlicher Daten über Social Media wie Facebook …

> **„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 „Schockfrosten" 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

des Fahrverhaltens im Pkw eingebaut sind. „Wearables“ oder Smartwatches gewinnen an Beliebtheit. Unter anderem zeichnen sie Puls, Schrittzahl, Aktivitäts- und Ruhephasen, Schlafrhythmus 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!

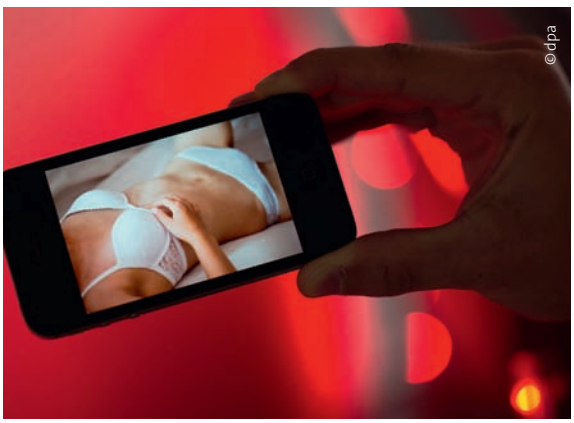
Ein weites Feld im Bereich des Datensammelns sind international tätige amerikanische Großkonzerne, die die Entwicklung des Internets und der sozialen Medien in den letzten Jahren prägen. Es darf bezweifelt werden, ob Außenstehende noch durchschauen, welche Art von Daten diese Firmen unbemerkt vom Nutzer 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

© serpeblu – fotolia.com

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,

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

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 Außenstehen 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 „Mindestspeicherfristen" (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 beweiserheblicher 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

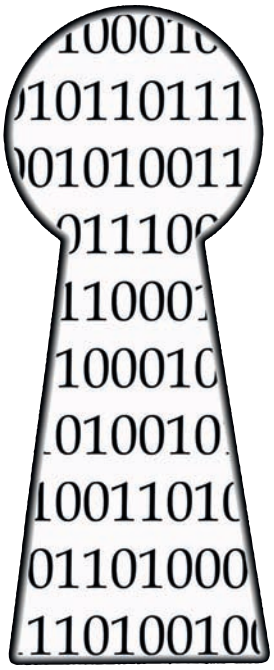
können. Ziel der meist organisiert vorgehenden Tätergruppen sind nicht nur die Villen der Oberschicht, die entsprechend gut gesichert sind, sondern alle Bürger sind betroffen. Ein wirksamer Bekämpfungsansatz liegt in der Auswertung der Telekommunikationsspuren der Täter, eine effektive VDS wäre hierbei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

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

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, Böhnhardt und Zschäpe gewesen sind. Diese sind nach wie vor nicht alle bekannt.



© dpa

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 Cybercrime-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 juristischen Berater werden erst mal aufatmen, 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 diskutieren sein.

Dennoch: ein kleiner Schritt in die richtige Richtung ist getan. Ein rechtspolitisches Versäumnis seit dem Verfassungsgerichtsurteil von 2010 ist geheilt, wichtige Ermittlungs- und Fahndungslücken lassen sich ungeachtet der skizzierten Mängel schließen.

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.

WOCHEN SCHAU VERLAG

... ein Begriff für politische Bildung

POLITIKUNTERRICHT

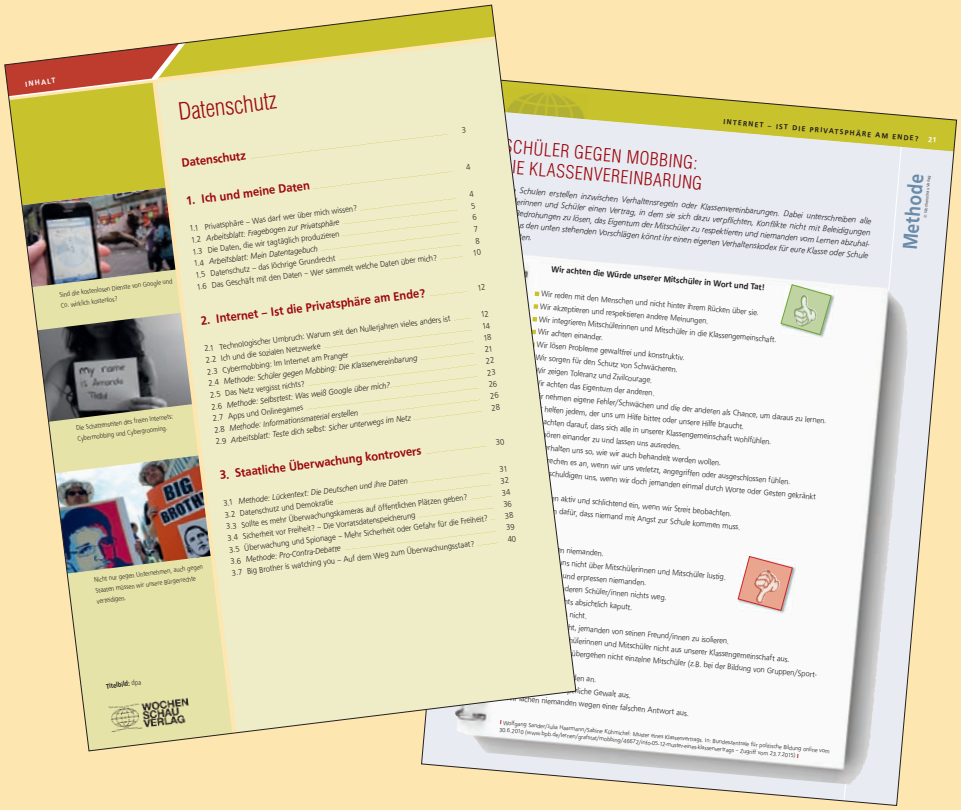
Datenschutz

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

Tel. 06196/86065 · www.wochenschau-verlag.de · info@wochenschau-verlag.de · www.facebook.com/wochenschau.verlag

Big Data und Datenschutz – ein unversöhnlicher Gegensatz?

von SABINE LEUTHEUSSER-SCHNARRENBERGER,
Bundesministerin a. D.

Contra

Die Digitalisierung durchdringt inzwischen alle Lebensbereiche. Es entstehen täglich unvorstellbare Datenmengen, deren Speicherung, Verarbeitung, Analyse und Vernetzung kaum mehr technische Grenzen gesetzt sind. Das Smart Home, Gesundheits-Apps, das Auto als rollendes Smartphone und online-Bankgeschäfte jeglicher Art sind nur einige Aspekte des immer transparenter werdenden Verhaltens der Menschen. Mittels Algorithmen werden die erfassten Daten von global agierenden Konzernen für ihre Geschäftszwecke analysiert und vernetzt. Das betrifft gerade nicht nur statistische, technische Daten, sondern vorwiegend Daten mit Bezug zu Personen, die aus ihrem online- und Surfverhalten mit und ohne ihr Wissen gewonnen und zu Profilen zusammengeführt werden, um sie dann z. B. für das Angebot gezielter Werbeplätze zu verwenden. Durch angelegte Verhaltensmuster, also Datenraster, künftiges Verhalten vorhersehbar zu machen und damit dem Nutzer ein auf ihn zugeschnittenes Angebot von Produkten und Dienstleistungen präsentieren zu können, gehört zu einem der immer erfolgreicher werdenden Geschäftsmodelle.

Data mining, Big Data, künstliche Intelligenz und das Internet der Dinge kennzeichnen diese rasante digitale Entwicklung. Die Digitalisierung des Lebensraums ist einer der Megatrends der kommenden Jahre, an dem viele mitverdienen wollen: die internationalen IT-Konzerne, die Energiewirtschaft, die Gesundheitsbranche, die Automobilindustrie, die Telefonhersteller und die Versicherungen. Neben den unbestreitbaren Vorteilen dieser Entwicklungen für Wirtschaft und Wohlstand dürfen die Risiken nicht vergessen werden. Politiker beschwören gern in ihren Sonntagsreden das 21. Jahrhundert als das Jahrhundert der Daten und lassen sich auf Messen wie der Ifa oder Cebit gern mit den neuen Hightech-Geräten abbilden. Es entsteht der Eindruck, dass die neue Technik bedingungslos angenommen und die Gefahren bewusst ausgeblendet werden. Jede neue Technik hat neben Chancen auch Nachteile. Entscheidend ist, wie sie eingeschätzt werden und wie damit umgegangen wird. Eines ist unstreitig: Daten sind Macht. Wer über sie verfügt, verfügt über den Rohstoff oder das Gold oder die Schmierseife der größten technologischen Entwicklung, der Digitalisierung.

Eines ist unstreitig: Daten sind Macht

Die Kehrseite dieser Technik ist die fundamentale Gefahr für die Selbstbestimmung des Einzelnen und für den Schutz seiner Privatsphäre. Je m ehr Daten aus- und verwertet werden, umso mehr wird die Privatsphäre des Einzelnen eingeschränkt. Auch wenn sich die Grenze zwischen öffentlich und privat durch die Digitalisierung verschieben mag, gehört die Privatsphäre unverzichtbar zur Persönlichkeit eines jeden Menschen.

Der rechtliche Gestaltungsrahmen

Das Bundesverfassungsgericht hat mit der Grundsatzentscheidung zur Volkszählung unmissverständlich erklärt, dass zum allgemeinen Persönlichkeitsrecht das Recht des Einzelnen gehört, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte von ihm preisgegeben werden. Es hat die Gefahren gesehen, die dem Persönlichkeitsrecht unter den Vorzeichen der automatisierten

„Die Entscheidungen, die wir im Gefühl treffen, frei zu sein, werden bald manipuliert sein."

Byung-Chul Han, Philosoph, Humboldt-Universität Berlin

© dpa

Abstimmung über den Gesetzentwurf zur Vorratsdatenspeicherung am 16.10.2015 im Bundestag

Datenverarbeitung drohen, und reklamiert, dass der Einzelne davor besonders geschützt werden muss.

„Eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung, in der der Bürger nicht mehr wissen könne, wer was wann und bei welcher Gelegenheit über ihn weiß, ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Wer unsicher sei, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, werde versuchen, nicht durch solche Verhaltensweisen aufzufallen. (...) Dies würde nicht nur die individuellen Entwicklungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung einer auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen, demokratischen Grundordnung sei. Hieraus folge: Freie Entfaltung der Persönlichkeit setze unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz sei daher von dem Grundrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen." (BVerfGE 65, 1-71)

Die Privatsphäre gehört unverzichtbar zur Persönlichkeit jedes Menschen

Ist das etwa eine Entscheidung aus einer anderen Zeit ohne heutige Relevanz? Weit gefehlt. Damals haben die Richter vorausschauend geurteilt, auch wenn die Dynamik und Dimension der Digitalisierung nicht vorhersehbar war.

Die damals aufgestellten Anforderungen an Eingriffe in das Recht auf informationelle Selbstbestimmung sind heute genauso aktuell, vielleicht sogar noch bedeutsamer. Es geht um die grundgesetzlichen Freiheitsrechte, die die Grundlage unserer Demokratie sind und die durch technische Entwicklungen nicht ausgehöhlt werden dürfen. Ihnen liegt das Menschenbild des selbstbestimmten Individuums zugrunde, das nicht mehr Objekt, sondern Subjekt staatlichen und wirtschaftlichen Handels ist. Wenn manche IT-Firmen die Auffassung vertreten, das sei alles eine alte Idee, die Rechte des einzelnen Bürgers hätten sich überholt, mit der neuen Technik wolle man etwas Neues ausprobieren, was nicht so bürokratisch wie die Demokratie sei, dann wird damit das kantische Menschenbild der Aufklärung aufgegeben. Dann würde im „Informationskapitalismus" (Hofstetter 2014, 230) der Primat des Menschen gegenüber allen intelligenten Maschinen aufgegeben. Die Gewinnmaximierung ist erklärtes Ziel jeder kapitalistischen Erscheinungsform. Das ist nicht illegitim, das sind die berechtigten Interessen eines kommerziellen Unternehmens. Da ohne die „Ware persönliche Daten" dieses Geschäftsmodell der Big-Data-Unternehmen aber nicht funktionieren kann,

haben sie sich die Verfügungsmacht und Verwertung persönlicher Daten angeeignet, ohne dass der eigentlich Verfügungsberechtigte, der einzelne Träger der Daten, der Mensch, konkret danach gefragt wird. Es bedarf deshalb dringend eines rechtlichen digitalen Gestaltungsrahmens mit den Kernelementen des Datenschutzrechtes. Dazu gehören,

- dass es keine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten geben darf,
- dass der Bürger genau wissen muss, welche seiner Daten wo, von wem, wie lange und zu welchem Zweck erfasst und verarbeitet werden,
- dass die Sensibilität der Daten sich aus ihrem Verwendungszusammenhang ergibt. Nicht das einzelne Datum ist so entscheidend, sondern seine Nutzbarmachung und die Gesamtbewertung. Das hat große Auswirkung, denn es gibt heute kaum noch ein Datum, das nicht in seiner Gesamtbetrachtung einen Personenbezug hat und damit datenschutzrelevant ist.

Unternehmen in Deutschland agieren nicht frei von der Verfassung. Die Grundrechte entfalten auch ihnen gegenüber Wirkung und binden sie an die durch die Grundrechte geschaffene objektive Wertordnung (BVerfGE 7. 198 ff. – Lüth-Urteil).

Deshalb muss der Gesetzgeber endlich gemeinsame Datenschutzstandards in Europa schaffen, die auch für internationale IT-Konzerne gelten, die ihren Sitz außerhalb der Europäischen Union haben. Wenn diese Daten europäischer Bürgerinnen und Bürger erfassen, analysieren und vernetzen, also vollumfänglich verarbeiten und für ihre Zwecke nutzen und dann ihre Dienstleistungen in der Europäischen Union anbieten, müssen sie sich nach dem Marktortprinzip an europäisches Recht halten. Sie dürfen sich mit der Wahl ihres Sitzortes – derzeit z. B. sehr häufig in Irland – nicht einem effektiven Datenschutz entziehen. Mit dem Projekt der europäischen Datenschutzgrundverordnung soll das Machtverhältnis zwischen dem Kapital und der negativen Freiheit, in Ruhe gelassen zu werden (vgl. Schirrmacher 2014), wieder besser justiert werden. Die seit über drei Jahren andauernden Beratungen im europäischen Gesetzgebungsverfahren müssen endlich zu einem Abschluss gebracht werden, der nicht die Interessen der Wirtschaft bevorzugt. Es darf nicht dem Nutzer aufgebürdet werden, selbst allein für seine Datensicherheit sorgen zu müssen. Die lapidare Aussage, niemand sei gezwungen, soziale Medien und vielfältige Online-Angebote zu nutzen, ist wohlfeil und leugnet die reale Machtkonstellation. Von keinem Nutzer kann verlangt werden, sich von der IT-Entwicklung abzukoppeln und zu isolieren. Es

Es darf nicht dem Nutzer aufgebürdet werden, für seine Datensicherheit zu sorgen

ist die Aufgabe und Verpflichtung der Politik und des Gesetzgebers, das Recht zur informationellen Selbstbestimmung der Bürgerin und des Bürgers im digitalen Zeitalter abzusichern.

Genauso ernst muss die Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) zum „Recht auf Vergessen“ genommen werden (Urteil vom 14. Mai 2014). Erstmals wurde die Verpflichtung der Betreiber von Suchmaschinen begründet, bei namensbasierten Recherchen Links zu Online-Artikeln zu löschen, deren Inhalte nicht mehr zutreffend, veraltet oder unangemessen sind. Die Begründung für diese Verantwortung der „Intermediäre“ oder „Gatekeeper“ wird aus der Dimension der Verbreitung von Informationen durch Suchmaschinen hergeleitet, die im Gegensatz zu Papierzeitungen und -zeitschriften alte Artikel unbegrenzt und millionenfach zugänglich macht. Dieses neue Recht des Nutzers auf Löschung von Links sollte in seiner globalen Reichweite und besonders verfahrensmäßig gesetzgeberisch abgesichert werden. Es darf im Interesse der Grundrechte der Nutzer nicht der Rechtsprechung allein überlassen bleiben, sich um den europäischen Grundrechtsschutz verdient zu machen.

„Kein Mensch darf zum Objekt eines Algorithmus werden.“
Heiko Maas, Bundesminister der Justiz und für Verbraucherschutz

Anlasslose Vorratsdatenspeicherung – eine Geschichte des juristischen Scheiterns

Genauso ist es die Verpflichtung des Staates, alles zu unterlassen, was die Privatsphäre und das Datenschutzrecht der Bürger unverhältnismäßig einschränkt. Das gilt u. a. für die anlasslose Vorratsdatenspeicherung, eine Geschichte des juristischen Scheiterns des nationalen deutschen und europäischen Gesetzgebers.

Vorratsdatenspeicherung hat keine signifikante Auswirkung auf die Aufklärungsquote von Verbrechen

Angesichts der jahrelangen intensiven und streitigen Debatte über die anlasslose Vorratsdatenspeicherung aller Telekommunikationsverbindungsdaten sollte man annehmen, dass die Behauptungen der Unverzichtbarkeit der anlasslosen Vorratsdatenspeicherung durch eindeutige rechtstatsächliche Untersuchungen belegt seien. Denn neben gravierenden Eingriffen in das Kommunikationsverhalten aller Bürgerinnen und Bürger durch die massenweise Speicherung der dadurch entstandenen Daten verursacht diese gesetzliche Verpflichtung millionenfache Investitionen der Telediensteanbieter, die vom Staat weder teilweise noch ganz erstattet werden.

Aber das Gegenteil ist richtig. Die dieses Instrument bis heute fordernden Polizeibehörden auf Bundes- und Landesebene haben neben einzelnen Beispielfällen keine umfassenden Untersuchungen vorgelegt, die die Notwendigkeit belegen. Aus den statistischen Erhebungen (Stand der statistischen Datenerhebungen im BKA aus dem Jahr 2010) der erfassten Telekommunikationsverbindungsdaten ergibt sich, dass sich die überwältigende Zahl der Anschlüsse (ca. 85 %) auf die Ermittlung der dynamischen IP-Adressen bezieht und nur ca. 15 % auf retrograde Verkehrsdaten. Diese aber beherrschen die politische Debatte.

Erstmals legte das Max-Planck-Institut für ausländisches und internationales Strafrecht eine umfassendere Studie über die Auswirkungen des Fehlens von Vorratsdaten im Juli 2011 vor. Sie basiert auf statistischen Materialien des Bundesamtes für Justiz über die Verkehrsdatenerhebung nach § 100 g Abs. 4 StPO, Materialien der Bundesnetzagentur und als wichtigste Erkenntnisquelle auf qualitativen Inter-

© dpa

Der Bundesvorsitzende des Bündnis90/Die Grünen, Cem Özdemir (4. v. l.) demonstriert am 16.10.2015 vor dem Reichstag in Berlin gegen die Vorratsdatenspeicherung.

Protest am 20.6.2015 vor dem Willy-Brandt-Haus in Berlin

views mit den an der Vorbereitung, Durchführung und Auswertung von Verkehrsdatenabfragen beteiligten Praktikern. Zudem wird der Evaluierungsbericht der EU-Kommission vom 18.4.2011 bewertet. Als Gesamtergebnis wird bei vorsichtiger Betrachtung des kurzen Beurteilungszeitraums und des nur eingeschränkt vorliegenden Zahlenmaterials festgehalten, dass die Vorratsdatenspeicherung keine signifikante Auswirkung auf die Aufklärungsquote von Verbrechen hat.

Auch das Urteil des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08, NJW 2010, 833 ff.), mit dem die sechsmonatige, vorsorglich anlasslose Speicherung der Telekommunikationsverbindungsda-

Bei 500 Millionen Menschen entsteht ein diffuses bedrohliches Gefühl der permanenten Überwachung

ten durch private Diensteanbieter in der Fassung der §§ 113a und 113b TKG für unvereinbar mit Art. 10 GG erklärt wurde, hat die Befürworter der Vorratsdatenspeicherung nicht überzeugen können und die Debatte in Richtung der Frage gelenkt, wie groß denn der noch auszuschöpfende Spielraum zur Wiedereinführung der Vorratsdatenspeicherung sei.

Vor diesem Hintergrund sollte mit dem bahnbrechenden Urteil der Großen Kammer des EuGH (8. April 2014, Az.: C-293/12 und C-594/12) eigentlich ein juristischer Schlusspunkt unter diese politische Debatte und unter diese in der Geschichte der Europäischen Union wohl umstrittenste Gesetzgebung gesetzt worden sein. Der vom irischen High Court und dem österreichischen Verfassungsgerichtshof wegen der bei ihnen anhängigen Klagen einer NGO, einer Landesregierung und von mehr als 11 000 Einzelpersonen angerufene EuGH stellt unmissverständlich in seiner Entscheidung fest, dass die massenweise anlasslose Speicherung von Daten sowohl das Recht auf Schutz der Privatheit gemäß Art. 7 als auch den Schutz der persönlichen Daten gemäß Art. 8 der Charta der Grundrechte berührt und den Verhältnismäßigkeitsgrundsatz nach Art. 52 Abs. 1 der Charta verletzt.

Die in der Richtlinie aufgestellte Verpflichtung zur Speicherung und die Erlaubnis zur Verarbeitung stellen als solche einen besonders schwerwiegenden Eingriff in diese beiden Grundrechte dar (Rdn. 35, 36, 37). Die immer wieder gern verwandte Argumentation, dass nicht die Speicherung der Daten, sondern erst der Zugang zu ihnen und die weitere Verwendung und Verarbeitung grundrechtsrelevant seien, ist damit vom EuGH klar zurückgewiesen worden. Wie schon das Bundesverfassungsgericht in seiner Rechtsprechung herausgearbeitet hat, entsteht durch die unterschiedslose massenweise Speicherung der Daten auf Vorrat bei den Bürgerinnen und Bürgern in der Europäischen Union, also bei ca. 500 Millionen Menschen, ein diffuses bedrohliches Gefühl der permanenten Überwachung und damit des Vertrauensverlustes in die Vertraulichkeit der Kommunikation informationstechnischer Systeme. Sie alle werden potenziell in die Ermittlungen staatlicher Behörden zur Gefahrenabwehr und zur Strafverfolgung einbezogen. Diese Entgrenzung der staatlichen Überwachungstätigkeit unter Benutzung privater Diensteanbieter macht die Intensität des Eingriffs aus.

Auch wenn der EuGH die generelle Geeignetheit der Vorratsdatenspeicherung bejaht, da es im Interesse des Gemeinwohls liege, organisierte Kriminalität und Terrorismus zu bekämpfen, und wegen der wachsenden Bedeutung elektronischer Kommunikationsmittel die

„Wir werden vermessen."
Uwe Jean Heuser,
Wirtschaftswissenschaftler und Publizist

„Es liegt im Wesen der Computertechnologie begründet, dass sie ubiquitär, universell und normativ ist."

Achim Clausing, Professor für Informatik an der Universität Münster

Vorratsdatenspeicherung theoretisch ein nützliches Mittel sein könne, lehnt er die anlasslose Speicherung klar ab, da sie nicht auf das unbedingt notwendige Maß beschränkt ist und keinen unmittelbaren oder noch nicht einmal einen mittelbaren Bezug zu einer Handlung hat, die zur Strafverfolgung Anlass gibt. Weiter rügt er zu Recht den fehlenden Zusammenhang zwischen den verpflichtend zu speichernden Daten und der tatsächlichen Bedrohung der öffentlichen Sicherheit. Mit seiner Kritik an der fehlenden geografischen und personellen Beschränkung der zu speichernden Daten erteilt er der anlasslosen Vorratsdatenspeicherung eigentlich eine endgültige Absage. Denn nur wenn es konkrete Kriterien für einen Anhaltspunkt oder konkreten Tatverdacht gibt,

Der beste Hüter der Rechte des Bürgers auf Datenschutz und Privatsphäre ist derzeit der EuGH

kann der Personenkreis eingegrenzt und auch räumlich ein engerer Rahmen gezogen werden.

Das hat die Bundesregierung nicht davon abgehalten, unter der täuschenden Bezeichnung sog. Höchstspeicherfristen einen Gesetzentwurf zur anlasslosen Speicherung der meisten Telekommunikationsverbindungsdaten vorzulegen und zu behaupten, dies sei zum Vorgehen gegen Terrorismus erforderlich. Auch wenn gewisse Vorgaben des Bundesverfassungsgerichtes berücksichtigt werden, handelt es sich um eine ohne jeden Anlass verpflichtende Speicherung, die auch bereits vom Bundestag und Bundesrat verabschiedet wurde und in Kraft getreten ist. Alle Äußerungen von Regierungsmitgliedern zu mehr Datenschutz, alle verbalen Bekenntnisse zum Grundrechtsschutz auch am Tag der deutschen Einheit sind Makulatur, wenn gleichzeitig im Gesetzgebungsverfahren das Gegenteil gemacht wird.

Auch die deutliche Kritik der EU-Kommission an diesem Gesetzentwurf zur Vorratsdatenspeicherung im Notifizierungsverfahren, u. a. an der nationalen Speicherung der Daten und dem Umgang mit den Daten von Berufsgeheimnisträgern, hat die Koalitionsfraktionen nicht von ihrem verfehlten Vorhaben abgebracht.

Der beste Hüter der Rechte des Bürgers auf Datenschutz und Privatsphäre ist derzeit der EuGH. Mit den Entscheidungen im Jahr 2014 zur Rechtsunwirksamkeit der Richtlinie zur Vorratsdatenspeicherung und zum „Recht auf Vergessen" sowie im Oktober 2015 zur Rechtsunwirksamkeit des „Safe Harbour"-Abkommens wird der europäische Raum der Freiheit, der Sicherheit und des Rechts mit Leben gefüllt. Datenschutz hat seinen Platz im digitalen Zeitalter. Unternehmen und der Staat müssen ihn beachten und ihm im Zweifel pauschale Sicherheitsbegründungen oder Praktikabilitätserwägungen unterordnen.

Datenschutz und Privatsphäre müssen das Zeitalter der „Big Data" mit prägen.

LITERATUR

Evaluation Report on the Data Retention Directive, Brüssel, 18.4.1011, COM (2011).

Hofstetter, Yvonne 2014: Sie wissen alles. Bielefeld.

Max-Planck-Institut für ausländisches und internationales Strafrecht 2011: Schutzlücken durch Wegfall der Vorratsdatenspeicherung? 2. erw. Fassung, Juli, Freiburg.

Schirrmacher, Frank 2014: ARD-Beitrag am 30.3.2014. Zitiert in: Hofstetter 2014, S. 285.

© Tobias Koch

Sabine Leutheusser-Schnarrenberger, ist eine deutsche Politikerin (FDP). Sie war von 1992 bis 1996 sowie von 2009 bis 2013 Bundesministerin der Justiz.