Privatsphäre als Menschenrecht

Edward Snowden und die Kontrolle der Macht

Von **Peter Schaar**

Im Juni 2013 sorgte Edward Snowdens Enthüllung der gigantischen Abhörung durch die US-amerikanische NSA und das britische GCHQ für einen globalen Aufschrei. Ein Jahr danach ist die Frage nicht nur berechtigt, sondern drängt sich geradezu auf, ob es überhaupt wirksame Mittel gegen die lückenlose Registrierung und Überwachung der Geheimdienste gibt.

Eines jedenfalls ist klar: Ein Zurück in die analoge Zeit vor dem Internet wird es nicht geben. Wenn wir auf die Segnungen der Informationstechnologie nicht verzichten wollen, werden wir uns damit arrangieren müssen, dass in erheblichem Umfang Daten – auch solche mit Personenbezug – verarbeitet werden. Illusorisch wäre auch die Hoffnung, die staatlichen Überwachungsaktivitäten auf Null zurückfahren zu können.

Trotzdem wäre es falsch, den Kopf in den Sand zu stecken und einfach der Dinge zu harren, die da noch kommen mögen. Es gibt durchaus einige Ansätze, die uns helfen können, die Überwachungsschraube zurück zu drehen und unsere Privatsphäre auch in der digitalen Welt besser zu schützen – auf rechtlicher wie auf politischer Ebene.

Allerdings entfalten Gesetze ihre Schutzwirkung grundsätzlich im jeweiligen territorial definierten Geltungsbereich. Das Internet ist dagegen so konstruiert, dass Landes- oder auch Kontinentalgrenzen technisch keine Rolle spielen. Wenn etwa ein deutscher Internetnutzer die Webseite eines deutschen Anbieters abruft, können die übertragenen Daten durchaus über amerikanische Netzknoten geleitet *(geroutet)* werden. Global agierende Internetunternehmen speichern Daten auf Servern, die auf verschiedene Kontinente verteilt sind.

Deshalb machen es sich, wenn es um globale Geheimdienstaktivitäten geht, diejenigen zu einfach, die stets nur auf die Einhaltung des heimischen Rechts pochen. Vertreter der amerikanischen und der britischen Regierung hatten offenbar kein Problem mit der Überwachung, soweit ihre Nachrichtendienste beteuerten, sich an – das eigene – Recht und Gesetz zu halten.

Heute wissen wir, dass dies gelogen war. Darüber hinaus blendet der Hinweis auf die angebliche Gesetzeskonformität gegenüber dem eigenen, heimischen Recht die in den letzten hundert Jahren entwickelten Rechtsprinzi-

* Der Beitrag basiert auf „Überwachung total: Wie wir in Zukunft unsere Daten schützen", dem neuen Buch von Peter Schaar, das soeben im Aufbau Verlag erschienen ist

pien weitgehend aus, die gerade nicht mehr territorial beschränkt sind. Auch wenn diese Prinzipien – insbesondere die Allgemeine Erklärung der Menschenrechte von 1948 – Reaktionen auf die Grausamkeiten des Zweiten Weltkriegs waren und Fragen des Umgangs mit Informationen nicht im Mittelpunkt standen, bieten sie Ansatzpunkte für die Zivilisierung der zunehmend globalisierten Informationsgesellschaft.

Hinzu kommt: Gerade bei der Auslandsaufklärung wird systematisch gegen Rechtsvorschriften im Operationsgebiet verstoßen. Selbst wenn sich die NSA an US-Recht hält und der GCHQ britische Gesetze beachtet, können sie durchaus ausländisches – etwa deutsches – Recht brechen. Und sie haben dies in der Tat getan: Wenn etwa ein ausländischer Geheimdienstcomputer deutsche Nutzer mittels Trojaner infiltriert und überwacht, erfüllt dies den Straftatbestand des Ausspähens von Daten. Auch Geheimdienste, die mittels Telekommunikation übertragene nichtöffentliche Daten deutscher Teilnehmer unter Anwendung von technischen Mitteln abfangen oder sich aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschaffen, begehen eine Straftat. Und auch die Tatsache, dass Spionage nicht gegen Völkerrecht verstößt, stellt Spione keineswegs straffrei. So verbietet Paragraph 99 StGB die geheimdienstliche Agententätigkeit für eine fremde Macht.

Das Versagen der deutschen Strafverfolgungsbehörden

Gleichwohl halten sich die deutschen Strafverfolgungsbehörden bei ihren Ermittlungen in Sachen NSA und GCHQ auffällig zurück. Offenbar spielt dabei – neben der Faktenlage – eine maßgebliche Rolle, ob von einem solchen Ermittlungsverfahren negative Auswirkungen auf die Beziehungen zu Großbritannien und den USA zu befürchten sind. Was für ein absurdes Argument angesichts der Tatsache, dass die Regierungen dieser Staaten für das massenhafte und gezielte Abfangen vertraulicher Informationen aus der Bundesrepublik Deutschland verantwortlich sind und damit ihrerseits die internationalen Beziehungen schwer belastet haben. Gerade von Rechtsstaaten wie den USA und Großbritannien darf man eigentlich Verständnis dafür erwarten, dass andere Staaten die gegen sie gerichteten Rechtsverstöße ahnden. Die Tatsache, dass der Generalbundesanwalt nahezu ein Jahr nach den ersten Snowden-Veröffentlichungen ein Ermittlungsverfahren gegen unbekannt wegen des Abhörens des Kanzlerinnenhandys eingeleitet hat, ist nicht dazu geeignet, die Zweifel am Aufklärungswillen der deutschen Strafverfolgungsbehörden auszuräumen. Offenbar können sie hinsichtlich des weitaus größeren Skandals der Massenüberwachung nicht einmal einen Anfangsverdacht erkennen.

Ein – leider immer wieder „vergessener" – völkerrechtlicher Grundsatz besteht darin, dass sich alle staatlichen Stellen an die Vorgaben des internationalen Rechts zu halten haben. Zu den wichtigsten gehören die unveräußerlichen Menschenrechte. Nach dem Zweiten Weltkrieg waren es gerade die Vereinigten Staaten, die sich nach den Gräueln des Nationalsozialismus

und den von ihm zu verantwortenden furchtbaren Verbrechen gegen die Menschlichkeit für verbindliches, international geltendes und durchsetzbares Recht einsetzten. Die Nürnberger Kriegsverbrecherprozesse von 1945 bis 1949 legen beredtes Zeugnis darüber ab, mit welcher Hartnäckigkeit insbesondere die amerikanischen und britischen Ankläger und Richter auf völkerrechtlich verbindliche Menschenrechte bestanden und diese auch mit strafrechtlichen Mitteln durchsetzten. In Abkehr von dieser Grundposition weigern sich die USA heute beharrlich, sich neuen internationalen Rechtsnormen zu unterwerfen.[1]

Dieses rechtliche Territorialdilemma lässt sich somit nur dann überwinden, wenn endlich wirksame, durchsetzbare Instrumente geschaffen werden, die die Menschenrechte mit Leben füllen. Dies gilt auch und insbesondere für den Datenschutz. Schon seit Jahren fordern daher Datenschützer internationale Standards zum Schutz der Privatsphäre[2] – bislang allerdings ohne durchschlagenden Erfolg. Seit dem Bekanntwerden der umfassenden Überwachungsaktivitäten der amerikanischen NSA und des britischen GCHQ ist aber Bewegung in die internationale Diskussion gekommen.

Die auf Snowden zurückgehenden Berichte riefen einer breiteren Öffentlichkeit wieder in Erinnerung, dass es sich bei dem Datenschutz um ein Menschenrecht handelt. In Artikel 12 der Allgemeinen Erklärung der Menschenrechte von 1949 stellte die Völkergemeinschaft fest: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen."

Bereits seit den 1960er Jahren befassen sich die Vereinten Nationen intensiver mit den Konsequenzen der automatisierten Datenverarbeitung. Durch Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte von 1966 wurde der Schutz der Privatsphäre zum verbindlichen Völkerrecht. Die Staaten, die diesen „Zivilrechtspakt"[3] ratifiziert haben, verpflichteten sich damit, diese Rechte zu achten und sie allen in ihrem „Gebiet befindlichen und seiner Herrschaftsgewalt unterstehenden Personen ohne Unterschied wie insbesondere der Rasse, der Hautfarbe, des Geschlechts, der Sprache, der Religion, der politischen oder sonstigen Anschauung, der nationalen oder sozialen Herkunft, des Vermögens, der Geburt oder des sonstigen Status zu gewährleisten."

Im Jahr 1990 beschloss die UN-Generalversammlung Empfehlungen über den Umgang mit personenbezogenen Daten in automatisierten Dateien. Es

1 So gehört die US-Regierung zu den härtesten Gegnern des Internationalen Strafgerichtshofs, der 2002 seine Arbeit aufgenommen hat. Zwar hatten die USA im Jahr 2000 dessen Statut unterzeichnet, die Unterschrift aber zwei Jahre später wieder zurückgezogen. Seither versuchen die USA durch Abschluss bilateraler Verträge mit Staaten, die sich der Entsprechung durch den Strafgerichtshof unterworfen haben, die Überstellung von US-Bürgern an das Gericht zu verhindern.

2 Vgl. Entschließung der 31. Konferenz der Internationalen Konfe- renz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 4.-6.11.2009 über internationale Standards zum Schutz der Privatsphäre.

3 Internationaler Pakt über bürgerliche und politische Rechte vom 19.12.1966 (BGBl. 1973 II 1553), im Folgenden zitiert als „Zivilrechtspakt".

blieb allerdings den Mitgliedstaaten überlassen, hierzu verbindliche Bestimmungen festzulegen. Insofern hätte es eigentlich außer Frage stehen müssen, dass zumindest die 167 Staaten, die den Zivilrechtspakt ratifiziert haben, darunter alle EU-Mitgliedsländer und die Vereinigten Staaten und die Russische Föderation – nicht jedoch die Volksrepublik China –, sich an die in Artikel 12 der UN-Menschenrechtscharta formulierten Vorgaben gebunden fühlen.

Snowdens Enthüllungen belegen, dass davon keine Rede sein kann. Am 25. Juni 2013 schlug ich daher in meiner damaligen Funktion als Bundesdatenschutzbeauftragter vor, anknüpfend an die bestehenden rechtlichen Instrumente des internationalen Rechts die völkerrechtliche Verankerung des Datenschutzes endlich zu verbessern. Die Bundesregierung und die Europäische Union, so meine Forderung, sollten sich für ein internationales Übereinkommen stark machen: „Ein Zusatzprotokoll zum Artikel 17 des UNO-Paktes für bürgerliche und politische Rechte wäre ein sinnvoller erster Schritt. Um ein solches verbindliches völkerrechtliches Protokoll in Kraft zu setzen, genügt die Unterstützung von 20 Staaten – angesichts der 27 EU-Mitgliedstaaten müsste dies doch zu schaffen sein. Staaten, die sich nicht dazu bekennen, müssten nachweisen, wie sie trotzdem Datenschutz, Privatsphäre und Fernmeldegeheimnis garantieren.“[4]

Bundeskanzlerin Angela Merkel griff diesen Vorschlag wenige Wochen später auf: „Das Auswärtige Amt setzt sich als federführendes Ressort auf internationaler Ebene dafür ein, ein Zusatzprotokoll zu Art. 17 zum Internationalen Pakt über bürgerliche und politische Rechte der Vereinten Nationen zu verhandeln.“ In dem Zusatzprotokoll sollten ergänzende und den heutigen modernen technischen Entwicklungen entsprechende internationale Vereinbarungen zum Datenschutz festgeschrieben werden – auch für die Tätigkeit der Nachrichtendienste, meinte die Bundeskanzlerin.[5]

Die große Entschärfung

Nachdem es zunächst so aussah, als würde diese Initiative der Bundesregierung auf breite europäische und internationale Unterstützung treffen, ruderten jedoch in den folgenden Wochen und Monaten einige der Regierungen, die zunächst ihre Zustimmung signalisiert hatten, zurück. Als sich abzeichnete, dass ein derartiges Zusatzprotokoll zum UN-Zivilrechtspakt nur geringe Durchsetzungschancen hatte (und zudem auch im günstigsten Fall eine eher langfristige Angelegenheit wäre), schlugen die Bundesregierung und die brasilianische Regierung, die ebenfalls massiv durch die NSA ausspioniert worden war, einen Resolutionsentwurf der Vollversammlung der Vereinten Nationen vor. Im Mittelpunkt des Erschließungsentwurfs stand die Forderung, das Menschenrecht auf Privatsphäre unabhängig vom Territorialprinzip auch außerhalb der eigenen Landesgrenzen zu wahren.

4 Vgl. meinen Gastbeitrag auf www.spiegel.de: Prism und Tempora: Zügellose Überwachung zurückfahren!, 25.6.2013.
5 Ebd.

Dagegen wandten sich Vertreter der Vereinigten Staaten. In einem der Zeitschrift „Foreign Policy" zugespielten Verhandlungspapier der US-Delegation[6] wird großer Wert darauf gelegt, dass nicht jede Überwachung zu verurteilen sei, sondern nur solche, die „gegen Gesetze verstößt". Da sich die USA und Großbritannien – wie auch andere Regierungen – allerdings immer wieder nur auf die eigenen Gesetze beziehen, wäre die Entschließung so zu einem Muster ohne Wert geworden.

Aufgrund der massiven Intervention der US-Regierung und anderer Mitglieder im exklusiven Überwachungsclub der sogenannten *Five Eyes* (USA, Großbritannien, Kanada, Australien und Neuseeland) wurde die Resolution schließlich teilweise entschärft, wie der „Spiegel" unter Berufung auf „UN-Insider" zu berichten wusste. So sei die Einbeziehung „extraterritorialer" Spähaktionen – also von einem Staat in den anderen – „ein schwieriger Punkt" gewesen. Immerhin blieb die Aussage, die Überwachung müsse global und nicht nur durch nationales Recht begrenzt werden, Teil der Entschließung. Allerdings ist jetzt nicht mehr von Überwachung generell die Rede, sondern nur noch von „ungesetzlicher Überwachung" und deren „negativem Einfluss".[7]

Trotzdem enthält die von der Generalversammlung angenommene Resolution „Das Recht auf Privatheit im digitalen Zeitalter" die deutliche Botschaft: Der Schutz der Privatsphäre ist ein internationales Menschenrecht, das auch und gerade im Zeitalter der globalen Kommunikation weltweit garantiert werden muss. Die Staaten müssen „die vollständige Einhaltung ihrer Verpflichtungen nach den internationalen Menschenrechtsnormen" sicherstellen und Maßnahmen „ergreifen, um Verletzungen dieser Rechte ein Ende zu setzen und die Bedingungen dafür zu schaffen, derartige Verletzungen zu verhindern".

Vielleicht am bedeutsamsten ist, dass das Thema Überwachung nach dem Beschluss der Vollversammlung auf der Tagesordnung der UN-Gremien bleiben soll. So soll die UN-Menschenrechtskommissarin dem Menschenrechtsrat und der Generalversammlung einen „Bericht über den Schutz und die Förderung des Rechts auf Privatheit im Kontext des innerstaatlichen und extraterritorialen Überwachens und/oder Abfangens von digitaler Kommunikation und Sammelns personenbezogener Daten, namentlich in massivem Umfang, samt Auffassungen und Empfehlungen" vorlegen, heißt es in der Resolution.

Europäisches Datenschutzrecht: Firewall gegen Überwachung?

Doch so wichtig die einhellige Meinungsbekundung der UN-Mitgliedstaaten ist – sie reicht bei weitem nicht aus. Notwendig sind vielmehr verbindliche völkerrechtliche Regelungen, die den globalen Überwachungsaktivi-

6 Colum Lynch, Exclusive: Inside America's Plan to Kill Online Privacy Rights Everywhere, http://foreignpolicy.com, 20.11.2013.
7 Vgl. Resolution gegen Abhöraktionen: Die Uno kuscht vor der NSA, www.spiegel.de, 26.11.2013.

täten einen Riegel vorschieben. Selbst wenn die USA, Russland und China, die sich in der globalen Überwachung besonders hervortun, im Bündnis mit autoritären Regimes versuchen, die Verabschiedung international durchsetzbarer Datenschutzstandards zu verhindern, darf sich insbesondere Europa hiermit nicht zufrieden geben.

Auch wenn die modernen Vorstellungen über den Schutz der Privatsphäre zunächst überwiegend in den USA entwickelt wurden, sind sie doch heute in weiten Teilen Europas weitaus stärker verankert als dort.[8] Nicht zu übersehen sind allerdings die großen Differenzen zwischen den europäischen Staaten. Nicht erst der Umgang der britischen Öffentlichkeit mit den Enthüllungen Snowdens belegt, dass staatliche Überwachung in Großbritannien auf weitaus größere Akzeptanz trifft als in Deutschland. So stößt etwa die nahezu flächendeckende Videoüberwachung im städtischen Bereich in Großbritannien kaum auf öffentliche Kritik, während entsprechende Maßnahmen in Deutschland heiß diskutiert werden.

Trotz dieser Unterschiede bieten die europäischen Datenschutztraditionen und die in den letzten Jahrzehnten formulierten europäischen Datenschutzstandards und -gesetze durchaus Ansatzpunkte für die Begrenzung der Überwachung. Mit der Europäischen Menschenrechtskonvention von 1953 und mit der Konvention zum Datenschutz von 1981 (Konvention 108) hat der Europarat bereits sehr frühzeitig – und lange vor der Europäischen Union – Maßstäbe zur Gewährleistung der Grundrechte und des Datenschutzes gesetzt.

Anknüpfend an die Allgemeine Erklärung der Menschenrechte der Vereinten Nationen bekennt sich die Menschenrechtskonvention des Europarats zur universellen und wirksamen Anerkennung und Einhaltung dieser Rechte. Und wie diese gesteht Artikel 8 der Menschenrechtskonvention jeder Person das Recht „auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ zu. Im Unterschied zur Allgemeinen Erklärung der Menschenrechte ist die Europaratskonvention für alle Unterzeichnerstaaten verbindlich. Zwar verpflichten sich die Vertragsparteien explizit nur dazu, die Rechte „allen ihrer Hoheitsgewalt unterstehenden Personen“ zuzugestehen. Durch ihren universellen Anspruch sind die Vorgaben der Menschenrechtskonvention jedoch auch im Rechtsverkehr der Staaten untereinander verbindlich und gelten damit auch für Aktivitäten staatlicher Stellen außerhalb des eigenen Territoriums.

Den vom zunehmenden internationalen Datenaustausch ausgehenden Gefährdungen trägt die Datenschutzkonvention des Europarats Rechnung. Für viele Staaten innerhalb und außerhalb Europas war sie die Blaupause für ihr nationales Datenschutzrecht. In ihrer Präambel heißt es, „dass es angesichts des zunehmenden grenzüberschreitenden Verkehrs automatisch verarbeiteter personenbezogener Daten wünschenswert ist, den Schutz der Rechte und Grundfreiheiten jedes Menschen, vor allem das Recht auf Achtung des Persönlichkeitsbereichs, zu erweitern.“ Artikel 8 der EU-Grundrechtecharta enthält zudem – anders als das deutsche Grundgesetz – ein

8 Louis Warren und Samuel Brandeis, The Right to Privacy, Boston 1890.

explizites Grundrecht auf Datenschutz: „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“ [9] Als Teil des am 1. November 2009 in Kraft getretenen Vertrags von Lissabon ist die Grundrechtecharta direkt anwendbares europäisches Recht. Damit ist der Datenschutz in Europa rechtlich erheblich tiefer verankert als etwa in den USA oder im asiatisch-pazifischen Raum.

Datenschutz mittels Safe-Harbor-Abkommen?

Eine entscheidende Rolle spielt dabei die 1995 in Kraft getretene EU-Datenschutzrichtlinie.[10] Sie verpflichtet die Mitgliedstaaten zur Gewährleistung eines hohen Datenschutzniveaus. In allen Mitgliedstaaten sind die Vorgaben der Richtlinie durch nationale Rechtsvorschriften umgesetzt worden, etwa in Deutschland durch das Bundesdatenschutzgesetz.

Wie wichtig der EU-Datenschutz ist, belegt die jüngste Entscheidung des Europäischen Gerichtshofs in Luxemburg zu Google. Darin wurde der Suchmaschinenbetreiber dazu verpflichtet, bei überwiegendem Interesse des Betroffenen Verweise auf Webseiten mit persönlichen Daten aus der Ergebnisliste zu streichen. Ein solches Recht leitet das Gericht bereits aus der geltenden EU-Datenschutzrichtlinie ab. Demzufolge ist der Suchmaschinenbetreiber für die Verarbeitung der Daten verantwortlich.

Die Datenschutzrichtlinie legt fest, dass der Datenexport grundsätzlich nur dann zulässig ist, wenn im Empfängerland ein „angemessenes Datenschutzniveau“ gewährleistet wird. Über die Angemessenheit des Schutzniveaus in einem Drittstaat entscheidet die Europäische Kommission. So hat die Kommission die Angemessenheit des Schutzniveaus für jene Unternehmen festgestellt, die sich den mit der US-Regierung ausgehandelten *Safe-Harbor*-Prinzipien unterwerfen.[11]

Zuvor hatte die EU jahrelang mit den USA darüber verhandelt, wie die in die Vereinigten Staaten exportierten personenbezogenen Daten angemessen geschützt werden können. Die US-Regierung weigerte sich standhaft, mit dem europäischen Recht vergleichbare Datenschutzgesetze mit verbindlichen Vorgaben für US-Unternehmen auf den Weg zu bringen. Um gleichwohl den Datenexport in die USA zu erleichtern, einigte sich die EU-Kommission mit der US-Regierung im Jahr 2000 auf das Safe-Harbor-Abkommen.

9 Charta der Grundrechte der Europäischen Union vom 7.12.2000, (2000/C 364/01).
10 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-DSRL, ABl. EG Nr. L 281 31).
11 Entscheidung der Europäischen Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ (2000/520/EG).

Dessen Grundidee besteht darin, dass auch ohne ein allgemein gültiges US-Datenschutzgesetz ein angemessener Schutz der europäischen Daten für die Verarbeitung durch diejenigen Unternehmen angenommen wird, die sich zur Einhaltung der vereinbarten Prinzipien verpflichten. Die US-Regierung sagte im Gegenzug zu, die Prinzipien bei den Unternehmen durchzusetzen.

Die dem „sicheren Hafen" beigetretenen Unternehmen werden von den europäischen Datenschutzbehörden ähnlich wie Firmen behandelt, die personenbezogene Daten in Europa verarbeiten. So müssen europäische Unternehmen keine Genehmigungen bei den europäischen Datenschutzbehörden einholen, wenn sie Daten an Safe-Harbor-Mitglieder übermitteln wollen. Inzwischen ist Safe Harbor das wichtigste Instrument für den Transfer personenbezogener Daten in die USA – zur Zeit sind mehr als 4400 Firmen dem sicheren Hafen beigetreten, darunter alle großen US-Internetunternehmen.

Der Protest der Datenschützer

Allerdings haben Datenschützer von Beginn an kritisiert, dass die Safe-Harbor-Prinzipien deutlich hinter den Ansprüchen des europäischen Datenschutzrechts zurückbleiben. Ein weiterer Kritikpunkt richtet sich dagegen, dass die Unternehmen schon dann die Vorteile des Safe-Harbor-Systems genießen, wenn sie den Beitritt zum „sicheren Hafen" erklärt haben. So bedarf im allgemeinen die Datenübermittlung aus Europa an ein Safe-Harbor-Mitglied keiner Genehmigung durch die zuständige Datenschutzaufsichtsbehörde. Die Unternehmen sind nicht verpflichtet, bereits vor ihrer Aufnahme in die Safe-Harbor-Liste nachzuweisen, dass sie die Anforderungen erfüllen. Zudem können sie sich aussuchen, welche Stelle kontrolliert, ob sie die Bedingungen einhalten. Soweit bekannt, haben sich sämtliche Safe-Harbor-Unternehmen der Aufsicht durch die *Federal Trade Commission* (FTC) unterworfen und kein Einziges der Aufsicht einer europäischen Datenschutzbehörde.[12]

Nach den Snowden-Veröffentlichungen ist ein weiterer Kritikpunkt in den Mittelpunkt gerückt: Das Safe-Harbor-Abkommen nimmt die Verarbeitung von Daten zu Zwecken der „nationalen Sicherheit" explizit aus. Auf diese Ausnahme berufen sich sowohl die US-Behörden als auch jene Unternehmen, deren umfangreiche Datenweitergabe an die NSA jetzt kritisiert wird – wie etwa Google, Microsoft, Amazon, Apple und Yahoo.

Eigentlich müssten sich US-Sicherheitsbehörden, die etwa gegen einen Terrorverdächtigen ermitteln, im Wege der internationalen Rechtshilfe an die EU-Staaten wenden, wenn sie Daten aus Europa erhalten wollen. Vor der Übermittlung würde dann von den zuständigen europäischen Behörden – in Deutschland: vom Bundesjustizministerium – geprüft, ob die Voraussetzungen für die Datenübermittlung vorliegen. Dieses rechtsstaatlich einwandfreie, aber aufwändige Verfahren wird unterlaufen, wenn die europäischen

12 http://safeharbor.export.gov/list.aspx.

Daten quasi automatisch, ohne weitere Prüfung, auf Basis von Safe Harbor an ein US-Unternehmen übermittelt werden und von diesem an US-Geheimdienste gelangen. In Europa wächst deshalb der Druck, das Safe-Harbor-Abkommen zu kündigen. So hat sich etwa das europäische Parlament dafür ausgesprochen, das Abkommen neu zu verhandeln. Das Europäische Parlament verlangt seine Aussetzung, und Datenschutzbehörden haben erklärt, das Safe-Harbor-Abkommen nicht mehr als Rechtsgrundlage für die Datenübermittlung in die USA zu akzeptieren.[13]

Bei einem Nachfolgeabkommen zu Safe Harbor wird es entscheidend darauf ankommen, dass – anders als bisher – staatliche Zugriffe auf Daten umfasst werden, die dem europäischen Datenschutzrecht unterliegen oder die aus Europa in die USA übermittelt wurden. Es darf nicht länger hingenommen werden, dass US-Behörden ohne angemessene rechtsstaatliche Sicherungen auf aus Europa stammende Daten zugreifen, diese kopieren und zu Profilen zusammenführen. Eine generelle Ausnahme für die Verarbeitung der Daten zu Zwecken der „nationalen Sicherheit" kann nicht akzeptiert werden.

Rechtliche „Daumenschrauben" im EU-Datenschutzrecht

Welche Rolle Europa bei der Durchsetzung internationaler Datenschutzstandards spielt, wird sich auch an dem Schicksal der EU-Datenschutzreform messen lassen. Dabei geht es zum einen um die weitere Harmonisierung der Datenschutzregeln in den EU-Mitgliedstaaten und eine bessere Kooperation der Datenschutzbehörden. Mindestens genauso wichtig ist allerdings eine eher unscheinbare Änderung bezüglich des Anwendungsbereichs des EU-Datenschutzrechts: Bisher können sich Unternehmen wie Google dem europäischen Recht weitgehend dadurch entziehen, dass sie ihre Dienste aus den USA anbieten. In Zukunft würde diese Umgehungsstrategie nicht mehr klappen. Die EU-Kommission hat nämlich die Einführung eines „Marktortprinzips" vorgeschlagen. Danach soll das EU-Datenschutzrecht immer schon dann anwendbar sein, wenn Unternehmen Dienstleistungen oder Waren auf dem europäischen Markt anbieten und dabei in der Europäischen Union personenbezogene Daten erheben. Google und andere in Europa tätige US-Unternehmen müssten sich dann genauso an das europäische Recht halten wie die hier ansässigen Firmen. Auch wenn die jüngste Google-Entscheidung des Europäischen Gerichtshofs auf Basis der Datenschutzrichtlinie von 1995 schon heute die Anwendbarkeit des EU-Rechts im Fall des Suchmaschinenbetreibers festgestellt hat, muss durch die Datenschutzreform generell sichergestellt werden, dass sich auf dem europäischen Markt aktive Unternehmen generell nicht dem EU-Datenschutzrecht entziehen können.

Um der maßlosen Überwachung durch ausländische Behörden entgegenzuwirken, hat das europäische Parlament darüber hinaus die Aufnahme

13 Pressemitteilung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.7.2013.

einer weiteren „Daumenschraube“ in das EU-Datenschutzrecht vorgeschlagen: In Fällen, in denen Behörden oder Gerichte aus Drittstaaten den Zugriff auf Daten anordnen, die dem europäischen Datenschutzrecht unterliegen, benötigen die betroffenen Unternehmen eine Genehmigung der jeweiligen europäischen Datenschutzbehörde. „Urteile von Gerichten und Entscheidungen von Verwaltungsbehörden eines Drittstaats, die von einem für die Verarbeitung (der Daten) Verantwortlichen oder Auftragsverarbeiter verlangen, personenbezogene Daten weiterzugeben, dürfen weder anerkannt noch in irgendeiner Weise vollstreckt“ werden, so der Vorschlag des Europäischen Parlaments.

Die neue Vorschrift würde etwa zur Anwendung kommen, wenn das FBI oder die NSA die Herausgabe von in der Google- oder Microsoft-Cloud gespeicherten Daten anordnen. Die von derartigen Datenanforderungen betroffenen Unternehmen sollen verpflichtet werden, dies der zuständigen Datenschutzaufsichtsbehörde in der EU zu melden. Sie dürften die Daten nur dann an US-Behörden herausgeben, wenn die Datenschutzbehörde feststellt, dass die Herausgabe auch nach europäischem oder internationalem Recht zulässig ist. Zudem müssten die Betroffenen sowohl über die Anfrage als auch über die Autorisierung durch die Datenschutzbehörde informiert werden. Die Teilnahme an geheimen Überwachungsprogrammen wäre damit unzulässig.

Sollte die EU allerdings eine derartige Regelung beschließen, wäre ein Konflikt mit den USA vorprogrammiert: Nach US-Recht sind die Unternehmen zu strikter Geheimhaltung bezüglich der Datenherausgabe an Sicherheitsbehörden verpflichtet. Bisher ist es ihnen sogar untersagt, auch nur die Tatsache zu offenbaren, dass es entsprechende Anfragen – etwa der NSA oder des FBI – überhaupt gibt. Ob und wie dieser Konflikt aufgelöst werden kann, ist derzeit nicht abzusehen. Würde Europa allerdings aus wirtschaftlichen Gründen oder wegen des sich aufbauenden politischen Drucks der US-Regierung auf die Durchsetzung seiner datenschutzrechtlichen Standards verzichten, wäre der damit einhergehende Vertrauensverlust kaum zu kompensieren.[14]

Aus diesem Grund ist auch ein allgemeines Datenschutzabkommen zwischen der EU und den USA dringend erforderlich. Dieses muss garantieren, dass die EU-Bürger in den USA effektive Rechtsschutzmöglichkeiten gegen das Handeln staatlicher Stellen bekommen. Bisher weigert sich die US-Regierung, EU-Bürgern solche Datenschutzgarantien zu geben, auf die sich US-Bürger in Europa selbstverständlich berufen können. Daran hat sich seit Beginn der NSA-Affäre nichts geändert – allen Bekundungen Präsident Obamas zum Trotz, die USA würden zukünftig auch die Rechte von Nicht-Amerikanern im Ausland respektieren.[15] Auch müssen die USA garantieren, dass die auf amerikanischen Servern lagernden personenbezogenen Daten

14 Von großer Bedeutung wird auch sein, wie die Europäische Kommission die Verhandlungen mit der US-Regierung über das transatlantische Freihandelsabkommen TTIP fortführen wird. Es besteht die Gefahr, dass ein solches Abkommen den europäischen Datenschutz erheblich schwächt.

15 Vgl. Alexander Dix, Datenschutz und transatlantische Freihandelszone, Karlsruhe 2013, S. 8.

europäischer Provenienz denselben Schutzmechanismen gegen staatliche Zugriffe unterliegen wie die Daten, die aus den USA selbst stammen. Die schon seit Jahren wegen des hinhaltenden Widerstands der US-Seite ins Stocken geratenen Verhandlungen einer *High Level Contact Group* müssen endlich zu einem annehmbaren Abschluss gebracht werden. Ohne ein entsprechendes Ergebnis darf auch Safe Harbor nicht fortgeführt werden – massenhafte Verletzungen des in der Europäischen Grundrechtecharta garantierten Rechts auf Datenschutz darf die EU nicht in Kauf nehmen. Eine Lösung zeichnet sich bisher jedoch nicht ab, weil die US-Seite in all diesen zentralen Fragen nicht zu wesentlichen Zugeständnissen bereit war.

Die politische Kontrolle der Macht

Umso weniger kommt die Gesellschaft um die Frage herum, welchen anderen Ausweg aus der Überwachungsspirale es gibt.

Von zentraler Bedeutung ist dabei die Frage, wie wir zukünftig mit Risiken umgehen. Kaum jemand wird der These widersprechen, eine hundertprozentige Sicherheit vor Lebensrisiken sei nicht zu erreichen. Gleichwohl strebt unsere postindustrielle Gesellschaft genau danach, wenn es um den Umgang mit Gewalt, Kriminalität und Terrorismus geht. Wenn daher Politiker wie George W. Bush oder auch die deutschen Innenminister Otto Schily, Wolfgang Schäuble und Hans-Peter Friedrich die Sicherheit zu einem Grundrecht oder gar „Super-Grundrecht" erklärten, handelten sie durchaus in Übereinstimmung mit einer Mehrheitserwartung.

Allerdings haben die Enthüllungen Edward Snowdens die öffentliche Wahrnehmung erheblich verändert. Erst jetzt ist deutlich geworden, wie stark nach dem Elften September Freiheitsrechte eingeschränkt wurden. David Lyon beschreibt das Dilemma zutreffend: „Die Macht hat sich in einen globalen, extraterritorialen Raum verzogen, während die Politik, die einst zwischen den Interessen des Einzelnen und der Gemeinschaft vermittelte, an feste Orte gebunden bleibt und nicht auf globaler Ebene zu agieren vermag. Ohne politische Kontrolle wird Macht jedoch zur Quelle großer Unsicherheit, während die Politik in Bezug auf die Probleme und Ängste vieler Menschen offenbar jede Bedeutung verliert."[16]

Zunächst ist es deshalb von entscheidender Bedeutung, auch für die geheimdienstlichen Aktivitäten zur Terrorabwehr für viel mehr Transparenz zu sorgen. Die Maßnahmen und Gesetze, die unsere Sicherheit verbessern sollten, gehören dringend auf den Prüfstand. Es kann einfach nicht länger hingenommen werden, dass Sicherheitspolitiker immer wieder behaupten, die umfassenden Überwachungsmaßnahmen hätten Terroranschläge verhindert, ohne dafür den Nachweis zu führen. Beweise für diese Behauptung sind sie nämlich – häufig unter Hinweis auf die Notwendigkeit zur Geheim-

16 Zygmunt Bauman und David Lyon, Daten, Drohnen, Disziplin. Ein Gespräch über flüchtige Überwachung, Berlin 2013, S. 16; vgl. auch dies., Das Ende der Anonymität. Was Drohnen und Facebook verbindet, in: „Blätter", 10/2013, S. 51-62.

haltung – weitestgehend schuldig geblieben. Inzwischen haben Wissenschaftler und unabhängige Datenschutzbehörden den Umgang mit den gesammelten Daten überprüft. Das ernüchternde Ergebnis: Die massenhaften anlasslosen Datensammlungen haben so gut wie keine positiven Auswirkungen auf die Sicherheit gehabt.[17] Wesentlich effektiver sind nach wie vor klassische gezielte Ermittlungen. Zwar können auch dabei Unschuldige ins Visier der Sicherheitsbehörden geraten, aber in sehr viel geringerem Umfang als bei der anlasslosen Massenüberwachung.

Die neue Bürgerbewegung

Fest steht aber auch: Die Umkehr zu einem verbesserten Schutz unserer Daten wird nicht von selbst kommen. Nur wenn die Überwachung und die von ihr ausgehenden Gefahren stärker ins Blickfeld der Öffentlichkeit und der politischen Debatte rücken, werden sich die Kräfte, die für immer neue Instrumente zur Registrierung und Steuerung unseres Verhaltens eintreten, zurückdrängen lassen. Das Ringen um den Datenschutz ist eine politische Auseinandersetzung. Das Recht steht nicht außerhalb der Gesellschaft, es ist vielmehr Resultat – und zugleich Triebfeder der Entwicklung. Die Verfassungsgerichtsentscheidungen zur Volkszählung, zur Rasterfahndung, zum großen Lauschangriff und zur Online-Durchsuchung sind das Ergebnis gesellschaftlichen Ringens um einen tragfähigen Interessenausgleich zwischen Freiheit und Sicherheit und nicht bloß Ausdruck gelehrter Rechtsexegese.

Heute können wir beobachten, dass die Kräfte in der Zivilgesellschaft stärker werden, die die Überwachung nicht mehr als Schicksal hinzunehmen bereit sind. Und auch das hermetische System geheimer Überwachung, das seit 2001 errichtet wurde, zeigt die ersten Risse. Die auf Snowden zurückgehenden Veröffentlichungen haben die Fundamente dieses Gebäudes erschüttert. Seine Grundmauern allerdings stehen nach wie vor. Der Kampf dagegen bleibt also weiter unabdingbar.

Bei alledem darf derjenige nicht vergessen werden, dem wir die Kenntnis über die immensen Menschenrechtsverletzungen verdanken. Edward Snowden ist ein klassischer „Whistleblower", also jemand, der laut pfeift, weil er mit Rechtsbrüchen und unmoralischem Handeln konfrontiert ist. Dass er den Weg über China wählte und dann in Moskau „hängen blieb", tut seiner Leistung keinen Abbruch. Wenn die westlichen Demokratien ihren Ansprüchen und Grundwerten treu bleiben wollen, müssen sie ihm einen gesicherten Aufenthaltsstatus einräumen. Letztlich beweist sich nur am Umgang mit dem einzelnen Menschen, wie ernst es den Verantwortlichen mit den Grund- und Menschenrechten ist – und ob es sich dabei um einen echten Willen oder nur um papierne Bekenntnisse handelt.

17 Vgl. etwa Max-Planck-Institut für ausländisches und internationales Strafrecht, Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, Juli 2011; siehe auch den Report des PCLOB (Privacy and Civil Liberties Oversight Board) zur NSA-Überwachung vom 23.1.2014.