Peter Schaar

# Politische Handlungsmöglichkeiten nach dem NSA-Skandal auf nationaler Ebene

Peter Schaar zeigt auf, wie die Bundesregierung auf nationaler Ebene für einen besseren Schutz des Fernmeldegeheimnisses sorgen kann. Zunächst einmal sollte Deutschland als gutes Vorbild voran gehen und die bisher gesetzlich ungeregelte Auslandsüberwachung des BND einschränken. Zudem regt er eine konsequente Anwendung des deutschen Strafrechts gegen alle Spionageaktivitäten in Deutschland an. Schließlich sollte die NSA-Spionage mit einer gezielten Förderung sicherer Verschlüsselungstechniken und abhörsicherer Infrastrukturen gekontert werden. Für europäische Anbieter wären datenschutzkonforme Angebote ein Wettbewerbsvorteil gegenüber amerikanischen Konkurrenten, die tief in die in die NSA-Überwachungsaktivitäten verstrickt sind. Eine wesentliche Voraussetzung dafür ist jedoch, dass die zugrundeliegenden Technologien offen und transparent gestaltet werden, denn nur so bleiben sie demokratisch und öffentlich kontrollierbar. Das Prinzip der Geheimhaltung von Sicherheitstechnologien („*Security by Obscurity*“) habe dagegen ausgedient.

Nationale Handlungsmöglichkeiten gegen globale Überwachungsaktivitäten zu formulieren, erscheint vordergründig als unlösbare Aufgabe - sind doch die Aktivitäten von Regierungen und Parlamenten auf den eigenen Staat ausgerichtet, während die Überwachung der Datenströme vornehmlich exterritorial, außerhalb des jeweiligen nationalen Territoriums erfolgt. Trotzdem sollte man die Flinte nicht allzu schnell ins Korn werfen und allein auf die Entwicklung und Durchsetzung internationaler Rechtsinstrumente setzen, die der globalen Überwachung Grenzen setzen. So wichtig diese internationalen Regeln sind – etwa Art. 17 des UN-Zivilrechtspakts[1], der den Schutz des Privatlebens garantiert –, so schwierig gestaltet sich ihre Weiterentwicklung und vor allem ihre praktische Durchsetzung, solange große Staaten wie die USA, Russland und China sich verweigern. Nicht zuletzt wegen dieser Schwierigkeiten macht es also durchaus Sinn, über die Instrumente nachzudenken, die auf nationaler Ebene zur Verfügung stehen.

Zum einen haben nationale Aktivitäten in globalen Netzen auch direkte Folgen außerhalb des eigenen Territoriums. So wirkt sich nationale Gesetzgebung, die den eigenen Behörden beim Überwachen der Kommunikation Grenzen setzt oder entspre-

chende Aktivitäten ausländischer Geheimdienste unter Strafe stellt, auf die bi- und multilateralen nachrichtendienstlichen Informationstauschbörsen aus – jedenfalls dann, wenn die Bereitschaft dazu bei Regierungen, Behörden und Gerichten besteht.

Auch technologische Maßnahmen zur Härtung von IT-Infrastrukturen schützen die Computersysteme und Netzwerke nicht nur gegen inländische Angreifer, sondern auch gegen Infiltrationsversuche von Nachrichtendiensten. Die Bereitstellung anonymer Nutzungsmöglichkeiten im Netz, robuste Verfahren zur sicheren Authentifizierung, Verschlüsselungsmechanismen nach dem Stand der Wissenschaft und Technik machen es nicht nur Betrügern sondern auch ausländischen Geheimdiensten schwerer, an begehrte Informationen zu gelangen.

## Juristische Stellschrauben gegen Überwachung?

Traditionell entfalten Gesetze ihre Schutzwirkung im jeweiligen territorial definierten Geltungsbereich. Im Unterschied dazu ist das Internet aber 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. Im folgenden soll deshalb untersucht werden, wie weit dieses offensichtliche Territorialdilemma durch nationales Recht entschärft werden kann.

Die Tatsache, dass Spionage nicht gegen Völkerrecht verstößt, stellt Spione nicht straffrei. Geheimdienstliche Späh- und Lauschaktionen im Ausland beeinträchtigen regelmäßig die Rechte der davon betroffenen Zielpersonen und sind deshalb strafbar. Zwar heißt es in § 3 Strafgesetzbuch (StGB): „Das deutsche Strafrecht gilt für Taten, die im Inland begangen werden.“ Diese territoriale Begrenzung des deutschen Strafrechts wird aber durch § 5 StGB in Bezug auf bestimmte Auslandstaten eingeschränkt, die sich gegen inländische Rechtsgüter richten. Zu diesen unabhängig vom Tatort zu ahndenden Straftaten gehört auch die Verletzung von Betriebs- oder Geschäftsgeheimnissen, nicht jedoch das Post- und Fernmeldegeheimnis oder Verstöße gegen den Datenschutz. Gleichwohl können auch solche Straftaten nach deutschem Recht verfolgt werden, die aus dem Ausland initiiert wurden, sich aber im Inland auswirken („verwirklichen“). Wenn also ein ausländischer Geheimdienst Computer deutscher Nutzer mittels Trojaner infiltriert und überwacht, erfüllt dies den Straftatbestand des Ausspähens von Daten (§ 202a StGB).

Aus dem Ausland agierende Betrüger, die die Konten deutscher Bankkunden unter Verwendung ausspionierter PINs und Passwörter abräumen, machen sich nach deutschem Recht strafbar. 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. Schon die Vorbereitung einer

solchen Straftat, insbesondere das Ausspähen von Passwörtern oder sonstigen Sicherungscodes, die den Zugang zu vertraulichen Daten ermöglichen, ist strafbar.

Ebenso ist nach deutschem Recht strafbar, das nicht öffentlich gesprochene Wort abzuhören oder aufzuzeichnen – dies gilt auch für Telefonate, die mit dem Handy geführt werden. Schließlich verbietet § 99 StGB die geheimdienstliche Agententätigkeit für eine fremde Macht. Der Tatbestand stellt nicht auf konkreten Verrat ab, sondern erfasst jede auf die Beschaffung von Informationen für einen fremden Nachrichtendienst gerichtete Tätigkeit, die deutsche Sicherheitsinteressen beeinträchtigen kann. Geschütztes Rechtsgut ist die äußere Sicherheit Deutschlands im weitesten Sinne. Auch Wirtschaftsspionage kann nach § 99 StGB strafbar sein. Erfasst wird auch die Ausspähung von in Deutschland lebenden Ausländern für Nachrichtendienste ihrer Heimatländer. „Selbst eine Tätigkeit für Nachrichtendienste verbündeter Staaten verletzt deutsche Interessen, wenn sie nicht von deutschen Sicherheitsbehörden abgedeckt ist“, heißt es auf der Website des Generalbundesanwalts.[2]

Auch der Bruch des Fernmeldegeheimnisses ist eine Straftat – genauso wie das heimliche Eindringen in geschützte Computersysteme. Heute können kaum noch Zweifel daran bestehen, dass britische und amerikanische Geheimdienste gegen mehrere dieser Strafvorschriften verstoßen haben, etwa beim Abhören des Handys von Bundeskanzlerin Merkel, aber auch beim massenhaften Ausspähen deutscher Kommunikationsverkehre, die über ausländische Netzknoten und Transatlantikkabel geführt werden.

Dies gilt nicht nur für die genannten angloamerikanischen Nachrichtendienste, sondern auch für die Dienste anderer Staaten und auch für den Bundesnachrichtendienst. Wenn etwa der BND Telefone und E-Mails oder Mobilfunknetze im Hindukusch oder in anderen Operationsgebieten überwacht und dabei milliardenfach Metadaten absaugt, widerspricht dies natürlich dem dortigen Recht - und zwar völlig unabhängig davon, ob das deutsche BND-Gesetz derartige Aktivitäten erlaubt oder nicht, wie etwa im Untersuchungsausschuss des Deutschen Bundestags zu den NSA-Aktivitäten diskutiert wird.[3]

Bei der Rechtfertigung der geheimdienstlichen Tätigkeit im Ausland wird gern ausgeblendet, dass deutsche Behörden die zentralen Wertentscheidungen des Grundgesetzes, insbesondere die Achtung der Menschenwürde (Art. 1 Abs. 1 GG) stets zu beachten haben, egal wo sie tätig sind. Dies gilt unabhängig davon, ob die Beschränkungen, die etwa das G10- oder das BND-Gesetz dem Bundesnachrichtendienst setzen, nicht uneingeschränkt bei der Auslandsaufklärung gelten.

Auch bei nachrichtendienstlichen Lauschaktivitäten kann die Menschenwürde berührt sein: So hat das Bundesverfassungsgericht wiederholt festgestellt, dass es mit der Menschenwürde unvereinbar wäre, wenn staatliche Stellen einen „unantastbaren Kernbereich der Privatsphäre“ ausspionieren: „Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung ... nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung ... und dem Strafverfolgungsinteresse findet insoweit nicht statt.“[4] In weiteren Entscheidungen hat das Gericht festgestellt, dass zu diesem Kern-

bereich auch höchstpersönliche Lebensäußerungen gehören, die mittels Telekommunikation übertragen werden.[5]

Das lückenlose Abhören der Telekommunikation ist deshalb generell unzulässig, weil Gespräche abgehört werden könnten, die diesem absolut geschützten Bereich zuzurechnen sind. Jedenfalls müssen Vorkehrungen getroffen werden, dass Informationen, die zum Kernbereich privater Lebensgestaltung gehören, nicht aufgezeichnet oder jedenfalls unverzüglich gelöscht werden. Dies gilt nicht nur für inländische Überwachungsmaßnahmen, sondern auch für Aktivitäten des Bundesnachrichtendienstes als Auslandsgeheimdienst. Zudem gilt das deutsche Datenschutzrecht stets dann, wenn der BND personenbezogene Daten im Inland verarbeitet. Wenn der BND Daten aus der Auslandsaufklärung an die amerikanischen Nachrichtendienste weiterleitet – wie durch die Bundesregierung bestätigt[6] – muss er dabei deutsches Datenschutzrecht beachten.

Man muss also nicht allzu lange suchen, um im juristischen Instrumentenkasten Werkzeuge zu finden, die gegen eine überbordende Geheimdienstüberwachung eingesetzt werden könnten. Als eigentliches Problem entpuppt sich deshalb die zögerliche Anwendung und Durchsetzung der bestehenden rechtlichen Vorgaben, sei es aus außenpolitischer Rücksichtnahme oder aber auch im Interesse der deutschen Sicherheitsbehörden, die immer wieder darauf hinweisen, wie abhängig sie von den Informationen seien, die sie von ausländischen – namentlich amerikanischen – Diensten erhalten.

## Technik: Vom Teil des Problems zum Teil der Lösung

Der kürzlich verstorbene FAZ-Herausgeber Frank Schirrmacher verglich die Erkenntnisse aus den Snowden-Papieren mit dem „Sputnik-Schock“, den die Vereinigten Staaten 1959 erlitten hatten, als sie feststellen mussten, dass der erste Weltraumsatellit nicht etwa durch die US-Raumfahrtbehörde NASA auf den Weg gebracht worden war, sondern von den Russen. Unter Bezugnahme auf diese Erfahrung meinte Schirrmacher, es wäre angesichts der Meldungen zu geheimdienstlichen Überwachungsaktivitäten grundfalsch, wenn Europa den Kopf in den Sand stecken und sich mit einer digitalen Opferrolle abfinden würde. Vielmehr müsse die „brachliegende digitale Intelligenz“ Europas entfesselt werden, indem man Initiativen für „integre Netzwerke und, wer weiß, auch für Suchmaschinen politisch ins Leben ruft und fördert“.[7]

Was könnte diese „digitale europäische Intelligenz“ bewirken? Es gibt durchaus verschiedene technische und juristische Stellschrauben für einen besseren Schutz der Daten. Mehr noch: Angesichts des grassierenden Vertrauensverlusts in amerikanische Internetdienste und der begründeten Vermutung, aus den USA oder China stammende Produkte enthielten Hintertüren oder bewusst eingebaute Schwachstellen, lässt sich durchaus europäisches Kapital schlagen.

Dies gilt insbesondere auf dem Feld der Datenverschlüsselung. Seit der Erfindung der E-Mail wird deren Vertraulichkeitsgrad ziemlich zutreffend mit dem einer Postkarte verglichen: Jeder, der Zugriff hat, kann mitlesen. Zudem grassieren Datenmiss-

brauch und Identitätsdiebstahl im Internet. Auch die übrigen Internetdienste wurden zunächst völlig ohne Verschlüsselung betrieben, die Daten also offen und leicht abhörbar übertragen. Auch wenn seit Jahren an verbesserten Schutzmechanismen gearbeitet wird, waren viele der inzwischen etablierten Verschlüsselungsverfahren zu schwach, um geheimdienstlichen Angriffen zu widerstehen.

Die NSA und ihr britischer Partner-Geheimdienst GCHQ waren offenbar in der Lage, nicht nur die unverschlüsselten Daten, sondern auch den verschlüsselten Internetverkehr großflächig auszuwerten. Viele Informatiker setzen jedoch weiterhin auf die Datenverschlüsselung. Selbst wenn man Überwachung letztlich nicht völlig verhindern könne, bestehe zumindest die Chance, sie den Nachrichtendiensten deutlich zu erschweren und für sie teuer zu machen.

Die Möglichkeit eines absolut sicheren Verschlüsselungssystems mag es theoretisch geben. Praktisch muss man allerdings einige Abstriche machen. Alle funktionierenden kryptographischen Systeme gelten nur unter bestimmten Prämissen hinsichtlich der Fähigkeiten der „Gegenseite“, insbesondere in Bezug auf die Rechenkapazitäten als sicher. Die Sicherheit nahezu aller Verschlüsselungsalgorithmen ist zudem nicht vollständig nachgewiesen. Alle Feststellungen zur Sicherheit der jeweiligen Verfahren beruhen vielmehr auf der Prüfung und Diskussion durch die Fachöffentlichkeit. Deshalb ist es von entscheidender Bedeutung, dass Verschlüsselungsalgorithmen dokumentiert und öffentlich nachprüfbar sind.

Dagegen können Verfahren, deren Funktionsweise geheim gehalten wird, nicht durch unabhängige Experten und eine kritische „Netzcommunity“ nachgeprüft werden. Bisweilen wird die Geheimhaltung der Verschlüsselungsalgorithmen sogar als Argument für mehr Sicherheit verkauft. Eine derartige Sichtweise blendet aber aus, dass nicht nur externe Angreifer versuchen, die Verschlüsselung zu durchbrechen, sondern auch Insider, die Kenntnisse über Schwachstellen eines Verschlüsselungsverfahrens besitzen, an Angriffen auf gesicherte Daten mitwirken oder ihr Wissen Dritten verkaufen könnten.

An „*Security by Obscurity*“ sollte man spätestens jetzt nicht mehr glauben, nachdem bekannt ist, dass die NSA systematisch auf die Schwächung von Verschlüsselungsverfahren hingearbeitet hat. Deshalb sollten grundsätzlich nur solche Verfahren verwendet werden, deren Programmcode und Funktionsweise öffentlich dokumentiert sind („*Open Source*“).

Die Verschlüsselungsalgorithmen müssen in Software umgesetzt werden. Eine „schlampige“ oder bewusst nachlässige Programmierung kann dazu beitragen, dass an und für sich sichere Algorithmen unterlaufen oder umgangen werden können. Bekanntlich bieten derartige Schwachstellen den Geheimdiensten und anderen Insidern Ansatzpunkte zur Kommunikationsüberwachung. Auch hier gilt: *Open-Source-Software* ist solchen Programmen vorzuziehen, deren Programmcode und Funktionsweise von den Anbietern geheim gehalten werden.

Die Öffentlichkeit allein kann die Sicherheit von Verschlüsselungsverfahren zwar nicht garantieren, sie ermöglicht es aber, dass Fehler und Schwachstellen erkannt und behoben werden können. Ein weiterer Faktor für die Vertrauenswürdigkeit von kryptographischen Verfahren besteht darin, dass weder die Hersteller noch die Anbieter von Diensten rechtlich dazu verpflichtet werden, Hintertüren in ihre Systeme

einzubauen, die Geheimdiensten und anderen Sicherheitsbehörden den Zugriff auf die Kommunikation ermöglichen, wie etwa der US-amerikanische *Communications Assistance for Law Enforcement Act* (CALEA).

Ob bei der Kryptographie, beim Routing, bei der Gestaltung von E-Mail-Diensten oder bei den Anforderungen an Cloud-Speichern: Ansatzpunkte gibt es mehr als genug. Ob die sich hier bietenden Chancen allerdings auch wirklich wahrgenommen werden, ist indes noch ungewiss. Sehr ambivalent verhält sich etwa die Industrie, die bei anderer Gelegenheit nicht zögert, ihre Interessen einzufordern. Frank Schirrmacher weist darauf hin, dass der „deutsche" IT-Branchenverband *Bitkom* maßgeblich von Ablegern globaler US-Firmen beeinflusst werde und sich auch deshalb kaum als Speerspitze deutscher oder europäischer Interessen eigne. Und die Wirtschaftswoche berichtete über einen heftigen Streit in diesem Verband zum Umgang mit der NSA-Affäre. Aus dessen Protokollen gehe hervor, dass sich die amerikanischen Mitglieder vehement gegen den Vorschlag deutscher IT-Unternehmen gewehrt hätten, sichere Hard- und Software „Made in Germany" zu forcieren. Insbesondere die Forderung, Datenpakete von und nach Deutschland nicht mehr über Server in den USA und Großbritannien umzuleiten, weil diese von der NSA und dem britischen Geheimdienst GCHQ angezapft werden, sei von den Amerikanern blockiert worden.

Dabei gibt es genügend deutsche – und europäische – Unternehmen, die von einem neuen Geschäftsfeld Datenschutz und Datensicherheit profitieren würden. Bereits jetzt stehen leistungsfähige europäische Cloud-Services zur Verfügung, die ohne US-Beteiligung funktionieren. Dies hat US-Cloud-Anbieter dazu veranlasst, europäischen Kunden zuzusichern, dass deren Daten ausschließlich in Europa gespeichert würden.

Ob damit allerdings der gewünschte Schutz vor Überwachung erreicht wird, ist zumindest offen. Denn die amerikanischen Behörden bestehen darauf, dass die US-Unternehmen – völlig unabhängig von der europäischen Rechtslage – auch solche Daten herauszugeben haben, die nicht auf Servern in den Vereinigten Staaten gespeichert sind. Inwieweit die US-Unternehmen diesen Ansinnen folgen, die ggf. gegen das Recht der Staaten verstoßen, in denen die Server stehen, ist nicht bekannt.

Immerhin hat die Bundesregierung eine in der Öffentlichkeit kaum wahrgenommene erste Maßnahme getroffen, um rechtliche und technische Hintertüren zu verschließen, die es ausländischen Geheimdiensten ermöglichen, an vertrauliche Daten zu gelangen. In einem an das Beschaffungsamt des Bundesinnenministeriums gerichteten No-Spy-Erlass vom 30. April 2014 ist vorgesehen, dass in Vergabeverfahren des Bundes jeder Bieter Erklärungen abgeben muss, die heimliche Abflüsse schützenswerter Informationen an ausländische Nachrichtendienste betreffen. Weil dies kaum nachweisbar ist, wurden die Klauseln so ausgestaltet, dass eine Beweiserleichterung zugunsten der Bundesrepublik Deutschland eintritt. Für die Ablehnung eines Bieters bzw. für eine Kündigung des Vertrages soll es ausreichen, wenn nachgewiesen wird, dass der Bieter einer rechtlichen Verpflichtung zur Weitergabe von vertraulichen Informationen, Geschäfts- oder Betriebsgeheimnissen an Dritte unterliegt. Gegebenenfalls müssen entsprechende Weitergabeverpflichtungen im Vergabeverfahren offengelegt werden. Damit werden auch Fälle erfasst, in denen entsprechende Auskünfte nach ausländischem Recht geheim zu halten sind.[8]

In vielen Bereichen, insbesondere bei E-Mails, gibt es deutsche und europäische Alternativen, die den Vergleich mit der amerikanischen Konkurrenz nicht fürchten müssen. Insbesondere wenn gewährleistet wird, dass die Datenübertragung sicher verschlüsselt erfolgt, könnte die Wahl eines solchen Dienstes einen erheblichen Zugewinn an Sicherheit und Datenschutz bedeuten. Problematisch ist dabei bisher allerdings, dass die meisten Angebote für verschlüsselte E-Mails lediglich eine „Verbindungsverschlüsselung“ vorsehen, d.h., die verschlüsselt übertragenen E-Mails werden von den Anbietern temporär entschlüsselt und könnten an diesen Schnittstellen gegebenenfalls im Klartext mitgelesen werden. Technisch ist es allerdings möglich, auf professioneller Basis eine Ende-zu-Ende-Verschlüsselung zu gewährleisten. Es ist nur eine Frage der Zeit, bis entsprechende Angebote auf den Markt kommen.

Noch nicht – oder nicht mehr – wirklich konkurrenzfähig ist die europäische Industrie in weiten Bereichen der Netzwerktechnik. Amerikanische und chinesische Unternehmen haben hier außergewöhnlich starke Marktpositionen errungen. Europäische Kunden können bei beiden Herkunftsländern nicht sicher sein, dass die entsprechenden Produkte frei von Hintertüren und nicht dokumentierten Überwachungsschnittstellen sind. Hier hätte eine europäische Industriepolitik gute Chancen, mit gezielter Förderung sicherer und zugleich leistungsfähiger Produkte die Entwicklung marktgängiger Produkte „made in Europe“ zu erreichen, die sich in der Konkurrenz mit chinesischen und US-amerikanischen Anbietern behaupten. Wenn gewährleistet ist, dass die Systeme ohne Einbußen an Qualität und Komfort zugleich die Vertraulichkeit und Integrität der Datenübertragung garantieren, könnte sich hier eine interessante Marktposition gewinnen lassen, weit über Deutschland und Europa hinaus.

Als Reaktion auf die Berichte über die insbesondere durch die amerikanischen und britischen Geheimdienste betriebenen globalen Überwachungsmaßnahmen wurde schließlich vorgeschlagen, europäische Datenpakete nicht mehr über Netzknoten in Übersee zu senden. So forderten die Datenschutzbeauftragten des Bundes und der Länder, „zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.“ Das Internet-Routing sollte so konfiguriert werden, dass die innerhalb eines Gebiets versendeten Nachrichten dieses nicht mehr wie bisher verlassen.

Bemerkenswert ist insbesondere der Vorschlag eines „Schengen-Routing“, benannt nach dem Abkommen über den freien Reiseverkehr in Europa. Dabei würden die Datenpakete ausschließlich über Netzknoten in den Teilnehmerstaaten des Schengener Abkommens geleitet – Umwege über Drittstaaten, etwa die USA, wären auszuschließen. Der Schengen-Raum umfasst die meisten Mitgliedstaaten der Europäischen Union und einige andere europäische Staaten, nicht jedoch Großbritannien und Irland. Die Begrenzung auf die Schengen-Staaten könnte – so die Überlegung – nicht nur die NSA an einem Datenzugriff hindern, sondern auch den britischen Nachrichtendienst GCHQ, der im Rahmen des Programms Tempora maßgeblich an den Überwachungsaktivitäten beteiligt ist. Ein Nebeneffekt könnte darin bestehen, wichtige US-Internetunternehmen mit europäischen Hauptniederlassungen in Großbritannien und Irland zu umgehen.

Technisch ist es heute ohne weiteres möglich, Datenverbindungen, bei denen beide Kommunikationspartner sich in Europa befinden, nur über europäische Netzknoten

zu leiten. In den letzten Jahren wurden die europäischen Netzinfrastrukturen massiv ausgebaut, so dass jedes Datenpaket heute auf vielen Wegen innerhalb des Schengen-Raums geroutet werden könnte. Tatsächlich werden aber immer noch viele Datenströme über die USA geleitet. Derzeit erfolgt die Wegewahl im Internet im Wesentlichen nach den Kriterien Preis, Entfernung und Service-Qualität. Die Umleitung europäischer Datenpakete über US-Netzknoten hat weniger technische als finanzielle Gründe, denn die US-Anbieter bieten deutlich günstigere Konditionen als die europäische Konkurrenz. Das Schengen-Routing würde dementsprechend vermutlich zu erhöhten Kosten führen, jedoch kaum mit Einbußen in der Qualität der Verbindungen verbunden sein. Auch die Ausfallsicherheit des europäischen Netzes ist durch vielfach redundante Verbindungen heute weitgehend gewährleistet.

Trotzdem würden entsprechende Vorgaben zum Routing nicht automatisch zum Versiegen der Datenströme über den Atlantik führen. Zum einen werden Daten auch weiterhin stets dann in die USA übertragen, wenn die elektronischen Dienstleistungen von dort aus erbracht werden. Dazu kommt, dass amerikanische Anbieter die Daten ihrer Nutzer über ihre in den USA gelegenen Infrastrukturen leiten und überwiegend dort auf Servern ablegen. Wer einen amerikanischen E-Mail-Dienst nutzt oder *Google* als Suchmaschine verwendet, muss also – auch wenn das Schengen-Routing kommen sollte – weiterhin damit rechnen, dass seine Daten in den USA landen, auf dem Weg über Netzknoten und Überseekabel durch den GCHQ und die NSA abgehört und auf Anfrage an US-Sicherheitsbehörden herausgegeben werden. Dies gilt auch für Facebook, das seine Dienste seit einigen Jahren europäischen Nutzern offiziell unter der Firma „*Facebook Ltd.*“ aus Dublin anbietet, denn technisch wird der Dienst weiterhin überwiegend in den USA betrieben.

Nicht vergessen werden darf dabei, dass Vorgaben zum Routing auch Auswirkungen auf die Konkurrenzsituation europäischer Unternehmen untereinander haben können. So erntete die Deutsche Telekom auf ihren Vorschlag eines „nationalen IP-Routings“ empörende Reaktionen bei anderen deutschen Internet-Anbietern. Der Geschäftsführer des größten deutschen Internetknotens DE-CIX, Harald Summa, bezeichnete die Initiative der Telekom als „reine Marketingaktion und Irreführung der Politik“. Die Telekom selbst behindere den Verbleib der Datenpakete im deutschen Rechtsraum, denn sie organisiere den Transport ihrer Daten direkt mit anderen Netzbetreibern und beteilige sich nicht am öffentlichen, gleichberechtigten Datenaustausch („*public peering*“). Dies habe die Folge, dass nicht mit der Telekom verbundene Netzanbieter an Telekom-Kunden gerichtete Datenpakete vielfach nur über das Ausland zustellen könnten. Inzwischen scheinen sich die verhärteten Fronten zwischen den verschiedenen Internetanbietern jedoch aufzulösen. Wie zu vernehmen ist, verhandelt etwa die Deutsche Telekom mit dem Internetverband *Eco* über entsprechende Lösungen, die eine sichere Kommunikation über Providergrenzen hinaus ermöglichen.

## Fazit

Auch wenn globale Überwachungsaktivitäten nachhaltig nur durch internationales Recht und internationale Vereinbarungen zurückgefahren werden können, sollte nicht darauf verzichtet werden, die auf nationaler oder regionaler Ebene (EU) bestehenden technischen und rechtlichen Instrumente zum verbesserten Schutz der Privatsphäre und zur Gewährleistung der Vertraulichkeit der Kommunikation nutzen. Neben den direkten Schutzwirkungen entfalten solche Maßnahmen eine Ausstrahlung auf andere Nationen und Weltregionen. Globale Überwachung ist nicht schicksalhaft, sondern ein von Menschen verursachtes Phänomen. Der Einzelne, die Gesellschaft und die Weltgemeinschaft haben Mittel, diese Entwicklung wieder zurückzufahren.

**PETER SCHAAR** Jahrgang 1954, ist gelernter Ökonom. Er war ab 1980 in der Verwaltung der Hansestadt Hamburg tätig und wechselte 1986 zum Hamburger Landesdatenschutzbeauftragten. 2003 wurde er auf Vorschlag von Bündnis 90/Die Grünen vom Deutschen Bundestag zum fünften Bundesbeauftragte für Datenschutz gewählt. Seine zweite Amtszeit endete am 16. Dezember 2013. Seit September 2013 steht Schaar der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) vor.

## Anmerkungen:

1 Internationaler Pakt über bürgerliche und politische Rechte vom 19.12.1966 (BGBl. 1973 II 1553).
2 S. https://www.generalbundesanwalt.de/de/spionage.php.
3 Vgl. hierzu etwa die Sachverständigengutachten der ehemaligen Bundesverfassungsrichter Papier und Hoffmann-Riem, https://www.bundestag.de/bundestag/ausschuesse18/ua/1untersuchungsausschuss/-/280848.
4 BVerfG, Urteil zur akustischen Wohnraumüberwachung („großer Lauschangriff“), 1 BvR 2378/98 vom 3.3.2004.
5 Vgl. etwa BVerfG, Urteil zur präventiven Telekommunikationsüberwachung durch die Polizei, 1 BvR 668/04 vom 27.7.2005.
6 Vgl. BT-Drs. 17/14560, S. 8.
7 Schirrmacher, Europas Sputnik-Schock, FAZ v. 1.11.2013, S. 1.
8 S. Erläuterungen des BMI zum „No-Spy-Erlass", abrufbar unter http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/08/no-spy-erlass.html.