SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Zwischen Überwachung und Aufklärung

Die amerikanische Debatte und die europäische Reaktion auf die Praxis der NSA

Daniela Kietz / Johannes Thimm

Je mehr über den Umfang bekannt wird, in dem die National Security Agency und ihre Partner die Kommunikation und das Internetverhalten von Menschen überwachen, desto deutlicher wird auch in den USA die Kritik an den amerikanischen Nachrichtendiensten. Dennoch können die Europäer nicht darauf setzen, dass die USA ihre Überwachungspraxis korrigieren. Vielmehr sollten sie selbst aktiv werden. Wer von den USA Aufklärung fordert und den Datenschutz stärken möchte, sollte einen europäischen Ansatz verfolgen. Denn die Erfolgsaussichten für nationalstaatliches Handeln sind schlecht. Voraussetzung ist jedoch ein offener Umgang der Europäer mit der Rolle der Datenüberwachung ihrer eigenen Nachrichtendienste.

Anfangs klang Edward Snowdens Behauptung, er habe als Dienstleister für die US-Geheimdienste Zugang zu den persönlichsten Daten jedes Internetnutzers gehabt, noch übertrieben. Zwei Monate später haben sich die Hinweise verdichtet, dass seine Aussage weitgehend zutrifft. Zu Recht schlugen Aufsichtsbehörden, Kommentatoren und Politiker Alarm. Die US-Regierung versucht der Kritik zu begegnen, indem sie schrittweise die regulatorischen Bedingungen für Überwachungsprogramme wie Prism oder das Sammeln von Telefonverbindungsdaten offenlegt. Damit will sie demonstrieren, dass die National Security Agency (NSA) in einem rechtsstaatlichen Rahmen arbeitet. Doch diese Programme sind schon fast zu einem Nebenschauplatz geworden, seit alles darauf hindeutet, dass die NSA direkten Zugriff auf die Infrastruktur des Internets hat, also auf Server und Verbindungsleitungen und damit auf den gesamten Internetverkehr (siehe Kasten, S. 8). Die rechtsstaatlichen Kontrollmechanismen in den USA schützen nur US-Staatsbürger und Menschen, die in den USA leben, nicht jedoch die EU-Bürger.

Dabei werden der Öffentlichkeit noch immer konkrete und belastbare Informationen über rechtliche Grundlagen, Funktionsweise und Ausmaß der Überwachung vorenthalten. Trotz anderslautender Zusicherungen der US-Geheimdienste bestehen deshalb auch nach wie vor Zweifel, dass sie europäische Rechtsstandards einhalten.

Die der NSA zur Last gelegten Überwachungsaktivitäten fallen in zwei Kategorien. Zum einen greift die NSA in Zusammenarbeit mit Partnerdiensten und privaten Firmen auf Daten von Privatpersonen

Daniela Kietz ist Wissenschaftlerin in der Forschungsgruppe EU-Integration,
Dr. Johannes Thimm ist Wissenschaftler in der Forschungsgruppe Amerika

zu, die deren Kommunikation und Internetverhalten betreffen – einschließlich Informationen über Telefongespräche, Email-Verkehr, die Nutzung sozialer Medien und Cloud-Dienste. Diese Daten werden für lange Zeiträume gespeichert, um eine spätere Nutzung zu ermöglichen. Betroffen sind Menschen innerhalb und außerhalb der USA. Da für die Erfassung von Daten von Amerikanern gesetzliche Beschränkungen bestehen, gilt das für sie allerdings nicht im gleichen Maße.

Zum anderen soll die NSA nach Berichten des *Spiegel* (der sich auf durchgesickerte NSA-Dokumente stützt) Vertretungen der EU in den USA und EU-Institutionen in Brüssel ausgehorcht haben. Diese Berichte werden von den Institutionen und Mitgliedstaaten der Union sehr ernst genommen. Sollten sie zutreffen, wäre das klassische Spionage: Um sich einen Informationsvorsprung zu verschaffen, setzten die USA gegenüber Verbündeten auch Mittel ein, die nach dem Wiener Übereinkommen über diplomatische Beziehungen unrechtmäßig sind. Das ließe sich auch nicht als Maßnahme der Terrorabwehr rechtfertigen.

Trotz Kritik Kurskorrektur der USA unwahrscheinlich

Die Diskussion in den USA hat sich seit Beginn der Enthüllungen stark gewandelt. In Bevölkerung und Kongress nimmt die Kritik an der Überwachungspraxis zu. Zuletzt sah sich sogar Präsident Barack Obama genötigt, seine Bereitschaft zu bekunden, für mehr Transparenz und eine bessere institutionelle Kontrolle der Geheimdienstaktivitäten zu sorgen. Die Europäer sollten jedoch nicht zu viel von diesem Trend erwarten.

Das wachsende Unbehagen der Öffentlichkeit über das Ausmaß der Überwachung zeigt sich auch in den Meinungsumfragen. Laut einer Erhebung des Pew Research Center von Juli sind 47 Prozent der Befragten der Ansicht, dass die Anti-Terror-Politik der Regierung die Bürgerrechte zu sehr einschränkt; 35 Prozent glauben, die Regierung unternehme nicht genug gegen den Terrorismus. Zum ersten Mal seit 2004 überwiegt die Sorge um die Bürgerrechte.

Auch unter Kongressmitgliedern ist ein Stimmungswechsel zu verzeichnen. Nachdem sie die von der Presse enthüllten Überwachungsprogramme zunächst verteidigt hatten, kritisieren sie nun verstärkt deren Ausmaß. Dabei konzentriert sich die Diskussion vor allem auf Prism und Programme zur Erfassung von Telefondaten, die von der Regierung bereits bestätigt wurden. Auch die von Präsident Obama vorgeschlagenen Veränderungen betreffen diese Programme. Zu der umfangreicheren Abschöpfung von Daten direkt an der Infrastruktur des Internet hat die US-Regierung bislang nicht Stellung genommen.

Neue Gesetzesinitiativen und Gerichtsurteile in den USA

Zwei Gesetzespakete bilden die rechtliche Grundlage für die gegenwärtige Praxis. Der Foreign Intelligence Surveillance Act (FISA-Gesetz) von 1978 regelt die Auslandsaufklärung. Zu deren Kontrolle wurde ein besonderes, vertraulich entscheidendes Gericht (Foreign Intelligence Surveillance Court, FISA-Gericht) geschaffen. Der nach dem 11. September 2001 verabschiedete Patriot Act und diverse Novellierungen beider Gesetze erweiterten seitdem die Kompetenzen der Behörden und den Zuständigkeitsbereich des FISA-Gerichts.

Derzeit gibt es Bestrebungen, die NSA-Aktivitäten durch Veränderung des rechtlichen Rahmens einzuschränken. Konkrete Ergebnisse wurden noch nicht erzielt. Im Repräsentantenhaus ist ein Gesetzentwurf zur Beendigung der massenhaften Speicherung von Telefonverbindungsdaten mit 205 zu 217 Stimmen abgelehnt worden. Auch wenn das Gesetz spätestens am Senat oder am Veto des Weißen Hauses gescheitert wäre, ist das knappe Ergebnis ein wichtiges Indiz für den wachsenden Widerstand gegen die Überwachung.

Eine breite Koalition von linken Bürgerrechtlern über moderate Vertreter beider Parteien bis hin zu konservativ-libertären

Staatskritikern befürwortete den Gesetzentwurf. Mit Nein stimmten die jeweiligen Parteiführungen (der Republikaner John Boehner und die Demokratin Nancy Pelosi) sowie die meisten Mitglieder des Nachrichtendienstausschusses. Aufgrund ihrer Teilnahme an vertraulichen Sitzungen mit Vertretern der Nachrichtendienste übernehmen die Ausschussmitglieder häufig deren Bedrohungswahrnehmung. Hauptsächlich an sie fließen auch Wahlkampfspenden von Firmen des nachrichtendienstlich-industriellen Komplexes, die an Aufträgen der NSA verdienen. So wurde der Ausschuss, einst zur Kontrolle der Geheimdienste gegründet, zu ihrem verlässlichen Unterstützer. Dies gilt auch für den Geheimdienstausschuss im Senat. Dessen Vorsitzende Dianne Feinstein verteidigte das Telefondatenprogramm von Beginn an als rechtmäßig und notwendig, zumal es nur die Verbindungsdaten betreffe.

Dagegen sparte der Justizausschussvorsitzende Patrick Leahy in einer Anhörung am 31. Juli 2013 nicht mit Kritik. Im Lichte seiner Kenntnis einer vertraulichen Liste verhinderter Terroranschläge stellte er die Behauptung der Administration in Frage, dass dank Prism mehrere geplante Attentate vereitelt worden seien. Aufgrund der wachsenden Skepsis werden im Kongress weitere Gesetzesentwürfe vorbereitet, um die bisherige Überwachungspraxis der NSA einzuschränken. So wird diskutiert, die bisher geheime Arbeit des FISA-Gerichts transparenter zu machen oder beim Sammeln von Daten Umfang und Dauer der Speicherung stärker zu begrenzen.

Außerdem ist mit weiteren Klagen von Bürgerrechtsorganisationen zu rechnen. Im Februar hatte der Oberste Gerichtshof eine Klage von Amnesty International gegen die NSA abgewiesen (Clapper v. Amnesty International), die geltend machte, dass Teile des FISA-Gesetzes verfassungswidrig seien. Laut Urteilsbegründung könne die Klägerin nicht nachweisen, dass sie von Überwachungen betroffen war. Die jüngsten Enthüllungen könnten das Gericht zwingen, in der substanziellen Frage zu urteilen, ob das FISA-Gesetz das in der Verfassung verankerte Recht auf Privatsphäre verletzt. Bisher haben die Gerichte nur selten gegen den Willen der Exekutive in die Befugnisse der Sicherheitsbehörden eingegriffen.

Debattenwandel nur ein Teilerfolg

Der Verlauf der US-Debatte ist auch für Europa relevant, denn er zeigt, dass die Kritik an der Überwachung nicht nur auf deutscher Hysterie beruht. Nachfragen von Kongress und US-Presse an die Sicherheitsbehörden können außerdem neue Informationen über die Funktionsweise der Programme zutage fördern.

Doch die Kritik in den USA entlässt die europäischen Regierungen nicht aus der Pflicht, selbst aktiv zu werden und für den Schutz ihrer Bürger zu sorgen. Einerseits ist keineswegs sicher, dass es in den USA zu mehr als kosmetischen Korrekturen kommt. Andererseits ist die US-Debatte auf die Bürgerrechte von Amerikanern fokussiert. Der Kongress stellt vorrangig die Speicherung von Telefonverbindungen innerhalb der USA sowie Verfahren in Frage, bei denen im Zuge der Fernmeldeaufklärung auch massenhaft Daten von Amerikanern gesammelt werden. Im Augenblick deutet nichts darauf hin, dass die Auslandsaufklärung unter Beschuss gerät, darunter das systematische Erfassen von Daten zum Internetverhalten von EU-Bürgern. Kurz: Auch eine veränderte US-Gesetzgebung wird nur Amerikaner schützen. Wenn die Europäer Aufklärung und einen wirksamen Datenschutz wollen, müssen sie selbst Maßnahmen ergreifen.

Transatlantischer Exekutivdialog

Direkt nach Bekanntwerden der US-Programme forderte die EU-Kommissarin für Justiz, Grundrechte und Bürgerschaft, Viviane Reding, die US-Administration mit deutlichen Worten dazu auf, konkrete Informationen über deren Aufbau, Funktionsweise, Umfang, Rechtsgrundlagen und Auswirkungen auf europäische Bürger zu geben.

Auch die Regierungen der Mitgliedstaaten äußerten Kritik an der US-Überwachungspolitik, unternahmen aber nur zögerlich konkrete Schritte zur Klärung des Sachverhalts. Sie verständigten sich schließlich mit der US-Regierung auf transatlantische Gespräche, die nun hinter verschlossenen Türen stattfinden. Die Mitgliedstaaten akzeptierten dabei den amerikanischen Vorschlag, datenschutzrechtliche Aspekte der Überwachungspraxis getrennt von konkreten Fragen zu den Tätigkeiten der Nachrichtendienste zu behandeln.

Mit dem einen Themenkomplex, den Datenschutzfragen, befasst sich eine EU-US-Arbeitsgruppe. Die europäische Delegation umfasst neben Vertretern ausgewählter Mitgliedstaaten auch den EU-Anti-Terror-Koordinator sowie jeweils einen Vertreter des litauischen Ratsvorsitzes, der EU-Kommission, des Europäischen Auswärtigen Dienstes und der nationalen Datenschutzbehörden (»Artikel-29-Gruppe«). Nach einem ersten Treffen Ende Juli ist die nächste Zusammenkunft für Mitte September geplant. Der Forderung des Europäischen Parlaments (EP), an den transatlantischen Gesprächen beteiligt zu werden, haben die Mitgliedstaaten nicht entsprochen.

Über den zweiten Themenkomplex, die konkreten nachrichtendienstlichen Aktivitäten, können die Regierungen in Eigeninitiative bilateral mit den USA Gespräche führen. Die USA sprachen sich gegen eine Beteiligung der EU-Institutionen aus, und die Mitgliedstaaten unterstrichen ebenfalls, dass nachrichtendienstliche Belange in erster Linie in die nationale Hoheit fallen. Der Vorschlag, diese Thematik in einer zweiten Arbeitsgruppe zu diskutieren, in der neben den USA sämtliche EU-Mitgliedstaaten vertreten sind, scheiterte insbesondere am Widerstand Großbritanniens und Schwedens. Beide Staaten lehnen nicht nur eine Beteiligung der EU-Institutionen, sondern auch ein zwischen den Mitgliedstaaten abgestimmtes Vorgehen ab, wenn es um die Arbeit der Nachrichtendienste geht. Inwieweit konkrete Ergebnisse der bilateralen Konsultationen einem größeren Kreis zugänglich gemacht werden, insbesondere der Kommission und dem EP, ist nicht bekannt.

Die Regierungen haben nur bedingtes Interesse an Aufklärung

Mit dem Verweis auf die Kompetenzverteilung zwischen nationaler und europäischer Ebene verhindern die Mitgliedstaaten ein geschlossenes europäisches Vorgehen. Ihre widersprüchliche Haltung – einerseits fordern sie Aufklärung, andererseits geben sie sich im Verhältnis zu den USA diplomatisch – hat aber noch tiefer liegende Gründe.

Drei Aspekte stehen im Vordergrund. Erstens ist den Regierungen an einem transatlantischen Konflikt nicht gelegen. Die Mehrheit der EU-Mitgliedstaaten, mit Ausnahme Frankreichs, möchte insbesondere vermeiden, dass sich die Überwachungsdebatte negativ auf die Verhandlungen über eine Transatlantische Partnerschaft für Handel und Investitionen (TTIP) auswirkt. Ebenso wenig aufs Spiel gesetzt werden soll die in den letzten Jahren zusehends engere Zusammenarbeit bei der Kriminalitäts- und Terrorismusbekämpfung.

Zweitens divergiert der innenpolitische Handlungsdruck auf die Regierungen erheblich. In Deutschland ist Datenschutz ein traditionell sensibles Thema, die öffentliche Kritik an der Überwachung im europäischen Vergleich ausgeprägt. Hier ruft die Bevölkerung lautstärker nach Antworten als in Staaten wie Irland oder Großbritannien, in denen Überwachungsmaßnahmen größere gesellschaftliche Akzeptanz genießen oder auf Desinteresse stoßen.

Legten die USA auf europäischen Druck hin tatsächlich Fakten auf den Tisch, bestünde aus Sicht der Mitgliedstaaten, drittens, das Risiko, dass die Kooperation ihrer eigenen Nachrichtendienste mit den USA und die mitgliedstaatlichen Datenüberwachungsprogramme – die ebenfalls EU-Bürger betreffen – stärker in den Fokus rücken. Dies wollen die EU-Staaten um jeden Preis vermeiden. Der vorrangig bilaterale Ansatz soll gewährleisten, dass

die Übermittlung von Daten an die NSA durch das britische Government Communications Headquarters (GCHQ) oder den Bundesnachrichtendienst nicht Gegenstand einer größeren Debatte wird.

USA profitieren vom gewählten Format

Den USA spielt das primär bilaterale Vorgehen unter Ausschluss der Öffentlichkeit in die Hände, da der ohnehin begrenzte europäische Einfluss dadurch noch weiter eingeschränkt wird. Die US-Vertreter sehen sich insgesamt kaum zur Rechtfertigung gegenüber den Europäern gezwungen. Sie machten einen *symmetrischen* Dialog über die nachrichtendienstliche Informationsgewinnung der US-Behörden *und* der Behörden der EU-Mitgliedstaaten zur Vorbedingung für Gespräche mit den EU-Staaten. Obwohl die NSA-Programme ursprünglicher Anlass der Gespräche waren, konfrontierten die US-Vertreter die EU-Mitgliedstaaten mit einem umfassenden Katalog von Fragen zur Tätigkeit der europäischen Nachrichtendienste. Zu den eigenen Programmen machten sie in der Arbeitsgruppe kaum konkrete Angaben. Details sollen, wenn überhaupt, in den bilateralen Gesprächen mit den Mitgliedstaaten behandelt werden.

Hier wird zweierlei deutlich. Zum einen betreiben die USA weniger Aufklärung, sondern scheinen eher weitere Kooperationsmöglichkeiten auszuloten. Die US-Vertreter stellen viele Fragen, geben aber kaum Antworten. Zum anderen zeigt sich, wie schwierig es ist, die beiden Themenkomplexe in der Praxis zu trennen. Ohne Kenntnis der genauen Funktionsweise und des Umfangs der US-Programme können datenschutzrechtliche Fragen und die Auswirkungen auf EU-Bürger nicht angemessen beurteilt werden. Somit ist nicht zu erwarten, dass die beiden Stränge der transatlantischen Gespräche *verlässliche* Einschätzungen zu den Überwachungsprogrammen hervorbringen werden: Der Rahmen ist zu unverbindlich, die EU-Mitgliedstaaten sind uneins. Allgemein gehaltene Zusicherungen der NSA auf bilateraler Ebene, dass ihre Programme mit europäischen Rechtsstandards vereinbar seien, sind zu hinterfragen. Auch vor dem US-Kongress leugnete der Director of National Intelligence (DNI), James Clapper, zunächst, dass die NSA Daten von Millionen Amerikanern sammelt. Später musste er sich korrigieren. Ein Informationsblatt der NSA zu ihren Programmen wurde ebenfalls auf Druck von Senatoren wegen falscher Angaben zurückgezogen. Ähnlich könnte es auch den Zusagen an die EU-Staaten ergehen. In der Gesamtschau erscheint der transatlantische Dialog bestenfalls wie ein symbolischer Akt, mit dem die US-Administration den unter innenpolitischem Handlungsdruck stehenden europäischen Partnern entgegenkommt.

Reaktionen aus den EU-Institutionen

Zu den markantesten Kritikern der amerikanischen Nachrichtendienste gehörte in den letzten Wochen EU-Kommissarin Viviane Reding. Sie plädierte dafür, Sicherheitsbehörden von Drittstaaten strengere Vorgaben für den Zugriff auf europäische Daten zu machen, und kündigte an, die »Safe-Harbour«-Vereinbarung zwischen der EU und den USA bis Ende des Jahres zu überprüfen. Die Vereinbarung soll sicherstellen, dass Unternehmen mit Sitz in den USA bei der Übermittlung von personenbezogenen Daten europäischer Bürger an die USA ein angemessenes Datenschutzniveau wahren. Auch stellte sie zum Unmut der meisten Mitgliedstaaten und Kommissionskollegen die TTIP-Verhandlungen in Frage. Dabei ebneten Redings deutliche Worte zu Beginn der NSA-Affäre den Weg für die transatlantischen Gespräche. Sobald es aber konkreter wurde, verwiesen die Mitgliedstaaten die Kommissarin in ihre Schranken. Die Kommission spielt im letztlich vereinbarten transatlantischen Dialog nur eine begrenzte Rolle.

Redings entschlossenes Auftreten gegenüber den USA ist auch als Resultat des zunehmenden Drucks zu verstehen, den das EP auf die Kommissarin ausübt. Angesichts

widersprüchlicher einzelstaatlicher Interessen und einer von den Mitgliedstaaten ausgebremsten Kommissarin ist das EP noch am ehesten in der Lage, Öffentlichkeit zu schaffen und Druck aufzubauen, um eine – zumindest ansatzweise – Aufklärung der Überwachungsprogramme sowie einen verbesserten Datenschutz zu erwirken.

In einer Resolution vom 4. Juli 2013 fordert das Parlament eine umfassende Aufklärung über die US-Programme und das Ausspionieren europäischer Institutionen. Der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE) soll bis Ende des Jahres Experten anhören, Fakten zusammentragen und dem Europäischen Parlament Handlungsoptionen aufzeigen. Abgesehen von der NSA will sich der Ausschuss auch mit den Aktivitäten der mitgliedstaatlichen Nachrichtendienste befassen, unter anderem der britischen, schwedischen und deutschen Behörden, und deren Kooperation mit den USA beleuchten. Um Druck auf die USA aufzubauen, geht das EP deutlich weiter als die Regierungen der Mitgliedstaaten, indem es die beiden zentralen EU-US-Abkommen zur Terrorismusbekämpfung, das Fluggastdatenabkommen und das SWIFT-Abkommen, zur Disposition stellt.

Für die USA und die Mitgliedstaaten ist das EP in der Innen- und Justizpolitik ein schwer zu kalkulierender Akteur. Die christdemokratisch-konservative Mehrheit unterstützt zwar in der Regel eine weitreichende Datenüberwachung zum Zwecke der Terrorismus- und Kriminalitätsbekämpfung. Dennoch gelingt es einer bürgerrechtsliberalen Minderheit immer wieder, Koalitionen zur Begrenzung dieser Überwachung zu schmieden. So hat jüngst beispielsweise der zuständige LIBE-Ausschuss eine EU-Regelung zur Fluggastdatenüberwachung abgelehnt. Die Resolution zu den NSA-Aktivitäten wurde von den vier größten Fraktionen unterstützt und mit einer breiten Mehrheit verabschiedet. Agiert das EP halbwegs geschlossen, dürfte es in den kommenden Wochen den politischen Druck auf die Mitgliedstaaten und die Kommission aufrechterhalten können und sie zum Handeln bewegen. Seine mittlerweile umfassenden Mitentscheidungsrechte in der EU-Justiz- und -Innenpolitik bieten hierfür einen effektiven Hebel.

Reaktion entlang von drei Konfliktlinien

Beim Umgang mit der Überwachung sieht sich Europa drei miteinander verbundenen Konfliktlinien gegenüber. Die erste Konfliktlinie verläuft quer durch jeden Staat auf beiden Seiten des Atlantiks und durch die EU-Institutionen: Sicherheitsbehörden und Datenschützer haben unterschiedliche Auffassungen darüber, welche Mittel im Kampf gegen Terrorismus und Kriminalität nötig und zulässig sind. Der 11. September 2001 hat in den USA wie in der EU und ihren Mitgliedstaaten als Katalysator für eine Verschärfung der Sicherheitsgesetzgebung gewirkt. Die Neigung, von Terrorismus und Kriminalität ausgehenden Bedrohungen vorzugsweise mit technologischen Mitteln und umfassender Datenüberwachung zu begegnen, ist auf beiden Seiten des Atlantiks ein typisches politisch-administratives Reaktionsmuster.

Die zweite Konfliktlinie verläuft zwischen den einzelnen Mitgliedstaaten der EU, die sich jeweils in einer besonderen Beziehung zu den USA wähnen. Unter Nachrichtendiensten gilt das Prinzip, dass nur der Informationen erhält, der auch welche anzubieten hat. In der Konkurrenz der europäischen Nachrichtendienste um die Anerkennung der USA kommt es daher immer wieder zu Situationen, in denen die Gefahr besteht, dass europäische Grundrechtestandards auf der Strecke bleiben. Das britische Tempora-Programm ist nur das offenkundigste Beispiel.

Der Gegensatz zwischen Europa und den USA, auf den sich ein Großteil der Berichterstattung über die NSA-Affäre konzentriert hat, ist schließlich die dritte Konfliktlinie. Ein wesentlicher Aspekt ist dabei die gravierende Machtasymmetrie, die sich in der unterschiedlichen Ausstattung der Nach-

richtendienste ebenso ausdrückt wie darin, dass die USA ungeachtet aller Kooperation offenbar die EU und ihre Mitgliedstaaten ausspionieren. Ein anderer Aspekt ist die Tatsache, dass die USA den amerikanischen Sicherheitsgesetzen Vorrang vor europäischen Regelungen zum Schutz der Privatsphäre einräumen.

In jedem einzelnen dieser drei Konfliktfelder müssen die Mitgliedstaaten ihr Verhalten überprüfen, wenn sie der NSA-Praxis wirksam entgegentreten wollen. Grundsätzliches Ziel politischen Handels muss es hierbei sein, den Zugriff von Behörden aus Drittstaaten auf Daten von EU-Bürgern besser zu regulieren und die Einhaltung europäischer Grundrechtestandards zu gewährleisten. Die zentralen Ansatzpunkte hierfür sind hinreichend und seit langem bekannt, haben aber insbesondere seitens der EU-Mitgliedstaaten bei weitem nicht genug Unterstützung gefunden. Erstens geht es um die derzeit in Brüssel verhandelte EU-Datenschutz-Grundverordnung, zweitens um die dringend nötige Überprüfung der bereits erwähnten »Safe-Harbour«-Vereinbarung zwischen den EU und den USA, drittens um die lange Zeit von den USA blockierten Verhandlungen über ein transatlantisches Rahmenabkommen, das allgemeine Schutzbestimmungen für den Austausch personenbezogener Daten im Sicherheitsbereich festlegen soll. Die gegenwärtige Situation bietet allen Akteuren eine zweite Chance, die Verhandlungen der genannten Dossiers voranzutreiben. Die verschiedenen Vorschläge für eine Reform internationaler Datenschutzregelungen, etwa im Rahmen der Vereinten Nationen, sind ebenfalls zu begrüßen. Dass sie umgesetzt werden, ist mittelfristig jedoch kaum zu erwarten, nicht zuletzt weil sich Staaten wie die USA dagegen sperren würden. Die EU-Mitgliedstaaten sollten ihren Fokus daher auf die europäische Datenschutzreform und die transatlantischen Vereinbarungen legen.

Forderungen an die USA, europäische Schutzstandards zu gewährleisten, lassen sich jedoch nur dann glaubhaft stellen, wenn auch die eigenen Sicherheitsbehörden gesetzliche Standards strikt beachten. Dabei geht es nicht nur darum, die Gesetze der Form nach einzuhalten, sondern auch darum, ihrem Geist zu entsprechen. Mit dieser Vorgabe nicht vereinbar sind Arrangements, bei denen Nachrichtendienste zwar die Gesetze zum Schutz der eigenen Bevölkerung beachten, diese jedoch de facto wieder aushebeln, indem sie umfassend Informationen mit anderen Diensten austauschen (die in ihrer Auslandsaufklärung nicht an diese Gesetze gebunden sind). Die EU-Mitgliedstaaten riskieren ihre Glaubwürdigkeit nicht nur in den Beziehungen zu anderen Staaten, wenn sie jegliche Debatte über die Aktivitäten und Kontrolle ihrer Nachrichtendienste und deren Kooperation mit den USA abwiegeln. In der europäischen Öffentlichkeit haben die Berichte über die Arbeit der britischen, französischen, deutschen und anderer Dienste jedenfalls für Verunsicherung gesorgt. Die aktuelle Situation gibt Anlass, EU-weit eine offene, grundsätzliche Debatte über Kompetenzen und Kontrolle der Nachrichtendienste zu führen.

Schließlich ist zu begrüßen, dass einige Mitgliedstaaten die USA nun dazu drängen, auch die Spionagevorwürfe aufzuklären. Bilaterale Zusagen der USA, auf Spionage zu verzichten, reichen jedoch nicht aus. Denn solche Garantien müssen für die gesamte EU und die EU-Institutionen gelten. Im Übrigen können zusätzliche Abkommen nicht darüber hinwegtäuschen, dass die Aushorchung der Vertretungen von EU und Mitgliedstaaten bereits gegen das Wiener Übereinkommen über diplomatische Beziehungen verstößt.

Für den Umgang mit Spionage gilt ebenso wie für die Datenüberwachung: Bilateralismus und einzelstaatliche Aktionen sind nicht zielführend. Nur durch ein koordiniertes Vorgehen in der EU lässt sich erreichen, dass Klarheit über das Ausmaß der Überwachung geschaffen und der Schutz der Privatsphäre von EU-Bürgern gewährleistet wird.

Übersicht über bisher bekannte Überwachungstätigkeiten

Telefondaten: betrifft Verbindungsdaten von Telefongesprächen in den USA und zwischen USA und Ausland.
▸ *Rechtliche Grundlage:* laut Director of National Intelligence (DNI) eine Klausel im Patriot Act (Sektion 215). Sie ermächtigt das FISA-Gericht dazu, anzuordnen, dass Telefonanbieter Daten herausgeben. Erneuerung der Anordnung alle drei Monate.
▸ *Problematik:* umstritten, ob die gängige Praxis, die Übergabe von Verbindungsdaten routinemäßig und unabhängig von spezifischen Straftatermittlungen anzuordnen, vom Gesetz gedeckt ist. Verdachtsunabhängige Speicherung von Daten auf unbestimmte Zeit. Verbindungsdaten sind nach bisheriger US-Rechtsprechung nicht automatisch vom verfassungsmäßigen Recht auf Privatsphäre in der Kommunikation geschützt. Dabei bieten sie die Möglichkeit, persönliche Kontakte und Netzwerke, Aufenthaltsorte und Verhaltensmuster nachzuvollziehen.

Prism: Name einer Datenbank für Informationen, die Anbieter von Email-, Chat- und Cloud-Diensten, Suchmaschinen und sozialen Netzwerken, zum Beispiel Google, übermitteln.
▸ *Rechtliche Grundlage:* Abschnitt 702 des FISA Amendment Act von 2008 zur Regelung von Verfahren für die Auslandsüberwachung. Verfahren wird jährlich vom FISA-Gericht genehmigt, einzelne Anfragen kann der DNI und der Justizminister ohne besonderen Gerichtsbeschluss veranlassen. Laut Gesetz dürfen die Daten nur ausgewertet werden, wenn die Zielperson nicht aus den USA stammt oder sich in den USA aufhält.
▸ *Problematik:* Da es im Internet keine Grenzen gibt, ist die Unterscheidung zwischen In- und Ausland schwierig. Keine gesicherten Informationen über Art und Menge der übermittelten Daten. Potentiell besteht Einblick in die sensibelsten Bereiche des Internetverhaltens.

Tempora: Operation des Government Communications Headquarters (GCHQ), bei der in Abstimmung mit der NSA die über Glasfaserverbindungen zwischen Großbritannien und dem Ausland ausgetauschten Daten abgeschöpft, zwischengespeichert und gescannt werden. Durchführung mit Hilfe von sieben Telekommunikationsunternehmen, die die grundlegende Infrastruktur für das Internet betreiben, darunter Glasfaserleitungen zwischen Deutschland und Großbritannien sowie Server in Deutschland.
▸ *Rechtliche Grundlage:* unbekannt, laut britischer Regierung hält das GCHQ geltende Gesetze ein.
▸ *Problematik:* betrifft einen Großteil des europäischen Datenverkehrs. Anders als bei den oben erwähnten Programmen keine Einschränkung oder Kontrolle bekannt. Laut *Guardian* kann die Gesamtheit der Daten bis zu drei Tage gespeichert werden, eine Auswahl oder Verbindungsdaten auch länger.

X-Keyscore: Software zur Vernetzung, Filterung und Durchsuchung von Daten aus verschiedenen Quellen. Recherchieren zahlreicher Schlüsselinformationen wie Email- oder IP-Adressen, Schlagworte, bestimmte Sprachen und Ähnliches ist möglich. Die Datenbank wird aus rund 150 Standorten weltweit gespeist, die regional den Internetverkehr ganz oder teilweise abschöpfen, darunter wahrscheinlich auch die Daten von Tempora. Internetverkehr kann in Echtzeit verfolgt werden. Daten werden zwischen einem und fünf Tagen vollständig gespeichert, ausgewählte Daten auch bis zu fünf Jahre (laut *Guardian*).
▸ *Rechtliche Grundlage:* unbekannt.
▸ *Problematik:* Surfverhalten und internetbasierte Kommunikation eines Nutzers sind ebenso mitvollziehbar wie Aktivitäten in verschlüsselten Virtual Private Networks.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364