Humanistische Union

Editorial

aus: vorgänge Nr. 206/207 (Heft 2-3/2014), S. 1-6

Am 6. Juni 2013 veröffentlichte die britische Zeitung The Guardian erstmals vertrauliche Informationen über ein US-amerikanisches Überwachungsprogramm, mit dem die Verbindungsdaten aller Telefonate gespeichert werden, die innerhalb, von und mit den Vereinigten Staaten geführt werden. Die Zeitung berief sich dabei auf eine ihr vorliegende Überwachungsanordnung, nach der die Firma Verizon (einer der größten Telefonanbieter der USA) diese Daten täglich an den Geheimdienst National Security Agency (NSA) zu übermitteln habe. Wenige Tage später veröffentlichten der Guardian und die Washington Post Informationen über einen direkten Zugang der NSA auf die Kundenserver großer amerikanischer Internetanbieter (Programm PRISM). Die NSA kann demnach auf die Kontaktdaten, Dokumente, E-Mails und Fotos aller Kunden dieser Anbieter zugreifen. Betroffen sind u.a. die Firmen Apple, Facebook, Google, Microsoft und Skype.

Mit diesen Veröffentlichungen begann das, was in den Medien mittlerweile als NSA-Überwachungsskandal bezeichnet wird. Schnell wurde bekannt, dass die Informationen aus der selben Quelle stammen, einer Sammlung geheimer Unterlagen der NSA, die Edward Snowden einigen Journalisten zugespielt hatte. Seitdem reißen die Enthüllungen aus den „Snowden-Dokumenten“ kaum noch ab. Nahezu wöchentlich werden neue Details veröffentlicht(1), die verdeutlichen, wie umfassend, flächendeckend und perfide die geheimdienstliche Überwachungspraxis der NSA und ihrer Partnerdienste ist. Sie greifen die weltweiten Kommunikationsdaten auf den transatlantischen Glasfaserkabeln ab, lassen ganze Länder flächendeckend abhören und speichern die Inhalte aller dort stattfindenden Telefonate; sie kompromittieren technische Sicherheitsstandards beim Mobilfunk und der Verschlüsselung von Daten; sie fangen von Kunden bestellte IT-Geräte auf dem Versandweg ab und manipulieren diese ... Es besteht kein Zweifel, dass der NSA-Skandal die Maßstäbe dafür, in welchem Umfang staatliche Überwachungsaktivitäten heute denkbar und möglich sind und praktiziert werden, weit verschoben hat.

Die NSA-Überwachungsaffäre bildet den Ausgangspunkt für diese Ausgabe der vorgänge. Alle Beiträge des Schwerpunkts beziehen sich mehr oder weniger intensiv auf die damit verbundenen Erkenntnisse. Dennoch ist dies kein Schwerpunkt zur Überwachung durch die NSA, zeigen wir nicht mit dem Finger auf Amerika. Wir richten den Blick vielmehr auf die Arbeit der deutschen Geheimdienste, allen voran den BND. Warum das? Zum einen arbeitete und arbeitet die NSA mit zahlreichen europäischen Geheimdiensten – allen voran natürlich dem britischen Government Communications Headquarter (GCHQ), aber auch dem Bundesnachrichtendienst (BND) – eng zusammen. Darüber hinaus sehen wir auch bei den hiesigen Geheimdiensten, besonders im Bereich der Telekommunikation (TK), eine Tendenz zur grenzenlosen Überwachung, erhebliche Rechtslücken und unzureichende Kontrollmechanismen. Bevor sich Deutschland auf internationaler Ebene glaubhaft für eine menschen- und grundrechtsorientierte Beschränkung der Überwachungsaktivitäten einsetzen kann, sind aus unserer Sicht noch zahlreiche Hausaufgaben zu erledigen. Diese zu benennen, ist Anliegen und Anspruch des aktuellen **vor***gänge*-Schwerpunkts.

Nachdem die zahlreichen NSA-Überwachungsprogramme bekannt wurden, stellen sich viele Menschen hierzulande Fragen: Inwiefern sind wir von diesen Überwachungen betroffen? Waren oder sind deutsche Behörden an diesen Praktiken beteiligt? Was wusste die Bundesregierung über diese Vorgänge, und was unternimmt sie für einen effektiven Schutz unserer Daten? Zur Klärung dieser Fragen hat der Deutsche Bundestag einen Parlamentarischen Untersuchungsausschuss eingesetzt, der im April 2014 seine Arbeit aufnahm. Der Ausschuss führte zu Beginn seiner Tätigkeit eine Reihe von Sachverständigenanhörungen durch, um die Abgeordneten mit den technischen, rechtlichen und praktischen Aspekten der

Geheimdienstarbeit vertraut zu machen. ***Sven Lüders*** fasst die Stellungnahmen von drei zentralen Rechtsgutachten zusammen, in denen die bestehenden rechtlichen Schranken dargestellt werden, die Geheimdienste hierzulande bei der TK-Überwachung einhalten sollen. Darüber hinaus geben die Stellungnahmen einen guten Überblick über widersprüchliche oder zu weit gefasste Überwachungsbefugnisse, über bestehende Regelungslücken sowie die staatlichen Möglichkeiten und Verpflichtungen, gegen die ausufernden Überwachungsaktivitäten vorzugehen.

Die rechtspolitische Auseinandersetzung um geheimdienstliche Überwachungspraktiken ist immer auch eine Auseinandersetzung um Begriffe und Wertungen: sind es Geheimdienste oder Nachrichtendienste; werden unsere Gespräche überwacht oder Beschränkungsmaßnahmen durchgeführt? Das gilt auch für die Abhörpraktiken des BND. Bei dessen „strategischer Fernmeldeaufklärung“ werden jährlich Millionen von E-Mails, Telefonaten, Faxen etc. aus dem grenzüberschreitenden Verkehr nach bestimmten Begriffen durchsucht, die Treffer anschließend weiter verarbeitet. Ist das maschinelle Durchsuchen solcher Nachrichten bereits eine Form der Überwachung, oder handelt es sich dabei nur um einen harmlosen Filtervorgang? Reicht die Kontrolle dieser großflächigen Überwachungsmaßnahmen durch das G 10-Gremium, oder bedarf es weitergehender Rechtsschutzmöglichkeiten? Über diese Fragen diskutieren ***Kurt Graulich*** und ***Martin Kutscha*** im Streitgespräch zur Überwachungspraxis des BND. Ihr Gespräch fand im Rahmen des dritten Gustav-Heinemann-Forums im Juni 2014 in Rastatt statt, von dem auch zwei weitere Beiträge dieser Ausgabe stammen.

Die NSA-Affäre führt uns eine gravierende Diskrepanz vor Augen: Während viele Nachrichten heute durch weltweite Datennetze geschickt werden und die Überwachungstechniken sich den globalen Kommunikationsstrukturen längst angepasst haben, existieren verbindliche und durchsetzungsfähige rechtliche Regelungen für die Eingrenzung und Kontrolle dieser Aktivitäten nach wie vor nur auf nationaler Ebene. Das in den Verträgen verbürgte Menschenrecht auf Privatheit entfaltet kaum eine Wirksamkeit, es gibt (jenseits der EU) weder internationale Konventionen noch Zusatzprotokolle zum Datenschutz. Wohl gerade deshalb hat die NSA-Affäre eine Diskussion um verbindliche internationale Regeln für den Datenschutz angestoßen.(2) ***Eric Töpfer*** zeigt in seinem Beitrag, dass sich die Vereinten Nationen bereits im Vorfeld der Snowden-Enthüllungen verstärkt mit Fragen der Überwachung beschäftigten. Zwei Berichte von Sonderberichterstattern (Scheinin 2009 / La Rue 2013) wiesen bereits auf zahlreiche Missstände sowie den völkerrechtlichen Handlungsbedarf hin – fanden aber kaum die nötige Aufmerksamkeit. Neuen Aufschwung erhielt die Debatte in den UN durch die gemeinsam von Brasilien und Deutschland eingebrachte Resolution zum „Recht auf Privatheit im digitalen Zeitalter“, die die Generalversammlung am 18. Dezember 2013 verabschiedete. Mit dem Beschluss erging auch ein Auftrag an die UN-Menschenrechtskommissarin, einen Bericht über das Thema vorzulegen. Töpfer stellt die wesentlichen Ergebnisse des Berichts von Navi Pillay vom 16. Juli 2014 vor, der auch für die Überwachungspraxis deutscher Geheimdienste manche Empfehlung parat hält.

Wer sich in Deutschland über die Überwachungsaktivitäten der NSA beschwert, sollte vorher die „Fernmeldeaufklärung“ des BND zur Kenntnis nehmen. Zwar unterscheiden sich die beiden Dienste in ihrer personellen wie finanziellen Ausstattung um Größenordnungen, beim Abhören von Gesprächen finden sich dagegen viele Gemeinsamkeiten. So ist dem BND die gezielte Überwachung deutscher Staatsbürger_innen nur bei konkreten Verdachtsmomenten erlaubt, aber schon die grenzüberschreitende Kommunikation wird ohne konkreten Verdacht und großflächig überwacht. ***Bertold Huber*** stellt in seinem Beitrag die verschiedenen zulässigen Formen der TK-Überwachung durch den BND dar. Huber, der selbst stellvertretender Vorsitzender der G 10-Kommission ist, die solche Überwachungsanordnungen zu genehmigen und zu kontrollieren hat, schildert seine Erfahrungen mit den Verfahrensabläufen und Kontrollmöglichkeiten. Sein erschreckender Befund: Der BND betreibt eine weitere Form der Überwachung, nämlich im Ausland – im ganz großen Stil und vorbei an allen gesetzlichen Vorgaben und Kontrollmechanismen. Das macht deutlich, wie groß der rechtspolitische Handlungsbedarf hierzulande ist.

Mit dem rechtspolitischen Handlungsbedarf beschäftigen sich gleich drei Autoren unserer Ausgabe, wenn auch mit unterschiedlichen Akzenten: ***Dieter Deiseroth*** konzentriert sich auf die Zusammenarbeit der

deutschen Geheimdienste mit den Diensten der ehemaligen alliierten Mächte in Deutschland. Es gilt zwar der Grundsatz, dass in deutschen Gesetzen keine Befugnisse zur TK-Überwachung für ausländische Geheimdienste eingeräumt werden. Allerdings wird den hier stationierten Streitkräften der USA nach dem Aufenthaltsvertrag und einem Zusatzabkommen zum NATO-Truppenstatut das Recht eingeräumt, innerhalb der ihnen überlassenen Liegenschaften Überwachungsmaßnahmen für ihre Sicherheitszwecke auszuführen, bei denen amerikanisches (und nicht deutsches) Recht anwendbar ist. Aus Veröffentlichungen von Edward Snowden und Josef Foschepoth(3) gibt es Hinweise darauf, dass weitere zwischenstaatliche Vereinbarungen über – bisher nicht öffentliche – Rechtsgrundlagen für Überwachungsbefugnisse ausländischer Streitkräfte und ihres Geheimdienstpersonals in Deutschland bestehen. All diese Vereinbarungen sind nicht nur intransparent, sondern mittlerweile von der Geschichte überholt. Deiseroth formuliert deshalb neun Thesen zum rechtspolitischen Handlungsbedarf. Sie reichen von Klarstellungen in Artikel 10 Grundgesetz (GG) sowie dem Ausführungsgesetz, der Offenlegung aller bestehenden völkerrechtlichen Verpflichtungen zum Gewährenlassen ausländischer Dienste, einer Stärkung der parlamentarischen Kontrollrechte bis zur Reform von Aufenthaltsvertrag, NATO-Truppenstatut und Deutschlandvertrag.

Alexander Dix beschreibt, mit welchen Mitteln die Bundesregierung gegenüber den amerikanischen Verhandlungspartnern für mehr Datenschutz sorgen kann. Er verweist dazu auf die bestehenden Datenschutzvereinbarungen zwischen der EU und den USA, allen voran die Safe Harbor-Vereinbarung, auf deren Grundlage deutsche und europäische Unternehmen ihre Daten in die USA übertragen und dort verarbeiten dürfen. Die Vertragsgrundlage dieser Vereinbarung könnte nach den bisherigen Erkenntnissen der NSA-Affäre obsolet sein, eine Neuaushandlung des Abkommens ist deshalb zwingend erforderlich. Daneben sei die Einhaltung datenschutzrechtlicher Mindeststandards auch bei den derzeitigen Verhandlungen über das internationale Abkommen zum Handel mit Dienstleistungen (TISA) sowie das transatlantische Freihandelsabkommen (TTIP) zu beachten. Neben der Verabschiedung der längst überfälligen europäischen Datenschutzstandards (EU-Grundverordnung) und dem Schließen nationaler Kontrolllücken fordert Dix auch, dass sich der Staat stärker um die Entwicklung sicherer Kommunikationstechnik bemüht. Dazu sollte die Entwicklung anwenderfreundlicher Lösungen für Datenverschlüsselung sowie dezentrale Netzstrukturen staatlich gefördert werden. Zugleich sollte das Inverkehrbringen von Hard- oder Software mit geheimen Hintertüren unter Strafe gestellt werden. Nur so könne man den einfachen Anwender_innen eine vertrauliche Telekommunikation gewährleisten.

Auf die technikpolitischen Optionen der Bundesregierung geht ***Peter Schaar*** ausführlicher ein. In seinem Beitrag befasst er sich mit einer zentralen Voraussetzung für sichere Verschlüsselungstechniken: Deren Algorithmen und Verfahren müssen öffentlich dokumentiert sein, andernfalls beruhe die Sicherheit dieser Techniken auf purem Vertrauen in die jeweiligen Anbieter und deren Arbeit. Da fehlerfreie Software bisher noch nicht erfunden wurde und es in jeder Organisation Insider geben kann, die vorhandene Schwachstellen oder Fehler missbräuchlich ausnutzen, ist die Offenlegung von Quellcodes der beste Weg, um unbemerkte Fehler oder wissentlich eingebaute „Hintertüren“ in Programmen ausfindig zu machen. In der Sicherheitstechnik sollten daher Open-Source-Produkte bevorzugt gefördert werden. Mit ihnen lassen sich jene Hintertüren in unseren Computern schließen, die Kriminelle wie Geheimdienste für ihre digitalen Einbrüche nutzen. Schaar spricht sich dafür aus, eine starke IT-Sicherheit zum Markenkern europäischer Marktanbieter_innen zu machen. Sichere Webanwendungen, starke Kryptografieverfahren oder ein europäisches Routingnetz (das Nachrichten an den amerikanischen Überwachungsstationen vorbei lotst) könnten für die hiesigen Firmen zum Wettbewerbsvorteil werden.

Was Peter Schaar am Beispiel der Kryptografie diskutiert, behandelt ***Linus Neumann*** auf einer allgemeineren Ebene: Er erläutert zunächst, wie die verschiedenen Sicherheitslücken in Computerprogrammen entstehen, um davon ausgehend zu formulieren, mit welchen Mitteln sich eine sichere, alltagstaugliche Technik bereitstellen ließe. Dazu wäre es notwendig, dass der Staat weiterführende Maßnahmen gegen den florierenden (Schwarz-)Markt mit Softwarefehlern unternimmt, anstatt sich durch seine Geheimdienste (die solche Fehler gern aufkaufen) selbst daran zu beteiligen. Neumann fordert deshalb eine offene Sicherheitskultur, in der technische Verfahren und Instrumente genauso transparent zu machen sind wie die juristischen und Verwaltungsabläufe. Zudem sei eine von den Geheimdiensten und

Innenministerien unabhängige Sicherheitspolitik nötig, um das 2008 vom Verfassungsgericht formulierte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme endlich zu verwirklichen.

Dietrich Meyer-Ebrecht wagt sich abschließend daran, die verschiedenen politischen, rechtlichen, technischen und gesellschaftlichen Handlungsoptionen gegeneinander abzuwägen. Sein Beitrag stellt ein – wenn auch recht pessimistisches – Resümee aller vorangehenden Bemühungen dar. Die bittere Botschaft des Ingenieurs: die Technik allein kann das Problem nicht lösen. Ebenso unwillig zeigt sich derzeit (noch) die Politik, den Geheimdiensten oder der Wirtschaft engere Grenzen für den Umgang mit unseren Daten aufzuerlegen. Gesellschaftlich haben wir uns weitgehend damit abgefunden, dass wir für all die schicken Gadgets und die nützlichen Apps unsere Daten preisgeben. Solange sich dagegen kein ausreichender politischer Wille aus der Mitte der Gesellschaft formiert, wird uns auch kein Gesetzgeber vor den Gefahren der modernen Kommunikationstechnik bewahren können. Den Ausweg sieht Meyer-Ebrecht nicht im Verzicht, sondern darin, dass wir selbst tätig werden – nicht nur politisch, sondern auch indem wir mithelfen, eine daten- und sicherheitsbewusste Anwender_ innenschaft zu etablieren. Denn nur eine starke Nachfrage nach datenschutzkonformer Technik könne Wirtschaft und Politik dazu bewegen, selbst entsprechende Änderungen einzuleiten.

Die Sammelrezension einiger Neuerscheinungen zum Thema NSA-Affäre beschließt den Schwerpunkt.

–

Die geheimdienstlichen Befugnisse beschäftigen uns auch jenseits des aktuellen Schwerpunktthemas. ***Michael Plöse*** analysiert die zum 1. Januar 2015 erfolgte Reform der Antiterrordatei – jenes Werkzeugs zur Anbahnung von Datentransfers zwischen den beteiligten Polizei- und Geheimdienstbehörden. Die Reform geht auf eine Entscheidung des Bundesverfassungsgerichts vom 24. April 2013 zurück, die aus bürgerrechtlicher Perspektive in mancher Hinsicht hinter den Erwartungen zurückblieb. Dennoch enthält sie zahlreiche Vorgaben zu notwendigen Einschränkungen bei den geheimdienstlichen Datenübermittlungsvorschriften. Ob der Gesetzgeber diese Ansagen bei seiner Reform hinreichend beachtet hat, wird Plöse in einem 2. Teil seiner Besprechung (im nächsten Heft) erläutern.

Welche Auswirkungen Sicherheitsgesetze und -maßnahmen wie die Antiterrordatei haben, sollte in Evaluationsverfahren ermittelt werden. In der Sicherheitsgesetzgebung setzen sich derartige Untersuchungen langsam aber stetig durch. ***Heinrich Amadeus Wolff***, der selbst mehrere Gesetze begutachtet hat, spricht im Interview über seine Erfolge und Misserfolge bei dem Versuch einer Beratung des Gesetzgebers.

Die Beiträge von ***Axel Bußmer*** und ***Michael Kuhn*** stellen Ergebnisse eines von der Europäischen Kommission geförderten Projektes zu staatlichen Datensammlungen in der EU dar, an dem sich die Humanistische Union in den vergangenen beiden Jahren beteiligt hat. Während Bußmer die Ergebnisse des länderübergreifenden Vergleichs zur Speicherpraxis in den untersuchten Ländern referiert, wagt sich Kuhn an den Vorschlag eines Datenschutzindexes, mit dem staatliche Datenbanken vergleichend bewertet werden können. Die Anwendung dieses Indexes führt er sogleich an der Antiterrordatei vor.

Obwohl die **vor***gänge* ihre Kompetenz eindeutig bei den innenpolitischen Themen sehen, wollte sich die Redaktion dem Konflikt in der Ukraine nicht verschließen. Die politischen Reaktionen in Ost und West sowie die damit verbundene militärische Eskalation zeigen, wie instabil die europäische Friedensordnung ist. Umso wichtiger erscheint uns die Suche nach geeigneten alternativen Strategien zur Eindämmung des Konflikts. Einen Beitrag dazu könnte das Dossier von Andreas Buro, Karl Grobe und Clemens Ronnefeldt leisten. Sie haben im Auftrag der Kooperation für den Frieden die Entstehung des Konflikts untersucht und nach geeigneten Möglichkeiten einer zivilen Lösung Ausschau gehalten. Eine gekürzte Fassung ihres

Berichts drucken wir als Hintergrund ab.

Weitere Stellungnahmen zu einem aktuellen Gesetzgebungsverfahren sowie die Besprechung eines jüngst ergangenen Urteils des Europäischen Gerichtshofes zum „Recht auf Vergessen“ im Internet und eine Besprechung des aktuellen Films über den Auschwitz-Prozess schließen diese Ausgabe der **vor***gänge* ab. Die gesamte Redaktion wünscht Ihnen wie immer eine anregende Lektüre mit der neuen Ausgabe und freut sich über Ihre Anmerkungen, Kommentare und Kritiken.

Claudia Krieg und Sven Lüders
für die Redaktion

VORSCHAU

vor*gänge* 208 Europäische Abschottungstendenz nach Innen und Außen

vor*gänge* 209 Gesetzgebung zum Verbot der Suizidbeihilfe

Anmerkungen:

(1) Übersichten zu den bisherigen Enthüllungen finden sich beispielsweise bei Wikipedia (Stichwort: „Globale Überwachungs- und Spionageaffäre“), bei Zeit-Online (http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal) oder beim Onlinemagazin Heise (http://www.heise.de/ extras/timeline-2013/#vars!date=2013-06-06_10:12:00!). Die American Civil Liberties Union (ACLU) macht die Originaldokumente aus dem NSA-Fundus online zugänglich: https://www.aclu.org/nsa-documents-search.

(2) Vgl. dazu auch den zivilgesellschaftlichen Forderungskatalog: „Internationale Grundsätze für die Anwendung der Menschenrechte in der Kommunikationsüberwachung“ in vorgänge Nr. 203 (3-2013), S. 121 ff.

(3) Josef Foschepoth, Überwachtes Deutschland – Post- und Telefonüberwachung in der alten Bundesrepublik. Vandenhoeck & Ruprecht, November 2012.
