Prism & Co: Sicherheit auf Kosten der Freiheit?

Das *Prism*-Programm der *National Security Agency* (NSA) der USA steht als Symbol für eine Überwachungspraxis demokratischer Rechtsstaaten, deren Ausmaß bislang nicht absehbar ist. Sie ans Tageslicht geholt zu haben, gebührt als Verdienst dem *Whistleblower* Edward Snowden. Aber was bedeutet sein Befund? Steht er für die Wiederkehr oder gar Unüberwindbarkeit des Leviathan? In der Schrift gleichen Namens wirbt Thomas Hobbes 1651 nicht nur für einen allmächtigen Staat, sondern er setzt das Sicherheitsdenken frei: Der Staat rechtfertigt sich demnach ausschließlich durch seine Fähigkeit, „die Bürger im Innern und von außen her in Sicherheit leben" zu lassen. Dazu stattet Hobbes ihn mit unbeschränkten Vollmachten aus. So attestiert er ihm das Recht, „sowohl in der Gefahr selbst wie zu ihrer Abwendung schon vorher das Nötige zu veranstalten". Da Hobbes in „Meinungen" den eigentlichen Grund für „Handlungen" wie Bürgerkrieg oder andere Formen der Uneinigkeit erblickt, verlangt er, sie „unter Aufsicht" zu nehmen, „wenn man Frieden und Einigkeit in einem Staat erhalten will". Eine derartige Auffassung scheint uns spätestens seit der Aufklärung suspekt: zu groß die Versuchung des Totalitarismus, zu einseitig die Fixierung auf den Schutz physischer Unversehrtheit, zu wenig Platz für individuelle Freiheitsrechte. Dementsprechend gründen heutige Demokratien auf Gewaltenteilung und unveräußerlichen Grundrechten. Sicherheit und Freiheit scheinen in angemessener Balance, die mit Snowdens Enthüllungen jedoch in Zweifel steht: Verbirgt sich in jedem Staat stets auch ein unkontrollierbarer Leviathan, den das Recht eigentlich hegen sollte? Und trägt dafür die dem Staat eingeschriebene Sicherheitslogik nicht einen Großteil der Verantwortung? Zu diesem Themenkomplex kommen unterschiedliche Stimmen zu Wort: Die beiden ersten Beiträge durchleuchten das Verhältnis von Sicherheit und Freiheit aus den entgegengesetzten Polen, während die beiden anderen Artikel sich mit der Sicherheitslogik auseinandersetzen: Dabei problematisiert ein Autor die ihr immanente Tendenz zur Totalisierung, wohingegen die andere Verfasserin danach fragt, ob menschliche Sicherheit als Alternativkonzept taugt, das im Bereich der Freiheitsrechte weniger Kollateralschäden produziert als das herkömmliche Sicherheitsverständnis.

Sabine Jaberg

Sicherheit vor Terrorismus braucht Aufklärung

Joachim Krause

Seit den Terroranschlägen vom 11. September 2001 und den Attentaten in Madrid 2004 bzw. London 2005 hat es keine vergleichbaren Gewaltakte in Europa oder in den USA gegeben. Vielen gilt das als Zeichen dafür, dass die Gefahr vorbei ist. Nicht zuletzt die Enthüllungen des amerikanischen „*Whistleblowers*" Edward Snowden haben deutlich werden lassen, dass diese Sicherheit Ursachen besitzt, über die sich die wenigsten Menschen Rechenschaft abzulegen bereit sind: Die Bekämpfung des internationalen Terrorismus (besonders des islamistischen) war nur deshalb erfolgreich, weil Mittel und Methoden eingesetzt wurden, die die Öffentlichkeit hierzulande kritisch bewertet. Dazu zählen der Einsatz von Drohnen in für Truppen unzugänglichen Regionen Afghanistans, Pakistans, Jemens und Somalias ebenso wie das Sammeln und Auswerten von Informationen aus Internet und Mobilfunknetzen. Letzteres steht seit Monaten im Zentrum der deutschen Debatte, die das Recht auf Privatsphäre und informationelle Selbstbestimmung betont. Außerdem herrscht Entrüstung darüber vor, dass die USA sogar in Deutschland Aufklärungsaktivitäten betreiben, wo wir doch Freunde sind. Es wird Zeit, die Problematik nicht nur unter den Gesichtspunkten der informationellen Selbstbestimmung und der Kritik an amerikanischer Spionage zu betrachten, sondern ein komplexeres Bild zu entwickeln, welches eine sorgfältige Abwägung der Vor- und Nachteile erlaubt.

Die bislang vorliegenden Erkenntnisse über die Spähaktivitäten lassen erkennen, dass die amerikanische Regierung im Zusammenwirken mit Nachrichtendiensten anderer Staaten darum bemüht ist, den gesamten Datenverkehr des Internets auf Hinweise zu scannen, die Rückschlüsse auf Strukturen, Ziele und Planungen terroristischer Gruppen erlauben. Das hat wenig gemein mit den Umtrieben der Stasi in der DDR, die versuchte, über möglichst viele Bürger der DDR ein umfassendes Profil zu gewinnen, um dann gegen sie das politische Strafrecht anzuwenden. Heute geht es um das gezielte Herausfischen einzelner Hinweise, insbesondere auf terroristische Aktivitäten.

Das praktische Hauptproblem war und ist die schiere Menge an Daten, die täglich im Internet versandt werden. Diese Datenmengen stellen ein „natürliches" Hindernis gegen den Missbrauch des Aufklärungsapparates für andere, immer wieder unterstellte Zwecke dar, wie die Überwachung ganz normaler Bürger. Im vergangenen Jahrzehnt hat sich die Datenmenge von Jahr zu Jahr oftmals verdoppelt. Gegenwärtig soll sie bei 1428 Petabyte (das sind 1428×10^{15} Byte) pro Tag liegen. Davon kann die NSA nur einen Bruchteil erfassen (etwa 1,2 Prozent) und davon auch nur einen Bruchteil wirklich zur Kenntnis nehmen (das wären dann etwa 0,0004 Prozent des gesamten Datenverkehrs). Sie benötigt dazu spezielle Software, die sowohl das Scannen nach mehreren Gesichtspunkten erlaubt als auch Daten unterschiedlicher Natur berücksichtigt (Verbindungsdaten, Inhalte von Emails und Tweets, Dateitransfers, Inhalte von Webseiten, etc.). Dazu bedarf es auch gigantischer Speichermedien, die derzeit offensichtlich im großen Maßstab hergestellt werden. Dabei ist eine Speicherung des gesamten Internetverkehrs weder beabsichtigt noch möglich, die zeitweilige Speicherung von Verbindungsdaten schon. Diese Verbindungsdaten sind häufig wichtiger als die oft verschlüsselten Inhalte von Emails. Aus ihnen lassen sich Strukturen von

Gruppen erkennen, die Anschlagsplanungen betreiben. Im Zusammenspiel mit der Überwachung des Mobilfunkverkehrs, der traditionellen Funkaufklärung und anderen Quellen können sich Hinweise auf Anschlagsplanungen ergeben – sei es in den USA, in Europa oder auch an anderen Orten, etwa in Afghanistan und Pakistan. Ausgangspunkt für diese Ausweitung und Verdichtung der Überwachungsaktivitäten waren die Empfehlungen der „9/11 Kommission". Diese war zu dem Ergebnis gekommen, dass die Anschläge vom 11. September 2001 hätten verhindert werden können, wenn Geheimdienste und FBI zusammengearbeitet und ihre Informationen rechtzeitig ausgetauscht hätten (was ihnen teilweise gesetzlich verboten war). In den USA sind in den vergangenen Jahren auf diese Weise über 80 Anschläge vereitelt worden. In Deutschland konnten sowohl die Sauerland-Gruppe als auch die Düsseldorfer Gruppe rechtzeitig aufgedeckt werden. Ohne das Ausspähen des Internets wären bei uns Anschläge geschehen, die Hunderte, wenn nicht Tausende Menschen das Leben gekostet hätten.

Die Hauptziele der Informationsbeschaffung bestehen nicht nur in der Verhinderung von Anschlägen, sondern auch in der Gewinnung von Erkenntnissen darüber, welche Terrorgruppen es gibt, wie sie operieren, welche Personen dort welche Funktionen einnehmen und auf welchen Wegen Geld, Waffen und andere Mittel beschafft werden. Dazu ist das umfassende Scannen des *World Wide Web* und des globalen Email-Verkehrs ebenso unverzichtbar wie von Mobilfunk- und Festnetzen in Ländern, die zur Vermutung Anlass geben, dass dort Terroristen oder ihre Sympathisanten agieren. Dies können Länder mit fragiler Staatlichkeit sein, aber auch hoch entwickelte, demokratische Länder. Die Anschläge vom 11. September 2001 wurden nicht nur in Afghanistan geplant und vorbereitet, sondern auch in Deutschland. Heute stehen zudem mehr und mehr Fälle von hausgemachtem Terrorismus im Vordergrund, d.h. bislang unauffällige Personen, die im Land des (geplanten) Anschlags aufgewachsen sind oder schon länger dort leben, radikalisieren sich. Durch das Internet können sie Informationen beziehen und Kontakte zu Gleichgesinnten aufnehmen. Ohne die Informationsgewinnung der US-Nachrichtendienste blieben Bemühungen zur Terrorismusbekämpfung im Rahmen der Vereinten Nationen (VN), der Europäischen Union (EU) und der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) weitgehend ineffektiv.

Ähnlich verhält es sich mit der Bekämpfung der Ausbreitung von Massenvernichtungswaffen oder der Organisierten Kriminalität. Auch hier sind das Scannen des Internets und des Mobiltelefonverkehrs sowie die Nutzung der Satellitenaufklärung zentrale Voraussetzungen dafür, dass Hinweise auf Transfers von Technik oder illegalen Geldern, aber auch auf heimliche Entwicklungsprogramme für Waffen gesammelt und ausgewertet werden können. Dass derartige Ausspähaktivitäten auch auf deutschem Boden stattfinden (ohne dass die Politik davon etwas weiß) ist nicht neu. In den 1980er Jahren wussten amerikanische Dienststellen von der Mitwirkung deutscher Firmen an Projekten zur Herstellung von Massenvernichtungswaffen in Libyen und im Irak. Deutsche Nachrichtendienste waren dazu nicht in der Lage bzw. nicht befugt, diese Informationen zu beschaffen. Die deutsche Politik ignorierte die Hinweise amerikanischer Regierungsstellen bzw. wies sie zurück. Der politische Schaden war enorm. Der Skandal um die libysche Giftgasfabrik Rabta zählte ebenso dazu wie die Aufdeckung irakischer Chemie- und Kernwaffenprogramme in den Jahren nach 1991. Ich selbst habe 1991 bei den Vereinten Nationen miterleben können, wie Listen mit den Namen jener Firmen erstellt wurden, die an irakischen Raketen-, Atomwaffen- und Chemiewaffenprogrammen mitgewirkt hatten: Etwa 80 Prozent waren in Deutschland beheimatet. Von daher sollten wir hierzulande Bescheidenheit walten lassen, wenn wir das Recht auf informationelle Selbstbestimmung verteidigen. Wir sollten uns auch kritisch fragen, ob es richtig ist, dass unsere eigenen Geheimdienste im Zeitalter transnationaler Sicherheitsprobleme nur im Ausland agieren dürfen – zumindest sollten wir uns nicht darüber beschweren, wenn andere Geheimdienste dafür in Deutschland aktiv werden. Deutschland ist für den amerikanischen Geheimdienst unter anderem deshalb interessant, weil auch mehr als 25 Jahre nach Rabta in deutschen Häfen der illegale Handel mit Komponenten von Massenvernichtungswaffen, Kleinwaffen und Rauschgift blüht.

Derzeit geht es in der sicherheitspolitischen Debatte vor allem um zwei Fragen: Ist es im Sinne der Terrorismusbekämpfung angemessen, das Internet in derart großem Umfang auszuspähen, wie es amerikanische und britische Dienste derzeit tun? Und wenn ja, wie weit ist dieses Vorgehen mit dem Schutz der individuellen Privatsphäre kompatibel, die fester Bestandteil der Rechtsordnung westlicher Demokratien ist? Die Beantwortung beider Fragen kann nicht in der ständigen Wiederholung der immer gleichen Parolen bestehen, wie dies in Deutschland gegenwärtig der Fall ist. Vielmehr muss sich die Debatte darum bemühen, einerseits Kriterien dafür zu gewinnen, was im Sinne der Prävention von terroristischen Anschlägen und der Verfolgung von terroristischen Gruppen adäquat ist. Andererseits muss sie auch klären, worin der spezifische Wert bestimmter Maßnahmen liegt, die die Privatsphäre schützen sollen und was daraus für Einschränkungen für die Ausspähaktivitäten resultieren müssen. In erster Linie ist auch verbale Abrüstung angesagt. Das betrifft vor allem die immer wieder zu vernehmende Gleichsetzung der Abhörpraktiken der NSA mit den Tätigkeiten der Staatsicherheit der DDR oder der Gestapo.

Wir sind Nettokonsument amerikanischer Dienstleistungen im Bereich Sicherheit und sollten nicht unbedingt demjenigen Verbündeten die übelsten Absichten unterstellen, der uns vor einer Reihe tödlicher Anschläge bewahrt hat. Umgekehrt sollte sich jeder, der heute die informationelle Selbstbestimmung geradezu absolut setzt, fragen, ob er oder sie auch bereit ist, dafür den eigenen Tod oder den zahlreicher anderer Menschen in Kauf zu nehmen. Der oft bemühte Vergleich mit dem freien Automobilverkehr, der jährlich auch Tausende von Toten fordert, ist falsch: Im Straßenverkehr geht es um Unfälle (d.h. die Verkettung unglücklicher Umstände), beim Terrorismus um absichtlich herbeigeführten Mord, d.h. um Verbrechen, die zu verhüten der Staat verpflichtet ist, wenn ihm die dazu erforderlichen Mittel zur Verfügung stehen.

Dr. Joachim Krause ist Professor für Politikwissenschaft an der Christian-Albrechts-Universität zu Kiel und Direktor des Instituts für Sicherheitspolitik an der Universität Kiel (ISPK).

Überwachung – der Preis für mehr Sicherheit?

Martin Kutscha

„Ohne Sicherheit vermag der Mensch weder seine Kräfte auszubilden noch die Früchte derselben zu genießen; denn ohne Sicherheit ist keine Freiheit."[1] Dieser Satz des liberalen preußischen Politikers und Gelehrten Wilhelm von Humboldt ist insbesondere von Vertretern der Innenministerien in der Vergangenheit des Öfteren zitiert worden. Plausible Beispiele für die Notwendigkeit, im Interesse höherer Sicherheit die Freiheit ein Stück weit einzuschränken, lassen sich denn auch rasch finden: Um zu verhindern, dass Bomben in Flugzeuge geschmuggelt werden, ist es unverzichtbar, die Passagiere vor dem Einsteigen gründlich zu durchsuchen.

Allerdings hat von Humboldt, und das wird manchmal unterschlagen, zugleich für eine Beschränkung des Staates auf das Notwendige plädiert: Beim Schutz der Sicherheit der Bürger müsse „allemal auf die Größe des zu besorgenden Schadens und die Wichtigkeit der durch ein Prohibitivgesetz entstehenden Freiheitseinschränkung" Rücksicht genommen werden. „Jede weitere oder aus andren Gesichtspunkten gemachte Beschränkung der Privatfreiheit aber liegt außerhalb der Grenzen der Wirksamkeit des Staats."[2] Übertragen in heutige juristische Begrifflichkeit, meint diese Aussage: Eingriffe in die Freiheitsrechte sind nur nach Maßgabe des Verhältnismäßigkeitsprinzips zulässig – sie müssen also zur Erreichung des Ziels erforderlich, geeignet und angemessen sein. Wie aber steht es damit bei der heutigen Praxis massenhafter Erfassung und Auswertung von Daten, die bei der Telekommunikation und bei der Nutzung des Internets anfallen, durch etliche in- und ausländische Sicherheitsbehörden?

Diese Überwachungspraxis, so lautet zumeist die Rechtfertigung, sei zur Terrorismusbekämpfung unverzichtbar. Nun gab es im vergangenen Jahrzehnt in der Tat zehn Opfer von Mordanschlägen einer Terrorgruppe in Deutschland, nämlich des „Nationalsozialistischen Untergrunds (NSU)". Dass die Polizei diese Mordserie nicht stoppen und die Täter nicht festnehmen konnte, lag aber keineswegs an mangelnden Erkenntnissen der Behörden über die Täter. Wie Zielfahnder der Polizei vor dem NSU-Untersuchungsausschuss berichteten, wurden neonazistische Aktivisten seinerzeit vom Thüringer Landesamt für Verfassungsschutz gedeckt und wichtige Beweismittel vernichtet.[3] Auch das im Auftrag des Innenministeriums Thüringens erstellte Gutachten dreier unabhängiger Juristen gelangte zu dem bedrückenden Ergebnis, dass die Verfassungsschutzbehörde „die Tätigkeit der Strafverfolgungsbehörden bei der Suche nach dem Trio massiv beeinträchtigt hat."[4]

Wenden wir nun den Blick in die USA: Auch die Attentäter des 11. September 2001 waren keineswegs den Behörden unbekannte „Schläfer", wie zunächst verlautbart wurde. Den US-Geheimdiensten lagen durchaus Informationen über diese Personen vor, nur wurden aus diesen Datenbeständen nicht die richtigen Schlussfolgerungen gezogen, die die Anschläge hätten verhindern können. Dies spricht für die Annahme, dass Sicherheitsbehörden in der Flut der von ihnen gesammelten Daten nicht selten regelrecht „ertrinken" und deshalb bei der rechtzeitigen Abwehr einer Gefahr versagen. Über zahlreiche Daten nahezu der gesamten Bevölkerung der Industriestaaten zu verfügen, schafft mithin keineswegs ein Mehr an Sicherheit.

Auf der anderen Seite birgt die massenhafte Nutzung moderner Kommunikationstechnik ein gewaltiges Überwachungspotenzial, neben dem sich die in Orwells Roman „1984" beschriebenen Methoden geradezu harmlos und dilettantisch ausnehmen: Um zahlreiche Details über die Lebensgestaltung und die sozialen Kontakte von Menschen zu erfahren, ist es heute nicht mehr notwendig, deren Telefongespräche abzuhören oder deren Emails zu lesen (auch wenn Strafverfolgungsbehörden dies nach wie vor tun). Dafür reicht die systematische und automatisierte Auswertung der Verbindungsdaten der Kommunikation per Telefon oder Internet – auch Verkehrsdaten oder Metadaten genannt. Anschaulich beschrieben hat dies das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010: Aus diesen Daten ließen sich „bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten (deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen), Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönliche Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden."[5]

Ohne Frage greifen solche Auswertungen tief in das durch Art. 10 Grundgesetz geschützte Fernmeldegeheimnis ein und, soweit sie die Intimsphäre des Ausgeforschten betreffen, auch in dessen durch die Menschenwürdegarantie absolut geschützten „Kernbereich privater Lebensgestaltung"[6]. Das Grundgesetz billigt dem Einzelnen eben durchaus einen Bereich zu, der den neugierigen Augen und Ohren des Staates nicht zugänglich sein soll. Wer demgegenüber meint, anständige und rechtstreue Bürger hätten vor dem Staat „nichts zu verbergen", offenbart damit ein totalitäres Staatsverständnis und seine Geringschätzung der vom Grundgesetz verbürgten Freiheitsrechte.

Aber könnte hier nicht das vom Bundesinnenminister evozierte „Supergrundrecht auf Sicherheit" als Gegengewicht zum Einsatz kommen? Zunächst: Im Text des Grundgesetzes sucht man ein solches Recht vergebens. Allerdings sprechen die Europäische Menschenrechtskonvention in Art. 5 und die Europäische Grundrechtecharta in Art. 6 von einem „Recht auf Freiheit und Sicherheit." Diese europäischen Grundrechtsverbürgungen zielen freilich auf die „Abwehr hoheitlicher Übergriffe"[7] und sollen vor willkürlichem Freiheitsentzug

1 Wilhelm von Humboldt, Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staats zu bestimmen (1792), Reclam-Ausgabe 1967, S. 58.
2 Wilhelm von Humboldt a.a.O., S. 128.
3 Vgl. „Berliner Zeitung" vom 8.8.2013.
4 Gerhard Schäfer/Volkhard Wache/Gerhard Meiborg, Gutachten zum Verhalten der Thüringer Behörden und Staatsanwaltschaften bei der Verfolgung des „Zwickauer Trios", 2012, S. 220.
5 BVerfGE 125, 260 (319).
6 Vgl. BVerfGE 109, 279 (313) – Lauschangriff.
7 Manfred Baldus, in: Sebastian F. Heselhaus/Carsten Nowak (Hrsg.), Handbuch der Europäischen Grundrechte, 2006, S. 448.

schützen. Das – von dem konservativen Staatsrechtler Josef Isensee bereits vor drei Jahrzehnten erfundene[8] – „Grundrecht auf Sicherheit" soll dagegen dem Staat als Legitimation zur Einschränkung von Freiheitsrechten dienen. Seinem Charakter nach ist es damit ein Anti-Grundrecht mit einem schier uferlosen Geltungsanspruch, weil sich hundertprozentige Sicherheit niemals erreichen lässt und wirkliche oder vermeintliche „Schutzlücken" immer irgendwo ausgemacht werden können. Definitiv beendet wäre der „Krieg gegen den Terror" erst dann, wenn Regierungsvertreter der mächtigsten Staaten vor den Fernsehkameras verkünden würden, endlich sei der letzte Terrorist weltweit hinter Schloss und Riegel gebracht und deshalb seien weitere Überwachungsmaßnahmen entbehrlich. Dass sich diese Hoffnung jemals erfüllen wird, darf angesichts der fortbestehenden politischen und sozialen Ursachen terroristischer Phänomene bezweifelt werden. So werden denn die Freiheitsrechte weiter Stück für Stück im Mahlstrom eines auf Dauer gestellten Ausnahmezustandes zerrieben. Ein Zugewinn an Sicherheit lässt sich damit allerdings nicht erreichen: Wenn niemand mehr sicher sein kann, von staatlicher Überwachung verschont zu bleiben, dann wird statt Sicherheit „Unsicherheit durch Unberechenbarkeit öffentlicher Gewalt"[9] geschaffen.

Es darf allerdings nicht übersehen werden, dass sich nicht nur staatliche Stellen im In- und Ausland als Datenkraken betätigen. Häufig bedienen sich diese Dienste aus den wohlgefüllten Töpfen weltweit aktiver Privatunternehmen, die sich ihrerseits höchst effektiv als *Big Brothers* betätigen. Unternehmen wie *Facebook* und *Google* haben inzwischen faktisch eine Monopolstellung inne und können damit den Millionen von Internetnutzern ihre Bedingungen diktieren. Die scheinbar kostenlosen Dienste werden in Wahrheit durch die Preisgabe zahlreicher persönlicher Daten der Nutzer erkauft – darauf beruht das Geschäftsmodell dieser Firmen. Der Traum grenzenloser Freiheit und Kreativität, den viele ursprünglich mit dem Internet verbanden, weicht inzwischen der bitteren Erkenntnis, dass dort „Konsum und Überwachung" dominieren, wie der weißrussische Netzpionier Evgeny Morozov beklagt.[10] Der Rat mancher Politiker, Emails doch zu verschlüsseln, verrät entweder Ahnungslosigkeit oder Zynismus. Schließlich sind in manche der Verschlüsselungsprogramme längst „Hintertürchen" für die Geheimdienste eingebaut.

Aus bürgerrechtlicher Sicht ist zunächst zu fordern, dass der Staat und seine Sicherheitsbehörden die Grundrechte respektieren und keine Massenüberwachung Unschuldiger quasi auf Vorrat betreiben. Darüber hinaus muss der Staat seiner Schutzpflicht für die Grundrechte nachkommen, indem er für die Durchsetzung strengerer Regeln für das *Data Mining* durch Privatunternehmen sorgt, und zwar über Ländergrenzen hinweg.[11] Es ist höchste Zeit für eine Globalisierung des Datenschutzes!

Dr. Martin Kutscha ist Professor für Staatsrecht an der Hochschule für Wirtschaft und Recht in Berlin und Vorstandsmitglied der Humanistischen Union.

8 Josef Isensee, Das Grundrecht auf Sicherheit, 1983.
9 Christine Hohmann-Dennhardt, in: Adolf-Arndt-Kreis (Hrsg.), Sicherheit durch Recht in Zeiten der Globalisierung, 2003, S. 109.
10 Evgeny Morozov, in: „Die Zeit" Nr. 33 v. 3.8.2013.
11 Vgl. Martin Kutscha/Sarah Thomé, Grundrechtsschutz im Internet? 2013, S. 48 ff. u. 127 ff.

Totalisierungstendenzen im Streben nach Sicherheit

Lothar Brock

Als ich zu Zeiten des Ost-West-Konflikts Austauschschüler in Pennsylvania war, nahm ich jeden Morgen in der *High School* vor dem Unterricht an einem kleinen Ritual teil. Erst wurden wir auf die Fahne der USA eingeschworen. Dann fragten wir im Chor: „What is the price we pay for liberty?" und antworteten uns dann selbst: „Eternal vigilance!" Das hat mich ziemlich irritiert. Denn „vigilance" bedeutet zweierlei: Wachsamkeit und Überwachung. Ein Staat mit wachsamen Bürgern ist eine zivilisatorische Errungenschaft; ein Überwachungsstaat ist ein zivilisatorischer Rückschritt, wie ihn die USA Anfang der 1950er Jahre unter dem McCarthyismus erlebt hatten. Natürlich bekannten wir Schüler der *High School* uns zur bürgerlichen Wachsamkeit, aber die Überwachung der Bürger im Kampf gegen den internationalen Kommunismus wurde gleich mitgedacht: Die Unterscheidung zwischen Wachsamkeit und Überwachung erwies sich als ziemlich dünn. Wie stellt sich das Verhältnis von bürgerlicher Wachsamkeit und staatlicher Überwachung im Kontext der Aktivitäten von NSA, *Prism* & Co dar?

Demokratie setzt das Engagement der Bürger voraus – ein Engagement, das die Beobachtung des Staates und seiner politischen Praxis einschließt. Aber wenn die Bürger zu wachsam werden und unerwünschtes Licht in die *arcana imperii* bringen, verfolgt man sie auch in der Demokratie als Verräter, wie dies Edward Snowden gegenwärtig widerfährt. Hier kollidiert die Wachsamkeit des Bürgers mit dem Anspruch des Staates, ein Monopol auf die Gewährleistung von Sicherheit zu haben und damit zugleich die ausschließliche Definitionsmacht darüber, welche Form von Wachsamkeit akzeptabel ist und welche als inakzeptabel zu gelten hat.

Der Staat übt diese Definitionsmacht aus, indem er die Überwachung der Bürger als Gewährleistung ihrer Freiheit ausweist und gegen jede Einrede abschirmt. So wird das ewig prekäre Verhältnis von Freiheit und Sicherheit unter Berufung auf einen Notstand immer wieder aufs Neue zugunsten der Sicherheit verschoben. Dazu tragen die Sicherheitsapparate heute im Kampf gegen den Terror (aber offenbar auch im Kampf um Marktanteile) bei, und sie tun es mit rasant wachsenden Fähigkeiten den Bürger auszuspähen. Die Geheimdienste nisten sich dabei nicht länger auf den Dachböden der Republik ein (wie früher in der DDR) oder in ramponierten VW-Bussen (wie in der alten BRD); sie agieren im Herzen der modernen gesellschaftlichen Kommunikation – im Netz. Technisch sind die staatlichen Apparate schon heute in der Lage jede Bewegung, jede Verbindung, jede Schwäche eines Menschen auszuspähen, der sich bewusst im Netz bewegt oder über das Netz mit Hilfe neuester Kommunikationstechnologie beobachtet werden kann, ohne dass er weiß, dass dies geschieht. Die so generierten Daten lassen sich dann bestimmten Verhaltensmustern zuordnen, die ihrerseits per Korrelationsanalyse mit bestimmten Sicherheitsbedrohungen in Verbindung gebracht werden.

Eine Einstufung als akutes oder potenzielles Risiko hat eine *gezielte* Beobachtung der Verdächtigten zur Folge. Das kann

bedeuten, dass man auf schwarze Listen gerät, ohne dagegen juristisch etwas unternehmen zu können. Der Bürger ist unter diesen Umständen nicht in erster Linie Träger „demokratischer Sittlichkeit" (Axel Honneth), er verkörpert vielmehr ein Risiko für das Gemeinwesen. Diese Verwandlung geht mit der Aushöhlung zentraler Grundsätze der Rechtsstaatlichkeit (ganz zu schweigen vom Grundrecht auf informationelle Selbstbestimmung) einher, ohne die eine Demokratie nicht überlebensfähig ist. Besonders exponierte Verdächtige sind im Kampf der USA gegen den Terror bekanntlich zum Objekt von Drohnenangriffen geworden. Die Wahrscheinlichkeit derartiger Exekutionen unter Ausschaltung des Rechtsweges wird durch die Gefahr einer automatisierten Kriegführung, die mit der Weiterentwicklung der Drohnen einhergeht, potenziert. Man kann in diesem Sinne von Totalisierungstendenzen in der staatlichen Sicherheitspolitik sprechen. Warum regen sich darüber vergleichsweise wenige Menschen auf?

Die Geheimdienste vergewissern sich bei der Ausspähung der Bürger und Bürgerinnen der Kooperation nichtstaatlicher Netzbetreiber, die an der Datenerhebung über ihre Kunden interessiert sind. So verbinden sich politische und kommerzielle Interessen in einer Weise, die den Bürger als Kunden der Netzbetreiber der Politik als Beobachtungsobjekt ausliefert. Auf diesem Wege erscheint die staatliche Überwachung auch als Fortsetzung der öffentlichen Selbstprofilierung, mit der die Menschen im Netz um Aufmerksamkeit und Anerkennung ringen. Der Bürger misst der eigenen Inszenierung im Netz offenbar mehr Bedeutung zu als dem Versuch irgendeines Apparates, sich ein eigenes Bild von ihm zu machen. Außerdem: Ist es nicht bequem und geradezu eine Geste der Fürsorge, wenn uns der Versandhandel nach Erstellung unseres Persönlichkeitsprofils über die eigenen Vorlieben und Schwächen aufklärt und gleich das entsprechende Angebot parat hat, das dann per Mausklick ohne weitere Umstände geordert werden kann? „Der größte Antrieb für den gläsernen Menschen ist die Bequemlichkeit, also die Delegierung möglichst vieler Aufgaben an ‚intelligente' Alltagsdinge, die untereinander kommunizieren. […] Das Leben der Menschen wird einfacher und zugleich kontrollierbarer", schreibt der Medienwissenschaftler Roberto Simanowski.[12]

Wir nutzen mit Begeisterung jede Neuerung auf dem Gebiet der elektronischen Kommunikation, die es uns erlaubt, noch leichter, schneller und kostengünstiger „online" zu sein als bisher, und wir nehmen dabei in Kauf, noch besser, genauer und folgenreicher überwacht werden zu können: „So wird das Gerät, von dem wir glauben, es trüge die digitale Freiheit in sich, zur digitalen Fußfessel."[13] Und wir lernen, es zu lieben, wie Dr. Strangelove einst lernte, die Bombe zu lieben.

Und mehr noch: Der Bürger kann sich immer leichter auch selbst an der Ausspähung des Anderen beteiligen. Das hat er auch früher schon in Gestalt eines Denunzianten getan, aber heute verfügt er über weitaus bessere technische Hilfsmittel, um die Spuren anderer zu verfolgen. Die Möglichkeiten, die die moderne Kommunikationselektronik bietet, könnten ausreichen, um eine neue Generation „informeller Mitarbeiter" entstehen zu lassen, die allerdings nicht nur als Zuträger für staatliche Dienste, sondern zunehmend auch auf eigene Rechnung arbeiten könnten, indem sie die Erkenntnisse über andere auf dem wachsenden Datenmarkt an private Abnehmer verhökern. So finden sich alle – Geheimdienstler, Nutzer und Hacker jeglicher Herkunft – in der großen Datenwolke wieder, von der wir uns vorstellen, dass sie über unseren Köpfen schwebt, weshalb sich die Beteiligten auch fast wie im Himmel fühlen, obwohl sie sich virtuell im Bunker des *Utah Data Center* aufhalten.

Diese Konditionierung des Einzelnen könnte erklären, warum die aus rechtsstaatlicher Sicht skandalösen Überwachungspraktiken von NSA, *Prism* & Co in der liberalen Öffentlichkeit nicht zu einem Aufschrei der Empörung geführt haben. Die Totalisierungstendenzen im Streben nach Sicherheit reichen offenbar tiefer als die bloße Gegenüberstellung von wachsamem Bürger und überwachendem Staat vermuten lässt.

Der jetzige NSA-Skandal hat eine Vorgeschichte: Im Januar 2002 wurde von der US-amerikanischen *Defense Advanced Research Projects-Agency* (DARPA) ein Programm aufgelegt, das in größtmöglichem Umfang Personendaten erheben (bzw. generieren) und auf Auffälligkeiten im Verhalten jedes Einzelnen hin analysieren sollte. Ziel des Programms war es, im Kampf gegen den Terrorismus „Total Information Awareness" herzustellen. Dafür wurde sogar eine Abkürzung geschaffen: TIA. Das Programm stieß in den Medien und der Zivilgesellschaft auf Widerstand – nicht zuletzt auch wegen seines Leiters, John Poindexter, der unter Präsident Ronald Reagan in die Iran-Contra-Affäre verwickelt gewesen und in diesem Rahmen der Lüge gegenüber dem Kongress überführt worden war. Poindexter wandte gegen die Kritik am TIA ein, es ginge keineswegs darum, US-amerikanische Bürger auszuspionieren, sondern lediglich darum, terroristische Netzwerke zu identifizieren und zu überwachen. Der Kongress folgte dem Argument nicht. Aufgrund der Gefahr für den Schutz der Privatsphäre amerikanischer Bürger und für ihre Freiheitsrechte strich er die Weiterfinanzierung des TIA.

Dieser Vorgang scheint sich aber als weitgehend kosmetische Operation zu erweisen. Der Kern des Projekts wird nach Einschätzung von Fachleuten weitergeführt, jetzt allerdings auf der erwähnten Grundlage einer *public-private partnership*. Trotz Wandel der Form besteht so gesehen eine erhebliche Kontinuität in der Sache. Das gilt auch für die Rechtfertigung der Überwachung. Der Leiter der NSA, General Keith Alexander, erklärte auf der Hacker-Konferenz „Black Hat" Anfang August dieses Jahres in Las Vegas, in den USA sei eine vorbildliche Kontrolle der Geheimdienste gewährleistet. Das System der rechtsstaatlichen Aufsicht sei einzigartig und müsse zum globalen Standard werden.[14] In der deutschen Debatte wurden solche Selbstauskünfte der Geheimdienste in Regierungskreisen dankbar aufgenommen, um lästige Debatten in nicht opportunen Zeiten zu verhindern. Der einschlägige Bundestagsausschuss befasste sich mit den Ausspähaktivitäten ausländischer Geheimdienste in Deutschland, stellte aber keine eigenen Ermittlungen an. Das von Ulrich Beck so genannte „digitale, globale Freiheitsrisiko"[15] existiert fort, weil die Logik

12 Roberto Simanowski, Ignoranz und Bequemlichkeit, Neue Zürcher Zeitung 20.9 2013, S. 23.
13 Morten Freidel, Das Smartphone ist die freiwillige Fußfessel von morgen, FAZ, 3.8.2013, S. 34.
14 Patrick Bahners, Wir finden alles über euch heraus, FAZ 2.8.2013, S. 31.
15 Digitaler Weltstaat oder digitaler Humanismus? (Gespräch mit Ulrich Beck), FAZ, 20.7.2013, S. 40.

des Sicherheitsstrebens darin besteht, dass es sich selbst nie genügt, sondern mit jeder neuen Erkenntnis die Suche nach weiteren Erkenntnissen vorantreibt – eine Endlosschleife, bei der die Katastrophe mit Beck formuliert darin besteht, dass „das Katastrophale als solches gar nicht mehr erkennbar ist“[16].

Prof. em. Dr. Lothar Brock ist Lehrender am Institut für Politikwissenschaft an der Goethe-Universität in Frankfurt/M. und Gastprofessor an der Hessischen Stiftung Friedens- und Konfliktforschung (HSFK) ebenfalls in Frankfurt/M. sowie Senior Expert Fellow am Käte Hamburger Kolleg „Politische Kulturen der Weltgesellschaft“ in Duisburg, Essen und Bonn.

Menschliche Sicherheit als Alternative?

Cornelia Ulbert

Noch ist das Ausmaß der Datenausspähung durch die US-amerikanische *National Security Agency* (NSA) und andere Geheimdienste nicht genau bekannt, aber täglich kommen über die Medien neue Einzelheiten ans Licht. Obwohl es hierbei unter anderem zu einer offensichtlichen Verletzung der Pressefreiheit in Großbritannien kam, als der *Guardian* von britischen Sicherheitsbehörden gezwungen wurde, Datenmaterial des US-amerikanischen *Whistleblowers* Edward Snowden zu vernichten, hält sich der Sturm der Entrüstung über die Verletzung von Freiheitsrechten und Datenschutz bislang weltweit in Grenzen.

Dies ist ein erklärungswürdiger Befund in demokratischen Gesellschaften, die für sich Rechtsstaatlichkeit und den Schutz individueller politischer und bürgerlicher Freiheitsrechte reklamieren. Ordnen wir diese Rechte einer staatlichen Sicherheitslogik unter? Hätte es eine weniger ausufernde Überwachungspraxis gegeben, wenn menschliche Sicherheit (*human security*) die Handlungslogik der politisch Handelnden bestimmen würde?

Einer breiteren Öffentlichkeit wurde der Begriff der menschlichen Sicherheit mit dem *Human Development Report* des Entwicklungsprogramms der Vereinten Nationen (UNDP) von 1994 bekannt. Nach diesem Verständnis sollte nicht mehr der Staat, sondern der einzelne Mensch den Ausgangspunkt für entwicklungs-, aber auch sicherheitspolitische Überlegungen bilden. Ziel sollte es sein, Menschen ein Leben in *freedom from want* und *freedom from fear*, also in Freiheit von Not und Angst zu ermöglichen. In der nachfolgend einsetzenden wissenschaftlichen Debatte wurde das Konzept als zu vage und analytisch wenig brauchbar kritisiert, weil es insbesondere die Grenzen zwischen dem Sicherheits-, Entwicklungs- und Menschenrechtsdiskurs verwische und die Gefahr in sich berge, dass sich die den sicherheitspolitischen Diskurs prägenden Machtstrukturen und Handlungslogiken auch in den Bereichen Entwicklungspolitik und Menschenrechtsschutz durchsetzen würden.

Das Konzept menschlicher Sicherheit war von Anfang an darauf ausgelegt, praktisch-politisch Wirkung zu entfalten. Seine Förderer wollten vor allem einen Kontrapunkt gegen diejenigen setzen, die für einen erweiterten Sicherheitsbegriff warben, der faktisch darauf abzielte, aus klassischer sicherheitspolitischer Sicht neue Bedrohungslagen für den Staat zu identifizieren.

Daher sollte eine Politik der menschlichen Sicherheit nicht nur eine Sicherheitsdimension im engeren Sinne, also den Schutz der physischen und psychischen Unversehrtheit des Individuums umfassen, sondern auch menschliche Entwicklung in den Vordergrund rücken. Eine dritte Dimension bezieht sich auf den Schutz von Menschenrechten. In der praktischen Umsetzung wurden die drei Dimensionen jedoch bislang nie gleichberechtigt nebeneinander berücksichtigt. Kanada war jahrelang bemüht, menschliche Sicherheit in den Mittelpunkt seiner Außenpolitik zu stellen, betonte in der Umsetzung jedoch die physischen Bedrohungen für Individuen, wofür vor allem sein *Human Security Report Project* mit dessen mittlerweile eingestellten periodischen Berichten steht. Japan, ein weiteres Land, das explizit den Begriff menschlicher Sicherheit als Leitkonzept seiner Außenpolitik verwendet, legt den Schwerpunkt hingegen stärker auf Entwicklungsaspekte. In außenpolitischen Strategiepapieren der Europäischen Union wird auch die menschenrechtsorientierte Dimension betont. Aus dieser Perspektive wird argumentiert, dass internationale und regionale Institutionen von zentraler Bedeutung für die gemeinschaftliche Weiterentwicklung von Menschenrechten, für ihre nationale Implementierung oder gar gemeinschaftliche Durchsetzung sind und Rechtsstaatlichkeit sowie die Geltung von Menschenrechten eine wesentliche Grundlage für die Umsetzung menschlicher Sicherheit darstellen.

Wichtig in diesem Zusammenhang ist der Umstand, dass auch im Konzept menschlicher Sicherheit dem Staat eine entscheidende Rolle bei der Gewährleistung von Sicherheit und Wohlfahrt sowie beim Schutz von Menschenrechten zukommt bzw. dass im Falle seines Versagens die internationale Gemeinschaft in die Pflicht genommen wird. Gleichzeitig scheint in politischen Diskussionen eher ein Verständnis von menschlicher Sicherheit vorzuherrschen, in dem der Schutz von Menschenrechten stark auf die Abwehr von physischen Bedrohungen für Menschen verkürzt wird. Dies spiegelt sich auch in der Debatte um die Schutzverantwortung (*Responsibility to Protect*) wider, mit der einige „humanitäre Interventionen“ der letzten zwei Jahrzehnte gerechtfertigt wurden und die auch jetzt wieder als Begründung für ein mögliches Eingreifen westlicher Staaten in den syrischen Bürgerkrieg dient.

Der Ansatz menschlicher Sicherheit beschränkt sich allerdings nicht allein auf die Einhegung von Kriegen oder deren Auswirkungen. Vielmehr wurde auch das Spektrum möglicher Bedrohungen im Hinblick auf ein menschenwürdiges Leben erweitert: Terroristische Netzwerke, international organisierte Drogen- und Verbrecherkartelle sowie Flüchtlings- und Migrationsbewegungen beeinflussen demnach ebenfalls die Sicherheit und Lebensbedingungen von Menschen in einer Region oder einem Land. Diese konzeptuelle Ausweitung führte schnell zum Vorwurf, menschliche Sicherheit sei in der vorliegenden Breite ungeeignet, um aus ihr tatsächlich politische Prioritätensetzungen abzuleiten.

16 Ebd.

Prism & Co lehren uns momentan auf erschreckende Art und Weise, dass der Prozess der „Versicherheitlichung", bei dem immer mehr Sachverhalte in den sicherheitspolitischen Diskurs überführt werden, nun zurückschlägt und damit sehr wohl zu einer Prioritätensetzung führen kann. Die „Kodierung" von Menschenrechten als Sicherheitsthema erleichtert es auch den Vertretern eines lediglich erweiterten „klassischen" Sicherheitsverständnisses, Sicherheit nicht allein als Bedingung für den Schutz von Menschenrechten, sondern als einen Bestandteil von Menschenrechten zu interpretieren. Dementsprechend steht in der Rhetorik führender Politiker dann auch nicht der Schutz des Staates im Vordergrund, sondern – so etwa Bundesinnenminister Hans-Peter Friedrich – bei der Frage der Datenausspähung habe die Sicherheit der Bürger Vorrang vor anderen Rechten, da Sicherheit ein „Supergrundrecht"[17] sei. Ähnlich argumentierte auch der Präsident der USA Barack Obama, als er im Juni 2013 nach seiner Reaktion auf die ersten Berichte über geheime staatliche Ausspähprogramme befragt wurde: „But I think it is important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. We're going to have to make some choices as a society".[18] Nach Obamas Dafürhalten schließt das eine das andere aus. Diese Haltung zeigt deutlich die negativen Konsequenzen auf, wenn einzelne Risiken im Vergleich zu anderen Lebensrisiken als sicherheitsbedrohend eingestuft werden und damit der Bearbeitung im Modus „normaler", sprich rechenschaftspflichtiger und demokratisch legitimierter Politik entzogen werden. Eine derartige Versicherheitlichung der Grundrechtsdebatte führt zu einem permanenten Ausnahmezustand, was uns der seit dem 11. September 2001 andauernde „Krieg gegen den Terror" drastisch vor Augen führt, für den die extremen Auswüchse in Guantanamo und Abu Ghraib symbolträchtig stehen.

Damit will ich nicht behaupten, dass menschliche Sicherheit der Wegbereiter für den „Krieg gegen den Terror" und die Aushöhlung unserer Grundrechte war. Der ernüchternde Befund ist vielmehr, dass die Perspektive menschlicher Sicherheit, auch wenn sie in den USA politisch handlungsleitend gewesen wäre, die gegenwärtigen Entwicklungen sehr wahrscheinlich nicht verhindert hätte. Die Art und Weise, wie die Debatte um die Datenausspähung geführt wird, zeigt, dass selbst ein breites Verständnis menschlicher Sicherheit nicht zur Folge gehabt hätte, dass die drei Dimensionen Sicherheit, Entwicklung und Menschenrechte gleichberechtigt berücksichtigt werden. Mit der Versicherheitlichung eines Politikbereichs ändert sich, wie eine Situation wahrgenommen wird. Wenn jemand oder etwas bedroht wird, entsteht eine Abwehrhaltung und derjenige, der mein Wohlergehen bedroht, wird zum „Feind". Faktisch sind damit Handlungslogiken, die aus anderen Perspektiven auf das Wohlergehen und den Schutz der physischen Unversehrtheit von Individuen resultieren, der Handlungslogik von „Sicherheit" untergeordnet bzw. gehen in dieser auf.

In einem ist US-Präsident Obama zuzustimmen: Wir als Gesellschaft müssen Entscheidungen treffen. Die vielleicht anfängliche Empörung über die Verletzung der Privatsphäre wird vielfach achselzuckend mit der Aussage beiseite gewischt: „Ich habe ja nichts zu verbergen, und wenn es der Verbrechensverhütung dient ...". Sicherlich steht Strafverfolgungsorganen ein wichtiges Instrument der Verbrechensbekämpfung zur Verfügung, wenn verdächtige Personen auch in nicht öffentlichen Räumen überwacht werden können. Bei genauerer Betrachtung ist dieses Argument jedoch nicht haltbar: Auch wenn eine große Anzahl an Straftatbeständen in der „Privatsphäre" geplant und ausgeführt wird, kann damit in einer freiheitlichen Gesellschaft keine flächendeckende Ausspähung eigener oder fremder Bürger gerechtfertigt werden. Nicht umsonst sind der Verletzung der Privatsphäre in Rechtsstaaten enge juristische Grenzen gesetzt. Wozu das andernfalls führen kann, wissen wir Deutschen aus unserer eigenen Geschichte nur allzu gut, nicht zuletzt durch das Beispiel des gigantischen staatlich gesteuerten Überwachungsapparats in der ehemaligen DDR. Wenn Bürger sich permanent überwacht fühlen, wird das gesellschaftliche Zusammenleben nachhaltig negativ beeinflusst.

Letztendlich scheint der Ansatzpunkt zur kritischen Aufarbeitung der Ausspähaktionen nicht unbedingt das zugrundeliegende Sicherheitsverständnis zu sein, sondern unsere Vorstellung von persönlicher Freiheit und Privatsphäre und was davon wir gegebenenfalls bereit sind, dem Staat im Austausch gegen die Freiheit von Not und Angst im Kontext unseres Grundrechtekatalogs „preiszugeben". Ebenso kritisch müssen wir die Annahme überprüfen, der Staat sei in der Lage, uns immer und überall hundertprozentige Sicherheit zu garantieren. Er kann dies nicht. Und in vielen Bereichen sind wir auch nicht gewillt, dies vom Staat einzufordern. Einige Lebensrisiken gehen wir bewusst ein – schnelles Fahren auf der Autobahn, ungesunde und umweltgefährdende Lebensstile, um nur einige zu nennen. Die Eingriffsbefugnis des Staates in andere Bereiche ist zumindest heftig umstritten, wie die teilweise hitzige Debatte um ein Rauchverbot in der Gastronomie zeigt. Nur im Falle terroristischer Anschläge haben wir es uns seit den Anschlägen vom 11. September angewöhnt zu akzeptieren, dass der staatlichen Fürsorgepflicht keinerlei Grenzen gesetzt zu sein scheinen.

Menschliche Sicherheit in einem umfassenden Sinne zu gewährleisten ist eine der Grundaufgaben des Staates. Den Schutz des Individuums und die Freiheit von Not und Angst zum Anlass zu nehmen, eine Freiheit von Freiheit zu propagieren, indem Sicherheit abstrakt als Grundrecht anderen Grundrechten entgegengesetzt wird, ist der falsche Weg. Sicherheit impliziert die Frage „Wozu?". In liberaldemokratischen Gesellschaften besteht ihr Zweck stets auch darin, Freiheit zu gewährleisten. Die Grenzen dieser Freiheit festzulegen, muss den jeweiligen Gesellschaften selbst überlassen bleiben. Diese nicht zu thematisieren birgt die Gefahr der vermeintlich schweigenden Zustimmung. Daher sollten wir den längst überfälligen gesellschaftlichen Diskurs über das Verhältnis von Freiheit und Sicherheit endlich führen.

Dr. Cornelia Ulbert ist Wissenschaftliche Geschäftsführerin des Instituts für Entwicklung und Frieden (INEF) an der Universität Duisburg-Essen.

17 http://www.welt.de/118110002.
18 http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president.