Aufsätze

Thilo Weichert

Globaler Kampf um digitale Grundrechte

Die *Funktion des Rechts* ist es, in den Gesellschaften Ordnung herzustellen und dabei den ökonomisch oder militärisch Schwächeren vor ungerechten Übergriffen der Stärkeren zu schützen. Stärkere sind in der Regel nicht bereit, ohne Not und freiwillig auf Macht und Gewinn zu verzichten. Gibt es kein Recht, um ungerechtfertigte Machtausübung oder Ausbeutung zu verhindern, so gibt es für die Betroffenen zwei Alternativen – dies zu erdulden oder für die Etablierung von ordnendem Recht zu kämpfen.
Diese banalen Erkenntnisse – auf die Ausspähung durch den US-amerikanischen Geheimdienst *National Security Agency* (NSA) angewendet – lassen im Hinblick auf die Politik der deutschen Bundesregierung weitgehend den Schluss zu, dass diese sehr weitgehend bereit ist, Unrecht zu erdulden. Der vorliegende Beitrag will sich mit diesem Ergebnis nicht abfinden und sucht deshalb Wege zur Etablierung von Recht, mit dem die weiter fortgesetzte, fast ungehinderte Ausspähung durch die NSA eingehegt oder gar verhindert werden kann.

1. Die umfassende Überwachung des Internet

Für die Fakten sorgt insbesondere der Whistleblower *Edward Snowden*: Die NSA versucht, den globalen Internetverkehr, soweit er ihr relevant erscheint, zu überwachen, zumindest in großen Teilen abzuspeichern und die Erkenntnisse für nationale Zwecke zu verwenden.[1]
Dies tut die NSA nicht im Alleingang, sondern in enger Kooperation mit Geheimdiensten von weiteren Staaten: dem britischen Government Communications Headquarters (GCHQ) sowie den entsprechenden Diensten in Kanada, Australien und Neuseeland – den sog. „*Five Eyes*". Die Zusammensetzung dieser Kooperation ist nur auf den ersten Blick irritierend, weil diese Staatenkombination in der Weltpolitik regelmäßig nicht als Bündnis auftritt. Eine nähere Betrachtung ergibt aber, dass diese Staaten hinsichtlich der Kontrolle des Internet speziell bzw. generell der informationellen globalen Vernetzung sich ideal ergänzen, wenn die USA einen globalen Hegemonieanspruch wahrnimmt und die anderen Staaten ihre regionalen Interessen verfolgen: Großbritannien spielt in Europa regelmäßig nicht nur die Rolle eines Außenseiters in der Europäischen Union, sondern auch die des europäischen Brückenkopfes für die USA. Kanada spielt weltpolitisch zwar keine zentrale Rolle, stellt aber geopolitisch die Grenze zu einem der wichtigsten politischen Widersacher: Russland. Über Australien und Neuseeland kann der gesamte pazifische und asiatische Raum informationell

1 Einen Überblick mit verschiedenen Aspekten geben Bowden, The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens´ fundamental rights, Note, European Parliament, 2013; Beckedahl/Meister (Hrsg.), Überwachtes Netz, Edward Snowden und der größte Überwachungsskandal der Geschichte, 2013.

erschlossen werden.[2] Für eine informationelle Kooperation äußerst förderlich ist die gemeinsame englische Sprache – ein Vorteil, den die „Five Eyes" gegen das insofern viel heterogenere Europa ausspielen können – und ein gemeinsames, vom britischen Common Law geprägtes Rechtsverständnis. Hinsichtlich des Rechtsverständnisses ist nicht unerheblich, dass dieses nur in begrenztem Maße normierte Grundrechte kennt – auch insofern im Gegensatz zur Europäischen Union, die sich 2009 eine ausdrückliche und ausführliche Grundrechtecharta zulegte. Ein weiterer relevanter Kooperationspartner für die „Five Eyes" ist Schweden, worüber ein Großteil der Kommunikation zwischen Europa, Rußland und den USA geleitet wird.[3]

1.1 Spionage

Die primäre Motivation der informationellen Netzüberwachung war und ist nicht die *Terrorismusbekämpfung*, so wie dies die US-Administration im Frühstadium der Snowden-Enthüllungen noch glaubhaft zu machen versuchte. Die aktuelle Überwachung ist nichts anderes als die technologische Weiterentwicklung des NSA-Überwachungsprogramms Echelon, über das sich Europa um die Jahrtausendwende nur kurz empören konnte, bevor dieses Gefühl nach dem 11.9.2001 der unverbrüchlichen und uneingeschränkten Solidarität im gemeinsamen Kampf gegen den internationalen (islamischen) Terrorismus wich.
Die erste Motivation für die NSA ist *politische Spionage*. Die Ausspähung der Kommunikation sog. befreundeter Regierungschefs und Regierungen oder der europäischen Zentrale in Brüssel ist hierfür ein Indiz. Doch sollte bei aller Aufregung über das ausgespähte Merkel-Handy nicht aus dem Blick verloren werden, dass die Kontrolle fremder Regierungen nur ein winziger, zweifellos spektakulärer Bruchteil des NSA-Interesses war und ist. In Vordergrund stehen die bei Weitem nicht so berechenbaren, weniger institutionalisierten politischen Entwicklungen in den Ländern dieser Welt, also von Regierungsparteien und -strömungen, von parlamentarischen und außerparlamentarischen Oppositionen, von friedlichen und weniger friedlichen Interessenverbünden und Gruppierungen und nicht zuletzt von wirtschaftlichen Interessen im globalen politischen Wettbewerb.
Wirtschaftliche Geheimnisse sind dabei mehr als nur informationeller Beifang; sie sind auch nicht nur das nötige Hintergrundwissen für politische Interessen. Diese sind auch das Material für den politischen Fortschritt der nationalen Wirtschaft sowie für die Modernisierung der Verwaltung und der Gesellschaft. James R. Clapper, Director of National Intelligence, hat für die USA in einem offiziellen Statement eingeräumt, dass seine Geheimdienste ökonomische und finanzielle Angelegenheiten im Fokus haben, u. a. auch um Einsichten in die Wirtschaftspolitik und das wirtschaftliche Verhalten anderer Staaten zu erlangen.[4]
Der Umstand, dass politische und wirtschaftliche Spionage zu den ältesten Gewerben gehört, bestätigt den obigen Befund eher als dass dieser dadurch relativiert würde. Politische Spionage gilt schon seit Jahrhunderten dem politischen Gegner, von der institutionalisierten Opposition bis zu revolutionären Umtrieben, wie auch dem offiziellen „Freund" und Partner. Schon bei Echelon ist sie klar erkennbar. Erst jetzt ist aber eine neue Dimension der Spionage technisch möglich, deren Objekte nicht spezielle Interessen, Organisationen, Einzelper-

2 CSEC bespitzelt Fluggäste für NSA, Lauschangriff auf indonesische Regierung, DatenschutzNachrichten (DANA) 1/2014, 40.
3 Sander in Beckedahl/Meister (Fn. 1), S. 128.
4 Stadler in Beckedahl/Meister (Fn. 1), S. 145.

sonen und Gruppen sind, sondern das *kommunikative Verhalten der gesamten Bevölkerung*.

1.2 Massenüberwachung

Mit dieser quantitativen wie qualitativen Veränderung gewinnt die Spionage, die von Mata Hari bis James Bond immer auf Entscheidungsträger im politischen Raum zielte, eine massenhaft grundrechtliche Dimension: Es geht um die digitalen Grundrechte der Bürgerinnen und Bürger in allen Staaten dieser Welt. Zugleich dringt diese Spionage in einen Bereich hinein, der bisher von ihr getrennt gesehen wurde: in den der jenseits der Staatsgewalten erfolgenden demokratischen Prozesse. Wurden noch die technischen Möglichkeiten sozialer Netzwerke für die demokratische Erhebung im sog. „arabischen Frühling" gefeiert, so müssen wir nun zur Kenntnis nehmen, dass die Überwachung des Kommunikationsverhaltens der Bevölkerung im Internet der Schlüssel für die *Kontrolle und Manipulation der Wahrnehmung demokratischer Freiheiten* ist. Von der NSA, die sich dies anmaßt, gab es insofern nur halbherzige Dementis. Dieser wohl kritikwürdigste Umstand steht aber bisher bei vielen Kritikern der NSA noch nicht im Vordergrund. Tatsächlich ist dieser Eingriff in die Souveränität der überwachten Gesellschaften das zentrale Problem und zugleich der zentrale Ansatzpunkt für eine (völker-)rechtliche Bändigung der Geheimdienstaktivitäten.
Technisches Rückgrat der Digitalisierung ist zweifellos das Netz, also im weitesten Sinn das *Internet* mit seinen Anwendungen, Schnittstellen und Subsystemen. Dabei handelt es sich aber nicht um eine statische, sondern um eine sich prozesshaft weiterentwickelnde Infrastruktur, die aktuell geprägt ist vom Phänomen des Wearable Computing (Smart Glasses, Smart Watches),[5] dem „Internet der Dinge", das die menschliche Lebens- und Produktionswelt automatisiert, von „Big Data"[6] mit der damit verbundenen komplexen Datenauswertung und automatisierten Wirksystemen, die darauf hinauslaufen, dass ganze Lebensteilbereiche rein technisch reguliert sind. Diese Entwicklungen machen nicht nur die grundrechtliche Enteignung der Menschen, sondern auch die Herrschaft über eine Gesellschaft, die digitale Diktatur, möglich.

2. Digitale Grundrechte

Die *Idee digitaler Grundrechte*[7] setzt sich im wissenschaftlichen Diskurs langsam durch. In der öffentlichen und institutionellen Politik ist sie aber noch nicht angekommen. Deren faktische Grundlage wurde schon im Urteil des Bundesverfassungsgerichts zur Volkszählung 1983 formuliert: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden. … Dies würde nicht nur die Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens."[8]

5 Weichert, Google Glass, IT-Brillen und informationelle Selbstbestimmung, www.datenschutz.de 29.4.2013.
6 Weichert, Big Data und Datenschutz, ZD 2013, 251 ff.
7 Weichert, Codex Digitalis Universalis, in Schmidt/Weichert, Datenschutz, 2012, S. 345 ff.
8 BVerfGE 65, 43 = NJW 1984, 422.

Nicht nur direkter Zwang und Gewalt, sondern auch die *Macht über die Informationen* von Individuen kann die Wahrnehmung unserer demokratischen, wirtschaftlichen und sozialen Grundrechte beeinträchtigen. Unsere Freiheitsrechte, wie sie in der Zeit der Aufklärung entwickelt und in Deutschland in den Artikeln 1 bis 20 im Grundgesetz normiert wurden, haben mit der Digitalisierung unserer Gesellschaft eine digitale Dimension hinzugewonnen. Dies gilt insbesondere für die Pressefreiheit.[9] Aber auch die sonstigen Grundrechte – vom Gleichheitsgrundsatz über den Schutz von Familie, Wohnung und Eigentum oder über den Schutz vor politischer Verfolgung und der politischen Rechten auf Versammlung, Vereinigung und Meinung bis hin zu den sozialen Schutzvorkehrungen – sind heute nicht nur materiell bzw. genauer analog, sondern auch informationell bzw. genauer digital bedroht. Demgemäß bedarf es auch informationellen Schutzes.

Dieser kann sich nicht – ebenso wenig wie bei den analogen Grundrechten – auf reine Abwehrrechte gegen den Staat beschränken, sondern muss auch *Teilhaberechte und staatliche Gewährleistungen* vorsehen.[10] Dass diese Erkenntnis inzwischen zum Kernbestand des europäischen Grundrechtsschutzes gehört, ist auch ein Verdienst des deutschen Bundesverfassungsgerichts. Neben der Ableitung des Rechts auf informationelle Selbstbestimmung, des Grundrechts auf Datenschutz, war die Weiterentwicklung des allgemeinen Persönlichkeitsrechts zu einem Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme im Jahr 2008 ein wichtiger Meilenstein.[11] Die verbindliche Normierung der Grundrechte in der EU, einschließlich ihrer informationellen Bestandteile in der Grundrechtecharta von 2009, war ein weiterer Meilenstein. Ein bisher fast unbeachtet gebliebener Meilenstein ist die neue Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zur Meinungs- und Informationsfreiheit, die hieraus einen informationellen Teilhabeanspruch gegenüber dem Staat ableitet.[12]

Eine umfassende Betrachtung der Errungenschaften in Europa ergibt einen *weitgehend vollständigen Bestand* der digitalen Grundrechte, ohne dass dieser bisher systematisch und unter dieser Überschrift kodifiziert worden ist. Er schließt die digitalen Gewährleistungen des allgemeinen Persönlichkeitsrechts und die Kommunikationsfreiheit ebenso ein wie die in Art. 5 GG adressierten Themen der Meinungs-, Informations- und Pressefreiheit. Weitere Bestandteile sind die digitale Versammlungsfreiheit, das Petitionsrecht, die digitalen Komponenten der Freiheiten auf Religion, Familie, Beruf, Wohnung, Freizügigkeit; diese enden noch nicht bei der informationellen Gleichbehandlung einschließlich eines Diskriminierungsverbotes. Merkmale wie Geschlecht, Abstammung, Herkunft oder Glauben dürfen nicht diskriminierend verwendet werden.

Eine zentrale Erwägung des Grundrechtsschutzes ist die *Sicherung der Rechtsstaatlichkeit* und des gerichtlichen Rechtsschutzes durch das Verbot mit Erlaubnisvorbehalt bei informationellen Eingriffen. Prozessuale Absicherungen sind die Unschuldsvermutung, der Nemo-Tenetur-Grundsatz sowie der Anspruch auf ein faires Verfahren. Generell wird das materielle Recht durch technisch-organisatorische und verfahrensrechtliche Absicherungen flankiert. Generell gilt das Verbot heimlicher Eingriffe und zugleich ein auch als Demokratieschutz verstandenes Recht auf Transparenz. Eine institutionelle Absicherung besteht

9 Gutjahr in Beckedahl/Meister (Fn. 1), S. 57 ff.
10 Hoffmann-Riem, Freiheitsschutz in den globalen Kommunikationsstrukturen, JZ 2014, 56 ff.
11 BVerfG NJW 2008, 822; Hoffmann-Riem (Fn. 10), JZ 2014, 57.
12 EGMR U. v. 26.6.2013; Youth Initiative for Human Rights v. Serbia, 48135/06; DANA 2013, 164, vgl. Wegener, Der geheime Staat, 2006.

schon heute in unabhängigen digitalen Aufsichtsbehörden, die sich von ihrer Beschränkung auf den klassischen Datenschutz dadurch emanzipieren, dass sie die Aufgaben von Informations(freiheits)beauftragten wahrnehmen.
Die hier für Europa angedeutete Entwicklung wurde *in der übrigen Welt* teilweise im Ansatz und teilweise aber auch nicht nachvollzogen. Während insbesondere weitere Staaten in Nord- und Südamerika wie in Fernost Zusicherungen von digitalen Grundrechten entwickeln, findet insofern eine Totalblockade durch die digitalen Supermächte China, Russland und die USA statt.[13] Diese Blockade verfolgt in Bezug auf China und Russland unzweifelhaft das Ziel der Aufrechterhaltung eines autoritären Staatssystems und der Verhinderung von Demokratisierungsbestrebungen durch Zensur und Überwachung sowie die Bewahrung der oligarchischen Wirtschaftsordnung.[14]

3. Der US-amerikanische Diskurs

Anders die USA, der ein aktives Bekenntnis zur Demokratie nicht abgesprochen werden kann. Doch auch bzw. gerade dort erweist sich die Leugnung digitaler Grundrechte als ein zentraler demokratiefeindlicher Baustein für die *Wahrung politischer und ökonomischer Hegemonie*. Diese besteht in einer über viele Jahrzehnte aufgebauten Vormacht der NSA bei der Kontrolle des globalen Informationsnetzes mit dem Ziel der Absicherung der sicherheitspolitischen und militärischen Hegemonie.[15] Dies besteht aber auch in der Abwehr von Grundrechtsbindungen für die eigene IT-Wirtschaft.
Es ist verblüffend, dass sich die *herrschende Meinung* über die Anerkennung digitaler Grundrechte in den USA immer noch auf dem Stand der 70er Jahre des letzten Jahrhunderts befindet. Bis dahin waren die USA hier weltweit führend, beginnend mit dem Beitrag von Samuel D. Warren und Louis D. Brandeis zum „Recht auf Privatheit" aus dem Jahr 1890.[16] Allan F. Westin skizzierte im Jahr 1967 in seinem Klassiker „Privacy and Freedom" nicht nur die Risiken der Digitalisierung und die dazu erfolgte gesellschaftliche Auseinandersetzung, sondern auch die Ableitungen digitaler Grundrechte aus den Amendments zur US-Verfassung. Er beschreibt darin auch die damaligen politischen Widerstände aus der Wirtschaft und der Sicherheitsadministration hiergegen.[17] Ohne auf diese Diskussion direkt Bezug zu nehmen, vollzog das Bundesverfassungsgericht im Volkszählungsurteil von 1983 diese Argumentation inhaltlich nach. Die hierfür herangezogenen Grundsätze zum Schutz des allgemeinen Persönlichkeitsrechts waren dabei erheblich weniger konkret als es die Amendments der US-Verfassung waren und sind. Seitdem hat es trotz vielfacher Bestrebungen und Einzelregulierungen in den USA bis heute keine wesentlichen rechtlichen Entwicklungen zur Digitalisierung der Grundrechte gegeben.[18]
Im Gegenteil: Mit dem Foreign Intelligence Surveillance Act und *nach Nineeleven 2001* mit dem Patriot Act wurde die weitgehende Befreiung der Administration vor demokratischer und rechtsstaatlicher informationeller Kontrolle fest-

13 Weichert, Datenschutz und Überwachung in ausgewählten Staaten, in Schmidt/Weichert (Fn. 7), S. 419 ff.
14 Freiheitsfoo, Russia 1984, DANA 1/2014, 24.
15 Schaar in Beckedahl/Meister (Fn. 1), S. 118 ff.
16 DuD 2012, 755 = https://www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html.
17 Allan F. Westin, Privacy and Freedom, 1967.
18 Vgl. Weichert, Privatheit und Datenschutz im Konflikt zwischen den USA und Europa, RDV 2012, 113.

geschrieben.[19] Als nun die informationelle Hegemonie der US-IT-Unternehmen 2012 ernsthaft durch einen Entwurf der Europäischen Kommission für eine Datenschutzgrundverordnung angegriffen wurde, versuchte die US-Administration, diese durch eine Consumer Privacy Bill of Rights zu verteidigen, in der vollständig auf freiwillige unverbindliche Selbstverpflichtung gesetzt wird.[20]
Seit Edward *Snowden* hat sich die Interessenlage ein wenig geändert: Zum einen wurde die informationelle Überwachung des globalen Netzes durch die NSA aus dem Arkanbereich herausgerissen und dem Licht und dem Diskurs der Weltöffentlichkeit ausgesetzt. Zum anderen wurde die Interessenidentität von US-Sicherheitsadministration und IT-Industrie teilweise aufgebrochen. Durch die freiwillige und zugleich gesetzlich abgesicherte Komplizenschaft der IT-Industrie mit der Sicherheitsadministration in den USA droht nun Microsoft, Google, Facebook, Apple und Amazon ein großer Teil der Kundschaft untreu zu werden. So kommt es nicht von ungefähr, dass die IT-Industrie Ansätze zeigt, sich aus der Umarmung der US-Sicherheitsbürokraten wie Keith Alexander und James Clapper zu befreien.[21] Interessant ist auch, dass sich diese Bürokraten umgehend kompromissbereit zeigten, etwa durch Herstellung von vermeintlich etwas mehr Transparenz hinsichtlich der erfolgten Datenzugriffe. Ein vergleichbares Entgegenkommen zeigt die US-Administration gegenüber den europäischen „Freunden" nicht im Ansatz. Diese Modifikationen können nicht darüber hinwegtäuschen, dass sich an der Interessengemeinschaft von US-Wirtschaft und -Administration bei der Leugnung digitaler Grundrechte nichts geändert hat. Die Leugnung dieser Grundrechte bleibt für die US-IT-Unternehmen der Garant für ihre Vormacht auf dem Weltmarkt, insbesondere auch gegenüber der europäischen IT-Industrie, die insofern grundrechtlich vom Gesetzgeber wie auch von der staatlichen Aufsicht in die Pflicht genommen wird.

4. Europäische Reaktionen

Die Reaktionen der europäischen und der deutschen Öffentlichkeit auf die Snowden-Enthüllungen waren unterschiedlich: Während die Medien von Anfang an eine geheimdienstkritische Haltung einnahmen, die die öffentliche Meinung generell widerspiegelte, blieb die Reaktion der deutschen Bundesregierung äußerst verhalten: Die ursprüngliche Ungläubigkeit, dass dies „Freunde" tun würden, hat sich gewandelt in ein bis heute nicht überwundenes *Staunen über die Unnachgiebigkeit der USA* und dem damit verbundenen Rechtsnihilismus.[22] Die mediale Verarbeitung dieses Erstaunens ist unterschiedlich und pendelt zwischen Relativierung über symbolischen Aktionismus bis hin zu einigen wenigen sinnvollen Ansätzen in Richtung realer Veränderungen.
Symptomatisch für die *Relativierungen* ist die Reaktion des Präsidenten des Bundesamtes für Verfassungsschutz Hans-Georg Maaßen, der sich im Ergebnis auf die Seite seiner US-amerikanischen Geheimdienstkollegen stellte, Edward Snowden als einen Verräter und Wichtigtuer brandmarkte, ohne auch nur ansatzweise die bürgerrechtliche, demokratische oder rechtsstaatliche Dimension der NSA-Aktivitäten zu beleuchten.[23] Diese Sichtweise beruht auf gemeinsamen

19 Wolf, Der rechtliche Nebel der deutsch-amerikanischen „NSA-Abhöraffäre", JZ 2013, 1040; Zielcke, Schattenreich der Justiz, SZ 23.7.2013, 13; Richter, Die Angst, zu wenig zu wissen, SZ 23./24.11.2013, 9.
20 Weichert, http://www.datenschutzzentrum.de/gesetze/Consumer-Privacy-Bill-of-Rights.html.
21 Schulz, Die Schlüssel-Frage, Der Spiegel 12/2014, 74 f.
22 Amann/Gude/Schindler/Schmid, American Spy, Der Spiegel 46/2013, 44, 46.
23 Jakobs/Sigmund, Einspruch, Herr Snowden!, Interview mit Maaßen, Handelsblatt 29.1.2014, S. 1, 5.

Interessenlagen der Geheimdienste in Deutschland und den USA und der begründeten Erwartung, dass weiterhin Brosamen vom Tisch der NSA-Erkenntnisse auf den deutschen Diensteboden fallen mögen.

Es ist legitim zu hinterfragen, welche Erkenntnisse aus der Massenüberwachung generell erlangt werden können, welche davon die US-Dienste den deutschen „Freunden" zukommen lassen und welcher *Sicherheitsnutzen* damit verbunden ist bzw. sein kann. Eine neutrale Analyse ist insofern nicht nur ernüchternd, sondern erschreckend. Eine im Auftrag der New America Foundation, einer unabhängigen US-Kommission, erstellte Untersuchung von Januar 2014 über die anlasslose NSA-Telekommunikationsüberwachung kommt zu einem vernichtenden Ergebnis: „Wir haben bislang keinen Fall gefunden, in dem das Programm direkt dazu beigetragen hat, bislang unbekannte Pläne für einen Terroranschlag aufzudecken oder zu verhindern."[24] Auch die behaupteten positiven Effekte für die deutschen oder europäischen Sicherheitsbehörden sind weder plausibel noch wurden sie nachprüfbar belegt. Die Sicherheitsrisiken, die von der NSA-Überwachung ausgehen, wurden bis heute noch nicht im Ansatz ernsthaft erörtert.[25] Jenseits einer reinen Kosten-Nutzen-Abwägung ist zu erörtern und dann demokratisch zu entscheiden, welche Formen einer Massenüberwachung unter welchen Voraussetzungen rechtsstaatlich *akzeptabel und verhältnismäßig* sein sollen. Diese Diskussion, die das deutsche Bundesverfassungsgericht in einer Vielzahl von Entscheidungen den deutschen Sicherheitsbehörden und der deutschen Politik aufgezwungen hat, wird im Hinblick auf die NSA-Überwachung nicht geführt. Ja, man kann den Eindruck gewinnen, als wollte zumindest ein Teil des Sicherheitsapparates durch die NSA-Enthüllungen für sich neue Freiräume erschließen, so wie sie ihre US-Kollegen bisher genießen.

Unter die Kategorie des *symbolischen Aktionismus* fallen die Appelle an die US-Administration hinsichtlich mehr Transparenz und die vertrauensbildenden Gespräche mit den Verantwortlichen in den USA, bei denen die eigene Betroffenheit zum Ausdruck gebracht wird, verbunden mit der Hoffnung, die Vermittlung dieser Betroffenheit habe gegenüber den transatlantischen Partnern eine meinungsändernde Wirkung. In diese Kategorie sind auch die – im Ergebnis erfolglosen – politischen Bemühungen um ein sog. No-Spy-Abkommen einzuordnen, bei denen es lediglich um Absprachen auf Geheimdienstebene ging, nicht um eine Einschränkung der neuen freiheitsbedrohenden Dimension der Überwachung der Gesamtbevölkerung.[26] Es ist erstaunlich, wie wenig Mühe sich die US-Verantwortlichen bisher geben, zumindest den Eindruck eines Entgegenkommens und des Verstehens der deutsch-europäischen „Befindlichkeit" zu vermitteln.

5. Das deutsche historische Dilemma

Für die meistempörte Nation in Europa – also Deutschland – hat der Konflikt um digitale Grundrechte und Massenüberwachung eine historische Dimension: Die deutsche Sensibilität in Bezug auf Überwachung und Datenschutz ist zweifellos auch der *deutschen Geschichte* mit zwei Diktaturen und Überwachungsstaaten zuzuschreiben – dem Nationalsozialismus und dem im Osten 40 Jahre

24 Bergen u. a., Do NSA´s Bulk Surveillance Programms StopTerrorists", January 2014; Heidtmann, Warum die Überwacher gebändigt werden müssen, www.sueddeutsche.de, 17.1.2014; Biselli, NSA-Massenüberwachung nicht maßgeblich bei Terrorbekämpfung, netzpolitik.org 13.1.2014.

25 Dazu Benkler u. Weichert, in: Beckedahl/Meister (Fn. 1), S. 174, 180 f.; Bennhold, The hate that leads some men to terror, The New York Times International Weekly. 18.10.2013, 1, 4; Richter, Das Gold der NSA, SZ 22./23.6.2013, 8.

26 Baum, Auf dem Weg zum Weltüberwachungsmarkt, www.faz.net 20.2.2014.

lang real existierenden Sozialismus.[27] Derartige Erfahrungen sind kein deutsches Unikat. In Deutschland wurden aber einige Anstrengungen unternommen, um Lehren aus diesen historischen Erfahrungen zu ziehen. Dabei entsteht für die deutsche Wahrnehmung eine gefühlte Zerrissenheit: Waren es nicht letztlich vor allem die USA, die 1945 Deutschland vom Faschismus und vom Überwachungsstaat befreiten, also der Staat, der nun die globale Superüberwachung betreibt? Das deutsche historische Dilemma wurde öffentlich debattiert, als im Raum stand, dass es für die aktuell erfolgende Massenüberwachung in Deutschland durch US-Dienste Rechtsgrundlagen in geheimen Abkommen gäbe, die auf die Nachkriegssatzung und *alliierte Vorbehaltsrechte* zurückgingen. Es ist offensichtlich, dass vor diesem Hintergrund deutsche Stellen die Verletzung des Post- und Fernmeldegeheimnisses durch US-Dienste jahrelang nicht nur duldeten, sondern auch aktiv unterstützten. Es ist aber ebenso offensichtlich, dass mögliche alliierte rechtliche Vorbehalte spätestens seit der deutschen Wiedervereinigung keine Wirkung mehr zeigen können und ein Rückgriff auf Geheimverträge zur Rechtfertigung von Grundrechtseingriffen nicht möglich ist.[28]
Die deutsche *Dankbarkeit* für diese Befreiung gegenüber den USA soll ungebrochen bleiben. Sie darf aber nicht in eine Nachsicht gegenüber informationell totalitären Bestrebungen der heutigen USA münden. Vielmehr muss und sollte es die Pflicht des insofern geläuterten Deutschland sein, die früheren Befreier an ihre damals vermittelten demokratischen und freiheitlichen Werte zu erinnern. Tatsächlich haben sich die globalen Rahmenbedingungen von den 40er Jahren bis heute grundlegend verändert. Wenig verändert hat sich seitdem dagegen die dominante Rolle der USA in der Welt. Wurde diese vor 70 Jahren dafür eingesetzt, eine menschenverachtende Diktatur und einen mörderischen Krieg zu beenden, so geht es heute um Profaneres: um sicherheitspolitische Einflusssphären und um Profite. Dankbarkeit kann heute darin bestehen, die USA an ihre ursprünglichen demokratischen und freiheitlichen Werte in einer technisierten Welt zu erinnern.

6. Strategien

Wenn es zutrifft, dass das Internet „das freiheitlichste und effizienteste Informationsforum der Welt" ist, das „maßgeblich zur Entwicklung einer globalen Gemeinschaft" beiträgt, so wie dies der Deutsche Bundestag im Einsetzungsbeschluss einer Enquete zum Internet und zur digitalen Gesellschaft erklärt hat, so müssen hierfür auch rechtliche Strategien entwickelt werden.[29]

6.1 Völkerrecht

Nicht alle Aktivitäten der deutschen und europäischen Politik waren und sind nutzlos. Eine interessante, öffentlich kaum wahrgenommene Initiative ging insbesondere von den Regierungen Deutschlands und Brasiliens aus: Sie initiierten eine *Resolution bei den Vereinten Nationen* (UNO), die erstmals den digitalen Charakter der Gewährleistungen der allgemeinen Erklärung der Menschenrechte und des Paktes für politische und zivile Rechte herausstreicht.[30] Letztlich bleibt aber diese einstimmig beschlossene Resolution rechtlich unverbindlich und ohne

27 Biermann in Beckedahl/Meister (Fn. 1), S. 20 ff.
28 Ausführlich dazu Wolf (Fn. 19), JZ 2013, 1042 ff.
29 Zitiert nach Di Fabio, Ist das Grundrecht ein Ladenhüter?, www.faz.net 13.11.2013.
30 United Nations General Assembly 20.11.2013, The right to Privacy in the digital age, A/C.3/68/L.45/45/Rev.1; DANA 1/2014, 30 f.

weitere Wirkung, wenn diese nicht kurzfristig von weiteren völkerrechtlichen Initiativen fortgeführt wird.[31] Das Problem der UNO besteht darin, dass darin Überwacherstaaten ein wesentliches Wort mitzusprechen haben, so dass hierüber eine globale Rechtsentwicklung langfristig blockiert werden kann. Deshalb sind europäische Initiativen parallel dazu dringend nötig, bei denen Europa mit einzelnen Staaten oder Staatengruppen Bündnisse eingehen kann und sollte.

Trifft die Eingangsthese zu, nämlich dass die Aufgabe von politischer Macht und Profitmöglichkeit und die Etablierung von einklagbaren digitalen Grundrechten nur durch wirksamen Druck erreicht werden kann, so muss sich Deutschland und Europa vom Freund- und Partner-Denken befreien und genau das tun, was die US-Regierung schon immer tat: ihre Interessen vertreten – und zwar die Grundrechtsinteressen ihrer Bürgerinnen und Bürger. Dabei kommt der europäischen Position ein angenehmer Umstand zu Gute: Die *ökonomischen und politischen Interessen* sind weitgehend mit grundrechtlichen Interessen gleichgerichtet: Die Bindung der IT-Industrie an Grundrechtsstandards würde nicht nur rechtlich zu einer Gleichbehandlung der US-amerikanischen mit den europäischen Anbietern führen, sondern faktisch zu einer Verbesserung der Wettbewerbslage der Europäer, deren Angebote schon heute grundrechtlich gebunden sind. Es bedurfte erst eines Edward Snowden, dass dieser Umstand von der deutschen und europäischen Industrie akzeptiert und von der Politik wahrgenommen wurde. Dies führte – mit einer langen Zeitverzögerung – z. B. Anfang 2014 zu internen Konflikten im deutschen IT-Branchenverband Bitkom, in dem auch große US-Unternehmen vertreten sind.[32]

6.2 Schutz von Whistleblowern

Die wohl wichtigste Maßnahme Europas, um die Ernsthaftigkeit des grundrechtlichen Engagements zu demonstrieren, wäre eine einfache, weitgehend symbolisch, aber zugleich massiv wirkende Aktion: die Gewährung eines sicheren *Aufenthalts für Edward Snowden in Europa*. Hierdurch würde den USA vermittelt, dass der „Verrat" Snowdens kein Verrat an den demokratischen und freiheitlichen Werten, die Europa und die USA teilen, ist, sondern ein wichtiger Beitrag für einen dringend nötigen Läuterungs- und Selbstreinigungsprozess zum Wiedergewinn teilweise verloren gegangener und teilweise zum Gewinn noch nicht erkannter Werte – nämlich digitaler Grundrechte. Dieser hochpolitische symbolische Akt wäre zugleich ein Akt praktizierter Humanität für die Person von Snowden.[33]

Angesichts der immer restriktiveren Praxis in den USA bei der Pressefreiheit, der Informationsfreiheit und des Informantenschutzes muss eine Kampagne für digitale Grundrechte zwingend den verstärkten *Schutz von Whistleblowern* auf nationaler, europäischer und globaler Ebene beinhalten. Insofern besteht auch auf nationaler, deutscher Ebene hoher Nachholbedarf. Der fast einzigartig exemplarische Fall von Edward Snowden bietet den Diskussionen auf sämtlichen Ebenen eine ideale Vorlage.

6.3 Kooperationsvereinbarungen

Ein zentraler Ansatzpunkt zur Durchsetzung von Grundrechten sind sowohl für die USA wie für Europa die *Wirtschaftsbeziehungen*. Diese sollten nicht dazu

31 Dazu z. B. Hoffmann-Riem (Fn. 10), JZ 2014, 62 f.

32 NSA-Skandal entzweit den Bitkom, www.heise.de 19.2.2014.

33 Beckedahl in Beckedahl/Meister (Fn. 1), S. 18; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, ULD: Schutz unserer Daten durch Schutz von Edward Snowden, PM v. 18.7.2013.

genutzt werden, um im Sinne eines europäischen Werteimperialismus die eigenen Vorstellungen von digitalen Grundrechten durchzusetzen. Wohl aber können und müssen diese dazu genutzt werden, um einen grundrechtlichen Mindeststandard zu realisieren. Anderenfalls macht sich Europa durch Unterlassen an der Massenüberwachung mitschuldig. Bisher hatte Europa die USA hinsichtlich der informationellen Beziehungen gegenüber sämtlichen anderen Staaten der Welt mit dem Safe-Harbor-Abkommen privilegiert. Dieses erlaubt den personenbezogenen Datenaustausch mit den USA, ohne dass effektive Instrumente zur Durchsetzung von Datenschutz vorgesehen sind, weil man in Europa am informationstechnisch bedingten Aufschwung in den USA teilhaben wollte. Inzwischen hat sich dieses Blatt gewendet: Die Fortführung von Safe Harbor würde zu einer massiven ökonomischen Benachteiligung der eigenen Wirtschaft führen. Um einen klar erkennbaren Ausstieg aus Safe Harbor und zugleich einen sanften Einstieg der USA in den digitalen Grundrechtsschutz zu ermöglichen, wäre es förderlich, wenn Europa im Rahmen der Kündigung von Safe Harbor eine Roadmap von drei bis vier Jahren anvisieren würde, mit der sukzessiv realistisch zu erreichende Grundrechtsschutzmaßnahmen festgelegt werden, um diesen einen personenbezogenen Informationsaustausch von Europa aus zu ermöglichen. Im Endstadium muss Safe Harbor von seinem Sonderrechtsstatus befreit sein und grundsätzlich allen Unternehmen in unsicheren Drittstaaten zugänglich gemacht werden, so wie dies der britische Berichterstatter des NSA-Untersuchungsausschusses im Europaparlament Claude Moraes vorgeschlagen hat.[34]

Die Erörterungen über ein *Freihandelsabkommen* zwischen Europa und den USA müssen zumindest im Hinblick auf den informationellen Handel, der eine zunehmende Rolle spielt, ausgesetzt werden, bis von den USA ein Mindeststandard beim digitalen Grundrechtsschutz zugesichert wird. Dies ist nicht „Datennationalismus", so wie dies der US-Handelsvertreter Michael Froman behauptete, sondern Grundvoraussetzung für demokratische und freiheitliche Handelsbeziehungen.[35]

Eine vergleichbare Vorgehensweise sollte bei den *Kooperationsabkommen im Sicherheits- und im Finanzbereich* praktiziert werden. Die USA hat Europa einseitig Kooperationen beim Austausch von Fluggast- oder Bankdaten auferlegt, dem sog. Passenger Name Record- und dem sog. SWIFT-Abkommen. Der Datenaustausch mit den USA kann auch einen Ansatzpunkt darstellen für eine europäische rechtliche Überprüfung, da insofern unstreitig nationale bzw. europäische Grundrechte gelten.[36] Europa hat nun die Möglichkeit, gleichberechtigte Datenkooperationen unter Berücksichtigung des Grundrechtsschutzes zu verabreden. Auch insofern kann eine parlamentarisch vorgegebene Roadmap die Ernsthaftigkeit und die Realisierbarkeit des europäischen Bestrebens unterstreichen.

Bei dem Führen eines „transatlantischen Cyber Dialogs", wie dies der deutsche Außenminister Frank-Walter Steinmeier nannte, müssen zunächst die Praktiken hinterfragt werden: „Die Praktiken haben das Vertrauen in die USA bis zu einem Ausmaß geprüft, dass dies alle anderen gemeinsamen Aufgaben und Ziele gefährden könnte."[37] Hinsichtlich der Praktiken muss Transparenz durch die Beteiligten hergestellt werden; ein Rückgriff auf Whistleblower kann schon kurzfristig nicht genügen. In einem zweiten Schritt bedarf es der Entwicklung von

34 EU-Ausschuss will „Safe Harbor"-Abkommen kippen, futurezone.at 18.12.2013.
35 Ermert, US-Handelsvertreter warnt vor Datennationalismus, www.heise.de 19.2.2014.
36 Di Fabio, www.faz.net 13.11.2013 mit Verweis auf BVerfG, U. v. 24.4.2013 – 1 BvR 1215/07; Ewer/Thienel, Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals, NJW 2014, 35.
37 Braun, Das Gift des Misstrauens, SZ 1./2.3.2014, 5.

Normen, über die materielle Sicherungen, unabhängige Kontrollen und Rechtsschutz für die Betroffenen hergestellt wird.

6.4 Technische Infrastruktur

Um die informationstechnische Abhängigkeit von den USA abzubauen, müssen und können in Europa *eigenständige technische Strukturen* aufgebaut werden, wobei Großbritannien außen vor bleiben sollte, wenn dieses Land weiterhin nicht gewillt ist, den grundrechtlichen Weg mitzugehen. Unter dem Stichwort „Schengen-Routing" ist geplant, die territoriale Integrität des Internetverkehrs künftig besser zu gewährleisten.[38] Brasilien und die EU planen ein Datenkabel, um die NSA zu umgehen.[39] Die europäische IT-Industrie kann bisher einen Vorsprung vorweisen in Fragen des Datenschutzes und der Datensicherheit. Diesen gilt es weiter auszubauen durch entsprechende Forschungsförderung wie auch durch freiwillige Angebote und verpflichtende Implementierung. Ende-zu-Ende-Verschlüsselung, Identitätsmanagement, sicheres E-Government sind Stichworte, die inzwischen sogar Eingang in den schwarz-roten Koalitionsvertrag gefunden haben.[40]

6.5 Europäische Regelungen

Zum glaubwürdigen Aufbau einer europäischen Alternative gehört die Schaffung eines einheitlichen, hohen digitalen Schutzstandards in Europa.[41] Dieser muss aus einer Vielzahl von Bausteinen bestehen. Unabdingbar und zentral ist hierbei die geplante *Europäische Datenschutz-Grundverordnung*. Zweifellos darf hierbei die Geschwindigkeit der Verabschiedung nicht zu Lasten der Qualität gehen. Doch kann es dabei auch nicht um ein perfektes System gehen, wohl aber muss dieses das Grundgerüst für weitere Regelwerke zur Verbesserung des digitalen Grundrechtsschutzes sein.

Ein Baustein muss darin liegen, die eigenen nationalen Geheimdienststrukturen zu hinterfragen, die teilweise vergleichbare Tendenzen wie bei der NSA aufweisen. Im Interesse der Transparenz und des Rechtsschutzes müssen zusätzliche Restriktionen und rechtsstaatliche demokratische Sicherungen vorgesehen werden.[42] Es wäre nicht nur widersprüchlich und inkonsequent, sondern auch politisch gefährlich, diesen Aspekt beim Ziel der Realisierung eines digitalen Grundrechtsschutzes aus den Augen zu verlieren, zumal es insofern unheilige transatlantische Kooperationen gibt. Insofern sind einerseits nationale Regelungsansätze zu verfolgen, eine Rechtskontrolle über den Europäischen Gerichtshof für Menschenrechte anzustreben und letztlich auf EU-Ebene rechtsstaatliche Mindeststandards zu definieren.

Die *politische, rechtliche und wissenschaftliche Aufarbeitung* der globalen Massenüberwachung steht mit den Snowden-Enthüllungen erst am Anfang. Diese Aufarbeitung muss fortgeführt werden. Dies kann in der juristischen Aufarbeitung der Rechtsverletzungen von NSA und GCHQ und von deren Helfershelfer erfolgen – in Form von strafrechtlichen und parlamentarischen Ermittlungen oder z.B. in Form von grundrechtlichen Prüfungen, etwa durch den Europäi-

38 Kleinz, Die Telekom und der NSA-Skandal: Auf ins Schengen-Netz, www.heise.de 11.11.2013.
39 Cáceres, Leitung ohne Lauscher, SZ 24.2.2014, 1.
40 Abgedruckt in DANA 1/2014, 18 ff.
41 Masing, Herausforderungen des Datenschutzes, NJW 2013, 2310.
42 Heumann/Scott, Law and Policy in InternetSurveillance Programs: United States, Great Britain and Germany, 2013; Leisegang, Heumann/Scott in Beckedahl/Meister (Fn. 1), S. 133 ff., 149 ff.

schen Gerichtshof für Menschenrechte oder den Europäischen Gerichtshof.[43] Dabei sollten keine falschen Rücksichten genommen werden. Wenn ermittelte Sachverhalte Anklagen vor Strafgerichten oder diplomatische Sanktionen nötig machen, so ist es im Interesse des europäischen Grundrechtsschutzes, diese Schritte zu ergreifen.

7. Schlussbemerkung

Bei der Auseinandersetzung über die NSA-Überwachung ist von europäischer Seite bisher ein Aspekt zu kurz gekommen: Es müsste im wohlverstandenen Interesse der USA liegen, die Existenz und Durchsetzbarkeit digitaler Grundrechte zu akzeptieren. Mittel- und langfristig kann sich eine US-amerikanische Wirtschafts- und Sicherheitspolitik glaubwürdig von der Chinas und Russlands nur absetzen und letztlich durchsetzen, wenn sie ein glaubwürdiges Bekenntnis zu digitalen Grundrechten beinhaltet. Von Vorteil ist, dass die USA eine langjährige *bürgerrechtliche Tradition* vorweisen kann, die sich nicht nur auf Nichtregierungsorganisationen stützen muss, sondern auch auf eine stärker werdende Opposition, die aber bisher in Politik, Wissenschaft und Rechtsprechung Mindermeinung geblieben ist. Der Supreme Court ist bis heute in den USA eines der größten Hindernisse zur Entwicklung von digitalen Grundrechten.[44] Dies kann sich künftig ändern, zumal untere Instanzen teilweise schon grundrechtsfreundlicher entscheiden.[45] Förderlich ist sicher auch, wenn die Interessenkonflikte zwischen Sicherheitsadministration und IT-Wirtschaft in den USA zunehmen. Grundvoraussetzung für einen Wandel des Grundrechtsverständnisses in den USA ist, dass dieser nicht allein von außen – also von Europa – aufgezwungen, sondern auch aus „freien Stücken" gegangen wird und auf Einsicht beruht. Die USA unterstützen Demokratie- und Freiheitsbewegungen auf der ganzen Welt. Dies kann und sollte auch Europa tun – auch gegenüber den USA. Derartiges kann, sollte und darf nicht als Einmischung in fremde Angelegenheiten verstanden werden, sondern als transatlantischer Wertedialog.

Die globale Diskussion über digitale Grundrechte kann nur vorankommen, wenn Europa sich seiner eigenständigen Rolle bewusst wird und diese auch ausfüllt – ökonomisch wie politisch. Diese Rolle darf aber den Rest der Welt nicht ausblenden, muss vielmehr darauf aufbauend in eine globale grundrechtliche Charmekampagne einmünden. Zumindest mittelfristig sollte das von Anfang klar definierte Ziel darin bestehen, eine internationale digitale Menschenrechts-Charta aufzusetzen.

43 Ewer/Thienel (Fn. 36), NJW 2014, 30 ff.
44 Wolf (Fn. 19), JZ 2013, 1040; Arzt, Polizeiliche Überwachungsmaßnahmen in den USA, 2004.
45 Z. B. District Court of Columbia, Klayman et al. v. Obama et al., Dec. 16 2013.