Untersuchungsausschuss – 18. Wahlperiode
Deutscher Bundestag
Gutachten zur Rechtslage in den Vereinigten Staaten

Russell A. Miller Professor of Law
Washington & Lee University School of Law

I. Einführung

Der Untersuchungsausschuss befasst sich mit Fragen zu verschiedenen rechtlichen, politischen und gesellschaftlichen Aspekten, die mit den Enthüllungen der amerikanischen Geheimdienstpraktiken durch den ehemaligen NSA-Mitarbeiter Edward Snowden aufgeworfen wurden. Zu diesen Themen gehören das staatliche Interesse an nachrichtendienstlicher Informationsgewinnung durch Spionage, Überwachung und die Erfassung von Kommunikationsdaten, ferner die neuen und umfassenden Möglichkeiten des Einsatzes von Technologie, insbesondere für die Kommunikation, jedoch auch für zahlreiche andere Zwecke, von denen einige noch vor wenigen Jahren undenkbar schienen. Schließlich geht es noch um den Aspekt ernster Bedrohungen der Sicherheit, denen vor allem demokratische Staatswesen ausgesetzt sind. Spätestens seit den Terroranschlägen vom 11. September 2001 lassen sich solche Gefahren nicht mehr mit Schwarzseherei, ihre Schwere nicht mehr als im Sinne bestimmter Interessen erdachtes bloßes Schreckgespenst abtun.

Im Zeitalter der Globalisierung übersteigen diese Fragen – Beschaffung nachrichtendienstlich relevanter Informationen, Technologie und Sicherheit – naturgemäß den Horizont einer einzelnen Nation. Die Aufdeckung amerikanischer Geheimdienstpraktiken mit ihrer Erfassung wahrer Unmengen von Daten über Kommunikationsvorgänge – *deutscher Staatsbürger in Deutschland* –, selbst das Abhören des Mobiltelefons der Bundeskanzlerin, mahnt in aufrüttelnder Weise an die globale Natur dieser Angelegenheiten.

Um das Wesen der amerikanischen Geheimdienstpraktiken gründlicher zu erfassen und die Besorgnis vieler Deutscher über Snowdens Enthüllungen rechtlich einzuordnen, hat der Untersuchungsausschuss (im Folgenden „der Ausschuss“) mich gebeten, die Rechtslage in den Vereinigten Staaten in dieser Hinsicht zu erhellen. Dem komme ich in den folgenden vier Abschnitten nach. Abschnitt II befasst sich kurz mit der theoretischen Seite der Beziehung zwischen dem Staat als politischer Institution und nachrichtendienstlicher Informationsbeschaffung. Abschnitt III legt die institutionellen und rechtlichen Rahmenbedingungen für die US-amerikanischen Nachrichtendienste dar, ebenso ihre Geschichte, Infrastrukturen und rechtlichen Befugnisse sowie die (auch außergerichtliche) Kontrolle und die gesetzlichen Grenzen ihrer nachrichtendienstlichen Aktivitäten. Besonderes Augenmerk wird auf die National Security Agency (NSA) mit ihrer Erfassung von Daten über Kommunikationsvorgänge gerichtet. Abschnitt IV widmet sich dem Rechtsrahmen für den Datenschutz in den Vereinigten Staaten in Bezug auf

den privaten Sektor. Ich schließe in Abschnitt V mit einigen vergleichenden Betrachtungen der unterschiedlichen Weisen, mit denen die Themen und die Arbeit des Ausschusses rechtlich und politisch in Deutschland und den Vereinigten Staaten gesehen und aufgefasst werden.

II. Staatstheorie und nachrichtendienstliche Tätigkeiten

Fast alle Staatstheorien sehen in der Sicherheit nach außen und der Ordnung im Innern eine Grundlage für die Existenz des Staates.[1] Dies gilt, wenngleich mit grundlegenden Unterschieden der Erklärung und der Schlussfolgerungen, für die Auffassungen von Aristoteles,[2] Hobbes,[3] Locke,[4] und Rousseau.[5] Allgemein von einem „Gesellschaftsvertrag“[6] ausgehend fassen diese Philosophen die vergrößerte Macht des Staates als Notwendigkeit auf, um die für das Wohlergehen des Volkes nötige Ordnung und Schutz zu gewährleisten.[7] Einige Denker gingen sogar soweit zu behaupten, das Vermögen des Staates, für Ordnung und Schutz zu sorgen, sei notwendiger Bestandteil menschlichen Gedeihens.[8] Für Aristoteles trägt der Staat zur Sicherung eines „guten Lebens“ bei.[9] Für Hobbes war die Staatsmacht bekanntermaßen notwendig, um den Menschen aus dem „Naturzustand“ (und damit dem Kriegszustand) herauszuführen.[10] Nach Locke trägt der vom Staat gewährte Schutz dazu bei, das menschliche Potenzial auszuschöpfen, indem er die menschlichste aller Institutionen garantiert: das Eigentum.[11] Rousseau betonte die Fähigkeit des Staates, für die „kollektive Sicherheit“ zu sorgen.[12] Diese Aussagen beruhen auf einer Auffassung von Staat, die einer Pflicht zum Schutz der Gesellschaft vor Gewalt im Gemeinwesen und durch Übergriffe anderer Gesellschaften den Vorrang gibt.[13] Auf das amerikanische Verständnis von Regierung und Staatsmacht haben diese Ansichten nachhaltigen Einfluss gehabt.

Die deutsche *Staatslehre* beschäftigt sich weniger mit der Annahme eines Gesellschaftsvertrags als ausschließlicher Rechtfertigung öffentlicher Gewalt. Sie ist um die Erklärung von Staatsmacht aus anderen Begründungen bemüht, etwa der ideellen Behauptung einer vollständigen Entfaltung des menschlichen Geistes durch die Legitimierung des Staates oder der ideellen Behauptung der in das Gemeinwesen eingebetteten Individualität des Einzelnen. Die deutsche Staatstheorie sucht den Staat ferner auf der Grundlage der Umverteilungsmacht, die soziale Leistungen ermöglicht, zu legitimieren. Neben diesen Aussagen räumt die deutsche Staatslehre gleichwohl ein, dass die staatliche Schutzfunktion zu den Grundlagen der Ausübung öffentlicher Gewalt gehört.

Staaten nehmen ihre Schutzfunktion wahr, indem sie ordnende Kräfte im Innern (wie die Polizei) oder andererseits nach außen wirkende und militärische Kräfte bilden.[14] Ferner üben sie Spionagetätigkeiten aus, durch die sie an Informationen zu gelangen suchen.

Die wohl neutralste Charakterisierung dieser alten und allgemeinen Praxis besteht darin, sie als Produkt der Erkenntnis zu betrachten, dass Überraschung Asymmetrien schaffen kann, die die Macht des Staates in seinem Bemühen um Sicherheit und Ordnung vergrößern. Unter diesem Blickwinkel üben Staaten Spionage und nachrichtendienstliche Aufklärung aus zwei Gründen aus. Einerseits ermöglichen sie ihnen, vom Element der Überraschung in ihrem affirmativen Umgang mit anderen Mächten zu profitieren. Andererseits ermöglicht effiziente Informationsbeschaffung

einem Staat in einer defensiven Haltung, die Versuche anderer Mächte zu vereiteln, aus der Überraschung Vorteile zu ziehen.

Eine weitere weniger freundliche Charakterisierung der Spionage hat nicht so sehr mit der staatlichen Schutzfunktion, sondern mehr mit der Bedeutung zu tun, die der Informationsbeschaffung für das eigene Machtinteresse des Staates beikommt. Unter diesem Blickwinkel dient Spionage dem autonomen Interesse des Staates und seiner Institutionen, indem dieser mehr und mehr Informationen in seinen Besitz bringt. Besitzt die Floskel „Wissen ist Macht" einen realen Kern, dann beinhaltet diese Auffassung, dass die Geheimdienstaktivitäten des Staates zumindest teilweise seinem Streben nach Machtausweitung und sozialer Kontrolle dienen.[15] Im heutigen Informationszeitalter finden diese Bedenken besondere Resonanz.[16]

Diese Tradition, die eine nahezu unlösbare Verknüpfung von Staatsmacht und staatlicher Informationsbeschaffung umfasst, spiegelt sich in der völkerrechtlichen Ambivalenz des Themas wider.[17] Die ununterbrochene und allgemeine Spionagepraxis könnte vermuten lassen, dass nachrichtendienstliche Informationsbeschaffung ein im Völkergewohnheitsrecht verankertes und der Staatlichkeit eigenes Recht sei.[18] Dieser Annahme widerspricht jedoch die Tatsache, dass sich kaum belegen lässt, dass Staaten mit der Spionage einen *Rechtsanspruch* geltend machen. Eher ist geheimdienstliche Informationsbeschaffung wohl eine Frage von geopolitischem Realismus, von Machtprojektion und institutioneller Effizienz.[19] Im Völkerrecht gibt es keine explizite Billigung der Spionage. Auch gibt es kein ausdrückliches allgemeines Verbot staatlicher Spionagetätigkeiten. Die Charta der Vereinten Nationen beispielsweise verbietet sie nicht im konkreten Sinne.[20] Und Spionage ist auch nicht Gegenstand eindeutiger völkerstrafrechtlicher Verbote.[21] Dennoch mögen einzelne Elemente der Praxis der Informationsbeschaffung als völkerrechtswidrige Handlungen gelten. Beispielsweise kann Spionage in Form eines unbefugten Eindringens in das Hoheitsgebiet eines anderen Staates oder eines Eingriffs in seine politische Unabhängigkeit als Verletzung des Prinzips der Nichteinmischung betrachtet werden. Ferner könnten manche Aktivitäten der Informationsbeschaffung die Menschenrechtsverpflichtungen eines Staates betreffen, wenngleich der völkerrechtliche Grundsatz der Exterritorialität diese Möglichkeit erheblich einschränken würde.

III. US-Nachrichtendienste

Im Folgenden werden die amerikanischen Nachrichtendienste zusammenfassend dargestellt, ihre Geschichte, Infrastruktur, rechtlichen Befugnisse, die einschlägigen Kontrollmechanismen und die rechtlichen Beschränkungen von Geheimdienstpraktiken eingeschlossen.

A. Geschichte

Noch vor Verkündung der Verfassung von 1787, mit der die Vereinigten Staaten von Amerika gegründet wurden, spielten Spionage und Informationsbeschaffung in den Unabhängigkeitsbestrebungen der früheren englischen Kolonien in Nordamerika eine besondere Rolle. Seit je hat sich Amerika kräftig der Spionage bedient.

Die Geburt der Vereinigten Staaten verdankte sich in nicht geringem Maße der Entwicklung und Pflege eines effizienten Geheimdienstnetzes. Seine Geschichte mag sagenumwoben sein,[22] doch heißt es beispielsweise, dass John Honeyman die hessischen Söldner des Königs in die Irre führte und sie dem berühmten Überraschungsangriff von General George Washington in der Schlacht von Trenton am zweiten Weihnachtstag 1776 auslieferte.[23] Washington verfügte über zahlreiche Spione, darunter die Spionageorganisation *Culper Ring* in New York City.[24] Auch die Täuschungsmanöver und verdeckte Informationsbeschaffung eines James Rivington trugen wesentlich zum Erfolg der Truppen Washingtons in New York bei.[25] Washington musste mit seinen Spitzeln unentdeckt kommunizieren können; so wurden zahlreiche Sicherungsmaßnahmen ergriffen, um zu verhindern, dass Briefe, sollten sie vom Feind abgefangen worden sein, gelesen wurden. Dazu gehörte der Umgang mit „unsichtbarer" oder „weißer" Tinte.[26] Auch entwickelten sie Kodierungen für die Weitergabe von Nachrichten, insbesondere solcher, die von Spionen im Gebiet der Königstreuen an die Revolutionstruppen geschleust wurden.[27] Als Buchhändler schrieb Rivington geheime Botschaften und band sie zwischen Buchdeckel; die Bücher wurden dann von Agenten des Spionagenetzes gekauft und Washington übergeben.[28]

Nach dem Krieg würdigte Präsident Washington in seiner ersten Ansprache zur Lage der Nation den Erfolg dieses Nachrichtendienstes und bat den Kongress, einen Geheimdienstfonds einzurichten.[29] Dem kam der Kongress nach; bis Anfang des 19. Jahrhunderts wurden diese Mittel verwendet, um Operationen wie den Umsturzversuch in einer der nordafrikanischen Barbareskenstaaten oder die Bemühungen zu finanzieren, „Spanien zur Aufgabe der Gebiete in Florida zu bewegen."[30]

Im amerikanischen Bürgerkrieg unternahmen die Union ebenso wie die Konföderation umfassende Anstrengungen zur geheimdienstlichen Informationsbeschaffung. Die Union verfügte über ein organisiertes Netz, dessen einziger Zweck in Spionage und Gegenspionage bestand.[31] Die Konföderation operierte zwar weniger zentralisiert, war jedoch nachrichtendienstlich äußerst aktiv.[32] Beide schickten Agenten ins Ausland, um zu versuchen, fremde Regierungen zu beeinflussen.[33]

Auf dauerhafter, formeller Grundlage wurden Geheimdienstorganisationen in Amerika erstmals in den 1880er Jahren eingerichtet. Die Regierung schuf das *Office of Naval Intelligence* (ONI; „Marinenachrichtendienst") sowie die *Military Intelligence Division* (MID; „Heeresnachrichtendienst");[34] beide Einrichtungen machten sich während des spanisch-amerikanischen Krieges sehr um die amerikanische Sache verdient.[35] Durch Haushaltskürzungen nach dem Krieg wurde die Tätigkeit der Auslandsgeheimdienste eingeschränkt, selbst dann noch, als Europa in den Ersten Weltkrieg taumelte.[36] Im Ersten Weltkrieg blieben die stark beschnittenen amerikanischen Geheimdienste ohne nennenswerten Einfluss,[37] doch schuf die Armee einen speziellen Dienst innerhalb des MID für die Signalaufklärung.[38]

Das *Bureau of Investigation* im Justizministerium (aus dem später das *Federal Bureau of Investigation*, FBI, hervorging) wurde 1908 eingerichtet und war für die Gegenspionage im Inland zuständig.[39]

In der Zeit zwischen den Weltkriegen begannen die USA, ihre Signalaufklärung offensiver einzusetzen. Es wurden deutsche und japanische Nachrichten abgefangen und entschlüsselt, sodass die Amerikaner „Ende der 1930er und Anfang der 1940er Jahre eine höchst effektive Gegenspionage gegen Deutsche und Japaner sowie Sabotageakte in der westlichen Hemisphäre in Gang setzen konnten."[40] Gleichzeitig war der amerikanische Geheimdienstapparat bestrebt, eine Infiltration durch die Sowjetunion zu verhindern.[41] Diese Aktivitäten wurden vom *Office of the Coordinator of Information* (OCI) geleitet, das Präsident Franklin Roosevelt gegründet hatte.[42] Diese Stelle war für die Organisation der Beschaffung und Analyse der Informationen von Auslandsnachrichtendiensten zuständig.[43] Jedoch verhinderten krasse Fehler – und eine geschickte japanische Gegenspionage –, dass das OCI den japanischen Überraschungsangriff auf den amerikanischen Marinestützpunkt Pearl Harbor auf Hawaii vorausahnen und die Vereinigten Staaten warnen konnte.[44]

Dieses niederschmetternde Versagen – und die Tatsche, dass es unmittelbar zum Kriegseintritt der USA führte – bildet Ausgangs- und Bezugspunkt der heutigen US-amerikanischen Nachrichtendienste. Um die Konsequenzen aus diesem Scheitern zu ziehen und das Land in seinen Kriegsanstrengungen zu unterstützen, wurde das *Office of Strategic Services* (OSS) geschaffen.[45] In Kriegszeiten war es zuständig für die operative Beschaffung von Informationen in den USA.[46] Der Dienst trug wesentlich zum Sieg der Alliierten bei.[47] Ein Erfolg, der ebenso wie der sich abzeichnende Kalte Krieg für den Nachkriegs-„Geheimdienst-Boom" verantwortlich war. Der Kongress verabschiedete 1947 den *National Security Act*,[48] mit dem die *Central Intelligence Agency* (CIA) geschaffen wurde.[49] Die CIA ist weitgehend für die amerikanische Auslandsaufklärung zuständig.[50] Kurze Zeit später wurde die *National Security Agency* durch Präsidialerlass gegründet und mit der Signalaufklärung mandatiert.[51]

Als der Kalte Krieg heißer wurde und die Furcht vor sowjetischer Unterwanderung wuchs, wurden auch die Befugnisse der jungen amerikanischen Nachrichtendienste ausgeweitet.[52] Ihre Leistungen allerdings waren nicht immer lobenswert. So konnten die Sowjets die Welt mit ihrem erfolgreichen Raumfahrtprogramm überraschen, das von den amerikanischen Nachrichtendiensten anscheinend unentdeckt geblieben war.[53] Die Inlandsaufklärung hatte angeblich erbracht, dass Amerikaner aller

sozialer Schichten mit dem Kommunismus sympathisierten.[54] Der langjährige Chef und Gründungsdirektor des FBI weitete die Befugnisse des Dienstes aufs äußerste aus, insbesondere als der amerikanische Gesetzesvollzug sich mühte, sich auf das vom Obersten Gerichtshof mit beeinflusste neue freiheitliche und am verfassungsrechtlichen Schutz orientierte Klima einzustellen.[55] Das FBI führte Akten über die Bürger, und die Bevölkerung wurde angehalten, jeden zu melden, der eine Bedrohung des amerikanischen Way of Life hätte sein können.[56] Die so geschürte Hysterie führte zu schwarzen Listen und Hetzjagden, bis sich die Vorwürfe als unhaltbar erwiesen. Die Rolle der Nachrichtendienste in der antikommunistischen Angstwelt der McCarthy-Ära hatte in der nachfolgenden öffentlichen Debatte keinen besonderen Stellenwert.

Im Zuge der von Unruhen begleiteten sozialen Veränderungen im Nachkriegsamerika fiel auf die Nachrichtendienste ein gerechter Anteil des allgemein auf die Institutionen und den Staat gerichteten Argwohns. Dies war Teil eines Klimas, in dem man immer weniger Toleranz gegen Polizeiexzesse zeigte und eine zunehmende Abneigung gegen Geheimdienstoperationen im Innern hegte. Die CIA erlitt die Schmach der Schweinebucht. Gleichwohl diente sie als Spitze des Speers, den die Vereinigten Staaten noch gegen Südostasien schleudern sollte. Die USA versanken in Gewalt, Chaos und Attentaten, von den Nachrichtendiensten nicht eingedämmt – und in manchen Fällen gefördert.

In den 1960er und 1970er Jahren versuchten amerikanische Gerichte und Kongressabgeordnete, die verschiedenen Dienststellen der Nachrichtendienste zu kontrollieren. Gesetze wurden verabschiedet, um den Amerikanern ein gewisses Maß an Schutz der Privatsphäre zu gewährleisten. Der internationale Terrorismus wurde als stets wachsende Bedrohung erkannt. Auch ließ die neue Rolle als Supermacht die Erwartungen an die Auslandsnachrichtendienste wachsen, die sowohl Bedrohungen für die Vereinigten Staaten und die Verbündeten vorhersagen als auch die amerikanische Vormachtstellung bewahren sollten.

Die 1980er Jahre waren für die Geheimdienste desaströs. Die Nachrichtendienste konnten weder vor der iranischen Revolution noch vor der Besetzung der amerikanischen Botschaft in Teheran warnen bzw. die Vorbereitungen dazu aufdecken. Es folgte eine schlecht durchdachte Operation mit Waffenverkäufen an den Iran, mit denen die nicaraguanischen Contras finanziert werden sollten. Dies sollte zudem die Freilassung amerikanischer Geiseln im Libanon ermöglichen. Die Operation verstieß gegen amerikanisches Recht und ließ das Vertrauen der Öffentlichkeit in die Nachrichtendienste weiter schwinden.

Die in den 1990er Jahren zunehmenden Terrorakte beschäftigten den Kongress; er verlangte von mehreren Diensten Berichte darüber, wie effizient sie Informationen beschaffen und analysieren konnten.[57] Die dem Kongress vorgelegten Berichte zeichneten ein düsteres Bild: Die Nachrichtendienste waren zwar in der Lage, enorme Datenmengen zu sammeln, doch fehlten ihnen Mittel und Personal, die Informationen sinnvoll auszuwerten.[58] Es wurden verschiedene Pläne zur Reform der Geheimdienste entwickelt, doch waren es erst die Anschläge vom 11. September 2001, die Veränderungen erzwangen.[59]

Und die erfolgten nahezu abrupt. Das „Gesetz zur Stärkung und Einigung [US-]Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu blockieren", kurz USA PATRIOT Act, wurde bereits gut einen Monat nach dem 11. September vom Kongress verabschiedet.[60] Gedacht war es als Reaktion auf den bis dahin „erfolgreichsten" Angriff auf die Vereinigten Staaten. Eine Reihe von Punkten, ob sie nun zum Versagen bei der Aufdeckung oder Verhinderung der Anschläge beigetragen hatten oder nicht, sollte verändert werden: Das Gesetz erweiterte bzw. modifizierte die Informationsbeschaffung nach den bisherigen gesetzlichen Regelungen. So wurden beispielsweise die Befugnisse der Behörden für Fahndungen nach dem *Foreign Intelligence Surveillance Act* (FISA, etwa „Gesetz zur Überwachung in der Auslandsaufklärung") erheblich ausgeweitet.[62] Das Gesetz ermöglicht (ja fordert), dass die verschiedenen Gewalten im Staat die Ergebnisse von Ermittlungen einander weitergeben.[63] Ferner vergrößert es den Ermessensspielraum des *Foreign Intelligence Surveillance Court* (FISC, „Gericht für die Überwachung in der Auslandsaufklärung") hinsichtlich der Ausstellung von Anordnungen.[64] Auch die Möglichkeit von Aktenanforderungen wurden nach Umfang und Anwendungsbereichen erweitert. Die Nachrichtendienste können nun Einsicht in die Geschäftsbücher von Bibliotheken und Buchhandlungen erlangen.[65] Des Weiteren erlaubt das Gesetz einen ausgedehnteren Einsatz von Verbindungsdaten-Erfassungssystemen. Dazu gehört inzwischen jegliche elektronische Überwachung des E-Mail-Verkehrs sowie Daten zum Routing und Navigieren im Internet.[66] Schließlich werden die Möglichkeiten zur Überwachung mit „aufgeschobener Bekanntgabe" erweitert. Haftbefehle „mit aufgeschobener Bekanntgabe" können ausgestellt werden, wenn die Bekanntgabe negative Folgen „haben könnte", zum Beispiel die „Einschüchterung potenzieller Zeugen".[67] Der Aufschub ist auf bis zu neunzig Tage ausgedehnt worden.[68]

Der USA PATRIOT Act wurde mehrfach verlängert, erst jüngst mit Zustimmung von Präsident Obama.

Der PATRIOT Act blieb nicht die einzige Reaktion auf die Terroranschläge vom 11. September. Durch ein Dekret schuf Präsident Bush das *Office of Homeland Security* (OHS),[69] aus dem der *Homeland Security Act* 2002 das *Department of Homeland Security* (DHS, Heimatschutzministerium) machte, um die dem „Heimatschutz" dienenden Funktionen in einem einzigen Organ der Exekutive zusammenzuführen.[70] Mit dem *Intelligence Reform Act* wurde 2004 der *Director of National Intelligence* (DNI, „Direktor der nationalen Nachrichtendienste") geschaffen.[71] Das Heimatschutzministerium nimmt zahlreiche Aufgaben im Innern wahr, die ohne Bezug zur Informationsbeschaffung sind, verfügt jedoch auch über ein *Office of Intelligence and Analysis*, dass für die Erfassung und Analyse von Informationen über terroristische Aktivitäten zuständig ist.[72] In der Zuständigkeit des DNI liegt es, für den Präsidenten aktuelle kurze Zusammenfassungen der gewonnenen Informationen und Erkenntnisse zusammenzustellen und zu analysieren.[73]

B. Infrastruktur

Die heutigen amerikanischen Nachrichtendienste umfassen die sich zuweilen überschneidenden Aktivitäten einer Reihe von Institutionen der Exekutive, die unter lockerer Kontrolle des *Director of National Intelligence* (DNI) stehen.[74] Geschaffen wurde das Amt des DNI 2004 durch den

Intelligence Reform Act;[75] es wurde ein *Office of the Director of National Intelligence* (ODNI) eingerichtet, das den DNI bei der Wahrnehmung seiner Aufgaben unterstützt.[76] Der DNI ist die oberste Leitung der amerikanischen Nachrichtendienste.[77] Er oder sie wird vom Präsidenten ernannt und vom Senat bestätigt.[78] Der DNI ist der Chefberater des Präsidenten in den die nationale Sicherheit betreffenden nachrichtendienstlichen Angelegenheiten.[79] Als Leiter der Geheimdienste formuliert der DNI ferner „Ziele, Prioritäten und Leitlinien für die Nachrichtendienste, um die rechtzeitige und effiziente Beschaffung, Verarbeitung, Analyse und Verbreitung nachrichtendienstlich relevanter Informationen zu gewährleisten."[80] Der DNI ist dafür verantwortlich, dass diese Informationen mit den betreffenden Stellen ausgetauscht werden.[81]

Zu den für die Informationsbeschaffung zuständigen Institutionen gehören: die *Central Intelligence Agency* (CIA – über zwei ihrer vier Direktorate),[82] das Verteidigungsministerium (über eigenständige Stellen wie die *National Security Agency* [NSA][83] und die *Defense Intelligence Agency* [DIA][84] sowie die Nachrichtendienste der Teilstreitkräfte) und mehrere den Ministerien nachgeordnete Stellen (das *Federal Bureau of Investigation* [FBI] des Justizministeriums,[85], das Finanzministerium,[86] das Außenministerium,[87] das Energieministerium[88] und das neu geschaffene Heimatschutzministerium[89]).

Jede dieser Einrichtungen wurde durch eigenes Gesetz, Verordnung oder Dekret des Präsidenten errichtet. Ferner besitzt sie ein je spezielles Mandat, Zuständigkeits- oder Spezialgebiet.[90]

Aus mehreren Gründen werde ich nun den Schwerpunkt auf die *National Security Agency* (NSA) setzen. Ich unternehme hier nicht den Versuch, die Infrastruktur und rechtliche Grundlage sämtlicher US-amerikanischen Nachrichtendienste im einzelnen darzustellen. Zunächst kann die NSA hinsichtlich Gesetzesauftrag und Funktion innerhalb der Exekutive als in gewisser Weise repräsentativ für die anderen Elemente der amerikanischen Geheimdienstlandschaft gelten. Zweitens ist mir bewusst, dass sich die Untersuchungen des Ausschusses weitgehend auf die Enthüllungen um das Ausspähen von Kommunikationsdaten durch die NSA richten. Und drittens würde ein umfassenderer Überblick über die nachrichtendienstliche Infrastruktur einen weit größeren Aufwand erfordern, als durch die mir vom Ausschuss vorgelegten Fragen gerechtfertigt erscheint.[91]

Die NSA geht auf die *Signal Security Agency* (SSA) zurück, die geschaffen wurde, um die Kodes und Nachrichten der Achsenmächte abzufangen und zu entschlüsseln. Die SSA gehörte zu den vielen Stellen, die im Zweiten Weltkrieg der Informationsbeschaffung dienten. Die Vielfalt der auf diesem Gebiet tätigen Dienststellen wurde von der politischen und militärischen Führung der USA als ernstes Problem betrachtet.[93] Ein großer Teil der Informationen floss in mehrere Dienste, die jedoch unabhängig von einander operierten. Engstirnigkeit und Machtkämpfe zwischen diesen Stellen schufen eine Konkurrenzsituation – die Dienste hüteten die je eigenen Informationen eifersüchtig und tauschten sie nur widerwillig aus.[94] Dem abzuhelfen, wurde die SSA mit der *Army Security Agency* (ASA), dem Nachrichtendienst der US-Armee während des Zweiten Weltkrieges, zusammengelegt.[95] Die nun erweiterte ASA war dafür zuständig, das wachsende Geheimdienstsystem mit Informationen aus der Fernmeldeaufklärung zu versorgen.[96]

Der *National Security Act* von 1947 vermehrte die bürokratische Konfusion noch durch die Schaffung dreier neuer Aufklärungsdienste.[97] Jede dieser Stellen diente einer anderen Teilstreitkraft.[98] Die mangelnde Abstimmung blieb ein Problem.[99] Um Effizienz und Koordination zu verbessern, wurden die drei Dienste 1949 zusammengelegt und weiter umstrukturiert – es entstand die *Armed Forces Security Agency* (AFSA).[100] Als militärische Einrichtung betrachtete man die AFSA als weniger sensibel für die nachrichtendienstlichen Interessen ziviler Stellen[101] Zudem war die AFSA durch interne Machtkämpfe zwischen den drei früheren kryptologischen Diensten, die ihr nun unterstellt waren, beeinträchtigt.[102]

Präsident Truman schuf die NSA 1952 durch Präsidialerlass; ihr Auftrag: Beschaffung und Analyse von Informationen aus der Signal- und Fernmeldeaufklärung[103] Der neue Dienst sollte die entsprechenden Potenziale neu erschließen und ausschöpfen, indem er die Funktionen der Vorgängerstellen konzentrierte und zusammenführte.[104] Er sollte ferner Trumans Überzeugung Nachdruck verleihen, dass die Signalaufklärung und Kryptologie eine zivile, nicht bloß militärische Angelegenheit sei.[105] Zudem war er dazu gedacht, die anhaltenden Missstände bei der ASFA zu überwinden, auch die Missgunst zwischen den Stellen, die ihre Effizienz beeinträchtigte.[106] Vor allem hoffte Truman, die amerikanische Überlegenheit bei der Entschlüsselung und Aufklärung zu festigen und zu sichern, die das Land zum Ende des zweiten Weltkriegs errungen hatte.[107] Der Auftrag des Dienstes, später durch ein Dekret Präsident Reagans präzisiert und erweitert,[108] ist so umfassend wie uneindeutig. Aufgabe der NSA ist es, „Informationen aus der Signalaufklärung sowie Daten für die Zwecke der Auslandsnachrichtendienste und die Gegenspionage zu beschaffen (auch durch geheime Operationen), zu verarbeiten, zu erstellen und zu verbreiten, um die Erfüllung des nationalen Auftrags und der ministeriellen Aufgaben zu unterstützen."[109]

Die NSA ist nahezu ausschließlich die Domäne des Präsidenten. Als lobenswertes Beispiel ziviler und demokratischer Kontrolle des Militärs erklärt die Verfassung der Vereinigten Staaten den Präsidenten zum „Oberbefehlshaber der amerikanischen Streitkräfte."[110] Die Macht des Präsidenten in militärischen Angelegenheiten ist nahezu umfassend, mit zwei bemerkenswerten Ausnahmen: die Verfassung sieht vor, dass nur der Kongress befugt ist, den Militärhaushalt festzulegen und den Krieg zu erklären.[111] Bezeichnenderweise schuf Präsident Truman die NSA als Abteilung des Verteidigungsministeriums, damit sie in dieser eifersüchtig gehüteten Domäne der Exekutive operiere. Ihr Direktor muss, auch wenn sie weitgehend mit zivilem Personal besetzt ist, ein hochrangiger Militär sein.[112]

Heute stellt sich die NSA selbst mit folgenden zurückhaltenden und beruhigenden Formulierungen dar:

- Das „Leitbild" der NSA ist, „durch reaktionsfähige Präsenz und Netzwerkvorteile die globale kryptologische Vorherrschaft zu erlangen;[113]
- Zu den „Werten" der NSA gehört der „Schutz der nationalen Sicherheitsinteressen durch höchste Verhaltensstandards."[114]

Die NSA ist der größte, verschlossenste und wohl auch der teuerste der US-amerikanischen Nachrichtendienste. Man schätzt, dass sie rund 40.000 Mitarbeiter beschäftigt, auch wenn der stellvertretende Leiter einmal witzelte, ihre Zahl belaufe sich auf zwischen 30.000 und einer Milliarde.[115] Ihre Signalaufklärung und Informationsbeschaffung – angeblich nur auf das Ausland gerichtet – soll die Ausspähung von täglich 1,7 Milliarden Funk-, E-Mail-, Telefon-, Internet- und anderen Kommunikationen leisten, wovon nur ein Bruchteil nach siebzig verschiedenen Kategorien von Sicherheitsinteressen eingeordnet wird.[116]

C. Kontrolle

Die amerikanischen Nachrichtendienste, die NSA eingeschlossen, unterliegen der Kontrolle durch Exekutive und Legislative. Die Kontrolle durch die Exekutive obliegt dem *Intelligence Advisory Board* des Präsidenten, dem *Joint Intelligence Community Council*, dem *Office of the Inspector General* und dem *Office of Management and Budget*. Die Kontrolle durch die Legislative üben der Ständige Ausschuss für Geheimdienstliche Aufgaben und der Sonderausschuss des Senats für die Nachrichtendienste aus.

1. Kontrolle durch die Exekutive

Der *President's Intelligence Advisory Board* (PIAB) ist ein Beirat aus 16 Mitgliedern, „die keine Vollzeitbeschäftigten der Bundesregierung sind."[117] Diese werden vom Präsidenten bestellt und sind ohne Vergütung tätig.[118] Die Hauptaufgabe des PIAB besteht darin, „die Qualität, Quantität und Eignung der Informationsbeschaffung, der Analysen und Einschätzungen sowie der Gegenspionage- und anderen nachrichtendienstlichen Aktivitäten zu beurteilen."[119] Beim PIAB ist ein *Intelligence Oversight Board* (IOB, Kontrollbeirat) angesiedelt, der dafür zuständig ist, den Präsidenten und den Justizminister über jegliche Maßnahmen der Informationsbeschaffung zu unterrichten, die „gesetzwidrig sein oder gegen ein Dekret oder eine Direktive des Präsidenten verstoßen könnten."[120] Der PIAB übermittelt Bedenken dem DNI, in dessen Verantwortung es wiederum liegt, die entsprechenden Änderungen zu veranlassen.[121] Aufgrund der Geheimhaltungsstufe der dem IOB vorliegenden Angelegenheiten gibt es kaum Informationen über seine Aktivitäten. Dennoch richtet die gemeinnützige Organisation *Electronic Privacy Information Center* 2005 (und erneut 2009) eine Eingabe nach dem Informationsfreiheitsgesetz an das FBI, die sich auf eine Reihe von Fällen elektronischer Überwachung zwischen 2002 und 2004 bezog. Aus der veröffentlichten Dokumentation geht hervor, dass es beim IOB ein Beratungsverfahren gibt, das sich mit der gründlichen rechtlichen Kontrolle von Geheimdienstoperationen befasst.[122] Daraus ist jedoch nicht ersichtlich, welche Disziplinarmaßnahmen der IOB empfehlen kann.

Mit dem *Intelligence Reform and Terrorism Prevention Act* von 2004 wurde der *Joint Intelligence Community Council* (JICC) geschaffen.[123] Aufgabe des JICC ist es, den DNI (der den Vorsitz des JICC innehat) bei der „Kontrolle und Auswertung der Leistungen der Nachrichtendienste" zu unterstützen.[124] Der JICC nimmt hauptsächlich Haushalts- und beratende Aufgaben wahr; die

Bandbreite der Angelegenheiten, die er untersuchen kann, richtet sich jedoch nach den Vorstellungen des DNI, da er jedes ihm geeignet erscheinende Thema beim Rat einbringen kann.[125] Gleichzeitig mit dem Rat des DNI können die Mitglieder des JICC dem Präsidenten ihre abweichenden oder bestätigenden Auffassungen unterbreiten.[126] Mitglieder des JICC können auch den Kongress beraten.[127] Da dem JICC die Außen-, Verteidigungs-, Energie-, Heimatschutz- und Finanzminister sowie der DNI und der Justizminister angehören,[128] liegt es nahe, dass der JICC die Beiträge dieser übergeordneten Behörden zu den Nachrichtendiensten lediglich formalisiert.

In den letzten Jahren war der Kongress bestrebt, die Kontrolle der US-amerikanischen Nachrichtendienste durch die Exekutive zu verstärken und auszuweiten. So verabschiedete der Kongress beispielsweise 2004 den *Intelligence Reform and Terrorism Prevention Act.*[129] Mit dem Gesetz wurde das Amt des Beauftragten für den Schutz der Bürgerrechte (Civil Liberties Protection Officer, CLPO) eingerichtet, der dem *Office of the Director of National Intelligence* zugewiesen ist.[130] Nach dem Gesetz obliegen dem CLPO, der vom DNI bestellt wird, verschiedene mit der Wahrung des Rechts auf Achtung der Privatsphäre verbundene Aufgaben. In der Verantwortung des CLPO liegt es, dafür Sorge zu tragen, dass der Schutz der Privatsphäre bei allen nach dem *National Intelligence Program* ergriffenen Maßnahmen beachtet wird.[131] Der CLPO ist ferner dafür zuständig zu gewährleisten, dass der *Director of National Intelligence* alle nach Verfassungs-, Gesetzes- und Gewohnheitsrecht erlassenen Regelungen zum Schutz der Privatsphäre einhält.[132]

Der Datenschutz- und Bürgerrechtskontrollbeirat (Privacy and Civil Liberties Oversight Board) wurde ebenfalls mit dem Gesetz von 2004 eingerichtet.[133] Er soll ähnliche Funktionen wie der CLPO wahrnehmen, hat also eine beratende Rolle. Während der CLPO Mitglied des ODNI ist und dem DNI Rechenschaft ablegt, berät der Kontrollbeirat „den Präsidenten und die Ministerien, Behörden und anderen Einrichtungen der Exekutive."[134] Er wurde gebildet, weil der Kongress das Potenzial für gefährliche Übergriffe der Regierung ausmachte und den Eindruck hatte, dieses Risiko erfordere „ein verbessertes System gegenseitiger Kontrolle, um die kostbaren Freiheiten zu schützen, die für unser Leben wesentlich sind."[135] Der Beirat wurde aus der Erkenntnis eingerichtet, dass „die Frage, ob Sicherheit oder Freiheit schwerer wiege, falsch gestellt ist, denn nichts gefährdet die Freiheiten in Amerika mehr als der Erfolg eines terroristischen Anschlags in der Heimat. Unsere Geschichte lehrt uns, dass Unsicherheit die Freiheit bedroht. Doch wenn unsere Freiheiten eingeschränkt werden, gehen wir der Werte verlustig, für deren Verteidigung wir kämpfen."[136]

Über seine Beratungsfunktion hinaus überprüft der Beirat geplante Vorschriften darauf, ob sie die Bürgerrechte und den Schutz der Privatsphäre achten.[137] Der Beirat kann ferner feststellen, dass ein Ministerium einen Datenschutz- oder Bürgerrechtsbeauftragten benötigt, falls dieses Ministerium nicht bereits gesetzlich dazu verpflichtet ist.[138] Der Beirat erhält und prüft Berichte, spricht den Kontrollbeauftragten Empfehlungen aus und ist wiederum den zuständigen Kongressausschüssen rechenschaftspflichtig.[139]

Historisch bedingt ist die Kontrolle durch die Exekutive immer von größter Rücksicht gegen die Nachrichtendienste geprägt gewesen. Im amerikanischen System der Gewaltenteilung, das zum Teil darauf beruht, dass jede Teilgewalt ihre eigenen Interessen offensiv verfolgt, um die nötigen Kontrollen und Gegenkontrollen zu realisieren, zeigen die einzelnen Teilgewalten nur geringe

Neigung zur Bescheidenheit und Zurückhaltung.[140] Insbesondere das Machtgleichgewicht zwischen Kongress und Präsident führt zu der Tendenz, dass die jeweiligen Teilgewalten die Möglichkeiten ihrer Befugnisse ausreizen.[141] Daher besitzt die Exekutive eine besondere Handlungsbereitschaft. Präsidenten befürchten häufig den Verfall ihrer Macht, wenn sie von ihr keinen Gebrauch machen; insbesondere fürchten sie, dass der Kongress ein Nichttätigwerden als Nachgiebigkeit auslegt und die nicht ausgeübte Macht für sich selbst beansprucht. Diese Dynamik gilt genauso für die nachrichtendienstlichen Tätigkeiten der Exekutive. Eine Konsequenz daraus ist, dass die Kontrolle durch die Exekutive wenig unternimmt, um die Aktivitäten der Nachrichtendienste einzuschränken.

Gleichwohl sorgt das politische System der USA dafür, dass sich despotische Neigungen nicht auszahlen.[142] Amtsinhaber, die eine weitere Amtszeit anstreben, sind sich durchaus der Macht der Wählerschaft bewusst; wer unpopuläre Entscheidungen trifft, insbesondere bei Fragen, die für Freiheit und Sicherheit wichtig sind und polarisieren können, hat einen steinigen Weg zur Wiederwahl vor sich.[143] Daher wird ein Präsident, der einen Wandel der nationalen Stimmungslage kommen sieht, bestrebt sein, daraus seinen Nutzen zu ziehen.[144] Die Rockefeller-Kommission ist ein Beispiel dafür, wie diese politischen Trends sich auf die Nachrichtendienste auswirken können. Präsident Gerald Ford, der sich der Aufmerksamkeit, die der CIA durch die Medien zuteil wurde, ebenso bewusst war wie der genauen Prüfung, die ihr der Church-Ausschuss noch angedeihen lassen würde, hatte die Kommission als Ermittlungsorgan eingerichtet.[145] Sie legte, bevor sie durch verschiedene Kongressausschüsse ersetzt wurde, einen Bericht vor.[146] Darin schreibt die Kommission über ihre Erkenntnisse zu Folgendem: „Abfangen von Post; Koordination der Nachrichtendienste; 'Operation CHAOS' (Beschaffung von Informationen über Dissidenten); Schutz der Behörde gegen drohende Gewalt; andere Ermittlungen des Sicherheitsbüros; Beteiligung der CIA an unangemessen Aktivitäten für das Weiße Haus (einschließlich Watergate); Aktivitäten des *Directorate of Operations* im Innern; Aktivitäten des *Directorate of Science and Technology* im Innern; Beziehungen der CIA zu anderen Bundes-, bundesstaatlichen und kommunalen Behöšrden; Register und Akten zu amerikanischen Bürgern sowie Behauptungen im Zusammenhang mit dem Attentat auf Präsident Kennedy.“[147]

2. *Kontrolle durch die Legislative*

Auch dem Kongress kommt bei der Kontrolle der Nachrichtendienste besondere Bedeutung zu. Beispielsweise kann sich der Ständige Sonderausschuss des Repräsentantenhauses für die Nachrichtendienste an Ermittlungen der Dienststellen beteiligen, solange diese Ermittlungen vom Vorsitz und dem Mitglied der Minderheitspartei mit der längsten Amtszeit gebilligt wurden.[148] Der Ausschuss kann sich mit Verschlusssachen befassen, doch sind seinen Mitgliedern darin, wie sie das Material außerhalb der nichtöffentlichen Sitzungen erörtern können, Grenzen auferlegt.[149] Der Sonderausschuss verfügt über einen Unterausschuss, der sich speziell der Kontrolle widmet.[150]

Der Sonderausschuss des US-Senats für die Nachrichtendienste (SSCI) besitzt ein ähnliches Mandat. Er wurde eingerichtet, „um die nachrichtendienstlichen Tätigkeiten und Programme der

US-Regierung zu überwachen und fortlaufend zu untersuchen, dem Senat geeignete Gesetzentwürfe zu unterbreiten, dem Senat über diese Aktivitäten und Programme Rechenschaft abzulegen und als Organ der Legislative die nachrichtendienstlichen Tätigkeiten der Vereinigten Staaten wachsam zu beaufsichtigen, um zu gewährleisten, dass diese Aktivitäten der Verfassung und den Gesetzen der Vereinigten Staaten entsprechen."[151] Er veranstaltet Anhörungen zu nachrichtendienstlichen Angelegenheiten, nimmt Funktionen bezüglich Haushalt und Mittelzuweisungen wahr und führt ferner Prüfungen und Ermittlungen zu Programmen der nachrichtendienstlichen Informationsbeschaffung durch.[152] Der Senatsausschuss ist ferner in Verschlusssachen eingeweiht, was dem Ziel der Kontrolle durch den Kongress zugute kommen soll.[153] Eines der ersten bedeutenderen Vorhaben des SSCI war eine sorgfältige Einschätzung vor der endgültigen Abstimmung, nachdem der *Foreign Intelligence Surveillance Act* (FISA) als Gesetzentwurf in den Kongress eingebracht worden war.[154] Dem SSCI oblag ferner der Entwurf des Berichts des Sonderausschusses über die nachrichtendienstliche Einschätzung der Vorkriegssituation im Irak.[155] Der am 9. Juni 2004 vorgelegte Bericht kam zu dem Schluss, dass diese Einschätzung der irakischen Massenvernichtungswaffen „entweder die Fähigkeiten [des Iraks] überbewertete oder durch die zugrundeliegenden nachrichtendienstlichen Angaben nicht gestützt wurde. Eine Reihe von Fehlern, insbesondere analytisch-handwerklicher Art, führte zu einer falschen Darstellung der Informationen."[156] Ein späterer Phase II-Bericht deutete an, dass die Exekutive die Informationen gezielt falsch dargestellt haben könnte, um Mutmaßungen als Gewissheit erscheinen zu lassen.[157]

Möglicherweise wegen des von ihm als klar empfundenen Mandats der Bevölkerung, dem Sicherheitsbedürfnis der Amerikaner größeren Stellenwert einzuräumen, hat der Kongress die Arbeit der Nachrichtendienste nicht streng beaufsichtigt.[158] Die Kontrolle durch den Kongress muss weitgehend als dienstwillig, wenn nicht als ausgesprochen unterwürfig angesehen werden.[159]

3. Church Committee

Es gibt einige wenige bemerkenswerte Fälle, in denen es der Kongress für notwendig hielt, in die Arbeit der Nachrichtendienste einzugreifen. Davon war keiner dramatischer und wichtiger als die Arbeit des „Sonderausschusses des US-Senats zur Untersuchung des Regierungshandelns mit Bezug zu Aktivitäten der Nachrichtendienste" (1975-1976).[160] Der Ausschuss wurde nach dem Nachnamen seines Vorsitzenden benannt, Senator Frank Church aus Idaho. Der Church-Ausschuss sollte 1975 tätig werden, nachdem die *New York Times* enthüllt hatte, dass Zehntausende Amerikaner von der CIA bespitzelt wurden, darunter Kongressabgeordnete, oft aufgrund direkter Anordnungen der Nixon-Administration. Die Bespitzelung zielte auf die Überwachung und Untergrabung der Antikriegsbewegung, insbesondere ihrer Vertreter in der Studentenbewegung 1968.[161] Leicht untertrieben bezeichnete die *New York Times* die in den USA begangenen Einbrüche und Lauschangriffe der CIA als „massive Ungesetzlichkeit" und einen klaren Verstoß gegen die CIA-Gründungsurkunde von 1947, die ihr eine Beteiligung an Operationen im Innern verbietet.[162]

Die offensive und peinlich genaue Untersuchung der amerikanischen Nachrichtendienste durch den Church-Ausschuss ist nach wie vor „die umfassendste und sorgfältigste kritische Studie zur Schattenwelt der US-Geheimdienste, die je unternommen wurde."[163] Etwas Vergleichbares gab es

seitdem nicht mehr, nicht in den Vereinigten Staaten und wohl auch nicht in irgendeinem anderen Land. Der Church-Ausschuss hatte die Aufgabe, die nachrichtendienstlichen Aktivitäten im Innern zu überprüfen, um festzustellen, ob sie gesetzeskonform waren, insbesondere die verfassungsmäßigen Grenzen der Exekutive und den durch die Verfassung verbrieften Schutz der Freiheit des Einzelnen achteten. Die Ermittlungen erstreckten sich auf die Präsidentschaften beider Parteien, bis zurück zur Kennedy-Administration. Zum bescheidenen Projekt des Ausschusses gehörte: jeden Winkel des verschlossenen amerikanischen Geheimdienstreiches über mehr als ein Vierteljahrhundert auszuleuchten (CIA, FBI, Defense Intelligence Agency und NSA eingeschossen, neben anderen Institutionen auch die Bundessteuerverwaltung), und dies gegen die Ablehnung durch Präsidenten und Behörden.

Der Church-Ausschuss bewältigte eine 18monatige Untersuchung, zu der Folgendes gehörte: mehr als hundert Anhörungen, hunderte weiterer Anhörungen vor Unterausschüssen, zahllose Zeugenvernehmungen, die Prüfung von fast einer Tonne Unterlagen (vorgelegt nach mit Strafandrohung versehenen Anweisungen) sowie die Veröffentlichung etlicher Berichte. Es handelte sich um die nach den gegebenen Umständen umfassendste Untersuchung der US-Nachrichtendienste; sie schloss den gesamten Zeitraum seit Beginn des Kalten Krieges ein. Die Arbeit des Church-Ausschusses fand ihren Abschluss 1976 mit der Veröffentlichung eines 14-bändigen schockierenden Berichts.

Darin wurden Jahrzehnte missbräuchlich eingesetzter Überwachungen dokumentiert (Infiltration eingeschlossen), die über eine die nationale Sicherheit betreffende Informationsbeschaffung hinausgingen und bis zur Erfassung persönlicher und politischer Ansichten reichten. Häufig genug sollten die Operationen ihre Ziele schädigen, vernichten oder in Misskredit bringen. Es wurde belegt, dass diese Aktivitäten dem politischen Vorteil von Präsidenten dienen sollten. Vor allem schien der Hunger nach Inlandsaufklärung stetig zu wachsen. Es ist schwierig, bestimmte Einzelheiten aus einem solch umfangreichen Vorhaben hervorzuheben, das in mehr als 50.000 Seiten an Berichten, Protokollen von Zeugenaussagen, anderen Dokumenten und Kommentaren mündete. Das Folgende mag einen Eindruck von den weitreichenden und beunruhigenden Erkenntnissen des Ausschusses vermitteln. Zunächst waren zahlreiche US-Amerikaner (gewöhnliche Bürger ebenso wie prominente – darunter Präsident Richard Nixon und Senator Frank Church) ins Visier der Überwachung geraten, die den Zugriff auf Post und telegrafische Nachrichten, Telefonüberwachung und den Einsatz von Agenten umfasste. Diese weit verbreiteten und in die Privatsphäre eingreifenden Überwachungsmaßnahmen hatten Bezeichnungen wie COINTELPRO oder „Houston Plan“. Zweitens war das gesamte politische Spektrum von diesem Missbrauch betroffen, von der Frauenbewegung bis zur neokonservativen John Birch Society. Drittens und typisch für die Vereinigten Staaten spielt die Rassenzugehörigkeit eine einzigartig und krankhaft zentrale Rolle. Der Church-Ausschuss deckte auf, dass eine der ältesten und einflussreichsten schwarzen Bürgerrechtsorganisationen der USA, die NAACP, über mehr als drei Jahrzehnte ein spezielles Ziel der intensiven Überwachung war. Groteskerweise dokumentieren die Berichte des Ausschusses auch, dass selbst Martin Luther King von den Nachrichtendiensten verfolgt wurde. Der „verdeckte Krieg“ zur Diskreditierung des Führers der schwarzen Bürgerrechtsbewegung erreichte seinen Tiefpunkt mit den wiederholten Versuchen, King mit

Drohungen, die Aufzeichnungen aus seinen verwanzten Hotelzimmern zu veröffentlichen, zum Selbstmord zu zwingen.

Vor dem aktuellen Hintergrund gibt es gute Gründe, sich hier etwas näher mit dem 165-seitigen fünften Bericht des Church-Ausschusses zu befassen („The National Security Agency and Fourth Amendment Rights"). Schon der Titel kommt einer Aufdeckung gleich: Bis zu den Ermittlungen des Ausschusses war die NSA den Amerikanern nahezu unbekannt, sodass ihr Akronym bei den amerikanischen Nachrichtendiensten in der Zeit des Kalten Krieges witzelnd als „No Such Agency" gelesen wurde. Um die Risiken, die diese verschlossene Institution für den Genuss der Freiheiten und Privatsphäre birgt, vollständig zu erfassen, ist der Bericht des Church-Ausschusses über die NSA unverzichtbar. Er bietet wertvolle Erkenntnisse über das Gesetz zur Auslandsaufklärung und Spionageabwehr (FISA), das, wie weiter unten erörtert, hier der maßgebliche Rechtsakt zu den US-Geheimdiensten ist. Dieses Regelwerk hatte sich in den Erörterungen und Anhörungen, die in den Bericht des Church-Ausschusses über die NSA mündeten, bereits angekündigt. Hinsichtlich der Risiken bezeichnete der Ausschuss die NSA als den geheimsten und verschlossensten aller Geheimdienste: Es gebe kein gesetzliches Mandat, und ihre Gründungsurkunde bestehe aus Dekreten, die keine klare Definition der „technischen und nachrichtendienstlich relevanten Informationen" enthielten, zu deren Beschaffung die NSA eingerichtet wurde. Dem Church-Ausschuss zufolge hatten Vertreter der NSA dem Kongress noch nie Rechenschaft über die Aktivitäten des Dienstes abgelegt. In Worten, die heute unangenehm nachklingen, kam Senator Church zu dem Schluss, dass die NSA ein enormes Potenzial für Missbrauch birgt:

> Die NSA ist in der Lage, die private Kommunikation amerikanischer Bürger zu überwachen, ohne etwas zu „verwanzen" oder „anzuzapfen". Das Abfangen internationaler Kommunikationssignale gehört zur Aufgabe der NSA; und dank moderner Technologie bewältigt sie diese sehr gut. Die Gefahr liegt in der Fähigkeit der NSA, diese eindrucksvolle Technologie gegen den Nachrichtenverkehr im Inland zu richten … … eine frühere Regierung und ein früherer NSA-Direktor haben sogar befürwortet, dieses Potenzial gegen US-Bürger für inlandsnachrichtendienstliche Zwecke einzusetzen.

Der Ausschuss stellte fest, dass derartige Exzesse tatsächlich vorgekommen waren. Beraten vom Harvard-Juristen Philipp Heymann drang der Church-Ausschuss auf gesetzgeberische Maßnahmen, um den Schutz der Freiheitsrechte zu gewährleisten. Professor Heymann riet dem Ausschuss nachdrücklich zu befürworten,

> dass der Kongress ein Gesetz verabschiedet, das geeignete Standards festlegt und richterliche Anordnungen [für NSA-Aktivitäten] vorsieht … Der Kongress muss für die Regelungen sorgen, die Gerichte für Durchführung und Anwendung.

Von den Berichten des Church-Ausschusses gedrängt, tat der Kongress genau dies.

Dem Church-Ausschuss kommt das Verdienst zu, eine Reihe von Reformen angestoßen zu haben, die zu gesetzlichen Beschränkungen der Geheimdienstaktivitäten und der Pflicht zur ständigen Kontrolle des Geheimdienstapparates durch den Kongress geführt haben. Wenngleich von den strammsten Kalten Kriegern verteufelt, sollten solche Reformen für den Schutz und für Befugnisse der amerikanischen Nachrichtendienste sorgen, indem sie diese mit soliden gesetzlichen Grundlagen, klaren Regelungen für ihre Aktivitäten und der Versicherung versahen, dass sie keiner politischen Zweckdienlichkeit geopfert werden. Ein Beispiel für Letzteres ist der Hughes-Ryan-Act; danach muss das Weiße Haus alle verdeckten Aktionen im Ausland schriftlich genehmigen, sodass der Präsident die Schuld für stümperhafte Geheimprogramme nicht mehr skrupellosen und unverantwortlichen Geheimdienstleuten anlasten kann.

Doch es ist die erwähnte Reform – mit ihren Standards, richterlichen Anordnungen und der Kontrolle durch den Kongress –, die sich am nachhaltigsten auf die US-amerikanischen Geheimdienstoperationen auswirkte. Aus den Ermittlungen des Church-Ausschusses sind mehrere neue diesen Zielen verpflichtete Gesetzesprogramme hervorgegangen; das bedeutendste ist der *Foreign Intelligence Surveillance Act* (FISA) von 1978. Es war eben die von Professor Heymann in seinen Ausführungen bei den Anhörungen vor dem Church-Ausschuss befürwortete Reform. Und dieses Gesetz ist der bedeutendste Teil des für die Snowden-Affäre relevanten Rechtsrahmens.

Wie ich weiter unten etwas eingehender darstellen werde, realisierte der *Foreign Intelligence Surveillance Act* eben genau das, worauf der Church-Ausschuss gehofft hatte. Zunächst legte das Gesetz Standards für die Überwachung durch amerikanische Nachrichtendienste fest. Zweitens schuf es ein der Durchsetzung dieser Standards dienendes Geheimgericht, den *Foreign Intelligence Surveillance Court* (FISC). Drittens sah es die ständige Kontrolle des Kongresses über diese Operationen vor. Das Regelwerk erstreckt sich über eine große Bandbreite des Regierungshandelns in Geheimdienstangelegenheiten, von der elektronischen Überwachung und Leibesvisitationen über den Einsatz von Geräten zur Erfassung von Telefonnummern und anderen elektronischen „Adressen“ bis hin zum Zugriff auf Geschäftsbücher für nachrichtendienstliche Zwecke. Wie der Gesetzestitel zeigt, sollen die Standards und Verfahren auf die auslandsnachrichtendienstliche Informationsbeschaffung angewendet werden, also von Informationen, die außerhalb der Vereinigten Staaten durch vom Gesetz als „Nicht-US-Bürger“ bezeichnete Personen übermittelt werden.

D. Rechtliche Befugnis zur Beschaffung von Kommunikationsdaten

Im Präsidialerlass, mit dem die NSA geschaffen wurde, heißt es, dass die Behöšrde „die gegen andere Staaten gerichtete nachrichtendienstliche Informationsbeschaffung organisieren und kontrollieren“ soll.[164] Das Mandat der NSA besteht aus zwei Teilen: einer nachrichtendienstlichen Spezialisierung auf die Erfassung und Analyse von „Signalen“ und einer territorialen oder jurisdiktionellen Ausrichtung auf die Informationsbeschaffung außerhalb der Vereinigten Staaten.

Der Auftrag der NSA bezieht sich auf die Signalaufklärung (SIGINT) und nicht auf die geheimdienstliche Nachrichtengewinnung durch Agenten (HUMINT). Dabei wird Fernmelde- und elektronische Aufklärung definiert als „sämtliche Verfahren und Methoden, die beim Abfangen von

Nachrichten und der Gewinnung von Informationen aus solchen Nachrichten durch andere als die vorgesehenen Empfänger eingesetzt werden."[165] Die Vollmachten der NSA wurden durch das Dekret 12.333 bestätigt,[166] das Präsident Ronald Reagan am 4. Dezember 1981 erließ.[167] Dem Dekret Reagans zufolge ist es Aufgabe der NSA, „Informationen aus der Signalaufklärung sowie Daten für die Zwecke der Auslandsnachrichtendienste und die Gegenspionage zu beschaffen (auch durch geheime Operationen), zu verarbeiten, zu erstellen und zu verbreiten, um die Erfüllung des nationalen Auftrags und der ministeriellen Aufgaben zu unterstützen."[109] Um diese Arbeit zu unterstützen, erhält die NSA die Befugnis, „Aktivitäten der administrativen und technischen Unterstützung innerhalb und außerhalb der Vereinigten Staaten durchzuführen, wie es falsche Identitäten erforderlich machen."[169]

Das novellierte und kodifizierte Dekret betont, dass die NSA für SIGINT- und keine anderen als SIGINT-Aktivitäten zuständig ist.[170] Es räumt jedoch die Möglichkeit ein, dass zur vollständigen Erfüllung dieses Auftrags eine Agententätigkeit notwendig sein kann. Es wird sogar, wenn auch nicht ausdrücklich, erklärt, dass die NSA ermächtigt ist, ihre Mitarbeiter an andere staatliche Institutionen für unterstützende Tätigkeiten abzustellen, um diesen Agenten falsche Identitäten zu verschaffen.[171] Dies in Verbindung mit dem zugegebenermaßen verdeckten Modus der NSA-Informationsbeschaffung errichtet und legitimiert ein umfassendes Mandat für die Spionage über den SIGINT-Auftrag der Behörde hinaus.

Der Auftrag der NSA richtet sich auf die Auslandssignalaufklärung. Die gültige Fassung des *National Security Act* von 1947 definiert als Erkenntnisse aus der Auslandsaufklärung „Informationen in Bezug auf Fähigkeiten, Absichten oder Aktivitäten anderer Staaten oder ihrer Bestandteile."[172]

Zur Erfüllung ihres Auftrags hat der Direktor der NSA die Aufgabe, die „Signalaufklärung und die Auswertung der erfassten Informationen zu kontrollieren"[173] und „für die Erfordernisse von Regierung und Ministerien sowie für die Durchführung militärischer Operationen Unterstützung durch die Signalaufklärung zu leisten."[174]

Der Kongress ermächtigte den Präsidenten, an den Justizminister die Vollmacht zu übertragen, ohne richterliche Anordnung die auslandsnachrichtendienstliche elektronische Überwachung – die Signalaufklärung eingeschlossen – in die Wege zu leiten.[175] In der Folge erließ Präsident Carter ein Dekret, das den Justizminister mit der pauschalen Befugnis ausstattete, eine Überwachung ohne gerichtliche Anordnung einzuleiten.[176] Eine solche Überwachung kann sich über ein Jahr erstrecken.[177] Um sie einzuleiten, muss der Justizminister dem *Foreign Intelligence Surveillance Court* jedoch immer noch bestätigen, dass Vorkehrungen getroffen werden, um die Operation auf ein Mindestmaß zu beschränken.[178]

Das PRISM-Programm als exponierter Teil der Snowden-Enthüllungen macht deutlich, wie umfassend die NSA ihr Mandat auslegt. PRISM ist ein Programm zur massenhaften Erfassung und Auswertung elektronischer Medien und elektronisch gespeicherter Daten, beispielsweise Internet-Telefonie, Online-Chats und E-Mail-Verkehr.[179] Die NSA schuf eine Datenbank zur Speicherung all dieser Daten, damit die Regierung im Falle von Ermittlungen eine gerichtliche Anordnung

erhalten kann, die es ihr rückwirkend erlaubt, diesen gewaltigen Datenspeicher zu nutzen und zu analysieren[180]

Das NSA-Programm zur massenhaften Telefonmetadatenerfassung, ebenfalls durch investigative Medienarbeit ans Licht der Öffentlichkeit gezogen, ist ein weiteres Beispiel für die großzügige Auslegung der Behörde ihres Mandats.[181] Nach diesem Programm verlangt die US-Regierung von Telefonanbietern, ihr „die Rufnummern der Gesprächsbeteiligten … [sowie] Angaben zu Ort und Dauer, eindeutige Kennungen sowie Zeitpunkt und Dauer aller Gespräche" auszuhändigen.[182] Wenngleich keine Inhalte gespeichert werden, ermöglicht dies der NSA, rückblickend ein „vollständiges Bild dessen zu zeichnen, wer jemanden wie und wann und wohl auch von wo kontaktiert hat."[183]

Zumindest machen Programme wie PRISM oder jenes zur Metadatenerfassung das menschliche Risiko (oder gar die Möglichkeit) deutlich, dass der gesetzliche Auftrag der NSA breit und auch zu breit auslegt wird. Ohne ausreichende Kontrolle beispielsweise konnte ein Ermittler auf weitaus mehr Informationen zugreifen als das Programm zur Metadatenspeicherung ursprünglich vorsah.[184] PRISM sollte NSA-Mitarbeitern eigentlich ermöglichen, nur auf bestimmte ihnen zugewiesene Teildatensätze zuzugreifen, um Verletzungen der Privatsphäre zu begrenzen. Leider funktioniert das Programm so nicht. NSA-Mitarbeiter konnten die Telefone von Paaren abhören und verfolgen, mit wem sie wie lange sprachen.[185] Auch Aufzeichnungen von E-Mail-Verkehr und Video-Chats waren verfügbar, ebenso Facebook-Profile.[186]

Was die Untersuchungen des Ausschusses angeht, so liegt der bedeutendste Aspekt des gesetzlichen Auftrags der NSA darin, dass er der Behörde offenbar die Vollmacht zur Informationsbeschaffung im Ausland ohne Kontrolle einräumt.

E. Gesetzliche Beschränkung der Erfassung von Kommunikationsdaten

1) Durch die Verfassung vorgegebene Beschränkungen

Als höchstes Recht im Lande[187] und als oberste Instanz für den Schutz der Freiheitsrechte[188] sollte die Verfassung der Vereinigten Staaten die wichtigste Möglichkeit zur Beschränkung der Informationsbeschaffung seitens der US-Regierung bieten, die Erfassung von Telekommunikationsdaten durch die NSA eingeschlossen. Die Verfassung garantiert den Schutz der Privatsphäre vor staatlichem Eindringen durch mehrere tiefgreifende Regelungen. Die Privatsphäre bildet explizit und implizit den Kern einer Reihe spezifischer Schutzvorschriften. So ist sie beispielsweise implizit ein Teil des Rechts auf freie Meinungsäußerung.[189] Und sie ist explizit ein Teil des mehr oder weniger ruhenden Verbots, Angehörige der Streitkräfte in private Wohnungen einzuquartieren.[190] In einem Fall befand der Oberste Gerichtshof der Vereinigten Staaten, dass der Begriff der Freiheit einer Verbindung der in der Bill of Rights verbrieften Freiheitsrechte entspringt, die zusammengenommen in ein eigenständiges – wenn auch unausgesprochenes – Recht auf Achtung der Privatsphäre münden.[191] Eine weitere bedeutende Grundlage des verfassungsrechtlichen Schutzes der Privatsphäre ist die persönliche Eigenständigkeit, die durch die Jurisprudenz des Obersten Gerichtshof zum „substantive due

process“ [angemessener substantieller Rechtsprozess] garantiert wird. Der verfassungsrechtliche Schutz der Privatsphäre, der für die Informationsbeschaffung durch die amerikanischen Nachrichtendienste wohl am bedeutsamsten ist, liegt im eher expliziten Schutz gegen unbillige oder willkürliche Haussuchungen und Beschlagnahmen, der durch den 4. Zusatzartikel zur Verfassung der Vereinigten Staaten garantiert wird.[192]

Es handelt sich um einen komplizierten doch soliden verfassungsrechtlichen Schutz der Privatsphäre. Und obwohl er in einigen Fällen zu langen und erbittert geführten Auseinandersetzungen geführt hat, bewältigt er seit mehr als zweihundert Jahren die der Verfassung innewohnende Herausforderung, ein Gleichgewicht zwischen dem staatlichen Interesse an der Wahrung von Sicherheit und Ordnung einerseits und dem Interesse des Einzelnen an Freiheit, Privatsphäre und Würde andererseits herzustellen.

Aus mehreren Gründen jedoch ist der verfassungsmäßige Schutz der Privatsphäre als Beschränkung der nachrichtendienstlichen Informationsbeschaffung (insbesondere der Erfassung von Telekommunikationsdaten deutscher Bürger in Deutschland), mit der sich der Ausschuss befasst, weniger aussichtsreich. Zunächst ergibt sich dies aus dem Urteil des Obersten Gerichtshof, dass die Verfassung der Vereinigten Staaten, wenn überhaupt, nur begrenzte Wirkung für amerikanische Maßnahmen gegen Bürger anderer Staaten oder die Grenzen der amerikanischen Gebietshoheit übersteigende Maßnahmen hat. Zweitens könnte die Substanz des den Schutz der Privatsphäre betreffenden amerikanischen Verfassungsrechts – insbesondere den Schutz des 4. Zusatzartikels gegen unbillige oder willkürliche Haussuchungen und Beschlagnahmen – die in der Öffentlichkeit als verfassungsrechtlich schutzwürdig dargestellten Telekommunikationsdaten gar nicht betreffen. Drittens zeigen die durch den Obersten Gerichtshof auf der Grundlage des 4. Zusatzartikels herausgearbeiteten Schutzregelungen für die Privatsphäre ihr größtes Gewicht im Rahmen der strafrechtlichen Verfolgung. Wenn die Regierung verfassungswidrig beschaffte private Informationen nicht als für die strafrechtliche Verfolgung relevante Beweise verwendet, dann sind die zur Anfechtung des Eindringens in die Privatsphäre verfügbaren Rechtsmittel unvollkommen und schwach.

Die folgende Erörterung leite ich ein mit einer Zusammenfassung des für den Schutz der Privatsphäre relevanten Verfassungsrechts. Zunächst beschreibe ich eine Reihe weniger relevanter (zumindest was die NSA-Affäre betrifft) oder weniger expliziter sich aus der Bill of Rights ergebender Schutzaspekte, darunter das Prinzip angemessener substantieller Rechtsprozesse („substantive due process“). Sodann stelle ich die eher relevante Rechtsprechung zum Schutz der Privatsphäre auf der Grundlage des 4. Zusatzartikels dar und berücksichtige dabei die Möglichkeit, dass dieser Schutz, als Angelegenheit des materiellen Rechts, auf die Erfassung von Telekommunikationsdaten durch die NSA gar nicht anwendbar wäre. Ferner beschreibe ich die Grenzen der Durchsetzung des 4. Zusatzartikels in dieser Hinsicht. Schließlich gehe ich auf die Beschränkungen ein, denen die Anwendung der Verfassung auf Ausländer oder das Verhalten der US-Regierung an Orten außerhalb der Vereinigten Staaten unterliegt.

a) Substanz eines verfassungsrechtlichen Schutzes der Privatsphäre

i) Wörtliche und implizite Bestimmungen zur Privatsphäre

Die Gründerväter Amerikas waren sich der menschlichen Bedeutung der Privatsphäre zutiefst bewusst. Man hatte sich auf die Risiken eines Neubeginns in den Kolonien eingelassen, durch ein Weltmeer vom Mutterland getrennt, und strebte eine Ungestörtheit an, die wesentlicher Bestandteil eines freien und eigenständigen Lebens ist. Die ersten Verfassungen der Kolonien boten ausdrücklichen Schutz der Privatsphäre. Doch ist auch einzuräumen, dass nach vorherrschender Meinung zur Zeit der Unabhängigkeitsbewegung die größ§te Gefahr für die Freiheit des Einzelnen ein Übermaß an Staat sei. Man war fest davon überzeugt: Wichtigste Grundlage persönlicher Autonomie – die Privatsphäre eingeschlossen – ist ein kleiner, schwacher und begrenzter Staatsapparat. Das überkommene *Common Law* mit seinen Vorstellungen von Privatheit und Besitzstörung würde den notwendigen Schutz der Autonomie gegen Eingriffe bieten. Diese Geisteshaltung macht erklärbar, weshalb die Gründer der Vereinigten Staaten für möglich hielten, die Verfassung von 1787 ohne einen definierten Katalog an Grundrechten zu formulieren und zu ratifizieren.[193]

Dadurch gewinnt die Tatsache noch mehr an Bedeutung, dass die Bill of Rights, als sie die amerikanische Verfassung als Konvolut von Zusätzen 1791 ergänzte und ratifiziert wurde, eine Reihe von Schutzbestimmungen enthielt, die sich explizit oder implizit mit der Privatsphäre befassen.

Der 1. Zusatzartikel – zur freien Meinungsäußerung, zur Versammlungs- und Religionsfreiheit – impliziert das Recht auf Achtung der Privatsphäre. Der Oberste Gerichtshof befand beispielsweise, dass die mit einer Mitgliedschaft in zivilgesellschaftlichen Gruppen verbundene Privatsphäre (etwa politische Parteien, Gewerkschaften, Bürgerinitiativen) vor staatlicher Ausforschung zu schützen ist. Eine solche Aufdeckung dieser Mitgliedschaft, so die Auffassung des Gerichtshofs, würde politische Aktivitäten und Äußerungen dämpfen, die beide nach dem Recht auf freie Meinungsäußerung und auf Versammlungsfreiheit geschützt sind.[194] Schutz der Privatsphäre in Bezug auf diese Formen von Aktivitäten und Optionen gilt als notwendig für die Wirksamkeit der Garantien der Freiheit der Meinungsäußerung und Religionsausübung nach dem 1. Zusatzartikel.

Das Verbot der Einquartierung von Soldaten in Privatwohnungen während Friedenszeiten nach dem 3. Zusatzartikel deutet ebenfalls auf das Recht auf Achtung der Privatsphäre hin.[195] Den Vätern der Bill of Rights war sehr wohl bewusst, dass der Zwang zur Einquartierung von Soldaten des Königs keinen privaten Freiraum außerhalb der prüfenden Blicke des Staates mehr lassen würde, in den man sich sonst in nahezu vollständiger Autonomie zurückziehen könnte. Der im 3. Zusatzartikel implizierte Schutz der Privatsphäre erkennt an, dass der Einzelne eines geschützten Raumes bedarf, wo er ohne Furcht vor Beobachtung durch staatliche Instanzen leben kann.

Der 5. Zusatzartikel garantiert Angeklagten das Recht, nicht gegen sich selbst aussagen zu müssen.[196] Mit diesem Schutz wird eine innerste Sphäre der Selbstbestimmtheit anerkannt, in die der Staat nicht eindringen darf. Dies gilt insbesondere hinsichtlich der Überlegenheit des Staates, wenn er jemanden wegen einer Straftat anklagt. In diesem Zusammenhang fordert der 5. Zusatzartikel, dass der Staat die private und autonome Persönlichkeit achtet, indem er den

Angeklagten davor schützt, gegen sich selbst auszusagen. Hingegen obliegt es dem Staat, die Beweislast zu übernehmen, die Schuld also mit seinen eigenen Mitteln nachzuweisen, und der Angeklagte hat das Recht, den Staat zur Übernahme dieser Last zu zwingen.

Die Gründer wollten ferner festhalten, dass die Bill of Rights keinen umfassenden Katalog vor staatlichen Übergriffen zu schützender Freiheitsrechte bildet. Der 9. Zusatzartikel erkennt an, dass durch die Verfassung keine „andere[n] dem Volke vorbehaltene[n] Rechte versagt oder eingeschränkt werden" dürfen.[197] Dies könnte ein Verweis auf die fortbestehende Gültigkeit der Freiheitsrechte nach dem *Common Law* [Fallrecht und Richterrecht] sein, das Recht auf Privatsphäre eingeschlossen. Es ist ferner sicherlich ein Anerkenntnis der zahlreichen eigenen Rechte der jeweiligen bundesstaatlichen Verfassungen, deren viele der Bundesverfassung von 1787 zeitlich vorausgingen.[198] Die durch sie garantierten Rechte bleiben hinsichtlich der Ausübung staatlicher Gewalt durch die jeweiligen Staaten wirksam, solange sie keine Freiheitsrechte formulieren, die hinter die in der Bill of Rights festgelegten Rechte zurückfallen. Allerdings können die durch die bundesstaatlichen Verfassungen garantierten Rechte größere Freiheiten als jene der Bill of Rights bieten. Zahlreiche bundesstaatliche Verfassungen enthalten explizite Bestimmungen zum Schutz der Privatsphäre.[199] Schließlich lässt der 9. Zusatzartikel den Schluss zu, dass die Bill of Rights selbst eine flexible und dynamische Auslegung ermöglicht, sodass sie als Grundlage für den Schutz der Freiheit auch dort dienen kann, wo dies der Wortlaut nicht ausdrücklich vorsieht.

In einem Fall griff der Oberste Gerichtshof auf die letzte dieser Möglichkeiten zurück und gelangte zu der Auffassung, dass das Spektrum der in der Bill of Rights implizierten, für den Schutz der Privatsphäre relevanten Bestimmungen insgesamt einen eigenen, wenn auch nicht ausgesprochenen verfassungsrechtlichen Schutz der Privatsphäre bilden. Richter William Douglas, der in *Griswold v. Connecticut* die Mehrheitsauffassung formulierte,[200] argumentierte, dass die Verfassung das Recht auf Achtung der Privatsphäre auch dann schützt, wenn die Bill of Rights sich nicht explizit auf die „Privatsphäre" bezieht. Dieser Schutz, so Richter Douglas, finde sich in den „Randbereichen" und „Ausflüssen" der expliziten verfassungsrechtlichen Schutzbestimmungen, darunter der 1., 3. und 5. Zusatzartikel.[202] Das derart implizierte Recht auf Achtung der Privatsphäre, schlussfolgerte Richter Douglas, bestehe in einem Recht auf „Schutz vor staatlichen Eingriffen". Der Fall *Griswold* betraf auch die Anfechtung eines Gesetzes des Bundesstaates Connecticut, das ein Verbot der Verwendung von Verhütungsmitteln enthielt. Der Gerichtshof befand, das Gesetz verstoße gegen das Recht auf „eheliche Privatsphäre", weil es die polizeiliche Durchsuchung der Schlafräume von Paaren bei der Beweissicherung zur verbotenen Kontrazeptivaverwendung erlaube. Diese absurde Vorstellung, so Richter Douglas, beinhalte eine nicht hinnehmbare staatliche Einmischung in den intimsten Bereich der Privatsphäre.[203]

Der Begründung zum Fall *Griswold* hat sich der Oberste Gerichtshof kein weiteres Mal angeschlossen. Doch schlägt dieser Fall eine sinnvolle Brücke zu einer weiteren verfassungsrechtlichen Grundlage für den Schutz der Privatsphäre. Wie der Fall *Griswold* die höchst intime und private Sphäre der sexuellen und reproduktiven Freiheitsrechte betraf, so richtet sich auch die umfangreiche Rechtsprechung des Gerichtshofs zur Privatsphäre und zum „substantive due process" [der materiellen Rechtmäßigkeit staatlichen Handelns] auf den Bereich Familie, Ehe und sexuelle Freiheit. „Substantive due process" leitet sich aus dem 5. Zusatzartikel

(sich auf Maßnahmen der Bundesregierung erstreckend) und dem 14. Zusatzartikel ab (sich auf Maßnahmen der Bundesstaaten erstreckend). Beide Zusätze schützen davor, „des Lebens, der Freiheit oder des Eigentums ohne vorheriges ordentliches Gerichtsverfahren nach Recht und Gesetz beraubt [zu] werden".[204] Nach einer Lesart dieser Garantie ist bei aller Ausübung von Staatsgewalt, die jene persönlichen Freiheitsrechte betrifft, ein *prozedurales* Erfordernis zu erfüllen. Dabei habe der Staat den Betroffenen zumindest vorab und mit angemessener Frist von den Maßnahmen in Kenntnis zu setzen, damit dieser die Maßnahmen anfechten kann.[205] Das Mindestmaß an prozeduraler Rechtmäßigkeit staatlichen Handelns bietet dem Betroffenen ferner die Möglichkeit, gegen einen unbefriedigenden Beschluss zur ursprünglichen Klage vor einer höheren Instanz Berufung einzulegen. Eine weitere Lesart der verfassungsmäßigen Verpflichtung zum rechtsstaatlichen Verfahren besagt, dass letztere die Justiz befugt, die *Substanz* der Ausübung von Staatsgewalt (legislativer wie administrativer) zu prüfen, um zu gewährleisten, dass die Erwartungen der Gesellschaft an grundlegende Fairness, Gerechtigkeit und Freiheit erfüllt werden.

„Substantive due process" nach dem 5. und 14. Zusatzartikel hat sich als strittig erwiesen, nicht nur, weil sich dieses Prinzip anscheinend dem Naturrecht angleicht, sondern auch, weil es dem Obersten Gerichtshof als Grundlage diente, eine ganze Reihe kontroverser Schutzbestimmungen zur Privatsphäre zu formulieren, darunter, sehr Aufsehen erregend, ein Recht der Frau auf Schwangerschaftsabbruch. Richter Blackmun, der die Mehrheitsmeinung des Gerichts in *Roe v. Wade* formulierte,[206] erklärte, dass Gesetze, die die Möglichkeit zur Abtreibung einschränken, das Recht auf Privatsphäre in verschiedener wichtiger Hinsicht betreffen:

> Der Nachteil, der einer Schwangeren durch den Staat entsteht, indem er diese Möglichkeit verweigert, ist offenkundig. Selbst zu Beginn der Schwangerschaft kann eine medizinisch diagnostizierbare konkrete, unmittelbare Schädigung eintreten. Die Mutterschaft oder ein weiteres Kind kann für die Frau eine sorgenvolle Zukunft bedeuten. Ein seelischer Schaden ist nicht auszuschließen. Die seelische und körperliche Gesundheit kann durch die Kinderbetreuung belastet werden. Des Weiteren ist die für alle Beteiligten mit dem ungewollten Kind verbundene Verzweiflung zu nennen, sowie das Problem, dass ein weiteres Kind in eine Familie kommt, die psychologisch und auch sonst bereits nicht mehr in der Lage ist, es zu betreuen. In anderen wie auch in diesem Fall kommen die Schwierigkeiten und die dauerhafte Stigmatisierung hinzu, die mit einem unehelichen Kind verbunden sein können.[207]

Die Kritik, die daran geübt wurde, dass der Gerichtshof sich auf den Schutz der Privatsphäre stützt, die er aus dem Grundsatz des „substantive due process" ableitet, besteht fort, vor allem weil er seine Rechtsprechung auf andere gesellschaftlich sehr umstrittene Bereiche ausgedehnt hat.[208] In den letzten Jahren beispielsweise hat der Gerichtshof auch den Schutz der Homosexualität mit dem aus dem Grundsatz des *substantive due process* abgeleiteten Recht auf Achtung der Privatsphäre begründet.[209]

Bislang hat der Oberste Gerichtshof keine Notwendigkeit gesehen, einem aus dem Grundsatz des *substantive due process* abgeleiteten Recht auf Datenschutz Geltung zu verschaffen. In *Whalen v. Roe* (1977) beispielsweise urteilte der Gerichtshof, dass es ein solches Recht geben mag, dass jedoch das betreffende bundesstaatliche Gesetz nicht gegen die Verfassung verstoße. In diesem Fall ging es um ein Gesetz des Bundesstaates New York; danach mussten Ärzte und Apotheker eine Reihe personenbezogener Daten von Patienten, die bestimmte Arzneimittel verwenden, erfassen und an den Staat weitergeben.[210] Der Gerichtshof erkannte ein durch die Verfassung geschütztes Freiheitsrecht, das durch die Kontrolle der Offenlegung persönlicher Daten gewahrt wird. Jedoch befand der Gerichtshof ebenso, dass der Staat ausreichend legitimiert ist, mit dem Gesetz in diesen Bereich der Privatsphäre einzugreifen, und dass es für den Staat keine Notwendigkeit gibt nachzuweisen, dass die ergriffene Maßnahme erforderlich ist (das heißt, sehr eng gefasst oder so wenig eingreifend wie möglich). Ein weiteres Beispiel für die Zurückhaltung des Gerichtshofs: In *NASA v. Nelson* (2011) befand der Gerichtshof, dass die einheitlichen Einstellungsvorschriften der Bundesregierung nach 9/11 nicht gegen die Verfassung verstoßen.

Es ist nicht leicht – aber wohl nicht unmöglich –, dieses Geflecht für den Schutz der Privatsphäre relevanter verfassungsrechtlicher Bestimmungen auf die Informationsbeschaffung der NSA zu übertragen. Das weitreichende und unterschiedslose Ausspähen von Kommunikationsdaten steht in keinem offenkundigen Zusammenhang mit einer der wörtlichen Aussagen in der Bill of Rights, die als implizites Recht auf Achtung der Privatsphäre ausgelegt werden können. Nur der im 1. Zusatzartikel vorgesehene Schutz der Rede- und Versammlungsfreiheit scheint potenziell relevant. Doch die eher allgemeine Rechtsprechung des Gerichtshofs selbst zum 1. Zusatzartikel würde eine Verfassungsklage aus diesen Gründen erschweren. Seine Rechtsprechung, die Folgerungen aus der Bill of Rights eher dezent als Schutz der Privatsphäre auslegt, hat keine breite Anerkennung gefunden. Schließlich sind zwingende Unterscheidungen zu treffen zwischen den grundlegenden menschlichen Freiheitsrechten, um die es in den Fällen geht, die den Gerichtshof veranlassten, die Privatsphäre als Angelegenheit des „substantive due process" aufzufassen, und andererseits den durch die staatliche Informationsbeschaffung betroffenen Freiheitsrechten. Zu den ersteren gehört die Sexualität – der intimste und persönlichste Bereich der Privatsphäre. Wenngleich schwerwiegend, liegt es nicht auf der Hand, dass die durch nachrichtendienstliche Informationsbeschaffung betroffene Privatsphäre eine ähnliche Bedeutung für das Menschsein hat.

ii) Privatsphäre nach dem 4. Zusatzartikel

Der höhere mit dem Schutz der Privatsphäre verbundene Verfassungsanspruch hinsichtlich der nachrichtendienstlichen Informationsbeschaffung – das Erfassen von Telekommunikationsdaten eingeschlossen –, ergäbe sich aus der im 4. Zusatzartikel verbrieften Garantie der „ãSicherheit der Person und der Wohnung, der Urkunden und des Eigentums vor willkürlicher Durchsuchung, Festnahme und Beschlagnahme."[211] Der 4. Zusatzartikel war eine Reaktion auf die britische Praxis, Haussuchungsbefehle ohne hinreichenden Verdacht auszustellen.[212] Und der 4. Zusatzartikel, in dem Sinne, dass er den Einzelnen vor staatlichen Übergriffen schützt, ist auch Ausdruck der Prinzipien, die die Gründerväter mit der amerikanischen Form der Demokratie verbanden.

In seinem wegweisenden Urteil im Fall *Katz v. U.S* wies der Oberste Gerichtshof die herkömmliche Rechtsprechung zurück, die den im 4. Zusatzartikel implizierten Schutz der Privatsphäre mit Vorstellungen von Eigentum und Besitzstörung verband.[213] Im Fall *Katz* erklärte der Gerichtshof nachdrücklich, dass „der 4. Zusatzartikel Menschen schützt, nicht Orte."[214] Inhaltlich besteht dieser Schutz darin, dass eine Haussuchung nur dann durchgeführt werden darf, wenn sie durch einen ausführlichen und genauen Durchsuchungsbefehl legitimiert ist, der von einem neutralen und unvoreingenommenen Richter auf der Grundlage einer eidlichen Aussage, die einen hinreichenden Verdacht glaubhaft macht, ausgestellt wurde. Allerdings erkennt der Gerichtshof einige Ausnahmen zu den Anforderungen nach dem 4. Zusatzartikel, die Haussuchungen aus anderen „vertretbaren" Gründen zulassen. Von mancher Seite wird behauptet, diese Ausnahmen würden die Regel aufheben, sodass der 4. Zusatzartikel nur noch eine Floskel sei, die keinen wirksamen Schutz der Privatsphäre mehr biete.

Die entscheidende Frage ist dann, was als „Durchsuchung" im Sinne des 4. Zusatzartikels gilt. Weit mehr als die substanziellen Elemente des Schutzes nach dem 4. Zusatzartikel scheint diese vorab zu klärende Frage wohl die Anwendung dieses Verfassungszusatzes auf die Informationsbeschaffung der amerikanischen Nachrichtendienste und insbesondere die Telekommunikationsdatenerfassung zu komplizieren. Nach dem Fall *Katz* bedeutete eine „Durchsuchung" nicht mehr zwangsläufig, dass die Behörden physisch in private Räumlichkeiten eindringen. Hingegen stellte der Gerichtshof ein Eindringen in die persönliche Sphäre von Katz fest. In diesem Fall war eine „Wanze" auf der Außenseite einer gläsernen Telefonzelle angebracht worden, was den Polizeibeamten ermöglichte, Katzs Telefongespräche abzuhören.[215] Obgleich sie nicht physisch in die Telefonzelle eingedrungen waren, war der Gerichtshof der Auffassung, dass Katz die subjektive Erwartung haben konnte, dass „die Worte, die er in den Hörer sprach, nicht an die ganze Menschheit übermittelt werden", und dass die Gesellschaft eine solche Erwartung als angemessen anerkennen würde.[216] Dies ist heute die Norm, wenn festzustellen ist, ob eine „Durchsuchung" stattgefunden hat, ohne welche der substanzielle Schutz nach dem 4. Zusatzartikel nicht gilt: (1) jemand „hegt die konkrete (subjektive) Erwartung, die Privatsphäre sei geschützt"; (2) die Gesellschaft ist bereit, diese Erwartung als (objektiv) angemessen anzuerkennen.

Der Oberste Gerichtshof legte diese Norm in *Smith v. Maryland* zugrunde und befand, dass keine den 4. Zusatzartikel berührende Durchsuchung stattgefunden hatte.[217] Dies ist deshalb von Bedeutung, weil die Umstände im Fall *Smith* als jenen der Telekommunikationsdatenerfassung durch die NSA sehr ähnlich angesehen werden können. Im Fall *Smith* erbrachten Polizisten den Nachweis von Telefonkontakten des Verdächtigen und seiner Gespräche durch Installation eines Verbindungsdaten-Erfassungssystems auf seiner Telefonleitung in den Betriebsräumen der Telefongesellschaft. Mit einem solchen System werden nur die auf einer bestimmten Leitung angerufenen Nummern registriert. Der Inhalt der Telefongespräche wird nicht dokumentiert. Der Gerichtshof befand, dass nicht eines der den 4. Zusatzartikel berührenden Elemente gegeben war. Zunächst hatte Smith keine subjektive Erwartung an die Privatheit der von ihm gewählten Telefonnummern. Der Gerichtshof argumentierte wie folgt:

> Wir bezweifeln, dass man im Allgemeinen eine konkrete Erwartung hinsichtlich der Privatheit der gewählten Nummern hegt. Allen

> Telefonbenutzern ist bewusst, dass sie Telefonnummern an ihren Anbieter „übermitteln“ müssen, da erst durch die Schaltanlagen der Gesellschaft ein Gespräch zustande kommt. Allen Kunden ist ferner bewusst, dass die Telefongesellschaft über Einrichtungen zum Aufzeichnen der gewählten Nummern verfügen, denn sie finden ihre Gespräche auf ihren monatlichen Rechnungen aufgeführt. Genau genommen werden Verbindungsdaten-Erfassungs- und andere Systeme von den Anbietern „zum Zwecke der Abrechnung, der Betrugsermittlung und der Verhinderung von Gesetzesverstößen routinemäßig eingesetzt.“[218]

Zweitens befand der Gerichtshof, dass eine subjektive Erwartung an die Privatheit gewählter Telefonnummern – ohnehin unwahrscheinlich – als nicht angemessen betrachtet werden kann. Die Gesellschaft, so der Gerichtshof, erkennt objektiv an, dass elektronische Anlagen umfassend genutzt werden, um die gewählten Telefonnummern zu erfassen und aufzuzeichnen. Zumindest ist dies, wie der Gerichtshof feststellt, üblich (und allgemein bekannt), weil es für die Telefongesellschaften notwendig ist, um ihre Abrechnungsunterlagen führen zu können.

Der Gerichtshof urteilte, dass Smith durch das Wählen von Telefonnummern diese Daten anderen (zumindest der Telefongesellschaft) zur Verfügung stellt. Auf solch unterschiedslose Weise Informationen offenzulegen, die jeder subjektiven oder objektiven Erwartung an Privatheit entbehrt, bedeute, dass die Erfassung von Telefonnummern lediglich der Beschaffung nicht-privater Informationen gleichkomme. Eine den 4. Zusatzartikel berührende Durchsuchung habe nicht stattgefunden.

Richter William Pauley vom *Southern District* des *New York Federal Court* stützte sich auf die offenkundigen Parallelen der Sachlage im Fall *Smith* zur Metadatensammlung der NSA, als er im Dezember 2013 eine Anfechtung des Programms auf der Grundlage des 4. Zusatzartikels zurückwies.[219] Auf Smith zurückgreifend, urteilte Richter Pauley, dass Telefonkunden keine angemessene Erwartung an die Privatheit im Sinne der Rechte nach dem 4. Zusatzartikel hegen können, insbesondere hinsichtlich Informationen, die sie freiwillig Dritten überlassen, beispielsweise Telefongesellschaften.[220]

Einen scharfen Konflikt zwischen zwei Bundesgerichten erster Instanz schaffend, weigerte sich Richter Richard Leon vom *District of Columbia Federal District Court* jedoch, sich *Smith* in einem ähnlichen, doch eigenen Fall anzuschließen, bei dem es darum ging, das NSA-Programm zur massenhaften Telefondatenerfassung als Verstoß gegen den 4. Zusatzartikel anzufechten.[221] Beunruhigt durch den „Orwellschen“ Charakter des NSA-Programms,[222] wollte Richter Leon – quantitativ und qualitativ – unterschieden wissen zwischen den von der NSA einerseits und den von der Regierung im Fall *Smith* beschafften Informationen andererseits. In einem ebenfalls im Dezember 2013 gefällten Urteil befand Richter Leon, dass der Kläger aus mindestens vier Gründen eine angemessene Erwartung an die Privatheit der von der NSA erfassten Telefondaten hegen konnte. Erstens: Selbst wenn die Nutzung des Verbindungsdaten-Erfassungssystems im Fall *Smith* vernünftigerweise absehbar war, kann angemessenerweise nicht erwartet werden, dass die

Regierung ein langfristig angelegtes Programm der Datenerfassung wie jenes der NSA realisiert (über mehr als zehn Jahre).[223] Zweitens: Die antizipierte Aufdeckung von Telefonnummern im Fall *Smith* betrifft nur einen Bruchteil der enormen Menge persönlicher Informationen, die von der NSA auf der Grundlage von Aktivitäten in der Telekommunikation abgegriffen werden, ermöglicht durch einen technologischen Quantensprung seit dem Fall *Smith*.[224] Drittens: Die Verwendung von Telefonen zur Zeit des Falles *Smith* ist in keiner Weise vergleichbar mit dem heutigen höchst persönlichen Gebrauch von Telefonen und anderen Technologien.[225] Viertens: Zwar war zur Zeit des Falles *Smith* zu erwarten, dass die Regierung auf die Unterstützung der privaten Telefongesellschaft für die Erlangung von Telefondaten hoffen konnte, doch ist nicht von einer angemessenen Erwartung hinsichtlich der höchst synergistischen Zusammenarbeit zwischen der NSA und Telekommunikationsunternehmen auszugehen. Richter Leons Urteil verlangt eine dynamische und sich weiterentwickelnde Rechtsprechung zum 4. Zusatzartikel, die dramatischen technologischen Veränderungen Rechnung tragen kann.

Nachdem er festgestellt hatte, dass eine den 4. Zusatzartikel berührende Durchsuchung vorgekommen war, kam Richter Leon zu dem Schluss, dass der Kläger hinsichtlich der Begründetheit seiner Klage wahrscheinlich Erfolg haben würde.

b) Anwendung der Verfassung auf Ausländer oder die amerikanische Regierung

Handlungen außerhalb der US-amerikanischen Gebietshoheit

Der Wortlaut der Verfassung der Vereinigten Staaten bietet zur Frage ihrer Anwendung auf Ausländer oder über die Grenzen der Gebietshoheit hinaus keine klare und endgültige Antwort. Diese Frage, ebenso wie zahlreiche andere Aspekte durch die evidente Bedeutung des Verfassungstexts nicht zu klären, muss durch den Obersten Gerichtshof der Vereinigten Staaten beantwortet werden. Das amerikanische Verfassungsrecht, wie es vom Obersten Gerichtshof ausgelegt und angewandt wird, ist grundlegend von der anglo-amerikanischen Tradition des Common Law (Fallrecht und Richterrecht) geprägt. Dies muss erwähnt werden, weil die Rechtsprechung des Obersten Gerichtshofs zur Frage der ausländischen und exterritorialen Anwendung der Verfassung nicht zu einer klaren auf alle verwandten Fälle abstrakt anwendbaren Regel geführt hat. Hingegen ist diese Frage in einer Reihe besonderer Fälle über mehr als hundert Jahre behandelt worden, wobei jeder einzelne Fall eine besondere Facette des Problems auf der Grundlage des jeweils einmaligen Sachverhalts klärte. Hinzu kommt, dass zahlreiche dieser Urteile des Obersten Gerichtshofs sich aus einem Mosaik abweichender Meinungen der Richter zusammensetzen. Im Folgenden unternehme ich daher den Versuch, aus einem sich dynamisch entwickelnden Fallrechtskorpus eine allgemeine Regel herauszudestillieren.

Es wäre falsch zu sagen, dass die Verfassung der Vereinigten Staaten generell nicht auf das Handeln der US-Regierung außerhalb der Gebietshoheit der USA und mit Wirkung auf Nicht-Amerikaner anwendbar ist. Doch ist dies unter den gegebenen Umständen wenig hilfreich, weil der Gerichtshof hinsichtlich der eher für sich allein stehenden Frage der exterritorialen Anwendung des 4. Zusatzartikels zum Nutzen von Ausländern klar befunden hat, dass hier die US-Verfassung nicht geltend gemacht werden kann. Dies könnte nun natürlich exakt den Hintergrund der umfassenden

Erfassung von Telekommunikationsdaten deutscher Staatsbürger in Deutschland durch die NSA betreffen. In dem Urteil *United States v. Verdugo-Urquidez* befand eine Mehrheit der Richter, dass der Schutz nach dem 4. Zusatzartikel begrenzt ist auf das *Volk*, das die „nationale Gemeinschaft" (vor allem Staatsbürger) bildet, oder auf solche Personen mit einer Beziehung zu den Vereinigten Staaten, die in etwa der Zugehörigkeit zur nationalen Gemeinschaft entspricht.[226] Dies würde die von den Vereinigten Staaten weit entfernt lebenden Deutschen, deren Telekommunikationsdaten die NSA erfasst, ausschließen. Die Mehrheit der Richter kam ferner zu dem Schluss, dass Haussuchungen und Beschlagnahmen außerhalb der amerikanischen Gerichtsbarkeit nicht durch den 4. Zusatzartikel beschränkt sind. Zur Untermauerung dieser Position verwies die Mehrheit auf eine Reihe von Fällen, in denen die exterritoriale Anwendung eher allgemein ausgerichteter Schutzvorkehrungen für Freiheitsrechte (wie das im 5. Zusatzartikel formulierte Recht, nicht gegen sich selbst aussagen zu müssen) „energisch" zurückgewiesen wird. In einem dieser Urteile heißt es zur ungewöhnlichen Novität dieser Möglichkeit etwas geschraubt: „Eine solche exterritoriale Anwendung des Organgesetzes wäre eine so bedeutsame Neuerung in der Praxis der Staaten, dass, ob beabsichtigt oder wahrgenommen, sie wohl kaum keinen Anstoß zu aktuellen Kommentaren geben würde. Nicht eine Formulierung lässt sich zitieren. Nicht ein Urteil dieses Gerichtshofs unterstützt eine solche Auffassung."[227]

Auch wenn das Urteil des Obersten Gerichtshofs in *US v. Verdugo-Urquidez* die Anwendung des 4. Zusatzartikels auf die Erfassung der Telekommunikationsdaten deutscher Staatsbürger in Deutschland durch die NSA anscheinend ausschließt, so bleibt möglicherweise doch noch Raum für ein gewisses verfassungsrechtliches Lavieren.

Eine andere Regel würde greifen, wenn deutsche Telekommunikationsdaten in den Vereinigten Staaten abgegriffen würden. Dies wäre beispielsweise dann der Fall, wenn die Daten von in den Vereinigten Staaten ansässigen Telekommunikationsunternehmen erlangt oder durch Zugriff über eine in den Vereinigten Staaten befindliche Telekommunikationsinfrastruktur erfasst würden. Letzteres könnte etwa dann zutreffen, wenn sich die NSA in Glasfaserkabelnetze in den USA einhacken oder Zugriff auf in den USA liegende Server von Internetfirmen erlangte. In einer solchen Situation, in der ausländische Staatsbürger amerikanischen Handlungen unterworfen werden, die ihren Ursprung in den Vereinigten Staaten haben, wäre es nicht ausschlaggebend, wenn der fremde Staatsangehörige keine nennenswerten Beziehungen zur nationalen Gemeinschaft der USA hätte. Einerseits hinge die Beurteilung von der Art des amerikanischen Regierungshandelns sowie der Bedeutung seiner Auswirkungen auf den ausländischen Staatsbürger ab. Andererseits wäre in der Prüfung die Qualität und der Umfang des auf ihn auszudehnenden verfassungsrechtlichen Schutzes zu beurteilen.

Diese Option bezieht ihre Stärke aus dem Urteil des Obersten Gerichtshofs im Fall *Boumediene v. Bush*.[228] In diesem Fall befand der Gerichtshof, dass die Habeas-Corpus-Garantie der Verfassung ausländischen Inhaftierten im Gefängnis von Guantanamo Bay, das formell außerhalb der Gebietshoheit der Vereinigten Staaten liegt, nicht verweigert werden kann.[229] Dennoch sind hier einige wichtige Unterscheidungen zwischen diesem Fall und den möglichen Auswirkungen der NSA-Datenspionage auf Deutsche zu treffen. Erstens: Gleich wie übergriffig oder herabsetzend, es wäre schwierig zu argumentieren, das (geheime) Abgreifen von Telekommunikationsdaten in die

Nähe der staatlich auferlegten Härte der schändlich brutalen Gefängnishaft käme, die von den Guantanamo-Insassen zu erdulden ist. Zweitens: Ein Vergleich der Rechtsprechung des Obersten Gerichtshofs in den Kontexten von Habeas Corpus und 4. Zusatzartikel lässt die Möglichkeit offen, dass der Gerichtshof der verfassungsrechtlichen Habeas-Corpus-Garantie ein größeres Gewicht als dem verfassungsrechtlichen Schutz gegen nicht vertretbare oder willkürliche Haussuchungen und Beschlagnahmen einräumen könnte.

Und drittens schließlich: Selbst nach der großzügigeren Auffassung, die der Oberste Gerichtshof in *Boumediene v. Bush* anscheinend bestätigt, würde die Frage der Anwendung der Verfassung auf Umstände wie jene, mit denen sich der Ausschuss befasst, von mehreren Faktoren abhängen, etwa der Staatsbürgerschaft der Betroffenen, der Art des Ortes staatlichen Handelns, den pragmatischen Hindernissen für den Genuss der beanspruchten Rechte sowie der Bedeutung, die der Gerichtshof den beanspruchten Freiheitsrechten beimisst.

2. Gesetzliche Beschränkungen

a) FISA

Der *Foreign Intelligence Surveillance Act* (FISA) leistet im Grunde zweierlei. Zunächst bietet er die nötige Gesetzeskraft sowie die Normen und Genehmigungsverfahren, die eine geheimdienstliche Informationsbeschaffung dort angemessen sein lässt, wo der 4. Zusatzartikel als anwendbar gelten könnte. Sodann bietet er die nötige Gesetzeskraft sowie die Normen und Genehmigungsverfahren, die eine nachrichtendienstliche Informationsbeschaffung selbst dort angemessen sein lässt, wo der 4. Zusatzartikel nicht anwendbar ist, darunter Überwachungsmaßnahmen, die Nicht-US-Bürger im Ausland betreffen. Es gibt kein abschließendes Urteil des Obersten Gerichtshofs zur Vereinbarkeit des FISA mit dem 4. Zusatzartikel, wenngleich, und das überrascht nicht, man der Auffassung ist, dass der geheime *Foreign Intelligence Surveillance Court* regelmäßig entschieden hat, der FISA biete den erforderlichen verfassungsmäßigen Schutz.

Gemäß FISA gibt es für die amerikanische Regierung nur zwei Möglichkeiten der nachrichtendienstlichen Informationsbeschaffung, die jeweils eine besondere Voraussetzung erfüllen müssen. Zunächst kann der Präsident in Verbindung mit dem Justizminister Maßnahmen zur Informationsbeschaffung (elektronische Überwachung eingeschlossen) ohne irgendeine gerichtliche Anordnung treffen. Doch müssen diese besonderen Maßnahmen auf jeweils höchstens zwölf Monate beschränkt bleiben; sie müssen sich auf die auslandsnachrichtendienstliche Informationsbeschaffung richten, und sie dürfen nur ausländische Mächte oder ihre Agenten betreffen.[230] Unter diesen Umständen muss dargelegt werden, dass es keine nennenswerte Wahrscheinlichkeit dafür gibt, dass die Überwachung den Inhalt einer Kommunikation erbringt, an der ein US-Bürger beteiligt ist.[231] Der Justizminister muss all dies vor dem *Foreign Intelligence Surveillance Court* bezeugen und über die Einhaltung den zuständigen Kontrollgremien Rechenschaft ablegen.[232] Alternativ können Geheimdienstmitarbeiter beim *Foreign Intelligence Surveillance Court* eine richterliche Anordnung für die elektronische Überwachung beantragen.[233] Eine derartige Anordnung erfordert aber glaubhaft zu machen, dass das Ziel in einer ausländischen

Macht oder einem ihrer Agenten besteht – oder, seit 2004, dass es ein terroristischer „Einzelkämpfer“ ist, der in keiner Verbindung zu einem fremden Staat steht. Unter diesen Bedingungen stellt der FISC nur dann eine Anordnung aus, wenn das Risiko, Informationen über US-Bürger zu erlangen, in geeigneter Weise minimiert ist.[234]

Der FISA ist mehrfach novelliert worden, vor allem in der Zeit nach 9/11. Aber sein allgemeiner Rahmen, der nahezu unmittelbar auf den Church-Ausschuss zurückgeht, gilt nach wie vor. Die Gesetzesänderungen zeichnen sich durch zweierlei aus. Erstens wurde die Bandbreite möglicher FISA-Ziele erweitert. Zweitens wurde die Beweislast der Regierung in Fällen mit zufälligem Kontakt mit der Kommunikation eines US-Bürgers reduziert.

Die von Edward Snowden aufgedeckten Programme, darunter das umfangreiche Überwachungsprogramm mit dem Kürzel PRISM und die gewaltige Datengewinnungsoperation, wurden von der Obama-Administration als durchaus mit dem großzügigeren Rahmen der FISA-Novellierung 2008 vereinbar verteidigt. In Bezug auf PRISM sind Bürgerrechtler der Auffassung, dass die Novellen den durch den 4. Zusatzartikel gewährten Schutz aushöhlen, weil sie die zuvor erforderliche richterliche Anordnung zu einer Überwachung, die zufällig auch unbeteiligte US-Bürger treffen kann, durch Schadensbegrenzungsnormen ersetzen. Die Gesetzesänderungen von 2008 verlagern anscheinend auch den Schwerpunkt von fallbezogenen Genehmigungen in bestimmten Einzelfällen hin zur Genehmigung umfassender Überwachungsprogramme. In Bezug auf das Datengewinnungsprogramm der NSA vertritt die Obama-Administration die Ansicht, dass die fraglichen Informationen nie durch den 4. Zusatzartikel geschützt gewesen seien, der sich nicht auf Informationen erstrecke, die Dritten überlassen sind, etwa Internet- und Telekommunikationsanbieter.

Nach US-amerikanischem Recht ist das Abfangen elektronischer Kommunikation gesetzwidrig,[235] wenn keine richterliche Anordnung dazu vorliegt. Der FISA bietet den Rahmen, innerhalb dessen eine solche durch gerichtliche Anordnung legitimierte Informationsbeschaffung, die auch US-Bürger betrifft, durchgeführt werden kann. Im FISC amtieren Bundesrichter, die vom Obersten Bundesrichter des Obersten Gerichtshofs bestimmt werden.[236] Bei diesen Richtern können Anträge auf eine gerichtliche Anordnung gestellt werden, die die entsprechenden Stellen anweist, eine elektronische Überwachung durchzuführen, von der US-Bürger betroffen sind.[237]

Der Antrag auf eine gerichtliche Anordnung zur elektronischen Überwachung erfordert die genaue Darlegung des Ziels, des hinreichenden Verdachts, dass es sich dabei um einen ausländischen Agenten handelt, sowie der verlangten Schadensbegrenzungsmaßnahmen.[238] Werden diese Voraussetzungen erfüllt, dann ist der FISC befugt, eine gerichtliche Anordnung auszustellen, die eine elektronische Überwachung im Inland erlaubt.

Die Schadensbegrenzungsmaßnahmen sind so zu gestalten, dass „die Beschaffung öffentlich nicht verfügbarer Informationen, die US-Bürger ohne deren Zustimmung betrifft, auf ein Mindestmaß begrenzt wird.“Ò[239] Sie müssen ferner den Interessen des Staates Rechnung tragen.[240] Die Aufgabe des FISC besteht darin, ein angemessenes Gleichgewicht zwischen diesen beiden widerstreitenden Interessen herzustellen.[241]

Sollte die elektronische Überwachung zufällig und unbeabsichtigt den Inhalt einer Kommunikation erfassen, und sollten beide Seiten dieser Kommunikation US-Bürger sein, dann muss dieser Inhalt vernichtet werden, wenn er keinen Nachweis einer tödlichen Gefahr oder einer drohenden schweren Körperverletzung erbringt.[242]

Elektronische Überwachung, die nicht behördlich genehmigt ist, ist gesetzwidrig und wird mit Strafen von bis zu fünf Jahren Gefängnis belegt. Ferner wird der Öffentlichkeit ein Klageanspruch eingeräumt. Wer Opfer einer strafrechtlich relevanten Überwachung nach §1809 wird, kann einen Zivilprozess anstrengen und Schadenersatz erhalten.[244]

b) USA FREEDOM Act

Bedenken im Kongress hinsichtlich geheimdienstlicher Übergriffe führten zu einem Gesetzentwurf, der eine weitere Beschränkung nachrichtendienstlicher Tätigkeiten und einen besseren Schutz für US-Bürger bedeuten würde. Einige der umfassenden Bundesprogramme zur Datenerfassung sind in der Öffentlichkeit und von Datenschützern heftig kritisiert worden. Dies führte zum „Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-Collection and Online Monitoring Act", kurz USA FREEDOM Act [deutsch etwa „Gesetz zur Vereinigung und Stärkung Amerikas durch die Verwirklichung von Rechten und die Beendigung von Lauschangriffen, Schleppnetzfahndung und Online-Überwachung"]. Der FREEDOM Act wurde kürzlich vom Repräsentantenhaus verabschiedet und wird nun im Senat beraten.[245] Mit dem Gesetz sollen die Möglichkeiten der Inlandsaufklärung zur Erfassung von Daten über US-Bürger begrenzt werden. Angestrebt ist ferner, massenhafte Datenerfassungen zu verhindern. Dazu soll vorgeschrieben werden, dass ein Antrag auf Datenerfassung einen „spezifischen Auswahlbegriff" enthalten muss.[246] Ein solcher wird definiert als „eindeutiger Begriff, etwa ein Wort, das eine Person, einen Rechtsträger, ein Konto, eine Adresse oder ein Gerät genau bestimmt und von den Behörden verwendet wird, um den Bereich der gesuchten Informationen oder materiellen Dinge einzugrenzen."[247]

3.) Regulative Beschränkungen

Die NSA, wie alle anderen Regierungsstellen, unterliegt den vom Direktor verkündeten Vorschriften und Verfahren. Die Verfahren, die die Durchführung der Signalaufklärung regeln, sind geheim. Jedoch sind einige dieser geheimen Regeln nach außen gedrungen. In einem jüngst erschienenen Bericht der *Washington Post* heißt es, dass „nach den vom Präsidenten dargelegten Regeln die NSA davon ausgehen darf, dass alle im Ausland erfassten Daten ausländischen Staatsbürgern gehören."[248] Dies nur als Beispiel für die Art von Verfahrensregeln, die die Arbeit der NSA bestimmen.

4.) Beschränkungen auf der Grundlage von Dekreten oder Direktiven des Präsidenten

Bei der Informationsbeschaffung sind Agenten gehalten, „die am wenigsten einschränkenden Methoden zu nutzen, die in den Vereinigten Staaten durchführbar sind oder sich gegen US-Bürger im Ausland richten."[249] Die Dienststellen müssen sich ferner an die von den Abteilungsleitern

festgelegten Verfahren halten.[250] Zu den Vorgaben für die Festlegung von Verfahren gehört die Kooperation mit dem *Director of National Intelligence* (DNI), um zu gewährleisten, dass alle anwendbaren die Privatsphäre betreffenden Bundesgesetze eingehalten werden.[251]

Der Leiter jeder Einheit der Nachrichtendienste muss dem *Intelligence Oversight Board* (IOB) über jede Aktivität Rechenschaft ablegen, „die er für gesetzwidrig oder für einem Dekret oder einer Direktive des Präsidenten zuwiderlaufend hält."[252]

Vor dem Hintergrund der aktuellen Enthüllungen zu amerikanischen Geheimdienstaktivitäten erließ Präsident Obama eine Direktive, der zufolge die Nachrichtendienste bei der Auslandsaufklärung gewährleisten müssen, dass „jeder Mensch mit Würde und Respekt behandelt wird, ungeachtet seiner Staatsangehörigkeit oder seines Wohnsitzes; alle Menschen besitzen ein berechtigtes Interesse am Schutz ihrer Privatsphäre beim Umgang mit ihren persönlichen Daten."[253] Diese Direktive macht die Abwägung zwischen legitimen Sicherheitsoperationen und dem Vertrauen des Einzelnen auf Würde und Freiheit deutlich, die den Kern nachrichtendienstlicher Arbeit bildet. Die Nachrichtendienste müssen die ihnen übertragenen Pflichten erfüllen, jedoch ebenso die möglichen Auswirkungen ihrer Methoden auf die Freiheit des Einzelnen bedenken.

Mit der Direktive des Präsidenten wird auch die massenhafte Ausspähung von Telefondaten eingeschränkt. Auf diese Weise erfasste Daten dürfen heute nur noch verwendet werden, um bestimmte Verhaltensformen zu ermitteln.[254] Dennoch werden diese Daten im bestehenden Rahmen weiterhin erfasst.

5) Beschränkungen im Zusammenhang mit der Vereinbarung der Staaten der so genannten „Five Eyes"

Die Vereinbarung zwischen Großbritannien (UK) und den Vereinigten Staaten (USA), die Grundlage der Gruppe der „Five Eyes" ist, bietet für die Bürger der beteiligten Länder, die sich von nachrichtendienstlichem Missbrauch betroffen fühlen, keine neuen oder eigenständigen Rechtsmittel.[255] Die einzigen Rechtsmittel sind jene des Völkerrechts oder des innerstaatliches Rechts. Bezeichnenderweise behaupten Regierungsvertreter, die Vereinigten Staaten wären nie einem Vertrag beigetreten, der ihnen gegen andere Länder gerichtete Überwachungsmaßnahmen verboten hätte.[256] Qua Gesetz darf kein Abkommen, dem die Vereinigten Staaten nach dem 27. Dezember 2000 beigetreten sind, „eine an sich rechtmäßige und genehmigte nachrichtendienstliche Maßnahme der US-Regierung oder ihrer Mitarbeiter für gesetzwidrig erklären."[257] Nachrichtendienstliche Informationsbeschaffung unterfällt diesem Gesetz, wenn sie von einem „zuständigen Beamten" genehmigt wurde und eine Operation ist, die im Aufgabenbereich der ausführenden Behörde erfolgt.[258]

Es mag hier der Anschaulichkeit dienen, näher auf das britisch-amerikanische Geheimdienstabkommen einzugehen. In diesem zuvor höchst geheimen Abkommen, mit dem das weltumspannende Abhörsystem mit der Bezeichnung „Echelon" eingerichtet wurde,[259] kamen Großbritannien und die Vereinigten Staaten überein, die Ergebnisse ihrer auslandsnachrichtendienstlichen Informationsbeschaffung (ihre Signalaufklärung zu

Kommunikationen im Ausland eingeschlossen) zu teilen. Allerdings gab es einige Weiterentwicklungen bei dieser allgemeinen Vereinbarung. Beispielsweise wäre wichtig festzuhalten, dass „Kommunikationen im Ausland" definiert werden als „Kommunikationen von Regierung oder Streitkräften, Fraktionen, Parteien, Ministerien, Behörden oder Ämtern eines anderen Staates oder von Personen, die in deren Auftrag handeln oder zu handeln angeben; sie umfassen ebenso Kommunikationen der Staatsbürger eines anderen Landes, die wertvolle Informationen enthalten könnten."[260] Als Ausland gelten Länder, die weder die Vereinigten Staaten sind noch dem Commonwealth angehösren.[261]

Das Abkommen hindert eine Partei nicht ausdrücklich an der nachrichtendienstlichen Beschaffung von Informationen, die für die jeweils andere Partei relevant sind. Jedoch schließt es aus, dass die Parteien nachrichtendienstlich relevante Informationen austauschen, die die jeweils andere Seite betreffen.[262] Was immer das Abkommen auch vorsieht, festzuhalten wäre, dass jede nachrichtendienstliche Tätigkeit von Agenten einer ausländischen Macht – Großbritannien eingeschlossen – innerhalb der Vereinigten Staaten wohl als Verletzung amerikanischen Rechts gilt.[263] Sollte ein anderes Land versuchen, in den Vereinigten Staaten nachrichtendienstlich Informationen zu beschaffen, und würde der betreffende Agent gefasst, könnte ihn die ganze Härte der US-amerikanischen Gesetze treffen. So haben die Vereinigten Staaten den Agenten eines Verbündeten zu lebenslänglicher Haft verurteilt, mit der Möglichkeit, die Strafe nach dreißig Jahren auf Bewährung auszusetzen.[264]

Es hat den Anschein, als würde das ECHELON-Programm den beteiligten Ländern ermöglichen, in anderen beteiligten Ländern nachrichtendienstlich Informationen zu beschaffen und diese dann jenen Ländern verfügbar zu machen.[265] Dadurch könnten die Staaten der „Five Eyes"-Gruppe die jeweils eigenen Bestimmungen zum Schutz der Privatsphäre umgehen. Nach amerikanischem Recht können beispielsweise auslandsnachrichtendienstliche Informationen ohne gerichtliche Anordnung gesammelt werden, sofern davon kein US-Bürger betroffen ist.[266] Kürzlich nach außen gedrungene Dokumente lassen jedoch den Schluss zu, dass Australien als Mitglied der „Five Eyes" Kommunikationen zwischen einer nicht genannten US-amerikanischen Anwaltskanzlei und der indonesischen Regierung abgefangen hat.[267] Darauf hat Australien anscheinend angeboten, diese Kommunikationen an die NSA weiterzugeben.[268] Aufgrund der Schadensbegrenzungsvorschriften, die mit US-Bürger betreffenden Informationsbeschaffungen verbunden sind, handelt es sich um genau jene Art von Information, die zu beschaffen die NSA eigentlich nicht befugt ist.[269] Es gibt keine Anzeichen dafür, dass die NSA solcherlei Informationen von „Five Eyes"-Partnern akzeptiert hat, doch besteht diese Möglichkeit aufgrund des hohen Integrationsgrades bei der Signalaufklärung durchaus.

IV. Datenschutz

A. Einführung

Die Vereinigten Staaten besitzen kein einheitliches, umfassendes System von Datenschutzregelungen.

Datenschutz genießt in Amerika nicht den gleichen hohen Stellenwert wie in Deutschland (und anderen europäischen Staaten). Dieser markante Unterschied hat keine eindeutige Ursache. Das fundamentalistische Bekenntnis zur freien Meinungsäußerung in Recht und Kultur der Vereinigten Staaten mag ein Grund sein. Diese Mentalität bevorzugt den ungehinderten Fluss von Informationen auf einem „Markt der Ideen" , sodass jede Forderung nach einem Schutz von Informationen auf Misstrauen stößt. Dies ist auch der Tenor der amerikanischen Reaktionen auf das jüngste Urteil des Europäischen Gerichtshofs, das ein „Recht auf Vergessen" gegen den US-amerikanischen Internetkonzern Google bestätigte. Die amerikanische Zeitschrift *New Republic* berichtete über die damit zusammenhängenden Bestrebungen der EU-Kommission, ein „Recht auf Vergessenwerden" zu schaffen, und titelte dazu: „A Grave New Threat to Free Speech from Europe" [Neue schwere Bedrohung der freien Meinungsäußerung aus Europa].[270] Der „Digits"-Blog im *Wall Street Journal* schlug denselben Ton an: „Google Ruling: Freedom of Speech vs. the Right to Be Forgotten" [Google-Urteil: freie Meinungsäußerung gegen Recht auf Vergessenwerden].[271] Wie die obige Erörterung des amerikanischen Verfassungsrechts und des Schutzes der Privatsphäre zeigt, beruht die Bevorzugung der freien Meinungsäußerung auf ausformulierten Rechten: „Unser Recht auf freie Meinungsäußerung steht uns explizit zu, das auf Schutz der Privatsphäre bloß implizit."[272] Eine weitere Erklärung für den Unterschied zwischen den USA und Deutschland in der Frage des Datenschutzes ist die traditionelle amerikanische Haltung des *laissez faire* in der Wirtschaft, die nahezu jede Form der Regulierung ablehnt. Dies trifft insbesondere dort zu, wo es um starke Geschäftsinteressen geht, etwa bei den Absatzmöglichkeiten, die mit der Erfassung und Nutzung persönlicher Daten verbunden sind. Als zusätzliche Erklärung heranzuziehen wären auch die unterschiedlichen Rechtskulturen im anglo-amerikanischen und kontinentaleuropäischen Raum. Dabei kommen zwar grobe Verallgemeinerungen zu diesen vielfältigen Rechtssystemen ins Spiel, doch würde ich annäherungsweise festhalten: Die anglo-amerikanische Rechtstradition des Common Law ist gekennzeichnet durch eine normative Ethik des Fragmentarischen, Faktenspezifischen, Richterlich-Handwerklichen, Induktiven und Retrospektiven. Die europäische Tradition des [kodifizierten] Civil Law hingegen ist gekennzeichnet durch eine normative Ethik des Umfassenden, Systematischen, Abstrakten, Begrifflichen, Gesetzgeberischen, Deduktiven und *ex ante*. Wenn diese Verallgemeinerungen mehr als platte Klischees sind, so mag es nicht überraschen, dass es in den Vereinigten Staaten kein umfassendes und systematisches Gesetzeswerk zur *ex ante*-Regelung des von den Europäern als „Datenschutz" bezeichneten Bereichs gibt.

In gewisser Weise bestätigt das amerikanische Recht zum Datenschutz die Generalisierungen in Bezug auf die anglo-amerikanische Rechtskultur. Wie bereits erwähnt, besitzen die Vereinigten Staaten kein umfassendes System von Datenschutzregelungen. Doch gibt es ein aus Einzelstücken zusammengesetztes Geflecht von Gesetzen, dass der staatlichen und privaten Erfassung, Speicherung und Verbreitung persönlicher Daten einige Beschränkungen auferlegt. Aus verschiedenen Gründen versagen sich diese Regeln einer systematischen Integration. Zunächst unterliegt der Datenschutz, bedingt durch den amerikanischen Föderalismus, sowohl Bundes- als auch bundesstaatlichen Gesetzen. Es gibt eine Reihe einschlägiger Bundesgesetze und hunderte von einschlägigen bundesstaatlichen Gesetzen. Allein in Kalifornien gelten gut 25 Gesetze, die sich in

gewisser Hinsicht auf den Schutz persönlicher Daten und der Privatsphäre beziehen. In Anbetracht der großen globalen wirtschaftlichen Bedeutung Kaliforniens und der bedeutenden Beziehungen zur Technologiebranche weltweit wären seine Gesetze für eine vollständige Betrachtung des amerikanischen Datenschutzrechts relevant. Des Weiteren haben sich die datenschutzrelevanten amerikanischen Gesetze in Bezug auf bestimmte gesellschaftliche und industrielle Bereiche, auch in Bezug auf bestimmte Medienplattformen, unterschiedlich entwickelt.

Hinsichtlich persönlicher Daten als allgemeines und abstraktes gesellschaftliches Phänomen gibt es keine Regelungen. Allerdings gibt es Bestimmungen zur Erfassung, Speicherung und Verteilung von Daten, die von der *Federal Trade Commission* („Bundeshandelskommission") auf Akteure der Wirtschaft angewendet werden. Andere Vorschriften zum Schutz persönlicher Daten gelten im Bildungsbereich, wieder andere im Gesundheitswesen. Telekommunikationsdiensteanbieter und Kabel-TV-Betreiber unterliegen eigenen Regelungen zur Erfassung, Speicherung und Verbreitung persönlicher Daten. Die Aufzählung ließe sich fortsetzen.

Das Gesamtbild wird noch komplizierter dadurch, dass es zwischen den verschiedenen Regelwerken jurisdiktionelle (Bund/Einzelstaaten) und sektorielle Überscheidungen gibt.

Für die gesetzlichen Rahmenbedingungen des Datenschutzes in den einzelnen Bereichen bin ich kein Experte. Im Rahmen dieses Gutachtens kann ich nur einen Überblick geben. Ihm stelle ich eine kurze Zusammenfassung der für die staatlichen Behörden geltenden Datenschutzbestimmungen voran. Darauf folgt eine Übersicht über die für private Akteure relevanten Vorschriften. Ein besonderes Augenmerk richte ich auf die für persönliche Daten im Bereich der Kommunikationssysteme wichtigsten Gesetze.

B. Datenschutz und öffentliche Stellen

Der hohe Stellenwert, den Amerikaner einer transparenten Politik beimessen, hat zur Folge, dass viele amtliche Unterlagen für die Öffentlichkeit bereits zugänglich und verfügbar sind. In diesem öffentlich zugänglichen Bereich behördlicher Unterlagen ist eine Vielzahl persönlicher Daten erfasst. Selbstverständlich stehen nicht alle amtlichen Unterlagen der Öffentlichkeit zu Verfügung. Um allgemein zwischen den verschiedenen Arten amtlicher Dokumente zu unterscheiden, wird eine Tautologie verwendet: *öffentliche Dokumente* sind der genauen Prüfung durch die Öffentlichkeit zugänglich; *vertrauliche Unterlagen* (Verschlusssachen) werden vertraulich geführt, zumindest für eine bestimmte Zeit.

Öffentliche Unterlagen sind jedermann auf Antrag zugänglich, auch Journalisten oder Marketingunternehmen. Dies wurde begünstigt durch den Umstand, dass viele amtliche Aufgaben durch das Internet oder andere elektronische Plattformen unterstützt werden, ebenso durch die Bemühungen um die Digitalisierung archivierter amtlicher Informationen. In vielen Fällen sind amtliche Unterlagen heute durch einfache Internet-Suchanfragen einsehbar. Aus den folgenden im Allgemeinen geführten amtlichen Unterlagen sind der Öffentlichkeit in der einen oder anderen Form Informationen zugänglich: Geburtsregister, Standesämter, Verkehrsbehörden, Wahlbüros,

Katasterämter und Gerichte. Einige andere Bereiche gelten allgemein als vertraulich, darunter Soziales, Steuern und Bildung.

Bundesgesetze definieren „Unterlagen“ denkbar allgemein:

> Bücher, Urkunden, Fotos, maschinenlesbares oder anderes Dokumentationsmaterial, ungeachtet der physischen Form oder Merkmale, im Besitz einer öffentlichen Stelle der Vereinigten Staaten, gemäß Bundesgesetz oder in Verbindung mit amtlichen Vorgängen und zur Aufbewahrung genutzt oder dazu geeignet durch die betreffende Stelle oder ihre Rechtsnachfolger zum Nachweis der amtlichen Organisation, Funktion, Maßnahmen, Entscheidungen, Verfahren, Abläufe oder anderen Aktivitäten, oder in Verbindung mit dem informatorischen Wert der enthaltenen Daten.[273]

Bundesbehörden sind verpflichtet, die von ihnen erstellten Unterlagen zu verwalten.[274] Das Versäumnis, Unterlagen zu führen, sowie ihr Verlust oder unbefugte Vernichtung gilt im Bundesrecht als strafbare Handlung.[275]

Das wichtigste Bundesgesetz von Bedeutung für den Schutz persönlicher Daten in amtlichen Unterlagen des Bundes ist der *Privacy Act* von 1974. Der *Privacy Act* schützt die Privatsphäre amerikanischer Bürger durch prozedurale und materielle Rechte. Erstens sind amtliche Stellen verpflichtet, Einzelpersonen die Einsicht in die sie betreffenden Unterlagen zu gewähren. Zweitens müssen diese Stellen bei der Erfassung von und beim Umgang mit persönlichen Daten bestimmte Grundsätze beachten, so genannte „fair information practices“. Drittens schränkt das Gesetz die Möglichkeiten amtlicher Stellen ein, persönliche Daten an andere Personen oder Stellen weiterzugeben. Viertens räumt es Einzelpersonen einen Klageanspruch ein, um gerichtlich vorgehen und Schadenersatzansprüche für Verstößße gegen den *Privacy Act* geltend machen zu können. Der *Privacy Act* dient jedoch nicht ausschließlich dem Interesse des Einzelnen an einer Kontrolle der von den Ämtern erstellten und verwalteten Informationen. Das Gesetz sieht eine Reihe von Ausnahmen vor. Einerseits fördert das Gesetz die Effizienz der Ämter, indem es Beamten erlaubt, Unterlagen mit personenbezogenen Daten unter verschiedenen Umständen verfügbar zu machen, nämlich wenn diese Unterlagen für ähnliche Zwecke wir für die ursprüngliche Erfassung der Daten verwendet werden (die Ausnahme der „routinemäßigen Verwendung“), oder für statistische Untersuchungen, für den Gesetzesvollzug oder auf gerichtliche Anordnung. Andererseits fördern die Ausnahmebestimmungen des Gesetzes die Verwendung von Daten, die von den Behörden aus Gründen der Sicherheit erfasst werden. So kann einer Person die Einsichtnahme in amtliche Unterlagen mit personenbezogenen Daten verweigert werden, wenn diese Folgendes betreffen: den Gesetzesvollzug, nachrichtendienstliche Tätigkeiten oder vertrauliche amtliche Quellen.

Der *Electronic Communications Privacy Act* von 1986 (ECPA) wurde verabschiedet, um die Beschränkungen für staatliche Abhörmaßnahmen bei Telefongesprächen zu erweitern, sodass darunter auch die Übermittlung elektronischer Daten fällt. Das Gesetz wurde ferner um neue

Bestimmungen ergänzt, die es der Regierung untersagen, auf gespeicherte elektronische Kommunikationsdaten zuzugreifen. Diese Bestimmungen richten sich auf den Schutz des Inhalts der Kommunikation, nicht der Daten, die bei der Herstellung der Kommunikation erzeugt werden. Die Vorschriften dieses Gesetzes zu elektronischen Verbindungsdaten-Erfassungssystemen ermöglichen der Regierung, Kommunikationswege zu verfolgen.[276]

Ein weiteres bedeutendes Bundesgesetz zu amtlichen Unterlagen ist der *Freedom of Information Act* (FOIA, „Informationsfreiheitsgesetz“).[277] Es sagt Einiges über die unterschiedlichen Haltungen zum Thema Datenschutz aus, dass der Zweck dieses Gesetzes darin besteht, den Zugang zu amtlichen Unterlagen zu fördern, und nicht einzuschränken. Nach diesem Bundesgesetz (in den Einzelstaaten gelten ähnliche Gesetze) müssen zuvor nicht offengelegte Unterlagen der Exekutive auf formellen FOIA-gemäßen Antrag zugänglich gemacht werden. Das Gesetz sieht Strafen vor, die von selbst greifen, sobald amtliche Stellen versuchen, die Freigabe ordnungsgemäß beantragter Informationen zu behindern. Der FOIA formuliert eine Reihe von Ausnahmen von der lobenswerten Forderung nach transparenter Politik. Zu diesen Ausnahmen gehören den Gesetzesvollzug und die nationale Sicherheit betreffende Unterlagen. Die Ausnahmen bieten ein gewisses Maß an Datenschutz, da sie auch Personal- und medizinische Unterlagen von Bundesbediensteten betreffen, sowie „ähnliche Akten“, wenn eine FOIA-gemäße Offenlegung einen „eindeutig unberechtigten Eingriff in die Privatsphäre“ bilden würde. Doch was die FOIA-Ausnahmen in Bezug auf den Datenschutz auf der einen Seite einräumen, verweigern sie auf der anderen. Das Gesetz ermöglicht dem Präsidenten, Dekrete zu erlassen, um bestimmte Offenlegungen gemäß FOIA zu unterbinden, wenn dies im Sinne der nationalen Sicherheit oder auswärtiger Angelegenheiten ist. Die Präsidenten haben diese Befugnis bislang groß§zügig genutzt. So hat Präsident Reagan den Bundesbehörden erlaubt, große Mengen an Informationen wegen ihrer Bedeutung für die nationale Sicherheit zurückzuhalten. Als Reaktion auf die breite und anhaltende Verurteilung der Reaganschen Haltung schränkte Präsident Clinton die die nationale Sicherheit betreffenden Ausnahmen Mitte der 1990er Jahre erneut ein. Erst Präsident Obama erließ wieder ein Dekret, das Bundesbehörden ermöglicht, Unterlagen als für die nationale Sicherheit relevant und damit als von einer FOIA-gemäßen Offenlegung ausgenommen auszuweisen, wenn diese gemäß FOIA beantragt wurde. Ausländische Regierungen und ihre Agenten können mittels FOIA-Antrag keine Einsicht in nachrichtendienstliche Unterlagen der USA nehmen.

C. Datenschutz und private Stellen

Die amerikanischen Parlamente und Gerichte haben eine Vielzahl von Gesetzen und Vorschriften geschaffen, die für die Erfassung, Speicherung und Verbreitung von persönlichen Daten durch private Akteure relevant sind. Diese Datenschutzbestimmungen gelten für unterschiedliche Sektoren und unterscheiden sich danach, ob sie im Bund oder einem der fünfzig Bundesstaaten gelten.

Die *Federal Trade Commission* (FTC), die einen Teil des für den Verbraucherschutz relevanten regulatorischen Raumes ausfüllt, hat bei der Förderung des Datenschutzes in der Wirtschaft eine führende Rolle eingenommen. Ihre neue „Abteilung für den Schutz der Privatsphäre und den Identitätsschutz“ befasst sich mit Angelegenheiten wie „Privatsphäre der Verbraucher, Kreditauskunft, Identitätsdiebstahl und Informationssicherheit“. In erster Linie ist die FTC bestrebt,

den Schutz der Privatsphäre gemäß ihrem Mandat nach Artikel 5 des FTC-Gesetzes zu stärken, der „unlautere und irreführende Handlungen und Praktiken … verbietet, irreführende Angaben und unlautere Praktiken eingeschlossen, die die Nutzung oder den Schutz der personenbezogenen Daten von Verbrauchern betreffen." Dies bedeutet in der Regel, dass ein Wirtschaftsakteur einen „wesentlich anderen" Gebrauch von den vom Verbraucher erlangten persönlichen Daten macht als jener Gebrauch, den er laut seiner den Datenschutz betreffenden Geschäftsbedingungen davon macht. Ein aktuelles einschlägiges Beispiel betrifft eine Schlichtung durch die FTC zu Snapchat, einer Instant-Messaging-Anwendung für Smartphones und Tablets. Die FTC behandelte eine Beschwerde wegen „irreführender Handelspraktiken", weil, entgegen den Beteuerungen von Snapchat, dass die über seinen Dienst versendeten Fotos nur eine bestimmte Anzahl an Sekunden sichtbar seien und sich dann selbst zerstörten, es mit relativ einfachen Mitteln möglich ist, versendete Dateien wieder zu finden und wiederherzustellen. Die getroffene Schlichtungsvereinbarung gewährleistet jedoch nicht den die relevanten Daten betreffenden Schutz der Privatsphäre (geschweige ein Recht auf ihre Lösschung nach europäischem Muster). Hingegen untersagt der Schlichterspruch Snapchat lediglich, „den Umfang, in dem Snapchat oder seine Produkte oder Dienstleistungen die Privatsphäre, Sicherheit oder Vertraulichkeit der erfassten Informationen gewährleistet, irreführend darzustellen." In der Pressemitteilung zu dieser Vereinbarung beschreibt die FTC den Sieg als „Teil der anhaltenden Bemühungen der FTC, dafür Sorge zu tragen, dass Unternehmen ihre Apps wahrheitsgemäß vermarkten und ihre Zusicherungen hinsichtlich des Schutzes der Privatsphäre der Verbraucher einhalten."

Das Bundesgesetz zu Kabelkommunikationssystemen von 1984 sieht vor, dass Kunden über die Art der personenbezogenen Daten, die vom Anbieter erfasst werden, in Kenntnis gesetzt werden müssen,[278] ebenso über die Art der erlaubten Offenlegung.[279] Unterlagen kösnnen ohne Zustimmung des Kunden nur unter ganz bestimmten Bedingungen offengelegt werden. Von Interesse ist die Möglichkeit, diese Informationen nach einer vom FISC ausgestellten Anordnung „mit aufgeschobener Bekanntgabe" offenzulegen.[280] Selbst unter diesen Umständen ist es dem Anbieter untersagt, staatlichen Stellen die speziellen Videoauswahlen des Kunden verfügbar zu machen.[281]

Der *Federal Telecommunications Act* („Bundestelekommunikationsgesetz") von 1996 ist ein weiteres Beispiel sektorspezifischer Datenschutzbestimmungen. Das Gesetz wurde im vergangenen Jahrzehnt novelliert, um den Schutz der Routing- und Zielinformationen sowie der Netznutzungsdaten von Telekommunikationskunden zu gewährleisten. Ferner sind durch die Gesetzesänderungen die Rechnungsdaten der Kunden geschützt.[282] Dies unterliegt den üblichen Zulassungen für Offenlegungen der Geschäftsgepflogenheiten oder gesetzlich zulässigen Offenlegungen.[283] Dadurch wird zumindest gewährleistet, dass die Regierung nicht berechtigt ist, Kenntnis der von den Kunden besuchten Internetseiten zu erhalten, sofern nicht anderweitig gerechtfertigt.

Nach Bundesrecht ist es gesetzwidrig, die ein- oder ausgehende Telekommunikation einer Person ohne richterliche Anordnung zu verfolgen, sofern nicht eine der FISA-Ausnahmen zutrifft.[284] Ferner sind nach Bundesrecht auch Abhörmaßnahmen bei elektronischer Kommunikation gesetzwidrig.[285] Diese Schutzbestimmungen greifen als privatrechtlich durchsetzbare

Datenschutzvorschriften, weil bei Verstößen zivilrechtliche Rechtsmittel zur Verfügung stehen.[286] Wer gegen das Verbot von Abhörmaß§nahmen verstößt kann beispielsweise im Zivilprozess mit Geldstrafen von einigen Hundert bis mehreren Tausend Dollar pro Verstoß verurteilt werden.[287] Für die großen Telekommunikationsunternehmen scheinen die Entschädigungsmöglichkeiten jedoch eher keine wirksame Abschreckung zu sein. Das Kalkül ändert sich jedoch, wenn ein Unternehmen der behördlichen Anforderung von Massendaten folgt und man dabei die amerikanischen Zivilprozessregeln berücksichtigt, die Sammelklagen zulassen. Dann können die Entschädigungsleistungen, die auf die Telekommunikationsanbieter zukämen, beträchtlich sein. Dies bewog das Justizministerium, den Anbietern, die sich kooperationsbereit zeigen, zivil- und strafrechtliche Immunität anzubieten.

V. Vergleichende Betrachtungen

A. Einführung

Ich bin nicht der Auffassung, dass meine Dienste für den Ausschuss streng auf beschreibende Antworten auf die mir vorgelegten Fragen zu den Aktivitäten der US-Nachrichtendienste und zum Datenschutzrecht begrenzt sind. Ich betrachte dies auch als Gelegenheit, auf deutscher Seite zum tieferen Verständnis der rechtlichen Dimensionen beizutragen. Sollten die obigen Abschnitte der Stellungnahme überhaupt hilfreich zur Klärung dessen gewesen sein, *was* die Kernelemente des amerikanischen Rechts sind, so hoffe ich mit diesem Schlusskapitel ein wenig zum Verständnis dessen beizutragen, *weshalb* dieses Recht und die unterstützten Werte auf diesen Feldern so sind wie sie sind. Dies ist deshalb von besonderer Bedeutung, weil das hier dargestellte amerikanische Recht anscheinend in vielen Fällen Grundsätze und Werte vertritt, die den das deutsche Rechtsverständnis beseelenden Werten und Prinzipien klar widersprechen. Diese Unterschiede überraschen umso mehr, wenn man von der Annahme ausgeht, dass die westlichen Demokratien und die langjährigen, engen Verbündeten Deutschland und USA im Hinblick darauf sehr viele Gemeinsamkeiten haben, wie ihre jeweiligen Rechtssysteme – durch Verfassung wie durch Gesetz – Sicherheit und Freiheit in Einklang bringen.

Die folgenden Anmerkungen mögen zeigen, dass diese Annahme noch nie richtig war und an sich schon Quelle erheblicher Missverständnisse ist. Der so genannte „Westen“ war und ist keine Einheit, denn er umfasst eine Vielfalt unterschiedlicher Gesellschaften. Und enge Bündnisse sind nicht deshalb von Bedeutung, weil sie Gruppierungen identischer Gemeinschaften repräsentieren, sondern weil sie sehr unterschiedliche Gemeinschaften um gemeinsame Interessen miteinander verbinden. Zudem gibt es grundlegende Unterschiede zwischen allen Rechtssystemen, insbesondere im Verfassungsrecht. Wie Alan Watson, ein angesehener Fachmann für vergleichende Rechtswissenschaft, einmal treffend bemerkte: „Welche Verfassung sich ein Land gibt, zeigt, dass es doch seinen eigenen Kopf hat.“ Solche Unterschiede sind die Folge – um nur einige der eher offenkundigen Faktoren zu nennen – der je eigenen Geschichte, unterschiedlicher sozialer Kräfte, politischer Traditionen und Institutionen, unterschiedlicher Rechtskulturen und ökonomischer Bedingungen und Orientierungen. Auf dieser Grundlage stelle ich hier einige vergleichende Betrachtungen an.

B. Historische und kulturelle Unterschiede

Mit dem staatlichen Gebrauch von Überwachung und sozialer Kontrolle haben Amerikaner und Europäer im Laufe des 20. Jahrhunderts sehr unterschiedliche Erfahrungen gemacht. An Beispielen dafür, dass die amerikanische Regierung lange Zeit ein übermäßiges Interesse an der Erfassung von Informationen über ihre Bürger hatte, herrscht kein Mangel. Auch dass von diesen Informationen allzu oft ein unheilvoller Gebrauch gemacht wurde. Dennoch haben die Amerikaner noch nie brutalen und verhassten totalitären Regimen die Stirn bieten müssen, wie jenen, die persönliche Daten nutzten, um die Deutschen zwischen 1933 und 1945 oder die Ostdeutschen zwischen 1949 und 1990 zu terrorisieren. In anderen europäischen Ländern sind ähnliche, jüngere politische Traumata zu bewältigen.

Dieser jeweils eigene historische Hintergrund trägt zur Erklärung bei, warum die für den Schutz der Privatsphäre relevanten Bestimmungen in den Vereinigten Staaten impliziter Natur (auf der Ebene der Grundrechte) und fragmentiert (auf der Ebene gesetzlicher Vorschriften) sind. Die historischen Unterschiede helfen ebenso zu erklären, weshalb Europäer so darum bemüht waren und sind, den Schutz der Privatsphäre explizit als Grundrecht zu formulieren.

C. Demokratische Unterschiede

Politologen pflegen zu bemerken, dass die politische Kultur der Vereinigten Staaten weitaus empfänglicher für allgemeine, Mehrheiten erfassende Stimmungen ist als die eher konsensorientierte politische Kultur im Nachkriegsdeutschland. Diese unterschiedlichen Haltungen wurzeln eindeutig in der jeweils eigenen Geschichte der beiden Länder. Die amerikanische an Mehrheiten orientierte Politik geht zurück auf die Unabhängigkeitsbewegung und die Tradition des Individualismus. Diese Züge der amerikanischen Politikkultur sind der Grund dafür, warum Regierungen so leicht (und zuweilen sogar unergiebig) auf die allgemeine Stimmungslage reagieren. Das deutsche korporatistische Politikverständnis leitet sich aus der Ablehnung eines Liberalismus Weimarer Prägung und einer tiefen Sehnsucht nach politischer Stabilität ab. Das politische System Deutschlands spricht weniger direkt auf die breite Meinung an, weil es eine institutionalisierte Kooperation zwischen den großen Interessengruppen und den Eliten gibt. Der Parteienstaat und die Mitbestimmung in Unternehmen sind Beispiele für das korporatistische Politikverständnis. In den verschiedenen Politikkulturen drückt sich ferner die komplexe Vielfalt der amerikanischen Gesellschaft einerseits und die relative Homogenität der deutschen Gesellschaft andererseits aus.

Die an Mehrheitsstimmungen orientierte amerikanische Politikkultur ist hier deshalb von Bedeutung, weil sie den scheinbaren Vorrang der Sicherheitspolitik vor Konzepten zum Schutz der Privatsphäre erklären hilft. Die parteiübergreifende Überhöhung der Sicherheit – auf Kosten von Freiheit und Privatsphäre – ist zumindest teilweise bedingt durch ein elementares politisches Kalkül. In einem politischen System, das für populäre Stimmungen höchst empfänglich ist, ist es nachvollziehbar, dass die politischen Kosten der Zulassung (oder der Halbherzigkeit bei der Aufdeckung und Verhinderung) des nächsten verheerenden Terroranschlags in Amerika zwar unbekannt, aber aller Wahrscheinlichkeit nach extrem hoch sind. Die politischen Kosten der

Fortführung in die Privatsphäre eingreifender Geheimdienstaktivitäten, die auf die Verhütung eines weiteren Anschlags gerichtet sind, lassen sich besser einschätzen, und da sie verschleiert sind, werden sie möglicherweise ohnehin hin nicht realisiert. Eine solche Einschätzung, die sich der Folgen für das Abstimmungsverhalten völlig bewusst ist, begünstigt eindeutig eine positive Haltung zum Sicherheitsstaat. Keine der beiden Parteien im US-System würde eine politische Zukunft gutheißen, in der sie im populistischen demokratischen Prozess als die Partei auftreten muss, die einen weiteren schweren Terroranschlag zulässt, weil sie invasive Geheimdienstpraktiken ablehnt. In diesem Sinne könnte man sogar von einer Tyrannei der Mehrheit oder einem „demokratischen Sicherheitsstaat" sprechen.

D. Unterschiede in der Rechtskultur

Zwei Unterschiede in den Rechtskulturen Deutschlands und der Vereinigten Staaten scheinen für ihre unterschiedlichen Rechtskonzepte zu Sicherheit und Freiheit von Bedeutung zu sein. Der erste liegt in der jeweils eigenen Auffassung vom Rechtsstaat. Der zweite besteht in der Regulierungsdimension, deren Ausgestaltung durch ihre verschiedenen Wurzeln in den Traditionen von Common Law und Civil Law bedingt ist.

Deutschland und den Vereinigten Staaten ist ein eindeutiges Bekenntnis zum Rechtsstaat bzw. zur Rechtsstaatlichkeit gemeinsam. In Deutschland nimmt dies die Gestalt eines umfangreichen Rechtsrahmens materieller Grundrechte an, der vom Bundesverfassungsgericht energisch und umfassend ausgelegt und geltend gemacht wird. Das Verfassungsgericht verschafft der materiellen und tatsächlichen Wertordnung gegen ansonsten legitime demokratische Prozesse Geltung, deren Ergebnisse sich von den im Grundgesetz verbrieften Werten entfernen. Trotz der großartigen Tradition des Obersten Gerichtshofs in der Rechtsprechung zu den Grundrechten lässt sich das amerikanische Bekenntnis zur Rechtsstaatlichkeit als eher prozedural und weniger materiell orientiert beschreiben. Das heißt: Die Rechte in der amerikanischen Verfassung werden weitgehend ausgelegt und geltend gemacht in einer Weise, die die Rechtmäßigkeit und Gerechtigkeit der die Politik regelnden demokratischen Prozesse gewährleistet. Dies ist keine Jurisprudenz im Sinne einer materiellen Vorstellung von einer guten Gesellschaft. Die Unterscheidung zwischen den beiden Auffassungen von Rechtsstaat und ihrer Manifestation im amerikanischen Verfassungsrecht (im Sinne einer Verfahrensgerechtigkeit) und im deutschen Verfassungsrecht (im Sinne materieller Gerechtigkeit) wird auch von Rawls und Habermas bekräftigt.

Der Unterschied ist deshalb wichtig, weil er dazu beiträgt, den deutschen Sinn für die Verankerung des Schutzes der Privatsphäre als materielles Recht zu erklären, das durch die Justiz gegen politische Kräfte anzuwenden ist. Und er trägt zum Verständnis der amerikanischen Zurückhaltung bei, eben dies zu tun. Wie das Beispiel des Church-Ausschusses zeigt, ist die Frage, wie Amerika Sicherheit und Freiheit in Einklang bringt, genauso eine Angelegenheit politischen Handelns wie gerichtlicher Überprüfung. Es ist wahr, dass sich viele Freiheiten in Amerika dem Eingreifen der Gerichte verdanken. Dies zeigt kein Beispiel deutlicher als die Entscheidung des Obersten Gerichtshofs von 1954 im Fall *Brown v. Board of Education*; hier urteilte der Gerichtshof einmütig, dass die Rassentrennung in amerikanischen Schulen verfassungswidrig ist, wodurch er die Rassentrennungspolitik in den Vereinigten Staaten insgesamt in Frage stellte.[288] Bahnbrechende

Urteile des Obersten Gerichtshofs betreffen auch die Frauenrechte[289] und die freie Meinungsäußerung,[290] die Religionsfreiheit[291] sowie jüngst die Rechte Homosexueller.[292] Diese Errungenschaften lassen sich jedoch ebenso unter politischem Blickwinkel sehen. Und hinsichtlich des Verhältnisses von Freiheit und Sicherheit – ja sogar des umfassenderen Themas der exekutiven Gewalt – hat sich der Oberste Gerichtshof auffallend zurückgehalten. Dies hat viel zu tun mit seiner Achtung der komplizierten Gewaltenteilung, die durch die Verfassung vorgegeben wird – vom Gerichtshof häufig geltend gemacht mittels der von uns so genannten „Doktrin der politischen Frage". Hierbei handelt es sich eindeutig um ein prozedurales Verständnis von Rechtsstaatlichkeit.

Auch die verschiedenen Rechtstraditionen der beiden Länder – etwa Common Law und Civil Law – bieten einen wertvollen Erklärungsansatz für die unterschiedlichen Auffassungen davon, wie Sicherheit und Freiheit in Einklang zu bringen sind. Die Amerikaner erkennen großteils deshalb kein Recht auf informationelle Selbstbestimmung an, weil eine präventive Abwehr antizipierter Gefahren dem ordungspolitischen Verständnis des Common Law zuwiderläuft, das sich weniger an einer systematischen Prävention orientiert. Hingegen entwickelt sich das auf dem Common Law gründende amerikanische Recht an konkreten Einzelfällen. Das Common Law kennt keine Regulierung für potenzielle Probleme, sondern befasst sich dann mit Problemen, wenn sie tatsächlich auftreten. Für diesen faktenorientierten Pragmatismus ist das amerikanische Datenschutzrecht ein Beispiel. Wie weiter oben bereits erörtert, orientiert sich das Datenschutzrecht daran, sich mit konkretem Missbrauch personenbezogener Daten in je einzelnen Praxisbereichen zu befassen. Aus dem Blickwinkel des kodifizierten Rechts in Deutschland und Europa zeigt sich Datenschutz als abstraktes gesellschaftliches Phänomen, das *ex ante* durch umfassende und systematische Gesetze (Rechtsvorschriften in Verfassungen und Verträgen eingeschlossen) reguliert werden kann. Aus amerikanischer Sicht geht es weniger um potenziellen Missbrauch. Wichtig ist eher, dass ein konkreter Missbrauch nachgewiesen werden kann. Vor diesem Hintergrund ist die Frage – wenngleich man über die NSA sagen kann, unverhältnismäßige und schlecht durchdachte Programme zu verfolgen –, ob die personenbezogenen Daten zu Manipulationen und zu Missbrauch führten, wie sie etwa durch den Church-Ausschuss aufgedeckt wurden.