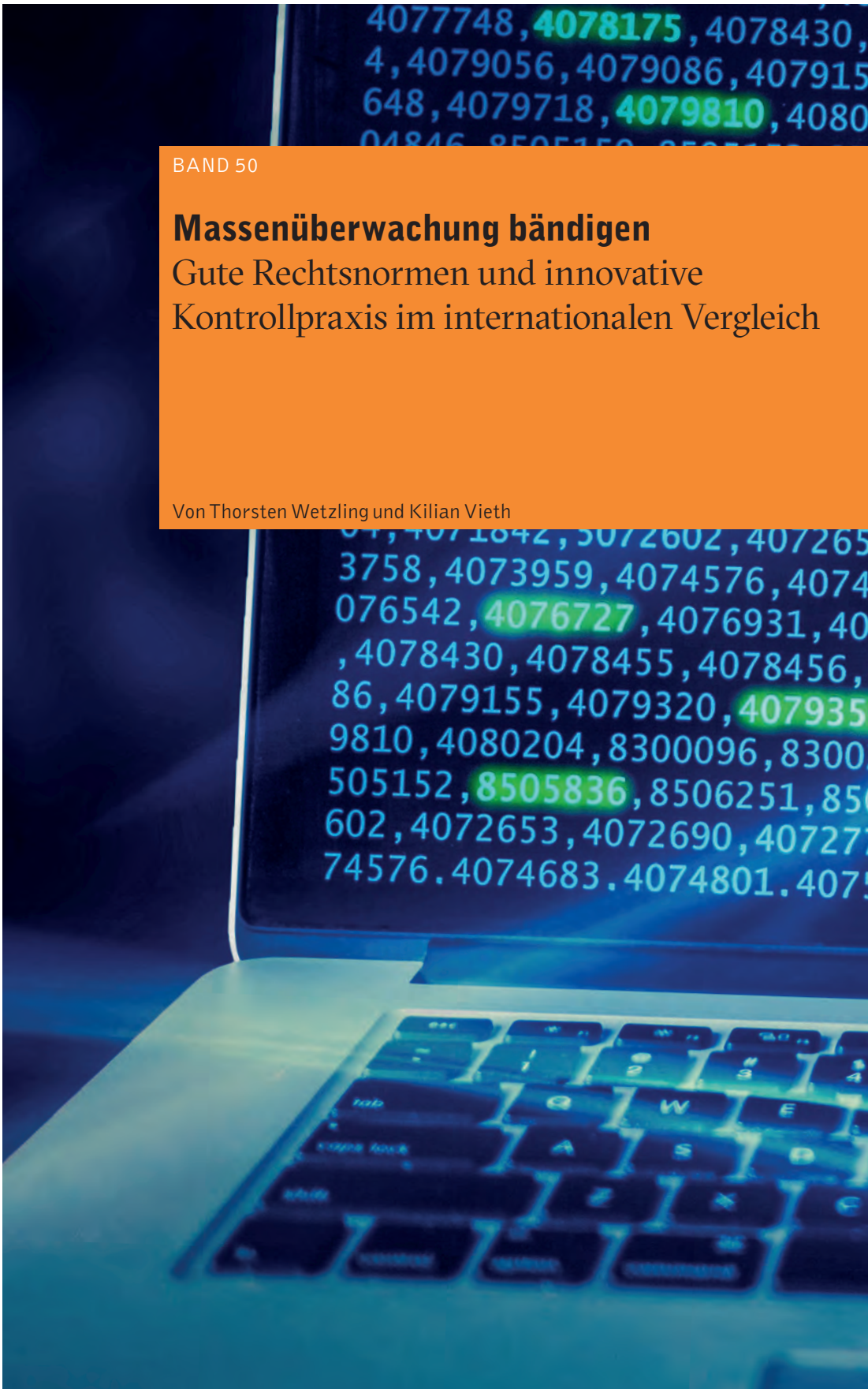
HEINRICH BÖLL STIFTUNG
DEMOKRATIE



BAND 50

Massenüberwachung bändigen

Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich

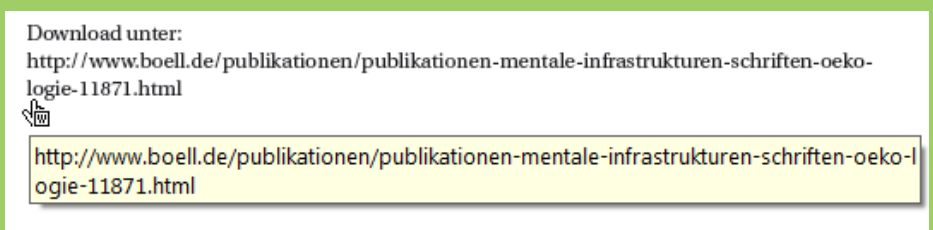
Von Thorsten Wetzling und Kilian Vieth

Stiftung Neue Verantwortung

Hinweis zu den Internetlinks

Einige Weblinks in dieser Broschüre sind durch technische Veränderungen im Satz wie z.B. Trennzeichen möglicherweise fehlerhaft. Andere können durch Veränderungen auf den adressierten Websites ungültig geworden sein.

Sie können die Vollständigkeit der Links mit dem Mauszeiger prüfen, wenn dieser auf dem Link steht und Sie das angezeigte Tiptool mit dem Druckbild vergleichen.



Im Bild wird der Link zwar vollständig übernommen, aber durch ein Trennzeichen fehlerhaft. Sie können den Fehler einfach im Browser-Fenster korrigieren.

In anderen Fällen ist es einfacher, Sie suchen das Dokument über Ihre Suchmaschine.

MASSENÜBERWACHUNG BÄNDIGEN

HEINRICH BÖLL STIFTUNG
SCHRIFTEN ZUR DEMOKRATIE

BAND 50

Massenüberwachung bändigen

Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich

Von Thorsten Wetzling und Kilian Vieth

Herausgegeben von der Heinrich-Böll-Stiftung

Die Autoren

Dr. Thorsten Wetzling leitet die Arbeit der Stiftung Neue Verantwortung im Themenfeld Überwachung, Grundrechte und Demokratie. Dort werden Ideen für eine effizientere und demokratischere Nachrichtendienstführung und -kontrolle in Deutschland und Europa entwickelt und mit Vertreter/innen der Zivilgesellschaft und Aufsichtsbehörden im neu gegründeten Europäischen Netzwerk Nachrichtendienstkontrolle (EION) vertieft. Thorsten Wetzling war Sachverständiger im Bundestag und im Europäischen Parlament, und seine sicherheitspolitischen Analysen sind in zahlreichen deutschen und europäischen Medien erschienen. Er ist Mitglied im Fachbeirat Europa/Transatlantik der Heinrich-Böll-Stiftung. Thorsten Wetzling hat am Genfer Hochschulinstitut für internationale Studien und Entwicklung in Politikwissenschaften promoviert.

Kilian Vieth koordiniert bei der Stiftung Neue Verantwortung den Themenbereich Überwachung, Grundrechte und Demokratie. Er erforscht und entwickelt dort Reformansätze für eine demokratischere und effizientere Überwachungs- und Nachrichtendienstpolitik in Deutschland und ganz Europa. 2018 wurde Kilian Vieth vor dem Hessischen Landtag als Sachverständiger für die Reform des Landesverfassungsschutzgesetzes gehört. Darüber hinaus liegen seine Forschungsinteressen im Bereich digitaler Menschenrechte, kritischer Sicherheitsforschung sowie politischer und sozialer Fragen algorithmischer Entscheidungsfindung.

Die **Stiftung Neue Verantwortung (SNV)** ist ein unabhängiger Think Tank, in dem konkrete Ideen zur Gestaltung des technologischen Wandels von Gesellschaft, Wirtschaft und Staat durch die Politik entwickelt werden. Um die Unabhängigkeit ihrer Arbeit zu gewährleisten, hat sich die Organisation für eine Mischfinanzierung durch unterschiedliche Geldgeber entschieden, darunter Stiftungen, öffentliche Stellen und Unternehmen. Fragen zur digitalen Infrastruktur, zu den sich wandelnden Beschäftigungsmustern, zu IT-Sicherheit oder Internetüberwachung betreffen mittlerweile wesentliche Bereiche der Wirtschafts- und Sozialpolitik, der inneren Sicherheit und des Schutzes der Grundrechte von Einzelpersonen. Die Expert/innen der SNV erstellen Analysen, entwickeln Vorschläge für die Politik und organisieren Konferenzen zu diesen und anderen Fachthemen. www.stiftung-nv.de

Massenüberwachung bändigen
Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich
Von Thorsten Wetzling und Kilian Vieth
Band 50 der Publikationsreihe «Schriften zur Demokratie»
Herausgegeben von der Heinrich-Böll-Stiftung

Übersetzung aus dem Englischen: Louise Hütz
Gestaltung: feinkost Designnetzwerk, S. Langer (basierend auf Entwürfen von blotto design)
Cover-Foto: «Data Security» Blogtrepreneur – flickr (CC BY 2.0)
Druck: ARNOLD group, Großbeeren
ISBN 978-3-86928-195-7

Diese Publikation kann bestellt werden bei: Heinrich-Böll-Stiftung, Schumannstr. 8, 10117 Berlin
T +49 30 28534-0 **F** +49 30 28534-109 **E** buchversand@boell.de **W** www.boell.de

INHALT

VORWORT

Moderne demokratische Gesellschaften sind in verstärktem Maße mit zwei schwer zu vereinbarenden Anforderungen ihrer Bürgerinnen und Bürger konfrontiert: dem Bedürfnis nach Schutz vor sich wandelnden Bedrohungslagen und dem Recht auf Unversehrtheit der Privatsphäre. Viele liberale Demokratien ringen darum, beiden Ansprüchen zu genügen, wie zahlreiche Beispiele der letzten Jahre – vom Versagen der Terrorprävention beim Anschlag auf dem Berliner Breitscheidplatz bis zu den Snowden-Enthüllungen über Massenüberwachung durch die NSA – zeigen.

Die prekäre Balance zwischen dem Bedürfnis nach Sicherheit einerseits und dem Recht auf Privatheit andererseits wird die Risikogesellschaft des 21. Jahrhunderts in verstärktem Maße begleiten, und die Kräfte der Globalisierung werden dazu beitragen, dass sich diese schwierigen Fragen in immer neuen Formen aufdrängen werden – sei es durch neue Bedrohungen des transnationalen Terrorismus oder der hybriden Kriegsführung, sei es durch neuartige technologische Überwachungsmöglichkeiten wie etwa der digitalen Gesichtserkennung. Umso wichtiger wird an dieser Stelle das gesellschaftliche Gespräch um ein vernünftiges Risikomanagement, das die Effektivität von Sicherheitsinstitutionen mit ihrer demokratischen Legitimität zusammen denkt.

Thorsten Wetzling von der Stiftung Neue Verantwortung ist diesen Fragen bereits in einer Studie der Heinrich-Böll-Stiftung aus dem Jahr 2016 nachgegangen: Im Band 43 unserer Demokratiereihe informierte er über den Stand der Nachrichtendienstkontrolle in Deutschland und zog eine ernüchternde Bilanz.

Mit der vorliegenden Studie wollen wir die Diskussion auf zweifache Weise verbreitern: Wir haben die Stiftung Neue Verantwortung gebeten, jenseits des deutschen Beispiels die Praxis der Nachrichtendienstkontrolle in einer Reihe von Schlüsselländern des transatlantischen Raums zu betrachten. Und wir wollen gleichzeitig über die Vergleichsstudie einen Perspektivwechsel in der Betrachtung des *Intelligence Oversights* versuchen und nicht mehr ausschließlich auf die Defizite der Nachrichtendienstkontrolle fokussieren, sondern auch ermutigende Beispiele herausheben, die sich in den jeweiligen Untersuchungsländern im Zuge der jüngsten Nachrichtendienstreformen gezeigt haben.

Die Studie darf sich daher durchaus auch als Aufforderung für die Community nationaler Regulierungsbehörden verstehen, über den nationalen Tellerrand zu schauen und sich von den *best practices* ihrer Nachbarländer inspirieren zu lassen.

Denn im Zuge der fortschreitenden Integration europäischer Außen-, Sicherheits- und Verteidigungspolitik und vor dem Hintergrund einer zunehmenden Kooperation westlicher Nachrichtendienste muss sich auch die demokratische Kontrolle dieser Dienste aus der nationalen Nabelschau befreien und den europäischen

und transatlantischen Austausch stärken. Dies gilt insbesondere in einer Phase westlicher Verunsicherung und autoritärer Versuchung, auch und gerade innerhalb der transatlantischen Gemeinschaft und der Europäischen Union. Denn robuste Kontrollgremien und gute Gesetze können als Bollwerk gegen die Aushebelung von Grundrechten dienen, sollte eine Regierung vom illiberalen Virus befallen werden, der zur Zeit in Europa und Amerika grassiert.

Wir erhoffen uns, mit der vorliegenden Vergleichsstudie gleichermaßen einem politischen und gesellschaftlichen Bildungsauftrag nachzukommen. Auf politischer Ebene erhoffen wir in Zeiten wachsender EU- und NATO-Skepsis den europäischen und transatlantischen Dialog über informationelle Selbstbestimmung und allgemein über individuelle Freiheits- und Menschenrechte voranbringen zu können. Denn die vorliegende Studie hat in vielen einzelnen Ländern ermutigende Beispiele effektiver demokratischer Nachrichtendienstkontrolle identifiziert, die eine breitere Würdigung verdienen würden. Eine liberale Wertegemeinschaft ist auf diesen Austausch von *best democratic practices* angewiesen.

Auf gesellschaftlicher Ebene erhoffen wir uns, durch unsere sehr detailgenaue Vergleichsstudie die Frage nach einer geeigneten Regulierung westlicher Nachrichtendienste ein wenig zu versachlichen. Denn die Nachrichtendienstdebatte krankt seit jeher an einem Mangel an professioneller Analyse und einem Überangebot an empirisch nicht überprüften Hypothesen bis hin zu Verschwörungstheorien.

Wir sind es unseren Leser/innen schuldig, ihnen die bestmögliche Handreichung für eine kritische Diskussion westlicher Nachrichtendienstpraxis zur Verfügung zu stellen, und hoffen mit dieser Studie die Debatte um demokratisch legitimierte und gleichzeitig effektive Nachrichtendienste ein Stück weitergebracht zu haben.

Berlin, im März 2019

Giorgio Franceschini
Heinrich-Böll-Stiftung
Leiter des Bereichs Außen- und Sicherheitspolitik

GELEITWORT

Am 13. September 2018 hat der Europäische Gerichtshof für Menschenrechte im Fall Big Brother Watch et al. v. UK eine weitreichende Entscheidung getroffen. Auf dem Prüfstand lagen unter anderem die massenhafte Kommunikationsüberwachung und der internationale Austausch nachrichtendienstlicher Erkenntnisse sowie deren Vereinbarkeit mit der Europäischen Menschenrechtskonvention. Mit dem Urteil hat der Gerichtshof erstmals die Einhaltung von Artikel 8 der Konvention, dem Recht auf Achtung des Privat- und Familienlebens, beim Informationsaustausch berücksichtigt. Im Vorfeld dieses Urteils hat die Stiftung Neue Verantwortung intensiv daran gearbeitet, Ihnen dieses Kompendium zur Massenüberwachung von ausländischer Kommunikation bereitzustellen.

Die Komplexität von Befugnissen zur Massenüberwachung durch Geheim- und Sicherheitsdienste zu untersuchen ist keine leichte Aufgabe. Dies gilt umso mehr, wenn es um die Organisation und praktische Umsetzung derartiger Befugnisse in den unterschiedlichen Ländern der westlichen Welt geht. Die Stiftung Neue Verantwortung hat ein beeindruckendes Ergebnis erzielt. Das vorliegende Kompendium zu guten rechtlichen Schutzmaßnahmen und Kontrollinnovationen beleuchtet die rechtlichen Schwierigkeiten der Massenüberwachung gründlich. Es verortet die Notwendigkeit angemessener Rechtsmittel und die zentrale Rolle, die Aufsichtsbehörden bei der Einhaltung dieser Rechtsmittel in der Praxis spielen. Zudem liefert das Kompendium uns – also den Aufsichtsbehörden in Deutschland und den Niederlanden – Denkanstöße und bringt uns zu den folgenden gemeinsamen Überlegungen:

Zunächst muss die nationale Gesetzgebung Aufsichtsbehörden robuste rechtliche Kriterien an die Hand geben, um die Nutzung von Befugnissen zur Massenüberwachung auszuwerten, sowie adäquate Kontrollmittel und -maßnahmen. Nur so können Aufsichtsbehörden die komplexe Verarbeitung großer Datenmengen, die mit diesen Befugnissen einhergeht, wirksam überwachen. Es ist unerlässlich, dass Gesetzgeber die rechtlichen Rahmenwerke anderer Länder kennen und von ihnen lernen.

Im nächsten Schritt müssen Aufsichtsbehörden ihre eigenen Kompetenzen und Kontrollpraktiken kritisch überdenken, um effektive Kontrollmethoden zu entwickeln. Um uns einer von technologischen Entwicklungen und einer verstärkten nachrichtendienstlichen Zusammenarbeit geprägten, operativen Wirklichkeit anzupassen, müssen wir unsere technische Expertise vertiefen und unsere Kontrollmethoden verbessern. Nur wenn wir uns darüber austauschen, wie wir Innovationen im Aufsichtsbereich vorantreiben, können wir von den Fortschritten und *best practices* der anderen lernen.

Zu guter Letzt müssen Aufsichtsbehörden enger zusammenarbeiten, um den internationalen Datenaustausch und die Entwicklungen zu einer ausgeweiteten

Kooperation von Nachrichtendiensten effektiver zu kontrollieren. Dazu könnten die gemeinsame Verarbeitung von Daten und die gemeinsame Ausarbeitung von nachrichtendienstlichen Produkten gehören. Aufsichtsbehörden müssen sich dringend zusammenschließen, um Mittel und Wege zu finden, wie sich eine solche nachrichtendienstliche Kooperation wirksam beaufsichtigen lässt.

Für all diese Aspekte ist das vorliegende Kompendium ein wichtiges Werkzeug. Es liefert einen exzellenten Überblick über die *best practices* bei rechtlichen Schutzmaßnahmen und bei der Entwicklung von Kontrollmöglichkeiten. Darüber hinaus ermöglicht es uns detaillierte Einblicke in die rechtlichen Schwierigkeiten der Massenüberwachung und die Entscheidungen, die bei der Strukturierung nationaler rechtlicher Rahmenwerke zur Regelung dieser Prozesse getroffen wurden. Das Kompendium hilft uns zu verstehen, warum rigorose und effektive Kontrollmechanismen so dringend benötigt werden und in welchen Bereichen unsere eigene Kontrollpraxis möglicherweise zu kurz greift. Nicht zuletzt bietet es einen hervorragenden Ausgangspunkt, um die Zusammenarbeit zwischen Aufsichtsbehörden zu stärken, und eine Basis zu finden, um das Zusammenwirken unterschiedlicher Nachrichtendienste gemeinsam zu beaufsichtigen.

Wir laden Sie ein, dieses Kompendium zu studieren – es ist eine hervorragende Lektüre und ein exzellenter Ausgangspunkt, um sich an der internationalen Diskussion zu beteiligen, die so dringend nötig ist.

Harm Brouwer
Vorsitzender der niederländischen Kontrollbehörde für die Nachrichten- und Sicherheitsdienste (CTIVD)

Bertold Huber
Stellvertretender Vorsitzender der G10-Kommission des Deutschen Bundestages

Zusammenfassung

Die beispiellosen öffentlichen Diskussionen über die Regierungsverantwortung und Kontrolldefizite seit den Enthüllungen von Edward Snowden haben nichts an der Tatsache geändert, dass alle großen Demokratien ihren Nachrichtendiensten auch weiterhin gestatten, Kommunikationsdaten im großen Stil abzufangen. Viele Menschen stellen zwar die Effizienz von Massenüberwachung und ihre Vereinbarkeit mit den Grundrechten in Frage. Andere machen sich Sorgen über die daraus erwachsenen Konsequenzen für das Sozialgefüge in demokratischen Gesellschaften.

Tatsache ist jedoch, dass die meisten Parlamente in den jüngsten Reformen des Nachrichtendienstrechts die Überwachungsbefugnisse ihrer Nachrichtendienste deutlich ausgeweitet statt beschnitten haben. Mehr noch: Erst kürzlich hat der Europäische Gerichtshof für Menschenrechte den schwedischen Rechtsrahmen für die Massenüberwachung von ausländischer Kommunikation bestätigt und in seinem «Big Brother Watch»-Urteil vom September 2018 die Vorgehensweise als «wertvolle Maßnahme» im Kampf gegen den Terrorismus bezeichnet. Wir dürfen also davon ausgehen, dass uns die Praxis der Massenüberwachung auch in den nächsten Jahren begleitet. Sollte dies der Fall sein, ist es höchste Zeit, nationale rechtliche Rahmenbedingungen und deren jeweilige Kontrollsysteme einer Vergleichsprüfung zu unterziehen und gute Praktiken zu identifizieren. Sowohl nationale Gerichte als auch der Europäische Gerichtshof für Menschenrechte haben nationale Regierungen schon häufig wegen Mängeln oder Schwachstellen in ihren Kontrollregimen gerügt. In seiner Entscheidung vom September 2018 hat der Europäische Gerichtshof für Menschenrechte erneut strengere und effektivere Kontrollmechanismen gefordert.

Was aber macht eine wirksame Kontrolle der massenhaften Kommunikationsüberwachung in der Praxis aus, insbesondere mit Blick auf die rasante Entwicklung der Überwachungstechnologien? Gerichte werden hier keine neuen Regeln entwerfen oder spezifische Maßnahmen zur Rechenschaftspflicht vorschreiben. Dies ist und bleibt die schwierige und notwendige Aufgabe demokratisch legitimierter Gesetzgeber.

Die vorliegende Studie zeigt Beispiele für gesetzliche Regelungen und Kontrollpraktiken auf, die sich als vergleichsweise ausgewogene oder innovative Antworten auf die vielen komplexen und oft unzureichend adressierten Fragen hervorheben. Das Kompendium identifiziert und kontextualisiert hervorhebenswerte Regeln und Praktiken verschiedener nationaler Überwachungsregime. Es zeigt, dass jedes Land – trotz verfassungsrechtlicher und politischer Unterschiede und ungeachtet der jeweiligen Reformprozesse – sehr viel von seinen internationalen Partnern lernen kann. Diese Beispiele sollten nach Möglichkeit in vielen Ländern erörtert und nachgeahmt werden, da sie die Legitimität und Effektivität einer kontroversen Praxis stärken, deren

gänzliche Unterbindung vor europäischen Gerichten derzeit nicht erstritten werden kann.

I Einleitung

Alle Demokratien brauchen Nachrichtendienste, um ihre offenen Gesellschaften zu schützen. Diese Dienste liefern Entscheidungsträger/innen nützliche Informationen zu einer Vielzahl von sicherheits- und außenpolitischen Themen. Ganz gleich, ob es zum Beispiel um Terrorismus, die Verbreitung von Massenvernichtungswaffen oder organisierte Kriminalität[1] geht: Es werden Informationen benötigt, die über die öffentlich zugänglichen Daten hinausgehen. Nachrichtendienste beherrschen eine Reihe geheimer Methoden, um an derartige Informationen zu gelangen. Einige Methoden, darunter die elektronische Überwachung von Kommunikationsdaten, sind nur schwer mit den Grundprinzipien der demokratischen Rechtsstaatlichkeit zu vereinbaren, wie zum Beispiel das Gebot der Transparenz und der Zurechenbarkeit. Zudem können sie Grund- und Menschenrechte verletzen, beispielsweise das Recht auf Privatsphäre, das Recht auf Meinungs- und Redefreiheit oder auf Vereinigungs- und Versammlungsfreiheit. Um das öffentliche Vertrauen und die Rechtmäßigkeit der Nachrichtendienstführung zu garantieren, müssen Demokratien sämtliche nachrichtendienstlichen Aktivitäten auf eine solide Rechtsgrundlage stellen und einer strikten und wirksamen Kontrolle unterziehen.

Dieser Umstand ist und bleibt eine große Herausforderung.[2] Zugegeben: Die Demokratisierung der Nachrichtendienste und die Professionalisierung von Kontrollmaßnahmen haben in den letzten Jahrzehnten in vielen etablierten Demokratien signifikante Fortschritte gemacht. Parlamente in Europa, in Nordamerika und Australasien beispielsweise haben ihre nationalen Nachrichtendienstgesetze immer wieder reformiert und den Zuständigkeitsbereich und die Ressourcen unabhängiger Aufsichtsbehörden im Laufe der Zeit ausgeweitet. Daneben haben Länder wie die USA Transparenzprinzipien eingeführt, die die Regierung verpflichten, der Öffentlichkeit mehr Informationen bereitzustellen, als dies jemals zuvor der Fall war.[3] Dennoch darf

1 Die Autoren bedanken sich herzlich für die sachkundige und tatkräftige Unterstützung von Mouna Smaali bei der Erstellung der vorliegenden Studie.

2 Aktuelle Erfahrungen und zukünftige Herausforderungen der demokratischen Kontrolle der Nachrichtendienste in unterschiedlichen Kontexten werden z.B. diskutiert in Goldman and Rascoff (Hrsg.): «Global Intelligence Oversight. Governing Security in the Twenty-First Century», 2016; Leigh and Wegge (Hrsg.): «Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World», 2018; Anderson: «New Approaches to Intelligence Oversight in the U.K.», 2. Januar 2018, https://www.lawfareblog.com/new-approaches-intelligence-oversight-uk; Wetzling: «Options for More Effective Intelligence Oversight», 2017, https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

3 U.S. Principles of Intelligence Transparency for the Intelligence Community, einsehbar unter: https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

eine demokratische Nachrichtendienstführung nicht als selbstverständlich betrachtet werden, wie die eklatanten Versäumnisse und Defizite im Bereich der Steuerung und Kontrolle der Fernmeldeaufklärung im Vorfeld der Snowden-Enthüllungen gezeigt haben. Es steht viel auf dem Spiel und die Versuchung, Privilegien wie die behördliche Geheimhaltung auszunutzen, ist groß. Die Legitimität nachrichtendienstlicher Tätigkeiten muss immer wieder aufs Neue erworben werden, und sollte, selbst im Falle schwerer Sicherheitsbedrohungen, nicht einfach für bare Münze genommen werden. Vielmehr sind die effektive Steuerung und demokratische Kontrolle von Nachrichtendiensten das Ergebnis komplexer, vielschichtiger Anstrengungen, die nicht allein in den Händen einiger weniger Technokrat/innen liegen dürfen. Neben internen Prüfungen sind eine strenge Fachaufsicht und parlamentarische Kontrolle vonnöten. Darüber hinaus bedarf es starker, unabhängiger und technisch versierter juristischer Kontrolle, um einzelne nachrichtendienstliche Maßnahmen zu genehmigen und zu prüfen. Außerdem sollten Gesetzgebungsverfahren und die Kontrollpraxis in Bezug auf Nachrichtendienste unabhängig und öffentlich durch kritische Medienberichterstattung und Forschung begleitet werden. Zusammen ergibt sich aus den Arbeitsprozessen auf diesen unterschiedlichen Ebenen die sogenannte Input-Legitimation (Fritz Scharpf) der Nachrichtendienste. Und sie stellen auch sicher, dass die Ergebnisse von nachrichtendienstlichen Strategien und Entscheidungen fundiert und wirksam sind (Output-Legitimation).

Die Nachrichtendienstführung ist also vielmehr ein Prozess als ein fertiges Produkt. Aufgrund der Geschwindigkeit des technologischen Wandels sollten Nachrichtendienstgesetze und der Kontrollrahmen regelmäßig aktualisiert werden. Der technologische Wandel bringt neue Werkzeuge oder vollkommen neue Praktiken ins Spiel, die zum Teil auch von Aufsichtsbehörden eingesetzt werden sollten, damit sie nicht ins Hintertreffen geraten und effizienter arbeiten können.[4] Auch der politische Druck, die allgemeine Sicherheit zu stärken, oder neue Enthüllungen über Rechtsverstöße von Nachrichtendiensten können erneute Prüfungen des Rechtsrahmens und der Kontrollarchitektur verlangen. Darüber hinaus – und das gilt nicht nur für das Vereinigte Königreich – scheint es, dass «viele der täglichen Aktivitäten der Sicherheitsbehörden nicht gesetzlich geregelt sind. Wichtige Fragen im Hinblick auf Ausrichtung, Durchführung und Kooperation mit anderen Behörden im In- und Ausland

4 Eine aktuelle Zusammenfassung zum Einsatz von KI-Methoden bei der Analyse großer Datensätze findet man z. B. bei Hoadley and Lucas: «Artificial Intelligence and National Security», 26. April 2018, 9, https://fas.org/sgp/crs/natsec/R45178.pdf.

sind zweifelsohne Gegenstand der internen Führung. Aber die Öffentlichkeit erfährt kaum etwas darüber, und noch weniger davon ist gesetzlich geregelt.»[5]

Wenn Demokratien ihren Nachrichtendiensten gestatten, im Namen der nationalen Sicherheit digitale Überwachungsbefugnisse auszuüben, müssen sie dies im Rahmen der Rechtsstaatlichkeit und der gegenseitigen Kontrolle tun. Angesichts der zahlreichen kulturellen, politischen und verfassungsrechtlichen Unterschiede, die allein schon zwischen den Demokratien bestehen, wird es in diesem Politikfeld auf absehbare Zeit keine allgemein verbindlichen Konventionen geben. Trotzdem lohnt es sich, genauer zu untersuchen, wie geläufige Herausforderungen in den unterschiedlichen Systemen angegangen werden. Daraus lassen sich dann innovative Ansätze und Ideen ermitteln, die über die einzelne Rechtsordnung hinweg wegweisend sein können.

In diesem Kompendium konzentrieren wir uns auf die Massenüberwachung von ausländischer Kommunikation. Damit meinen wir das Erheben und das weitere Verarbeiten von sehr großen Datenmengen, die über unterschiedliche Telekommunikationsnetze (Glasfaser-, Mobilfunk- und Satellitennetze) übermittelt werden. Die ausländische Kommunikation wird in Form von elektronischen Signalen abgefangen, die aus unterschiedlichen Arten von Verkehrs- und Inhaltsdaten besteht. Dies ist umstritten, da das Abhören «nicht gezielt» erfolgt – mit anderen Worten: nicht auf ein bestimmtes Individuum ausgerichtet ist.[6] David Anderson, ehemaliger unabhän-

5 McKay and Walker: «Legal Regulation of Intelligence Services in the United Kingdom», 2017, 1887, eigene Übersetzung. Einen aktuellen Überblick zu offenen Fragen in Bezug auf den internationalen Austausch von Nachrichtendiensten findet man hier: International Network of Civil Liberties Organizations: «Unanswered Questions – International Intelligence Sharing», Juni 2018, https://www.inclo.net/pdf/iisp/unanswered_questions.pdf. In Deutschland beispielsweise muss für den Erwerb und die anschließende Nutzung von Daten, die von Privatunternehmen oder dem Militär erfasst und von Nachrichtendiensten verwendet und verändert werden können, noch eine solidere Rechtsgrundlage geschaffen werden. Siehe: Wetzling: «Germany's intelligence reform: More surveillance, modest restraints and inefficient controls», 2017, 13–16, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

6 Viele Länder, darunter Deutschland und die USA, wenden unterschiedliche rechtliche Kriterien für die Massenüberwachung von ausländischer Kommunikation an. Kommunikation, bei der sowohl der Ursprung als auch das Ziel außerhalb des eigenen Landes liegen, wird anders behandelt als Kommunikation, bei der ein Ende im Hoheitsgebiet der überwachenden Behörde liegt. Andere Länder wie die Niederlande unterscheiden bei der Massenüberwachung nicht zwischen ausländischer und inländischer Kommunikation. Ob Überwachungsgesetze ausländische Personen rechtlich diskriminieren könnten oder nicht und ob es technologisch möglich ist oder nicht, unterschiedliche Datenschutzregelungen tatsächlich durchzusetzen, wird vielfach diskutiert. Siehe z. B. Swire, Woo, and Desai: «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft)», 2018, oder Lubin: «We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance», 2017, https://papers.ssrn.com/abstract=3008428. Dennoch gibt es gute Argumente gegen diese Praxis, siehe beispielsweise die aktuelle Anfechtung des BND-Gesetzes oder die Gutachten, die sich mit den technischen Mängeln der derzeitigen Datenfiltersysteme in Deutschland befassen: Rechthien: «Sachverständigen-Gutachten gemäß Beweisbeschluss, 1. Untersuchungsausschuss (NSA-UA) der 18. Wahlperiode des Deutschen Bundestages», September 2016, https://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf.

giger Gutachter für Anti-Terror-Gesetzgebung in Großbritannien, warnte, dass sich der Einsatz von Massenüberwachung sehr negativ auf Menschenrechte auswirken könnte. Derartige Befugnisse beinhalteten den potenziellen staatlichen Zugriff auf die Daten vieler Menschen, bei denen nicht der geringste Verdacht vorliege, die nationale Sicherheit zu gefährden oder in schwere Straftaten verwickelt zu sein. Jeder Missbrauch derartiger Befugnisse könne sich daher in großem Maße besonders auf Unschuldige auswirken. Schon der Eindruck, dass ein Missbrauch möglich sei und unter Umständen nicht ans Licht komme, könne ein zersetzendes Misstrauen fördern.[7]

Die Massenüberwachung von (Auslands-)[8]Kommunikation ist seit Jahren bestehende Praxis von Nachrichtendiensten. Ein verstärktes öffentliches Interesse nach den Enthüllungen von Edward Snowden und die Tatsache, dass es in vielen Ländern keinen ausreichenden Rechtsrahmen – geschweige denn eine effektive Kontrolle – dafür gab, hat seitdem viele Parlamente dazu gebracht, neue Gesetze zu verabschieden oder bestehende Regeln zu überarbeiten. Mittlerweile gibt es eine Vielzahl neuer Gesetze, neuer Kontrollinstitutionen und -verfahren, und der Europäische Gerichtshof für Menschenrechte hat im Juli und September 2018 entschieden, dass die Praxis der Massenüberwachung von ausländischer Kommunikation durchaus mit der Europäischen Menschenrechtskonvention[9] vereinbar sein kann.

Ein guter Zeitpunkt also, die nationalen Rechtsrahmen und Kontrollpraktiken auf den Prüfstand zu stellen. Einige derzeit noch anhängige Rechtsverfahren in nationalen und europäischen Gerichten könnten (und sollten unserer Meinung nach) dazu führen, dass bestimmte Rechtsrahmen überarbeitet werden müssen. Jedoch ist es unwahrscheinlich, dass die Praxis der Massenüberwachung von Kommunikation gänzlich untersagt wird. Im Gegenteil: Sie wird wohl eine der wichtigsten Praktiken moderner Nachrichtendienste bleiben.[10]

Umso wichtiger erscheint es daher, gute Lösungen für die vielen komplexen Probleme und offenen Fragen rund um die Regierungsverantwortung und die Effizienz der Kontrolle zu finden. Hierzu soll dieses Kompendium einen Beitrag leisten. Es identifiziert und kontextualisiert gesetzliche Regelungen und Beispiele aktueller

---

7 Anderson: «Report of the Bulk Powers Review», 9.6.2016, https://nls.ldls.org.uk/welcome.html?ark:/81055/vdc_100035016622.0x000001.

8 In einigen Ländern gibt es detaillierte Gesetze, die die Massenerfassung von Kommunikation, die vom In- ins Ausland geht, regeln. Doch diese Gesetze haben unter Umständen keinen expliziten Rechtsrahmen für Kommunikation vom Ausland ins Ausland. Andere wiederum unterscheiden in ihren jeweiligen Nachrichtendienstgesetzen überhaupt nicht zwischen aus- und inländischer Kommunikation. Wir versuchen zwar, die Regulierung der Massenüberwachung im Allgemeinen zu beleuchten, doch in gewissen Punkten wird die spezifische Bezugnahme auf ausländische Kommunikation wichtig für die Anwendung von rechtlichen Schutzklauseln und Kontrollpraktiken. In diesen Fällen nehmen wir konkret Bezug auf die jeweilige Regelung.

9 Europäischer Gerichtshof für Menschenrechte, «Case of Centrum För Rättvisa v. Sweden (Application No. 35252/08)», 2018, http://www.statewatch.org/news/2018/jun/echr-sweden-Judgment-bulk-interception-communications-FULL.pdf.

10 Die Entwicklungen im Bereich der verschlüsselten Kommunikation verschieben jedoch das Hauptaugenmerk zunehmend auf Techniken wie die Ausnutzung von Sicherheitslücken in Soft- und Hardware.

Kontrollpraxis für die Massenüberwachung von ausländischer Kommunikation aus unterschiedlichen Demokratien. Die Beispiele sind – verglichen mit anderen Systemen – hervorhebenswert, weil sie entweder die Vereinbarkeit mit den Grundprinzipien demokratischer Rechtsstaatlichkeit fördern oder den Menschenrechtsschutz stärken. Zudem werden Verfahren aufgeführt, die einen innovativen Versuch darstellen, die Effektivität der Kontrolle mithilfe neuer technischer Mittel oder grundlegend neuer Ansätze zu verbessern.

Wir sind überzeugt, dass alle Demokratien von einer umfassenden Diskussion über gute Rechtsnormen und innovative Kontrollpraxis profitieren können. Aller relevanten und berechtigten Kritik an den derzeitigen Nachrichtendienstreformen zum Trotz[11] haben die meisten dieser Reformen auch individuelle Änderungen mit sich gebracht, die signifikante Verbesserungen darstellen. Zusammengenommen zeichnen diese Praktiken ein neues Bild, das wiederum helfen kann, Chancen bei der Fortentwicklung nationaler Rechtsrahmen aufzuzeigen. Um daraus eine Reformagenda auszuarbeiten, ist Fachwissen erforderlich. Zudem bedarf es politischer Entschlossenheit, um nationale Schwachpunkte zu überwinden. Die Beispiele aus anderen Ländern zeigen den weiteren Spielraum für Reformen und beweisen, dass die Welt nicht untergeht, wenn ambitionierte Lösungen für besseren Grundrechtsschutz oder eine effektivere Kontrolle implementiert wurden.

11 Lubin: «Legitimizing Foreign Mass Surveillance in the European Court of Human Rights», 2. August 2018, https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.

II Methodik

Wenn Demokratien ihren Nachrichtendiensten gestatten, ausländische Kommunikation in großem Stil elektronisch zu überwachen, müssen sie dies im Rahmen der geltenden Gesetze tun. Gleichzeitig müssen sie sicherstellen, dass diese Vorgehensweise einer effektiven und unabhängigen Kontrolle unterliegt. Was aber bedeutet das in der Praxis? Und wie lässt sich am besten zwischen guten und schlechten rechtlichen Schutzmaßnahmen und effizienten und ineffizienten Kontrolldynamiken unterscheiden?

Um dies herauszufinden, haben wir eine Vielzahl an öffentlichen Quellen herangezogen, darunter Kommentare zum Recht der Nachrichtendienste, Berichte von Aufsichtsbehörden, Dokumente aus Gerichtsverfahren sowie Analysen zur Geheimdienstpolitik.[12] Wir haben ein eigenes Analyseschema entwickelt (Abbildung 1) und eine Reihe von Interviews mit unterschiedlichen Sachverständigen (darunter

12 Einige aktuelle Zusammenfassungen zu den neuen Nachrichtendienstgesetzen und der Reform der Kontrollmechanismen in Bezug auf Kanada, Frankreich, Deutschland, das Vereinigte Königreich und die USA sowie einige Vergleichsstudien findet man hier: Forcese: «Bill C-59 and the Judicialization of Intelligence Collection. Draft Working Paper 04-06-18», 2018; Parsons, Gill, Israel, Robinson, Deibert: «Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters)», 18. Dezember 2017. The Citizen Lab, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2017, https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf; Chopin: «Intelligence Reform and the Transformation of the State: The End of a French Exception», 2017, https://doi.org/10.1080/01402390.2017.1326100; Ohm: «The Argument against Technology-Neutral Surveillance Laws», 2010, https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr88&div=60&id=&page=; Tréguer: «From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France», Oktober 2016; Schaller: «Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden», 2018; Wetzling: «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficent Controls», 2017, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf; Anderson: «A Question of Trust: Report of the Investigatory Powers Review», 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf; McKay: «Blackstone's Guide to the Investigatory Powers Act 2016», 2018; Smith: «A Trim for Bulk Powers?», 7. September 2016, https://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html; Donohue: «The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law», 2017, https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law; Wizner: «What Changed after Snowden? A U.S. Perspective», 2017; Agentur der Europäischen Union für Grundrechte: «Surveillance by Intelligence Services – Volume I: Member States' Legal Frameworks», 22. Oktober 2015, http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services; Agentur der Europäischen Union für Grundrechte: «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update», 2017, http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega.

Rechts- und Computerwissenschaftler/innen, Verwaltungsexpert/innen in den Ministerien, Beschäftigte in Aufsichtsgremien und Industrievertreter/innen, siehe Anhang) geführt, um weitere Informationen zur derzeitigen Praxis zu erhalten. Nachdem wir ausreichend Material gesammelt hatten, haben wir einen ersten Entwurf des Kompendiums in zwei Workshops einer kritischen Prüfung unterzogen. Sowohl der Workshop des Europäischen Netzwerks Nachrichtendienstkontrolle im Mai 2018 mit Vertreter/innen von Aufsichtsgremien aus acht Nationen sowie der Workshop im Juni 2018 mit europäischen und nordamerikanischen Expert/innen aus der Zivilgesellschaft haben uns geholfen, unsere Erkenntnisse zu konkretisieren.[13]

Das Ergebnis dieser Arbeit ist das vorliegende Kompendium von *guten Praktiken zur Kontrolle von Massenüberwachung von (Auslands-) Kommunikation* aus unterschiedlichen nationalen Nachrichtendienstgesetzen und Kontrollsystemen in Europa, Nordamerika und Australasien. Unser Kompendium erhebt keinen Anspruch auf Vollständigkeit. Wir laden Sie ein, Ihre Gedanken und Vorschläge mit uns zu teilen. Wenn wir ein bestimmtes Beispiel aus einem Land aufführen, so bedeutet das im Übrigen nicht, dass es dieselbe oder eine ähnliche Praxis oder Regel nicht auch in einem anderen Rechtssystem gibt.

Wir betrachten eine Vorschrift oder einen Kontrollmechanismus als gut, wenn sie im Vergleich besseren Schutz vor potenziellen Rechtsverletzungen bieten, oder wenn eine Regelung vergleichsweise Rechtsnormen und innovative Kontrollpraxis in Bezug auf die verfassungsrechtliche Grundprinzipien stärkt oder weil sie ein technisches Mittel innovativ einsetzt, um eine effektivere Kontrolle zu ermöglichen.

Obwohl wir mithilfe unserer Methode gute Kommunikationsüberwachung identifizieren, haben wir nicht genügend Informationen zur Hand, um die generelle Qualität einzelner Überwachungsgesetze oder nationaler Kontrollarchitekturen zu beurteilen. Dabei spielen viele Faktoren eine Rolle, die wir an dieser Stelle nicht alle berücksichtigen können.[14] Jedes Land hat seine eigene soziale, rechtliche und politische Struktur, die die Regulierung und Reform des Nachrichtendienstrechts und das Recht und die Praxis der Kontrolle beeinflussen. Da wir uns hier nicht im Einzelnen mit diesen Unterschieden befassen können, werden wir auch keine Erklärungen zum übergeordneten Rechtsrahmen abgeben. Das bedeutet auch, dass die Anzahl der Nennungen eines nationalen Gesetzes oder eines Aufsichtsregimes nicht als Maßstab für die Bonität des gesamten Rechtsrahmens oder der demokratischen Nachrichtendienstkontrolle im jeweiligen Land interpretiert werden sollte.

13 Eine Liste der Befragten und der Workshop-Teilnehmer/innen ist im Anhang zu finden.

14 Eine Übersicht über diese Faktoren findet sich beispielsweise hier: Richardson and Gilmour: «Intelligence and Security Oversight. An Annotated Bibliography and Comparative Analysis», 2016; Zegart: «The Domestic Politics of Irrational Intelligence Oversight», 2011; Wetzling (Hrsg.): Same Myth, Different Celebration? Intelligence Accountability in Germany and the United Kingdom», 2010.

Im Fokus dieser Studie steht die strategische Fernmeldeaufklärung, mit besonderem Augenmerk auf ausländische Kommunikationsdaten.[15] Die strategische Fernmeldeaufklärung liefert Nachrichtendiensten «Massenzugriff [...] auf Daten von einer Bevölkerung, die selbst keiner bedrohungsbezogenen Aktivitäten verdächtigt wird».[16] Diese ungezielten (oder «massenhaften») SIGINT-Fähigkeiten gelten als Kronjuwelen der nationalen Nachrichtendienste. Es handelt sich um eine technisch ausgereifte und hochkomplexe Datenerfassungsmethode, die ein hohes Maß an internationaler Zusammenarbeit beinhaltet und sich über längere Zeit im Schatten vieler Demokratien entwickelt hat. Laut der National Security Agency (NSA) der USA leben wir «im Goldenen Zeitalter der elektronischen Überwachung».[17] Die Massenüberwachung ausländischer Kommunikation ist aber nur eine der vielen Methoden moderner nachrichtendienstlicher Arbeitsweisen.[18] Die gezielte Überwachung oder das Infiltrieren von Computernetzwerken sind zwei weitere bekannte Beispiele. Kommunikationsdaten können natürlich auch über das Eindringen in IT-Systeme massenhaft erfasst werden.[19] Aufgrund unserer beschränkten Ressourcen und im Sinne der Komplexitätsreduktion nehmen wir lediglich die massenhafte Überwachung von ausländischer Kommunikation im Rahmen der strategischen Fernmeldeaufklärung in den Fokus.

Welche Aspekte gilt es zu berücksichtigen, wenn es um die Schaffung einer Rechtsgrundlage für Massenüberwachung und deren juristische Kontrolle geht? Nach welchen Standards und Kriterien können wir die Qualität einer gesetzlichen

---

15 In diesem Bericht bezieht sich der Begriff «Kommunikationsdaten» sowohl auf den Inhalt von Kommunikation (z. B. der Text einer E-Mail) als auch auf Informationen über Kommunikation, auch bekannt als Metadaten bzw. Verkehrsdaten (z. B. die E-Mail-Adressen von Absender/in und Empfänger/in).

16 Forcese, 2018, 3, eigene Übersetzung.

17 National Security Agency/ Central Intelligence Agency: «(U) SIGINT Strategy», 2012, 2, https://edwardsnowden.com/wp-content/uploads/2013/11/2012-2016-sigint-strategy-23-feb-12.pdf, eigene Übersetzung.

18 Die gezielte Telekommunikationsüberwachung und aktive Operationen in fremden Computernetzwerken (z.B. der Zugriff auf Datensätze über das Hacken oder Stören von Computernetzwerken) sind nur zwei bekannte Beispiele für andere Methoden der Datenerfassung. Sie sind selbstverständlich auch wichtig und müssen ebenfalls streng beaufsichtigt und kontrolliert werden. Aufgrund unserer Ressourcen und zur Reduzierung der Komplexität konzentrieren wir uns in dieser Studie jedoch auf die massenhafte Überwachung von ausländischer Kommunikation. Bei der strategischen Fernmeldeaufklärung werden in der Regel große Datenmengen bei der Übertragung über Glasfaserkabel sowie Funk- und Satellitenverbindungen abgefangen. Daten lassen sich aber auch massenhaft durch Hacking-Aktivitäten sammeln. Um auf nicht verschlüsselte Daten zuzugreifen, ist das Hacking effektiver als die Erfassung von Daten auf dem Übertragungsweg, die heutzutage meist verschlüsselt sind.

19 Da immer mehr Menschen ihre Kommunikation verschlüsseln, wird diese Technik immer häufiger verwendet, da sie Nachrichtendiensten ermöglicht, vor der Verschlüsselung auf die Daten zuzugreifen. Auch das massenhafte Hacken von elektronischen Geräten (in Großbritannien «bulk equipment interference» genannt) muss streng kontrolliert werden. Eine aktuelle Diskussion zu diesem Thema findet man hier: Nyst: «Regulation of Big Data Surveillance by Police and Intelligence Agencies», 2018, https://1ing2s14id7e20wtc8xsceyr-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/Regulation-of-Big-Data-Surveillance-by-Police-and-Intelligence-Agencies.pdf.

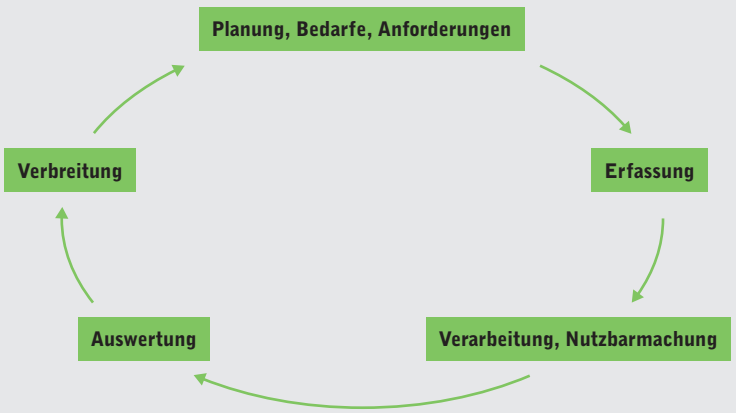
Abbildung 1: Analyseschema für die Steuerung und Kontrolle der strategischen Fernmeldeaufklärung

Bestimmung oder eines Kontrollmechanismus beurteilen? Klar ist: Diese Fragen müssen eingehender beleuchtet werden. Abbildung 1 unterteilt die relevantesten Aspekte bei der Steuerung und Kontrolle der massenhaften Überwachung von ausländischer Kommunikation in acht Phasen.

Ob es um die anfängliche strategische Planung, die Anordnungsprozesse oder die Genehmigungsverfahren geht, in der Gesetzgebung und der tatsächlichen Kontrollpraxis lassen sich eine Reihe von relevanten Standards beschreiben, die Demokratien einhalten sollten. Dasselbe gilt natürlich auch für die praktische Umsetzung von Befugnissen zur Massenüberwachung: Auch hier sind eine Vielzahl von Hürden und verfassungsrechtlichen Pflichten zu beachten, die offensichtlicher werden, wenn man den gesamten Prozess in einzelne Phasen unterteilt. Unser mehrphasiges Modell basiert auf dem sogenannten *Intelligence Cycle* (Abbildung 2), der traditionell in der einschlägigen Fachliteratur herangezogen wird, um die unterschiedlichen Phasen der nachrichtendienstlichen Informationsgewinnung zu erläutern.

Das Kompendium widmet jeder dieser acht Phasen (siehe Abbildung 1) ein eigenes Kapitel. Zunächst werden die typischen Aktivitäten der jeweiligen Phase kurz erklärt, ehe die relevanten Regulierungsaspekte und verfassungsrechtlichen Herausforderungen pro Phase beleuchtet werden. Anschließend präsentieren wir – soweit möglich – beispielhafte rechtliche Schutzmaßnahmen und konkrete Beispiele der Kontrollpraxis aus den von uns untersuchten Ländern. Beide Aspekte, sind extrem wichtig und bedingen einander. Ein umfassendes Nachrichtendienstrecht ist eine notwendige aber keinesfalls ausreichende Voraussetzung für die effektive, demokratische

Abbildung 2: Traditioneller «Intelligence Cycle»



Kontrolle der Massenüberwachung. Zwar lässt sich nicht alles rechtlich regeln[20], dennoch kann beispielsweise die Qualität eines Gesetzes oder die strikte Notwendigkeitsprüfung, die der Europäische Gerichtshof für Menschenrechte entwickelt hat, als Orientierungshilfe für Standards dienen, die ein modernes Nachrichtendienstrecht in unseren Demokratien erfüllen sollte.[21] Ob diese Standards in der Praxis dann auch wirklich eingehalten werden, steht dann aber auf einem ganz anderen Blatt. Dies muss unabhängig und wirksam geprüft werden. Hier kommt es auf die tatsächlichen Dynamiken der parlamentarischen und juristischen Kontrolle sowie deren Ressourcen, gesetzliche Befugnisse und technologische Hilfsmittel an.

Wir haben uns dabei auf Länder bezogen, in denen kürzlich Reformen durchgeführt wurden, und wo wir Zugang zu lokalen Ressourcen hatten. Genauer genommen traf dies auf Australien, Belgien, Dänemark, Deutschland, Frankreich, Kanada, Neuseeland, Niederlande, Norwegen, Schweden, Schweiz, USA und Vereinigtes Königreich zu.

Die hier aufgeführten Beispiele lassen sich unterschiedlichen Regulierungsdimensionen zuordnen, wie etwa »Einschränkung der Überwachungsbefugnis», »Transparenz» oder »Zugang zu Informationen», um nur einige zu nennen. Zur besseren

20 Aus Gründen des Quellenschutzes geben nationale Nachrichtendienste beispielsweise keine detaillierten Informationen zu einzelnen Werkzeugen, die in diesem Bereich eingesetzt werden. Andere legen nahe, dass es aufgrund der Geschwindigkeit, mit der sich Technologie wandelt, besser ist, technikneutrale statt technikspezifische Überwachungsrechte einzuführen. In diesem Punkt herrscht Uneinigkeit. Siehe: Ohm, 2010.

21 Siehe beispielsweise Malgieri and De Hert: «European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards ‚Good Enough' Oversight, Preferably but Not Necessarily by Judges», 2017, https://papers.ssrn.com/abstract=2948270; Murray, Fussey, and Sunkin: «Response to Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers», 2018, Punkte 3–14, https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf.

Orientierung enthält jedes Textfeld ein Symbol (Tabelle 1). Im IV. Kapitel (Diskussion) wird darauf Bezug genommen.

Tabelle 1: Regulierungsdimensionen der Praxisbeispiele mit entsprechenden Symbolen

Kategorie	Symbol
Einschränkung der Überwachungsbefugnis	
Transparenz	
Zugang zu Informationen	
Professionalität der Aufsicht	
Internationale Zusammenarbeit	
Regierungsverantwortung	
Sanktionen	
Einbindung des Privatsektors	

Es gibt eine Reihe wichtiger Vorbehalte, die wir den einzelnen Kapiteln noch voranstellen möchten: Beim Lesen des Kompendiums gilt es zunächst zu beachten, dass sowohl zwischen gezielter und ungezielter Überwachung (im Duktus des deutschen Nachrichtendienstrechts gesprochen: »Beschränkungen in Einzelfällen« und »strategischen Beschränkungen«) und zwischen nationalen und ausländischen Daten in vielen Nachrichtendienstgesetzen zum Teil gehörige Unterscheidungen mit Blick auf Schutzstandards und Rechtsfolgen getroffen werden (die mitunter noch immer einer gerichtlichen Prüfung unterliegen). Wenn wir hier Vergleiche aus Bereichen vornehmen, die diese Unterscheidungen tangieren, dann nur mit einem entsprechenden Verweis. Wenn wir Gefahr laufen, grundverschiedene Dinge miteinander zu vergleichen, erklären wir diese wichtigen Unterschiede und begründen, warum wir ausnahmsweise ein Regime zur gezielten Überwachung heranziehen, um auf eine bestehende Praxis aufmerksam zu machen, die in unseren Augen auch in Regimen

zur Massenüberwachung Berücksichtigung finden sollte. So ist es beispielsweise sinnvoll, einzelne Aspekte des US-Section-702-Programms in diesem Kompendium aufzuführen, das die Internet- und Telefondaten von Personen außerhalb der USA ins Visier nimmt, um an nachrichtendienstlich relevante Informationen zu gelangen.[22] Wir glauben, dass manche Rechtsnormen oder Kontrollpraktiken, die derzeit nur für die gezielte Überwachung gelten, ebenso für die massenhafte Datenerfassung geeignet wären, da auch sie sich, wie im Falle des Section-702-Programms klar mit Fragen rund um große Datenmengen befassen. Wenn wir uns im Kompendium also auf Programme zur gezielten Datenerfassung beziehen, machen wir dies mithilfe von orangefarbigen Textfeldern kenntlich.[23]

Darüber hinaus gibt es wichtige Unterschiede zwischen den Nachrichtendienstgesetzen von Ländern wie den USA und Deutschland, die sowohl per Gesetz als auch bei den Kontrollen noch stärker zwischen internationaler Kommunikation (z. B. wenn die Kommunikation entweder innerhalb der territorialen Zuständigkeit dieser Nation ihren Ursprung oder ihr Ziel hat) und ausländischer Kommunikation (z. B. wenn die Kommunikation nationales Hoheitsgebiet durchquert, aber weder ihren Ursprung noch ihr Ziel auf dem nationalen Gebiet liegt) unterscheiden. Andere Länder wie die Niederlande sehen in ihrem jeweiligen Nachrichtendienstrecht keine solche Unterscheidung vor. Auch dieser Umstand wird – wo erforderlich – berücksichtigt und in Kontext gesetzt.

---

22 Genauer gesagt, darf die US-Regierung nach Section 702 nur Ausländer zum «Überwachungsziel» erklären, die sich außerhalb der USA befinden. Das bedeutet allerdings nicht, dass sich diese Praxis nicht auch US-Amerikaner/innen auswirkt. Section 702 sieht zurzeit über 100.000 Ziele vor und beschränkt sich nicht auf Terroristen oder «Bad Guys», sondern auf alle Menschen im Ausland, deren Kommunikation sich möglicherweise auf die Durchführung der US-Außenpolitik bezieht, beispielsweise Diplomat/innen und Beamt/innen von befreundeten Staaten oder sogar Personen, die außerhalb einer US-Botschaft protestieren, eine globale Menschenrechtsorganisation unterstützen oder Blogs über internationale Beziehungen betreiben. Die Auswirkungen sind tiefgreifend: Section 702 kann unschuldige Ausländer/innen überwachen und im Verlauf die Kommunikation von unbescholtenen US-Bürger/innen abfangen, mit denen sie kommunizieren. Laperruque: «After ‹Foreign Surveillance› Law, Congress Must Demand Answers from Intelligence Community», The Hill, Januar 2018, https://thehill.com/opinion/cybersecurity/370271-after-foreign-surveillance-law-congress-must-demand-answersfrom. Siehe auch: Human Rights Watch: «Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act», 14. September 2017, https://www.hrw.org/news/2017/09/14/q-us-warrantlesssurveillance-under-section-702-foreign-intelligence-surveillance.

23 So wissen wir beispielsweise, dass der US Foreign Intelligence Surveillance Court (FISC) bei der Beaufsichtigung der «ungezielten» Datenerfassung («bulk collection») keinerlei Rolle spielt, seitdem das Section-215-Programm zur massenhaften Telefondatenerfassung im US Freedom Act beendet wurde. Wenn wir also eine einzelne Maßnahme herausgreifen, bei der der US FISC involviert ist, handelt es sich um eine Praktik, die sich auf die gezielte Datenerfassung bezieht. Während das Gesetz sehr deutlich zwischen massenhafter und gezielter Überwachung unterscheidet, gehen wir hier davon aus, dass diese Grenzen in der nachrichtendienstlichen Praxis in Wirklichkeit nicht so klar sind und dass die Debatte zur Regulierung von Massenüberwachung nach Möglichkeit gute Praktiken aus benachbarten Regimen heranziehen sollte.

Zweitens ist uns klar, dass unser mehrphasiges Modell zu linear aufgestellt ist. Nachrichtendienste verknüpfen häufig Daten, die sie mithilfe unterschiedlicher Techniken zusammentragen. So können Daten aus der Massenüberwachung weitere Maßnahmen nach sich ziehen. Die aus anderen Quellen gewonnenen Daten können in den verschiedenen Phasen der Datenverarbeitung und -auswertung wiederum mit den Daten aus der Massenüberwachung kombiniert werden. Unser Modell soll helfen, wichtige verfassungsrechtliche Regulierungsfragen zu identifizieren. Es beschäftigt sich aber nicht mit der Vermischung von Erzeugnissen unterschiedlicher digitaler Erfassungsmethoden moderner Nachrichtendienste. Daraus resultieren sicher weitere Herausforderungen für die demokratische Kontrolle, die in einer weiteren Studie untersucht werden könnten.

Drittens können einige der hier erörterten Rechtsnormen oder Kontrollpraktiken in anderen Phasen des Zyklus ebenfalls relevant oder sogar noch wichtiger sein. Wenn dies in unseren Augen der Fall ist, verweisen wir in der Diskussion auf die entsprechende Phase.

III Gute Praktiken im Überblick

Phase 1: Strategische Planung

Jede Regierung verfügt über begrenzte Ressourcen. Zudem können Gesetze die Erfassung von Daten in bestimmten Lebensbereichen untersagen oder beschränken. Der Grundrechtsschutz kann zum Beispiel der staatliche Datenerfassung entgegenstehen, wenn es um die Unverletzlichkeit der Wohnung geht.[24]

Unter Umständen sind Nachrichtendienste auch nicht in der Lage, zu viele Informationen effektiv zu verarbeiten, und müssen ihre Aktivitäten deshalb auf bestimmte Bereiche fokussieren.[25] Aufgrund dieser Faktoren müssen Regierungen politische und strategische Prioritäten setzen und die spezifischen Aufgaben ihrer Nachrichtendienste festlegen. In der ersten Phase des SIGINT-Prozesses geht es also darum, bestimmte nachrichtendienstliche Bedarfe zu identifizieren und zu formulieren. Im Idealfall fließen auch Erkenntnisse über den erzielten nachrichtendienstlichen Mehrwert bereits erfasster Daten in die strategische Planung ein.

Relevante Aspekte

Ein klares und spezifisches Mandat ist die Grundvoraussetzung für Transparenz und Rechenschaftspflicht bei der Erfassung von ausländischen Kommunikationsdaten. Das Mandat sollte spezifische Rechtsgrundlagen umfassen, anhand derer sich die Zulässigkeit und Verhältnismäßigkeit einer bestimmten Maßnahme beurteilen lassen. Zudem sollte es vorschreiben, welche Datenquellen oder Kommunikationsarten in die SIGINT-Datenerfassung einbezogen werden dürfen und welche nicht.

Laut der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Gerichtshofs der Europäischen Union ist Massenüberwachung nur zulässig, wenn sie für den Schutz der demokratischen Institutionen einer Gesellschaft zwingend

24 In Deutschland ist die Unverletzlichkeit der Wohnung zum Beispiel durch Artikel 13 des Grundgesetzes geschützt.

25 Es gibt Belege dafür, dass ein Überfluss an Daten zu einem Versagen der Nachrichtendienste führen kann: Gallagher: «Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure», 7. Juni 2016, https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/.

erforderlich ist.[26] Das bedeutet, dass die Nachrichtendienste der Unterzeichnerstaaten der Europäischen Menschenrechtskonvention und der Charta der Grundrechte der Europäischen Union Techniken zur massenhaften Datenerfassung nur in Bezug auf klar begrenzte Kategorien, die eine ernsthafte Bedrohung für eine demokratische Gesellschaft darstellen, einsetzen dürfen. Diese Kategorien sollten über ein generelles Verständnis dessen, was eine ernsthafte Bedrohung darstellt, hinausgehen.[27]

Hier spielen die bei der Festlegung der nachrichtendienstlichen Prioritäten beteiligten Akteure eine entscheidende Rolle. Unter Umständen gibt es sowohl eine externe Planung und Aufgabenverteilung durch Regierungsvertreter oder Minister außerhalb der Nachrichtendienste als auch eine interne Planung und Aufgabenverteilung durch diese Dienste. Die externe Planung und Aufgabenverteilung konzentriert sich üblicherweise eher auf eine strategische/politische Ebene, während die interne Planung in der Regel die Festlegung von Datenquellen oder Kommunikationsarten beinhaltet.

Wer kann diesen Prozess der Aufgabenverteilung beeinflussen und hinterfragen? Fließt bei der Planung zukünftiger Datenerfassung die Evaluation früherer Überwachungsmaßnahmen mit ein? Und wenn ja, wie genau? Wie werden kritische Positionen bei der Formulierung konkreter nachrichtendienstlicher Bedarfe einbezogen, auch solche, die als selbstverständlich erachtete Anforderungen hinterfragen? Angelegenheiten, die die Zusammenarbeit mit Nachrichtendiensten anderer Länder betreffen, müssen ebenfalls in dieser Phase angesprochen werden: Wird die Notwendigkeit, mit ausländischen Nachrichtendiensten zu kooperieren, gegenüber anderen Faktoren wie Menschenrechtsverpflichtungen und anderen nationalen Sicherheitsinteressen abgewogen? Falls ja, wie?

Gute gesetzliche Vorgaben

Keine Diskriminierung auf Grundlage der Staatsangehörigkeit

Im Nachrichtendienstrecht wird meist zwischen «inländischen» und «ausländischen» Daten unterschieden. In den meisten Ländern genießt inländische Kommunikation – entweder definiert über Staatsangehörigkeit oder über Territorialität – in der Regel einen höheren Schutz als die sogenannte «ausländische» oder «Übersee»-Kommunikation. Wie aber bereits viele Autor/innen zurecht herausgearbeitet haben, ist diese Unterscheidung aus rechtlicher und aus technologischer Warte problematisch: Technologisch betrachtet ist es in einer globalisierten, digitalisierten Umgebung sehr schwer, genau zwischen nationalen und nicht nationalen Daten zu unterscheiden.

26 Dies wurde sowohl vom Europäischen Gerichtshof für Menschenrechte (EGMR) als auch vom Gerichtshof der Europäischen Union (EuGH) festgelegt. Siehe z. B.: Urteil des EGMR und des Europarats im Fall Klass and Others v. Germany, Antrag Nr. 5029/71, 6. September 1978, Paragraf 42; Urteil des EGMR im Fall Szabo and Vissy v. Hungary, Antrag Nr. 37138/14, 12. Januar 2016, Paragraf 73; Urteil des EuGH im Fall Tele2 Sverige AB v Post-och telestyrelsen und Secretary of State for the Home Department v. Watson and Others, Fälle C-203/15, C-698/15, 21. Dezember, 2016, Paragrafen 108, 110, 116.

27 Murray, Fussey und Sunkin, 2018, 3, Punkt 9, https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf.

Sofern die Filterprogramme nicht hundertprozentig zuverlässig arbeiten, scheint die beiläufige Erfassung inländischer Daten unvermeidbar. Kein Auslandsnachrichtendienst kann im Vorfeld wissen, ob bei der massenhaften Erfassung nicht auch nationale Daten abgefangen werden.

Es gibt weitreichende Belege dafür, dass kein Filtersystem inländische Kommunikation in ausreichendem Maße aus einem Internet-Datenstrom aussortieren kann.[28] Selbst Kommunikation, die innerhalb desselben Landes versendet und empfangen wird, kann durch Drittländer geleitet werden. Die technischen Eigenschaften paketvermittelter Kommunikationsübertragungen im Internet machen es praktisch unmöglich, eine komplexe Datenkategorie wie «deutsche Bürger/innen» klar einzugrenzen. Selbst wenn Filter eine Genauigkeit von 99 Prozent erreichen würden, potenziert sich bei der Massenerfassung, wo Kommunikation in riesigem Umfang abgefangen wird, auch der kleinste Prozentsatz falsch kategorisierter Kommunikationsdaten. Dadurch wird das Fernmeldegeheimnis tausender unbescholtener Menschen verletzt. Schlecht dokumentierte und entwickelte Filtersysteme können also die Gefahr gesellschaftlicher *chilling effects* und das Risiko möglicher Rechtsverletzungen in keiner Weise ausräumen. Mehr noch: Die Unterteilung in bestimmte Bevölkerungsgruppen könnte mit dem Grundsatz der Nichtdiskriminierung unvereinbar sein, der in einigen nationalen Verfassungen, im EU-Recht und im internationalen Menschenrechtsgesetz festgelegt ist.[29] Außerdem billigt das internationale Recht die unbegründete Massenüberwachung nicht, auch wenn es sie nicht explizit verbietet. Demokratien wie Deutschland haben zudem die Pflicht, ihre nationalen Gesetze im Hinblick auf deren Vereinbarkeit mit internationalem Recht auszulegen. Dazu gehört das Recht auf Privatsphäre nach Artikel 17 des Internationalen Pakts über bürgerliche und politische Rechte, das – wie viele argumentieren – nicht als sogenanntes «Klubgut» ausgelegt werden darf.[30]

---

28 Eine aktuelle Diskussion zur Genauigkeit von Datenminimierungsprogrammen findet man hier: Rechthien, 2016, und Dreo Rodosek: «Sachverständigengutachten. Beweisbeschluss SV-13, 1. Untersuchungsausschuss der 18. Wahlperiode», 2016, https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisation_rodosek.pdf.

29 Z.B. Schaller, 2018, 944.

30 Selbstverständlich kann dieses Recht in den einzelnen Ländern unterschiedlich durchgesetzt werden. Ein kolumbianischer Bürger beispielsweise kann nicht unbedingt davon ausgehen, informiert zu werden, wenn seine Kommunikationsdaten vom deutschen Auslandsnachrichtendienst abgefangen werden. Weitere Informationen zum Thema Staatsangehörigkeit im nationalen Überwachungsgesetz: Swire, Woo und Desai: «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft)», 2018 (die Autoren plädieren dafür, dass die Nationalität wichtigster Faktor im Überwachungsgesetz sein sollte) sowie die Klage gegen das Bundesnachrichtendienstgesetz, die kürzlich beim Bundesverfassungsgericht eingereicht wurde (siehe: https://freiheitsrechte.org/home/wpcontent/ uploads/2018/01/GFF_Verfassungsbeschwerde_BNDG_anonym.pdf).

Niederlande:
Keine Unterscheidung zwischen aus- und inländischen Daten bei der Datenerfassung

Das niederländische Nachrichtendienstgesetz unterscheidet nicht zwischen nationaler und ausländischer Kommunikation und gewährt daher allen Menschen dasselbe Schutzniveau. Angesichts der ungelösten technischen Herausforderung, präzise zwischen nationalen und nicht nationalen Kommunikationsdaten zu unterscheiden – ganz zu schweigen von den verfassungs- und menschenrechtsbezogenen Problemen bei diesem Ansatz – scheint dies die konsistente und grundrechtsfreundliche Lösung für das Problem zu sein.

Die Vermeidung einer auf Staatsangehörigkeit fußenden Diskriminierung in den nationalen Nachrichtendienstgesetzen birgt allerdings das Risiko, dass sowohl für Bürger/innen als auch für Ausländer/innen ein insgesamt geringerer Grundrechtsschutz angewendet wird. Das liegt schlicht daran, dass eine Vereinheitlichung der Schutzmaßnahmen auf niedrigerer Stufe einfacher erscheint und eine umfassendere Datenerfassung ermöglichen würde, als wenn die Messlatte für alle höher gehängt würde. Im Idealfall zielen die nationalen Nachrichtendienstgesetze auf den höchstmöglichen Schutz vor massenhafter Kommunikationsdatenerfassung für alle Menschen ab, unabhängig von der Staatsangehörigkeit der überwachten Bevölkerung.

Das deutsche Nachrichtendienstrecht hat die auf Nationalität basierende Diskriminierung bei der Erfassung ausländischer Daten nicht abgeschafft. Aber die deutschen Gesetzgeber haben einen höheren Privatsphärenschutz für Daten aus der Europäischen Union festgesetzt, im Vergleich zum Schutzstandard für Kommunikation außerhalb der EU. Das BND-Gesetz (§ 6 (3) zusammen mit § 9 (2) und (5)) besagt, dass die Nutzung von Suchbegriffen, die auf öffentliche Organe der EU-Mitgliedstaaten oder EU-Institutionen abzielen, auf zwölf begründete Fälle begrenzt ist und Anordnungen erfordert, in denen die einzelnen Suchbegriffe aufgeführt sind. Die Nutzung von Suchbegriffen, die auf EU-Bürger abzielen, ist auf 21 begründete Fälle beschränkt.[31] Das beweist, dass die Gesetzgeber bereit sind, zumindest den europäischen Nachbarn ein höheres Maß an Datenschutz zu gewährleisten.

Der im deutschen Recht geschlossene Kompromiss wurde zurecht kritisiert, da er den Standard der Nichtdiskriminierung nicht erfüllt und die Probleme der technischen Machbarkeit – wie oben beschrieben – ignoriert. Berücksichtigt man allerdings die Gegebenheiten moderner Überwachungspraxis,[32] dann weicht die Einführung zusätzlicher Schutzmaßnahmen für bestimmte ausländische Bevölkerungsgruppen

31 Eine detailliertere Analyse der vier verschiedenen Standards findet man hier: Wetzling: «New Rules for SIGINT Collection in Germany: A Look at the Recent Reform», 23. Juni 2017, https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform.

32 Lubin, 2017.

die traditionelle Dichotomie von «wir» versus «sie» auf. Dass diese Grenze dadurch verschwimmt, kann als durchaus pragmatischer Schritt nach vorne gesehen werden.

Klare Regeln zur Bestimmung nachrichtendienstlicher Prioritäten

USA:
Zusätzliche Bändigung von Massenüberwachungsbefugnissen

Die Presidential Policy Directive 28 (PPD 28) schreibt der US-Regierung vor, die gezielte gegenüber der massenhaften Datenerfassung zu priorisieren, falls eine gezielte Überwachung zu den gewünschten Ergebnissen führt. Section 1 sagt aus, dass signalerfassende Aufklärungsaktivitäten so weit wie möglich zugeschnitten sein sollten. Bei der Bestimmung, ob Nachrichtensignale erfasst werden sollten, müssen die Vereinigten Staaten die Verfügbarkeit anderer Daten prüfen und dabei auch diplomatische und öffentliche Quellen berücksichtigen. Diese angemessenen und umsetzbaren Alternativen für die signalerfassende Aufklärung sollten priorisiert werden.

Bei der PPD 28 handelt es sich allerdings lediglich um eine nicht im Gesetz verankerte Durchführungsverordnung («Executive Decree»). Ein US-Präsident könnte sie daher einseitig ändern. Solange aber keine Änderung eintritt, ist die PPD 28 für die Exekutive bindend, sodass diese Grundprinzipien die Nutzung von Massenüberwachungsbefugnissen beschränken können. Die niederländische Regierung hat ebenfalls eine Regelung vorgeschlagen, nach der bestimmte Befugnisse so gezielt wie möglich eingesetzt werden müssen.[33] Diese Dienste sind bereits an das Verhältnismäßigkeitsprinzip gebunden. Doch die Einführung einer solchen Voraussetzung im Nachrichtendienstrecht sorgt für eine zusätzliche Dimension der Rechenschaftspflicht und stärkt die Notwendigkeit, Massenerfassungsmethoden nur dann einzusetzen, wenn sich ein gewünschtes Ziel durch weniger invasive Mittel nicht erreichen lässt.[34] Das neue niederländische Kontrollgremium für den Einsatz von Überwachungsbefugnissen TIB (Toetsingscommissie Inzet Bevoegdheden), muss das Prinzip «so gezielt wie möglich» in seine Überprüfung von Anordnungen einbeziehen, und die niederländische Kontrollbehörde für die Nachrichten- und Sicherheitsdienste CTIVD (Commissie

33 Artikel 29, niederländisches Gesetz über Nachrichten- und Sicherheitsdienste 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017), http://wetten.overheid.nl/BWBR0039896/2018-05-01.

34 Das Kriterium «so gezielt wie möglich» ist Teil eines verabschiedeten parlamentarischen Antrags und der Regelungen, die im April 2017 erlassen wurden. Außerdem ist es in einem Antrag zur Abänderung des ISS Act 2017 enthalten. Weitere Informationen: Houwing: «The Wiv 2017. A Critical Contemplation of the Act in an International Context», 2018, 17, https://www.burojansen.nl/pdf/2018-LotteHouwing-WivCriticalContemplation_final.pdf.

van Toezicht op de Inlichtingen- en Veiligheidsdiensten) hat den Auftrag, darüber zu berichten.

Deutschland:
Transparenz über die Akteur/innen, die an der Formulierung des Auftragsprofils des BND beteiligt sind

§ 6 (Absatz 1, Nr. 3) des BND-Gesetzes führt auf, welche Ministerien Anforderungen an die zukünftige Ausrichtung der strategischen (Auslands-) Aufklärung stellen dürfen. Demzufolge bestimmt das Bundeskanzleramt das Auftragsprofil des BND in Absprache mit dem Auswärtigen Amt, dem Bundesministerium des Innern, dem Bundesministerium der Verteidigung, dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung.

USA:
Jährliche Revision aller Aufklärungsschwerpunkte durch die Abteilungsleiter/innen

Section 3 der PPD 28 legt fest, dass alle zuständigen Abteilungsleiter/innen alle von ihren Abteilungen oder Behörden identifizierten Prioritäten oder Anforderungen prüfen und den Director of National Intelligence (DNI) dahingehend beraten müssen, ob diese beibehalten werden sollten.

Ein solches Gebot für eine regelmäßige Überprüfung stellt eine wichtige Maßnahme dar, um die Aktualität und Relevanz nachrichtendienstlicher Prioritäten zu garantieren. Zudem stärkt es die Regierungsverantwortung für die Gestaltung nachrichtendienstlicher Politik. Die jährliche Prüfung wird nur innerhalb der Exekutive durchgeführt – Input von Akteuren außerhalb der Korridore der Macht müssen nicht berücksichtigt werden. Ähnlich, wenn auch nicht gesetzlich festgelegt, beschreibt die Intelligence Community Directive 2014, wie das National Intelligence Priorities Framework in den USA erstellt wird.[35]

35 US National Intelligence Priorities Framework, ICD 204, siehe: https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

Niederlande: Eignungsprüfung für ausländische Kooperationspartner

Um zu beurteilen, mit welchen Ländern die Nachrichtendienste ihre Informationen austauschen können, werden Prüfvermerke für die Kooperationspartner angelegt. Diese Vermerke müssen immer auf dem neuesten Stand sein und liefern Informationen auf Grundlage der folgenden fünf, im Gesetz festgehaltenen Kriterien:

- die demokratische Einbettung der Geheim- und Sicherheitsdienste im entsprechenden Land;
- die Achtung der Menschenrechte im entsprechenden Land;
- die Professionalität und Verlässlichkeit des entsprechenden Dienstes;
- die rechtlichen Kompetenzen und Fähigkeiten des Dienstes im entsprechenden Land;
- das Maß an Datenschutz, das der entsprechende Dienst wahrt.[36]

Die strategische Planung der Informationsgewinnung bedarf auch einer soliden Rechtsgrundlage für die Zusammenarbeit von Nachrichtendiensten. Ausgehend von den fünf oben genannten Kriterien müssen die niederländischen Nachrichtendienste für jeden ausländischen Partnerdienst, mit dem sie zusammenarbeiten, einen Prüfvermerk erstellen. Das Prüfverfahren für die Erstellung dieser Vermerke beinhaltet eine Reihe obligatorischer Risikobewertungen.[37] Darüber hinaus besagen die entsprechenden Regelungen vom April 2018, dass Rohdaten aus der kabelgebundenen Fernmeldeaufklärung nur ausgetauscht werden dürfen, wenn ein entsprechender

36 Eijkman, Eijk und Schaik: «Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?», 2018, 31; siehe auch: Niederländisches Gesetz über Nachrichten- und Sicherheitsdienste 2017, Artikel 88–90.

37 In diesen Prüfvermerken bewertet die Regierung, wie weit die Zusammenarbeit mit einem ausländischen Nachrichtendienst gehen darf. Wenn es in dem jeweiligen Land Entwicklungen gibt, die eine Überprüfung der Zusammenarbeit nahelegen, wird der Prüfvermerk überarbeitet. Die niederländische Regierung schließt eine Kooperation mit Ländern, die diese Kriterien nicht erfüllen, nicht im Vorfeld aus, selbst wenn es nur begrenzt demokratische Kontrollmechanismen und eine schlechte Menschenrechtslage gibt. In diesem Fall spricht die Regierung von einem «Risiko-Dienst». Kooperiert die Regierung mit einem «Risiko-Sicherheitsdienst», ist eine zusätzliche Genehmigung vom zuständigen Minister erforderlich. Die Auswertung der Zusammenarbeit mit diesen Ländern und diesen Risiko-Diensten muss immer an den Minister weitergeleitet werden. Weitere Informationen zu den niederländischen Gewichtungsvermerken: Niederländische Kontrollbehörde für die Nachrichten- und Sicherheitsdienste (CTIVD): «Review Report on the Implementation of Cooperation Criteria by the AIVD and the MIVD», 2016, https://english.ctivd.nl/documents/review-reports/2016/12/22/index48.

Vermerk vorliegt, der diese Art des Austauschs abdeckt.[38] Anders gesagt: Fehlt für einen solchen Fall ein Prüfvermerk, kann der zuständige Minister die Weitergabe von Rohdaten nicht genehmigen. Die niederländische Aufsichtsbehörde CTIVD kann die Vermerke prüfen und dem Parlament melden, ob sie sie für korrekt und angemessen hält (siehe Abschnitt «Gute Kontrollpraxis» unten). Dies stellt einen innovativen Weg dar, um zu beurteilen, mit welchen Ländern Daten ausgetauscht werden dürfen. Es ist anzunehmen, dass auch andere Nachrichtendienste ähnliche Faktoren auswerten und ihre Entscheidungen entsprechend treffen. Aber dieses Verfahren gesetzlich festzuschreiben unterstreicht die Bedeutung einer angemessenen Risikoabwägung und gestattet Aufsichtsbehörden, den Prozess zu prüfen.

Deutschland:
Schriftliche Vereinbarungen zu den Zielen, der Art und der Dauer der internationalen Zusammenarbeit müssen vom Kanzleramt genehmigt werden

Im Bestreben nach einer umfassenderen Rechenschaftspflicht über die internationale nachrichtendienstliche Zusammenarbeit hat Deutschland neue gesetzliche Kriterien für bilaterale Vereinbarungen zwischen Nachrichtendiensten eingeführt.

Laut § 13 des BND-Gesetzes bedürfen Kooperationen des BND im Rahmen der Ausland-Ausland-Fernmeldeaufklärung mit Staaten der EU, der NATO und des Europäischen Wirtschaftsraums im Vorfeld eine schriftliche Absichtserklärung[39] sowie der Zustimmung des Bundeskanzleramtes.[40] Eine Liste genereller, zulässiger Kooperationsziele findet sich in § 13 (4) des Gesetzes.[41] Die Exekutive muss das parlamentarische Kontrollgremium über sämtliche Vereinbarungen informieren. Dazu gehört auch ein Gebot der Zweckbindung, dass die Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie erfasst wurden. Weiterhin besagt das Gebot, dass die Nutzung der Daten nach grundlegenden Prinzipien der Rechtsstaatlichkeit zu erfolgen hat. Die Vereinbarungen setzen außerdem eine Absprache voraus, nach der

38 Beim Austausch von Rohdaten, die aus anderen Überwachungsmaßnahmen stammen (z. B. gezielte Datenerfassung oder Eindringen in Computernetzwerke) gilt diese Regel nicht. Diese Daten dürfen ohne Vorliegen eines Prüfvermerks auf Grundlage von Article 64 ISS Act 2017 ausgetauscht werden, vorausgesetzt es liegt ein dringlicher und wichtiger Grund vor.

39 Ein SIGINT-Abkommen, das im Rahmen der Snowden-Enthüllungen öffentlich wurde, ist das zwischen den USA und Israel, welches hier zu finden ist: https://upload.wikimedia.org/wikipedia/commons/4/41/Israel_Memorandum_of_Understanding_SIGINT.pdf.

40 Bei Vereinbarungen mit ausländischen Partnern im weiteren Umfeld ist die Genehmigung des Kanzleramtschefs erforderlich.

41 Wetzling: «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls», 2017, 13–16, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

die ausländischen Kooperationspartner der Aufforderung des Bundesnachrichtendienstes nach Löschung der Daten nachkommen müssen. Letztendlich aber können deutsche BND-Mitarbeiter/innen die Genauigkeit der Zusicherungen, die sie diesbezüglich von ihren Kooperationspartnern erhalten, aufgrund fehlender internationaler Vereinbarungen nicht verifizieren.

Explizite Nennung von Zielen, die durch strategische Fernmeldeaufklärung nicht verfolgt werden dürfen

Viele der jüngeren SIGINT-Reformen scheuen davor zurück, der strategischen Fernmeldeaufklärung wirksame Grenzen zu setzen. Dass die USA im Jahr 2015 die sogenannte «About Collection» eingestellt und die massenhafte Erfassung von Telefonaufzeichnungen nach Section 215 des Patriot Act beendet hat, ist eine erwähnenswerte Ausnahme, die beweist, dass liberale Demokratien auf exzessive Überwachungspraktiken verzichten können. Zu den weniger bekannten Beispielen neuer Nachrichtendienstgesetze, die die zulässige Nutzung von Befugnissen zur Massenüberwachung weiter eingeschränkt oder beschnitten haben, gehören:

Deutschland:
Verbot der Wirtschaftsspionage

§ 6 (5) des BND-Gesetzes verbietet die Durchführung einer strategischen Ausland-Ausland-Fernmeldeaufklärung zum Zwecke der Erzielung von Wettbewerbsvorteilen.[42]

USA:
Verbot der Diskriminierung von geschützten Gruppen durch Massenüberwachung

Section 2 der PPD 28 legt fest: In keinem Fall dürfen Daten, die in großen Mengen gesammelt werden, zum Zwecke der Unterdrückung von Kritik oder Meinungsverschiedenheiten, zur Benachteiligung von Personen aufgrund ihrer ethnischen Zugehörigkeit, Rasse, ihres Geschlechts, ihrer sexuellen Orientierung oder Religion, der Gewährung eines Wettbewerbsvorteils für US-amerikanische

42 Wichtig dabei ist, dass diese Regelung nicht grundsätzlich ausschließt, dass die deutschen Nachrichtendienste private Organisationen wie beispielsweise Unternehmen ins Visier nehmen. Die Regelung wurde als unscharf und «nicht besonders gelungen» kritisiert, da sie den Begriff «Wirtschaftsspionage» nicht rechtlich angemessen definiert. Graulich: «Reform des Gesetzes über den Nachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und internationale Datenkooperation», 2017, 46, https://kripoz.de/wp-content/uploads/2017/01/graulich-reform-des-gesetzes-ueber-den-bundesnachrichtendienst.pdf.

Unternehmen und US-amerikanische Wirtschaftszweige gewerblich oder zur Erreichung eines anderen Zwecks als den in diesem Abschnitt genannten verwendet werden.

USA:
Strafrechtliche Haftung für Missbrauch von Überwachungsbefugnissen

Das Gesetz über Überwachung im Rahmen der Strafverfolgung verbietet den Einsatz von Echtzeitüberwachung (18 U.S. Code 2511(1)). Diese Bestimmung verbietet bestimmte Abhöraktivitäten und nennt dann Ausnahmen von diesem allgemeinen Verbot. Section 2511(4) nimmt rechtmäßige Überwachungsaktivitäten von diesem Strafrecht aus. Nachrichtendienstmitarbeiter/innen aber, die illegale Abhöraktivitäten durchführen, begehen eine Straftat.

Die Kriminalisierung bestimmter Formen der Überwachung schreckt davon ab, Überwachungsbefugnisse zu missbrauchen. Bei vorsätzlichen Verstößen gegen das Verbot der Überwachung im Rahmen des US-Wiretapping Act kann eine Haftstrafe von bis zu fünf Jahren anfallen (18 U.S. Code 2511(4)). Solche Straftatbestände sind im Bereich der Massenüberwachung selten. Aber sie könnten ein wirksames Mittel sein, um die Einhaltung der Vorgaben durchzusetzen.

Gute Kontrollpraxis

Das Festlegen strategischer Ziele und das Formulieren operativer Prioritäten gehören zu den Kernkompetenzen der Exekutive. Folglich finden wir nur eine sehr begrenzte Einbindung von Kontrollgremien in der Planungsphase. Erst kürzlich hat Privacy International aufgedeckt, dass zurzeit kein Aufsichtsorgan die Befugnis hat, den Austausch von nachrichtendienstlichen Daten zu genehmigen.[43] Das wirft nicht nur rechtliche und operative Fragen auf, sondern auch politische. Kann eine Regierung einem ausländischen Nachrichtendienst ausreichend trauen, um eine neue Zusammenarbeit einzuleiten? Interessanterweise beschäftigen sich einige Aufsichtsbehörden seit Kurzem damit, die Aufgabenverteilung und Zusammenarbeit zwischen Nachrichtendiensten zu überprüfen, wie folgendes Beispiel zeigt.

43 Privacy International: «Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards», 2018, https://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global.

Einbindung von Aufsichtsorganen in die Aufgabenplanung

Vereinigtes Königreich:
Der parlamentarische Kontrollausschuss muss regelmäßig über die operativen Zwecke informiert werden

Section 142 des Investigatory Powers Act beschreibt, wie die operativen Zwecke der Massenüberwachung festgelegt werden. Sämtliche operativen Zwecke müssen vom Secretary of State (142 (6)) genehmigt werden und über das hinausgehen, was bereits gesetzlich vorgeschrieben ist (142 (7)). Alle drei Monate muss der/die Secretary of State eine Kopie der Liste aller operativen Zwecke an das Intelligence & Security Committee des Parlaments aushändigen (142 (8)). Der Prime Minister muss die Liste der operativen Zwecke mindestens einmal pro Jahr prüfen (142 (10)).

Regelmäßige Unterrichtungen über die operativen Zwecke in der Praxis helfen Aufsichtsgremien, geänderte Prioritäten zu erkennen und deren Vereinbarkeit mit dem Rechtsrahmen zu bewerten. Gesetzliche Regelungen, die die genauen Zwecke oder Einsatzbereiche für die Fernmeldeaufklärung vorschreiben, sind ein erster Schritt. Noch besser aber sind konkrete Berichte darüber, wie Prioritäten in der Praxis festgelegt wurden.

Zugriff der Aufsichtsgremien auf internationale Vereinbarungen zum Austausch von nachrichtendienstlichen Daten

Kanada:
Vollständiger Zugriff auf die Dokumentation von Kooperationsvereinbarungen

Der Commissioner des Communications Security Establishment (CSE) kann auf alle relevanten Informationen über Datenaustauschaktivitäten des CSE zugreifen. Der CSE Commissioner hat alle Befugnisse eines Beauftragten nach Teil II des Inquiries Act, einschließlich der Befugnis Zwangsmaßnahmen anzuordnen («Power of Subpoena»), die ihm und seinen Mitarbeiter/innen ungehinderten Zugang zu allen Einrichtungen, Dokumenten und Mitarbeiter/innen des CSE gibt.[44]

44 Sollte Bill C-59 verabschiedet werden, wird eine zentrale Aufsichtsbehörde für alle relevanten Ministerien und Sicherheitsbehörden eingerichtet. Siehe auch Privacy International, 2018, 67.

Niederlande:
CTIVD kann die Prüfvermerke kontrollieren

Die niederländische Kontrollbehörde für die Nachrichten- und Sicherheitsdienste CTIVD ist befugt, die Prüfvermerke zu internationalen Kooperationspartnern und die daraus folgende internationale Zusammenarbeit zu kontrollieren. Die CTIVD muss außerdem über jeden Austausch von Rohdaten informiert werden.[45]

Deutschland:
Das parlamentarische Kontrollgremium muss über alle Absichtserklärungen (MoU) informiert werden

§ 13 (5) des BND-Gesetzes schreibt der Regierung vor, das Parlamentarische Kontrollgremium (PKGr) über alle unterzeichneten Absichtserklärungen zur SIGINT-Zusammenarbeit mit ausländischen Partnern zu informieren. Die Ad-hoc-Zusammenarbeit mit ausländischen Nachrichtendienstdaten ist davon ausgenommen.

Die drei oben genannten Praxisbeispiele sind Versuche, das Kontrolldefizit[46] bei der internationalen Zusammenarbeit von Nachrichtendiensten anzugehen. Der uneingeschränkte Zugriff auf sämtliche Kooperationsvereinbarungen ist ein wichtiger Schritt für Aufsichtsbehörden, um den Umfang und den Hintergrund des nachrichtendienstlichen Datenaustauschs besser zu verstehen. In einem Bericht aus dem Jahr 2016 kritisierte die CTIVD öffentlich einige der Ergebnisse der Nachrichtendienste: «In einem Fall erfüllt der ausländische Nachrichtendienst die Kriterien der demokratischen Verankerung, Professionalität und Verlässlichkeit sowie der Gegenseitigkeit nicht. Dennoch hat der MIVD [Militärischer Geheim- und Sicherheitsdienst] bestimmt, dass alle Formen der Zusammenarbeit zulässig sind. [...] Die CTIVD ist der Meinung, dass der Inhalt des Prüfvermerks dieses Ergebnis nicht erlaubt. Der MIVD gibt nicht an, welche zwingenden Gründe der Dienst als Grundlage dafür ansieht, dass er trotz der Nichterfüllung bestimmter Kooperationskriterien so eng mit dem ausländischen Dienst zusammenarbeiten kann.»[47] Dieses Beispiel zeigt, dass die CTIVD den auf Basis der Prüfvermerke gezogenen Schlussfolgerungen der Dienste öffentlich widersprechen kann.

45 Die Informationspflicht wurde durch zusätzliche Regeln ausgeweitet. Das Gesetz selbst sieht vor, dass die CTIVD über die Erfassung von SIGINT-Rohdaten informiert werden muss.

46 Bos-Ollermann: «Mass Surveillance and Oversight», 2017, 152.

47 CTIVD, 2016, 32, eigene Übersetzung.

Die in dieser Phase erörterten Praktiken beinhalten grundlegende Aspekte (wie die niederländische Praxis, die auf Staatsangehörigkeit basierende Diskriminierung bei der Massenüberwachung abzuschaffen), aber auch kleinere, eher inkrementelle Schritte hin zu einer besseren Kontrolle und Rechenschaftspflicht (wie die Einführung konkreter ministerieller Verantwortlichkeiten bei der Steuerung der Fernmeldeaufklärung).

Bemerkenswert ist, welche Rolle die internationale Zusammenarbeit in dieser Phase spielt. Insbesondere im SIGINT-Bereich, in dem die Lastenverteilung unter den ausländischen Partnerdiensten zu den Grundprinzipien zählt, sind Prüfvermerke und der bessere Zugriff der Aufsichtsbehörden auf internationale Vereinbarungen über den Austausch von nachrichtendienstlichen Daten lobenswerte Maßnahmen. Im Idealfall sollten Kooperationen an eine verpflichtende und regelmäßige Neubewertung durch die Aufsichtsbehörden geknüpft sein. Die ausdrückliche gesetzliche Erwähnung von Zielen und Zwecken, die keine massenhafte Datenerfassung erlauben, ist eine weitere wichtige Dimension bei der Verbesserung der Nachrichtendienstführung.

Phase 2: Antragsverfahren (Anordnungsverfahren)

Mit einer Anordnung stellt der Nachrichtendienst (oder gegebenenfalls das Ministerium, das die Fachaufsicht über einen bestimmten Nachrichtendienst ausübt) einen Antrag auf Genehmigung einer Beschränkungsmaßnahme des Fernmeldegeheimnisses. Diese Anordnungen müssen einzelne Maßnahmen zur Kommunikationsdatenerfassung beschreiben und eingrenzen, ausgehend von bestimmten, gesetzlich festgelegten Kriterien hinsichtlich der Form und des Inhalts der Anordnungen. Anordnungen sind ein Kernelement der Kontrolle von Nachrichtendiensten. Sie müssen jedoch konkrete Angaben enthalten, um einen wirksamen Schutz vor Missbrauch zu bieten.[48]

Im Bereich von SIGINT können Anordnungen dementsprechend an bestimmte Gruppen oder Kategorien von Personen oder Aktivitäten statt an spezifische Einzelpersonen gebunden sein. Uns ist bewusst, dass einige Rechtsordnungen sehr viel striktere Grenzen für den Rechtsbegriff der Anordnungen anwenden. In den USA und Kanada beispielsweise beziehen sich Anordnungen («warrants») immer auf gezielte Überwachungsmaßnahmen, bei denen ein Richter eingebunden ist, der diese Anordnungen genehmigt. Eine Reihe von Ländern in Europa wenden das Konzept der Anordnungen nur auf strafrechtliche Ermittlungen und nicht etwa auf die nachrichtendienstliche Datenerfassung an. Nach konventionellem Verständnis sind «Befugnisse zur Massenüberwachung nicht mit den rechtlichen Anforderungen an klassische Anordnungen vereinbar. Es gibt keine Spezifität. Per Definition ist die

48 Donohue im Interview mit Farrell: «America's Founders Hated General Warrants. So Why Has the Government Resurrected Them?», 14. Juni 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/?noredirect=on&utm_term=.2f3ee3b71c69.

massenhafte Datenerfassung nicht gezielt, sondern willkürlich.»[49] Nach dem Investigatory Powers Act des Vereinigten Königreichs dagegen wird der Begriff «warrant» für unterschiedliche Arten von Anträgen für die massenhafte Datenerfassung verwendet. Das setzt ein klassenbasiertes Anordnungsverfahren voraus, in dem umfassende Datenkategorien erhoben werden dürfen.

Obwohl die Terminologie schwierig ist und es in einigen Rechtsordnungen keine Anordnungen für die nicht gezielte Datenerfassung oder Massenüberwachung gibt, werden sie hier als hilfreiche Vergleichskategorie aufgeführt. Anordnungen können ein wirksames Werkzeug sein, um die Regeln zu Datenfilterung, die Genehmigungsvoraussetzungen und die Zweckbindung einer Maßnahme zu spezifizieren. Je spezifischer eine Anordnung zur Massenüberwachung ist, desto besser ist ihre Schutzfunktion. Anordnungen können auch eingesetzt werden, um bestimmte Datenkategorien von der Erfassung auszuschließen und die Nutzung der erfassten Daten einzuschränken.

Dabei sollte beachtet werden, dass viele solcher Einschränkungen und Bedingungen ebenso in einem Nachrichtendienstgesetz festgehalten werden könnten. Der große Vorteil von Anordnungen liegt allerdings in der aktiven Einbindung eines unabhängigen gerichtlichen Kontrollgremiums *vor* Beginn der Überwachung (siehe Phase 3). Dies erlaubt Einzelfallprüfungen. Im Idealfall wird ein klares rechtliches Mandat für die massenhafte Datenerfassung mit verpflichtenden, unabhängigen Vorabkontrollen aller Einsatzbereiche kombiniert.

Anordnungen legen auch häufig die Dauer einer bestimmten Erfassungsmethode fest. Das wiederum führt zu einer obligatorischen Evaluierung der Maßnahme und möglicherweise zu einer erneuten Antragstellung und Genehmigung. Daher ist die Festlegung eines Ablaufdatums nicht nur ein institutionalisierter Kontrollmechanismus, sondern auch ein regelmäßiger Effizienztest, der zur effizienten Ressourcenverteilung innerhalb der Dienste beiträgt.

Je gezielter eine geplante Überwachungsmaßnahme ist, desto spezifischer kann die Anordnung natürlich formuliert werden. Im Hinblick auf den Schwerpunkt dieser Studie – nämlich Kontroll-Innovationen für die strategische Kommunikationsüberwachung – haben wir hauptsächlich verschiedene Typen von Anordnungen für den Bereich der Massenüberwachung untersucht. Allerdings werden trotzdem interessante Merkmale von Anordnungen für die gezielte Überwachungsmaßnahmen diskutiert, wenn sie auf den Bereich der strategischen Erfassung anwendbar sind.

49 Forcese, 2018, 3, eigene Übersetzung.

Relevante Aspekte

Viele Nachrichtendienstgesetze beinhalten eine Liste von Kriterien, die bei jedem Einsatz einer SIGINT-Maßnahme berücksichtigt werden müssen.[50] Im Idealfall gehören dazu:

- der bzw. die Zweck(e) der beantragten Maßnahme;
- die alternativen verfügbaren Maßnahmen;
- die Privatunternehmen, die zur Zusammenarbeit verpflichtet werden sollen;
- die Dienste, die mit der Durchführung der Maßnahme betraut werden;
- der Zeitrahmen für die Bewertung und Genehmigung der Anordnung, einschließlich der Ausnahmeregelungen für Notfälle;
- die geografischen Gebiete oder Organisationen oder Personengruppen, auf die eine bestimmte Maßnahme abzielt;
- die technische Ausrüstung oder Einrichtung, an der Daten erfasst werden sollen;
- die Eignungstests, die im Vorfeld durchgeführt wurden;
- die Art(en) von Daten, die erfasst werden sollen;
- die eingesetzten Suchbegriffe oder Selektoren (z.B. ein bestimmter IP-Adressbereich);
- die vorgesehene Datennutzung und die geplanten Datenauswertungsmethoden;
- die Gültigkeitsdauer der Anordnung und Regeln für die Verlängerung;
- das zusätzliche Hintergrundmaterial, das zusammen mit der Anordnung eingereicht werden muss.

Dimensionen von SIGINT-Anordnungen

Die folgende Tabelle liefert Beispiele für unterschiedliche Typen von Anordnungen, die es in verschiedenen Rechtsordnungen gibt. Die Liste ist lediglich ein Auszug. Sie zeigt aber, wie vielfältig SIGINT-Anordnungen eingesetzt und genutzt werden. Die verschiedenen Anordnungen zur Massenüberwachung sind jeweils beispielhaft anhand eines Staates dargestellt, ähnliche Bestimmungen können aber auch in anderen Nachrichtendienstgesetzen verankert sein. Grundsätzlich veranschaulichen die unterschiedlichen Anordnungstypen zwei Aspekte: Zum einen können Anordnungen für unterschiedliche *Methoden* der Erfassung erforderlich sein, also die Techniken beschreiben, die zur Beschaffung von Kommunikationsdaten eingesetzt werden sollen. Zum anderen fordern viele Nachrichtendienstgesetze mittlerweile separate Anordnungen für die unterschiedlichen *Phasen* des SIGINT-Prozesses. So haben die Niederlande beispielsweise einen dreistufigen Prozess eingeführt, bei

50 So hat beispielsweise ein Zusammenschluss aus Vertretern der Zivilgesellschaft, der Industrie und internationalen Expert/innen eine Liste von 13 Grundsätzen formuliert, um den Menschenrechtsverpflichtungen im Hinblick auf die Kommunikationsüberwachung nachzukommen: Necessary and Proportionate Coalition: «Necessary & Proportionate. International Principles on the Application of Human Rights to Communications Surveillance», Mai 2014, http://necessaryandproportionate.org/principles.

dem Anordnungen für 1.) das Erfassen und Filtern (Artikel 48), 2.) die Aufbereitung der Rohdaten (Artikel 49)[51] und 3.) die Auswahl von Inhaltsdaten für die operative Nutzung und die automatisierte Datenanalyse (Artikel 50) erforderlich sind.[52] Darüber hinaus werden Anordnungen eingesetzt, um die Speicherung von Daten, die Weitergabe von Daten und sogar die Nutzung von Daten für Experimente und Schulungszwecke zu regeln. Auch wenn eine spezifische Anordnung für die Massenüberwachung im Kontext des allgemeinen Rechtsrahmens des jeweiligen Landes zu betrachten ist, zeigt die Tabelle, dass verschiedene Gesetzgeber vielfältige Einsatzmöglichkeiten für Anordnungen gefunden haben. Das stärkt die Rechenschaftspflicht der Exekutive für bestimmte Nachrichtendienstaktivitäten.

Tabelle 2: SIGINT-Anordnungen

Anordnungstyp	Beispielnorm
Massenhafte Datenerfassung	Vereinigtes Königreich: «Bulk Interception Warrants» (Section 136 (1) IP Act)
Massenhafter Datenerwerb	Vereinigtes Königreich: «Bulk Acquisition Warrants» (Section 158 (5) IP Act)
Auskunftsverlangen von personenbezogenen Datensätzen	Vereinigtes Königreich: «Bulk Personal Datasets Warrants» (Section 199 (1) IP Act)
Datenauswertung	Frankreich: «Data Exploitation Warrant» (Artikel L. 854-2.-III. des Gesetzes Nr. 2015-1556)[53]
Vorratsspeicherung	Vereinigtes Königreich: «Retention notice», die einem Datenverarbeiter vorschreibt, Kommunikationsdaten aufzubewahren (Section 87 (1) IP Act)
Analyse von Metadaten	Frankreich: Der Premierminister hat die Befugnis, die «Auswertung nicht individualisierter Verbindungsdaten» auf Antrag zu genehmigen (Artikel L. 854-2.-II. des Gesetzes Nr. 2015-1556)[54]

51 Die Vorbereitungsphase (Artikel 49 des niederländischen Nachrichtendienstgesetzes) dient dazu, entweder die Erfassung (Artikel 49 (1)) oder die Auswahl (Artikel 49 (2)) zu verbessern.

52 Niederländisches Gesetz über Nachrichten- und Sicherheitsdienste 2017, siehe auch: Eijkman, Eijk und Schaik, 2018, 22.

53 Im französischen Original: «exploitation de communications [...] interceptée». Eine ähnliche Anordnung für Datenanalyse ist z. B. auch im britischen Recht erforderlich: «Ein Nachrichtendienst darf keine Befugnis zur Prüfung eines von ihm gespeicherten persönlichen Massendatensatzes ausüben, es sei denn, die Prüfung wird durch eine Anordnung nach diesem Teil genehmigt» (Section 200 (2) United Kingdom, IP Act 2016, eigene Übersetzung).

54 Im französischen Original: «l'exploitation non individualisée des donnés de connexion interceptée».

Operative Unterstützung	Niederlande: Falls es keine formelle Kooperationsvereinbarung gibt, müssen die niederländischen Nachrichtendienste eine Genehmigung für operative Unterstützungsmaßnahmen einholen – so als würden sie die Überwachungsmaßnahme selbst durchführen. «Nach erteilter Genehmigung ist es den Diensten erlaubt, Befugnisse im Ausland auf Basis von niederländischem Recht auszuüben». (Artikel 90 des Gesetzes über Nachrichten- und Sicherheitsdienste 2017)[55]
Eignungsprüfung	Neuseeland: «Eine Anordnung zur Eignungsprüfung ermächtigt einen Nachrichten- und Sicherheitsdienst, eine ansonsten rechtswidrige Tätigkeit auszuüben, die erforderlich ist, um die Fähigkeiten der Behörde in Bezug auf die Erfüllung ihrer gesetzlichen Aufgaben zu testen, zu erhalten oder weiterzuentwickeln». (Intelligence and Security Act 2017 (2017/10) Section 91A, eigene Übersetzung)
Schulungen	Neuseeland: «Eine Schulungsanordnung ermächtigt einen Nachrichten- und Sicherheitsdienst, eine ansonsten rechtswidrige Tätigkeit auszuüben, die notwendig ist, um die Mitarbeiter/innen im Hinblick auf die Erfüllung der gesetzlichen Aufgaben der Behörde zu schulen». (Intelligence and Security Act 2017 (2017/10) Section 91B, eigene Übersetzung)

Ob unterschiedliche Anordnungen für separate Phasen der nachrichtendienstlichen Überwachung in der Praxis umsetzbar sind, wird mitunter in Zweifel gezogen. Es könnten Probleme auftreten, wenn die gesetzlich vorgeschriebenen Phasen nicht den tatsächlich aufeinanderfolgenden Schritten entsprechen. Im Falle der Niederlande meinen Expert/innen, dass die drei zu genehmigenden Schritte sehr eng miteinander verbunden sind und unter Umständen zeitgleich ausgeführt werden.[56] Demzufolge könnte dies bedeuten, dass unterschiedliche Anordnungen für separate Phasen des Prozesses in der Praxis nicht nacheinander genehmigt würden, sondern gleichzeitig, was den Zweck dieser Trennung untergraben könnte.

55 Eine ähnliche Art von Anordnung ist auch im neuseeländischen Nachrichtendienstgesetz vorgesehen: «Eine Nachrichten- und Sicherheitsbehörde darf ohne Genehmigung keine Regierung oder Entität in einer anderen Gerichtsbarkeit auffordern, eine Tätigkeit auszuüben, die – wenn sie von der Nachrichten- und Sicherheitsbehörde ausgeübt würde – rechtswidrig wäre» (Intelligence and Security Act 2017 (2017/10) Section 49 1A).

56 Siehe Electrospaces.net. «Collection of Domestic Phone Records under the USA Freedom Act», 14. Juli 2018, https://electrospaces.blogspot.com/2018/07/collection-of-domestic-phone-records.html; CTIVD opinion: «Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX», 26. August 2015, https://www.ctivd.nl/documenten/publicaties/2015/08/26/reactie-ctivd-conceptwetsvoorstel.

Die Detailtiefe, in der Anordnungen für strategische Kommunikationsüberwachung gesetzlich vorgeschrieben sind, variiert von Land zu Land. Dabei stechen eine Reihe von Beispielen heraus, weil sie sich auf wichtige Details konzentrieren.

Gesetzliche Vorgaben für SIGINT-Anordnungen

Frankreich:
Beschränkung der Anzahl der Dienste, die erfasste Daten nutzen dürfen

Laut dem französischen Gesetz über den Auslandsnachrichtendienst dürfen nur die in der Anordnung genannten Dienste die erfassten Daten verarbeiten. Diese Bestimmung dient als Schutz vor nachträglichem Datenaustausch der Dienste untereinander. Zudem sieht die Bestimmung vor, dass der in der Anordnung angegebene Zweck nicht geändert werden darf und die Daten nicht zu anderen Zwecken genutzt werden dürfen.[57]

Diese Regelung beschränkt die Weitergabe gesammelter Daten von einem Nachrichtendienst zu einem anderen. Andere staatlichen Stellen, die unter Umständen ein Interesse an bereits erhobenen Daten entwickeln könnten, werden durch diese Vorgabe daran gehindert, nachträglich Zugriff auf die Daten zu erhalten.[58]

Frankreich:
Nennung der automatisierten Auswertungsmethoden in den Anordnungen

Anordnungen für Ausland-Ausland-Überwachung müssen die zulässigen Methoden der automatisierten Datenauswertung aufführen sowie deren Zweck.[59]

57 Artikel L. 854-6. des französischen Gesetzes Nr. 2015-1556 zur internationalen Kommunikationsüberwachung.

58 Renan: «The Fourth Amendment as Administrative Governance», Mai 2016, 1068, http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2016/06/68_Renan_-_68_Stan._L._Rev._1039.pdf.

59 Artikel L. 854-2.-II. des französischen Gesetzes Nr. 2015-1556 zur internationalen Kommunikationsüberwachung.

Einer genauen Angabe darüber, wie ein Datensatz verarbeitet und genutzt wird, ermöglicht Kontrolleur/innen, den verursachten Grundrechtseingriff besser einzuschätzen. Das Ausmaß der Verletzung der Privatsphäre und die Auswirkungen auf andere Grundrechte können je nach Art der durchgeführten Untersuchung und je nach deren Zweck variieren. In Frankreich werden Analysemethoden zur Verarbeitung von massenhaft erfassten Metadaten allerdings vom französischen Premierminister genehmigt und nicht etwa von einer unabhängigen Aufsichtsbehörde.

Kanada:
Spezifische Anforderung, den nachrichtendienstlichen Mehrwert in einer SIGINT-Anordnung zu begründen

Nach dem geplanten CSE Act (Section 35 (2) (b) – wie in Bill C-59)[60] ist vorgesehen, dass der kanadische Nachrichtendienst CSE in seinem Antrag *unabhängig nachweisen* muss, warum die per Massenüberwachung zu beschaffenden Daten (kanadischer Begriff dafür: «unselected information», also nicht ausgewählte Daten) «nicht hinreichend mit anderen Mitteln beschafft werden können». Der CSE muss also beweisen, warum weniger tiefgreifende oder gezieltere Erfassungsmethoden nicht ausreichen.

Eine solche Spezifikation im Gesetz zu verankern (im Gegensatz zu einer Verordnung oder «executive decree») bietet auf den ersten Blick einen stärkeren Schutz, da die Regierungen sie nicht nach Belieben ändern können.[61] Allerdings sind Gesetzgeber natürlich auch nicht immun gegen die Übernahme von abgeschwächten Bestimmungen, die nach der Verabschiedung auch schwieriger zu ändern sind. Weitere Vorteile gesetzlich kodifizierter Bestimmungen sind, dass die Öffentlichkeit mehr Vertrauen in die Gründlichkeit der Verhältnismäßigkeitsprüfung haben kann und die Kontrollbehörde einen gesicherten Anspruch auf eine detailliertere Begründung durch die Dienste hat. Ähnlich verhält es sich in der Schweiz: Hier fordert das Gesetz ausdrücklich, dass Anträge für die »Kabelaufklärung« eine Begründung der Notwendigkeit enthalten müssen.[62]

---

60 Alle Bestimmungen, die sich auf den kanadischen Bill C-59 beziehen, befassen sich mit dem Gesetzentwurf, wie er zum Zeitpunkt des Verfassens im Sommer 2018 vorlag, d. h. nach erster Lesung im House of Commons. Online: http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading.

61 Im Vergleich: Das BND-Gesetz (§ 6 (7)) besagt lediglich, dass eine Dienstvorschrift die »technische und organisatorische Umsetzung» des Genehmigungsverfahrens bestimmt. Im Vereinigten Königreich hat das Investigatory Powers Commissioner›s Office (IPCO) vor Kurzem eine Advisory Note (01/2018) ausgegeben, in der es um die Prüfung von Anordnungen geht. Dies wird im Abschnitt über die Kontrollpraxis behandelt.

62 Artikel 40 (1b) des Schweizer Nachrichtendienstgesetzes («Genehmigungsverfahren für Kabelaufklärung»).

Deutschland:
Auflistung der Suchbegriffe in Anordnungen für die Ausland-Ausland-Fernmeldeaufklärung[63]

Anordnungen, die die strategische Ausland-Ausland-Überwachung in Bezug auf EU-Institutionen und öffentliche Organe von EU-Mitgliedstaaten berühren, müssen die zu verwendenden Suchbegriffe auflisten (§ 9 (2) BND-Gesetz).

Wenn Analyst/innen die Suchbegriffe im Vorfeld angeben müssen, kann dies einen Anreiz schaffen, Relevantes stärker einzugrenzen und restriktivere Begriffe zu verwenden. Dies trägt dazu bei, die Anzahl der von einer Maßnahme betroffenen Personen zu begrenzen. Außerdem wird vermieden, dass eine neue Anordnung eingeholt werden muss, wenn der Einsatz von zu weit gefassten Suchbegriffen zu viele unbrauchbare Daten liefert. Darüber hinaus sind Kontrollen der SIGINT-Praxis bei Kenntnis der verwendeten Suchbegriffe wesentlich aussagekräftiger.

Niederlande:
Bestimmung konkreter Glasfaserkabel für die Erfassung

In der Begründung der niederländischen Regierung wurde darauf hingewiesen, dass Anordnungen in der Regel angeben sollen, welche (Glasfaser-)Kabel überwacht werden sollen.[64]

Die Festlegung, welche konkrete technische Infrastruktur überwacht werden soll, kann eine wichtige Begrenzung von Überwachung darstellen. In den Vereinigten Staaten müssen Anordnungen zur nachrichtendienstlichen Überwachung nach dem Foreign Intelligence Surveillance Act (FISA) das Gerät, Konto oder die «Vorrichtung» benennen (50 U.S. Code 1805(a)), die überwacht werden soll. Ein bestimmtes Kabel kann in diesem Zusammenhang als «Vorrichtung» betrachtet werden.[65] Dieser Aspekt kann bei der Beurteilung der Verhältnismäßigkeit der jeweiligen Operation wichtig sein, da weniger Menschen davon betroffen sein könnten, wenn für das Ausleiten

63 Eine ähnliche Pflicht, «Kategorien» von Suchbegriffen aufzulisten, findet sich im Schweizer Nachrichtendienstgesetz (Artikel 40 c, «Genehmigungsverfahren für Kabelaufklärung»).

64 Anlage zum Schreiben des Innenministers über das niederländische Nachrichtendienstgesetz (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Bijlage bij brief Wiv 2017 en regeerakkoord), 2017, 3, https://www.aivd.nl/binaries/aivd_nl/documenten/kamerstukken/2017/12/15/kamerbrief-over-wiv-2017-en-het-regeerakkoord/20171215+Bijlage+bij+brief+minister+BZK+over+Wiv+2017+en+regeerakkoord.pdf.

65 Kris und Wilson: «National Security Investigations & Prosecutions 2d», 2012, 572f.

eines bestimmten Kommunikationsstroms ein spezifischer Zugangspunkt zugewiesen wird.

Deutschland:
Direkte ministerielle Verantwortung für die Aktivierung bestimmter Suchbegriffe

§ 9 (2) des BND-Gesetzes sieht eine Unterrichtung des Bundeskanzleramtes für solche Suchbegriffe vor, die auf EU-Institutionen oder Organe von EU-Mitgliedstaaten abzielen. Dies stärkt die ministerielle Rechenschaftspflicht – auch rückwirkend –, wenn es bei der Steuerung der Auslands-Fernmeldeaufklärung zu Verstößen kommt.

Ausgewählte Beispiele für die Laufzeit von Anordnungen

Die folgende Tabelle zeigt Beispiele für die Gültigkeitsdauer von Anordnungen zur Erfassung ausländischer Kommunikationsdaten in ausgewählten Ländern. Im Prinzip sollte die Dauer einer Anordnung im Hinblick auf die wesentlichen Kriterien für die Genehmigung festgelegt werden, also beispielsweise der operative Zweck der Datenerfassung. Eine kürzere Gültigkeitsdauer ist dann erforderlich, wenn sich die dem operativen Zweck zugrunde liegenden Bedingungen innerhalb kurzer Zeit ändern.

Tabelle 3: Gültigkeit von Anordnungen für strategische Fernmeldeaufklärung

Land	Gültigkeitsdauer	Rechtsgrundlage
Frankreich	12 Monate; kann um weitere 12 Monate verlängert werden	Artikel L. 854-2.-II. des Gesetzes Nr. 2015-1556 zur internationalen Kommunikationsüberwachung
Deutschland	9 Monate; kann um weitere 9 Monate verlängert werden 3 Monate; kann um weitere 3 Monate verlängert werden	§ 9 (3) BND-Gesetz § 10 (5) Artikel 10-Gesetz
Niederlande	3 Monate; kann um weitere 3 Monate verlängert werden[66]	Abschnitt 29 des Gesetzes über Nachrichten- und Sicherheitsdienste 2017
Vereinigtes Königreich	6 Monate; kann um weitere 6 Monate verlängert werden	Abschnitt 143 (1)(a) IP Act
Schweiz	6 Monate; kann jeweils um max. 3 Monate verlängert werden	Abschnitt 41 (3) ND-Gesetz

66 Dabei gilt zu beachten, dass die in Artikel 29 des niederländischen Nachrichtendienstgesetzes genannte Dreimonatsfrist eine Standard-Genehmigungsfrist für Sonderbefugnisse ist. Abweichungen finden sich in Artikel 48 (Erfassung, 1 Jahr), Artikel 49 (Suche, 1 Jahr) und Artikel 50 (automatisierte Datenanalysen, 1 Jahr).

Wenn die Bedingungen über einen längeren Zeitraum hinweg stabil sind, könnte eine längere Gültigkeitsdauer sinnvoll sein. Die Einführung solcher normativen Richtlinien zur Festlegung der Gültigkeitsdauer könnte eine noch größere Flexibilität bei der Genehmigung von Anordnungen bieten und dazu führen, dass die Laufzeit nach dem tatsächlichen Bedarf bestimmt wird.

Gute Kontrollpraxis

Da die Ausarbeitung von Anträgen für Überwachungsoperationen in der Regel die Zuständigkeit der Exekutive ist, ergab unsere vergleichende Überprüfung der Kontrollpraxis keine empfehlenswerten Beispiele, die für diese Phase im SIGINT-Regulierungsprozess relevant wären.

Zusammenfassung der Ergebnisse und Reformagenda

Anordnungen ebnen den Weg für eine detaillierte Kontrolle der operativen Aufgabenwahrnehmung der Nachrichtendienste. Auf ihrer Grundlage können Kontrollgremien die Rechtmäßigkeit und Verhältnismäßigkeit der Kommunikationsüberwachung vor der Durchführung prüfen. In einigen Ländern können die Nachrichtendienste geplante strategische Überwachungsmaßnahmen nicht ohne richterliche Aufsicht in die Praxis umsetzen. Im Gegensatz zur parlamentarischen Kontrolle, die häufig erst im Nachhinein erfolgt, ist dies ein wirksames Mittel, um die Überwachung schon vorab zu regulieren.[67] Detaillierte Anordnungen ermöglichen Kontrollgremien, aussagekräftigere Verhältnismäßigkeitsprüfungen durchzuführen, und ermuntern die Dienste, bei der Anwendung von Überwachungsmaßnahmen präzise und effizient vorzugehen.

Die unterschiedlichen Formen von Anordnungen zur Massenüberwachung, die es mittlerweile in vielen Ländern gibt, verdeutlichen das Potenzial, dieses Kontrollinstruments im Bereich der Überwachung ausländischer Kommunikation. Es besteht ein Bedarf, kreativ über weitere relevante Kriterien und zusätzliche Aspekte nachzudenken, um Anordnungen in der Fernmeldeaufklärung weiter zu präzisieren. So könnten Gesetzgeber beispielsweise die Exekutive auffordern, die tatsächliche Nutzung von Datenfilterungsverfahren konkret zu belegen und wie die Zugriffsschranken auf Datenbanken zu spezifizieren. Die Autoren freuen sich über zusätzliche Hinweise zu Schutzmechanismen für Anordnungen in nationalen Nachrichtendienstgesetzen. Dasselbe gilt für weitere Beispiele im Bereich von Kontrollinnovationen.

67 Natürlich kann es Notsituationen geben, in denen Nachrichtendienste ohne unabhängige Vorab-Prüfung Massenüberwachungsmaßnahmen ergreifen dürfen. Dennoch empfiehlt es sich, von vornherein Anordnungen zu nutzen. Dies gilt, wenn es sich um Anordnungen handelt, die systematisch von Gerichten oder speziellen Kontrollgremien überprüft werden, bevor die entsprechenden Maßnahmen in die Tat umgesetzt werden.

Phase 3: Genehmigungsverfahren

Wenn eine Anordnung ausgestellt wurde, muss die angeforderte SIGINT-Maßnahme von einem Kontrollgremium mit Blick auf die Notwendigkeit und Verhältnismäßigkeit geprüft und daraufhin genehmigt oder abgelehnt werden. Es gibt je nach Land verschiedene Regelungen bezüglich des Zeitpunkts, zu dem die unabhängige, gerichtliche Prüfung ins Spiel kommt. In einigen Ländern genehmigen der zuständige Minister oder andere Mitglieder der Exekutive die Anordnungen. Im Vereinigten Königreich beispielsweise ist die *Autorisierung (authorization)* von Anordnungen ein Vorrecht der Exekutive. Die ministerielle Autorisierung muss anschließend von unabhängigen Judicial Commissioners (Kommissionsmitglieder mit Berufserfahrung im Richteramt) *genehmigt (approved)* werden. Im deutschen Rechtsrahmen werden Anordnungen dagegen von der G 10-Kommission oder dem unabhängigen Gremium direkt genehmigt.

Die unabhängige Genehmigung der Datenerfassung ist ein wichtiger Schutzmechanismus vor Zweckentfremdung und Missbrauch der Überwachungsbefugnisse.[68] Die Rechtmäßigkeit der Überwachungspraxis hängt von der Kontrolle des exekutiven Verhaltens von außen ab. Das Genehmigen von Kontrollmechanismen *vor* deren Implementierung ist entscheidend, denn dadurch kann von bestimmten Maßnahmen abgeschreckt und deren Umsetzung verhindert werden. Die unabhängige Genehmigung generiert darüber hinaus einen wichtigen Lerneffekt, da die zuständigen Gremien ihre Kontrollen laufend optimieren und aus früheren Fehlern lernen können. Dadurch können sie wiederum besser begründen, warum bestimmte Maßnahmen nicht erforderlich sind oder kein ausreichender Nachweis erbracht wurde.

In vielen Demokratien hat sich ein Genehmigungsverfahren etabliert, das eine gerichtliche und eine exekutive Kontrollfunktion kombiniert. Ein gerichtliches Aufsichtsorgan – idealerweise ein Gericht – ist am besten geeignet, die rechtliche Überprüfung einer Anordnung durchzuführen. Aber wie zahlreiche Gespräche mit Vertreter/innen der Nachrichtendienstkontrolle gezeigt haben, kann die Beteiligung der politischen Führungsebene, z. B. der zuständigen Minister/innen oder Staatssekretär/innen, auch einen relevanten Schutz darstellen, insbesondere im Bereich des Auslandsnachrichtendienstes. Die Akzeptanz einer Überwachungsmaßnahme kann über rechtliche Kriterien der Notwendigkeit und Verhältnismäßigkeit hinaus auch in

68 «Im Fall Popescu v. Rumänien beschloss das Gericht, dass die rumänische Behörde, die die Überwachung angeordnet hatte (die Staatsanwaltschaft), nicht unabhängig von der Exekutive war. Das Gericht befand, dass die genehmigende Stelle unabhängig sein muss und die Aktivitäten der antragstellenden Behörde entweder gerichtlich oder unabhängig geprüft werden müssen. Ähnlich hob das Gericht in den Fällen Iordachi and Association for European Integration and Human Rights und Ekimdzhiev hervor, dass unabhängige Kontrollen sowohl in der Genehmigungs- als auch in der Durchführungsphase vorhanden sein sollten. Die Präferenz des Gerichtshofs ist die gerichtliche Genehmigung, auch wenn im Fall Kennedy vs. das Vereinigte Königreich das britische System der ministeriellen Genehmigung akzeptiert wurde.» Siehe: Venedig-Kommission: «Report on the Democratic Oversight of Signals Intelligence Agencies», 2015, Paragraf 106, http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

die politische Sphäre reichen. Die Einbeziehung politischer Erwägungen, wie etwa die mögliche Beeinträchtigung der diplomatischen Beziehungen zu einem anderen Land, kann den Genehmigungsprozess um eine wichtige Perspektive erweitern.

Relevante Aspekte

Die Komplexität und Vertraulichkeit der Thematik setzt voraus, dass das Kontrollgremium ausreichend qualifiziert ist (z. B. ein Fachgericht für Fernmeldeaufklärung) und über die erforderlichen Befugnisse und Ressourcen zur Durchführung der Genehmigung verfügt (z. B. Zugang zu allen relevanten Informationen).[69] Eine Grundvoraussetzung für jede Genehmigungsbehörde ist Unabhängigkeit. Zu den weiteren relevanten Aspekten gehören:

- Wer ist in den Genehmigungsprozess eingebunden?
  - Wie wird die Unabhängigkeit der Genehmigung sichergestellt? Eine einheitliche, voll ausgestattete Genehmigungsstelle mit vollen Zugriffsrechten ist beispielsweise besser gerüstet, um umfassende Überprüfungen durchzuführen.
- Wann findet die Prüfung statt? Vor oder nach der Umsetzung der Überwachungsmaßnahmen?
- Wie läuft die Genehmigung ab?
  - Werden alle Anordnungen unabhängig genehmigt oder sieht das Gesetz Ausnahmen vor? Gibt es beispielsweise Ausnahmen für Notfallverfahren? Falls ja, sind diese so gestaltet, dass sie keine Schlupflöcher für nicht genehmigte Operationen eröffnen?
  - Welche Bewertungskriterien werden angewendet?
  - Wie explizit benennen die Kontrollgremien ihre Kriterien, um Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit in der Praxis konkret zu bewerten?
  - Wie viel Zeit hat das Kontrollgremium, um eine Anordnung zu prüfen?
- Sieht das Gesetz ein Berufungsverfahren vor?
  - Sind die Genehmigungsentscheidungen rechtlich bindend?
  - Wird technischer und kontradiktorischer Rat in den Genehmigungsprozess eingebunden? Falls ja, wie?

69 «Das Gericht [...] hat befunden, dass [...] es im Grunde wünschenswert ist, einen Richter mit der Aufsichtskontrolle zu betrauen. [...] Die Aufsicht durch außergerichtliche Stellen kann als mit dem Übereinkommen vereinbar angesehen werden, sofern die Aufsichtsstelle von den überwachenden Behörden unabhängig ist und über ausreichende Befugnisse und Kompetenzen verfügt, um eine wirksame und kontinuierliche Kontrolle auszuüben.» Siehe: Urteil des Europäischen Gerichtshofs für Menschenrechte (EGMR) im Fall Roman Zakharov v. Russland, Antragnummer 47143/06, Paragraf 275, http://hudoc.echr.coe.int/eng?i=001-159324.

- Berücksichtigen die Anordnungen auch Metadaten und «sekundäre»[70] Daten?
- Berücksichtigt die Genehmigung bei der Bewertung einer neuen Anordnung andere (laufende) Überwachungsmaßnahmen?[71]
- Wie wird die Genehmigungsentscheidung dokumentiert? Gibt es öffentlich zugängliche Statistiken zur Anzahl der Ablehnungen und der Gesamtzahl der geprüften Anträge?

Gute gesetzliche Vorgaben

Ermessensspielraum der Kontrollgremien

Kanada:
Anordnungen können unter Vorbehalt genehmigt werden

Bill C-59 sieht eine Regel vor (Teil 2, Intelligence Commissioner Act, Section 21 (2 b)), die es dem Intelligence Commissioner gestattet, die Speicherung ausländischer Datensätze zu genehmigen, abzulehnen oder *unter bestimmten Bedingungen zu genehmigen*. Diese Bedingungen können sich auf «die Abfrage oder Nutzung des ausländischen Datensatzes oder die Speicherung oder Vernichtung des Datensatzes oder eines Teils davon» beziehen. Der Intelligence Commissioner muss begründen, warum die Genehmigung an bestimmte Bedingungen geknüpft werden muss.

---

70 Der Begriff «sekundäre Daten» («secondary data») wird im britischen Nachrichtendienstgesetz häufig verwendet. Laut Graham Smith bezeichnet er die «vielleicht wichtigste Datenkategorie innerhalb des IP Act. Grob gesagt, handelt es sich um Metadaten, die im Rahmen einer Anordnung für gezielte, thematische oder massenhafte Überwachung beschafft wurden. Daher unterliegen diese Daten nicht den Nutzungseinschränkungen, die für abgefangene Inhalte gelten. Insbesondere ist im Gegensatz zu Inhalten keine Anordnung für eine gezielte Untersuchung erforderlich, um Metadaten für die Prüfung unter Verwendung eines Selektors (z. B. einer E-Mail-Adresse) auszuwählen, welcher sich auf jemanden bezieht, der bekanntermaßen auf den Britischen Inseln lebt. Je breiter der Umfang der Sekundärdaten, desto mehr Daten können also ohne eine Anordnung für eine gezielte Untersuchung ausgewertet werden und desto mehr davon, was normalerweise als Inhalt gilt, wird einbezogen.» Quelle: Smith: «Illuminating the Investigatory Powers Act», 22. Februar 2018, https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html.

71 Das Konzept der «Überwachungsgesamtrechnung» wurde vom Bundesverfassungsgericht entwickelt (BVerfG-Urteil vom 12. April 2005 – 2 BvR 581/01). Das Konzept geht von der Prämisse aus, dass das Kontrollgremium bei der Entscheidung über die Genehmigung eines bestimmten Antrags kaum – falls überhaupt – die Gesamtheit anderer bestehender Maßnahmen berücksichtigt. Der Gerichtshof hat daher vorgeschlagen, bei der Genehmigung einer zusätzlichen Datenerhebung alle laufenden Überwachungsmaßnahmen zu berücksichtigen, um die allgemeine Verletzung der Grundrechte von Bürgern zu beurteilen.

Sollte Bill C-59 verabschiedet werden, gilt die Möglichkeit, Anordnungen unter Vorbehalt zu genehmigen, für sämtliche nachrichtendienstlichen Tätigkeiten (über den kanadischen Auslandsnachrichtenchtendienst CSE hinaus). Dieser Ansatz kann Aufsichtsbehörden zu mehr Kontrolle über die Durchführung von Überwachungsmaßnahmen verhelfen. Das könnte etwa bedeuten, eine bestimmte Anzahl von Tagen festzulegen, nach denen Daten gelöscht werden müssen, oder bestimmte Arten von Informationen zu definieren, die vor der Auswertung vernichtet werden müssen.

Öffentliche Berichterstattung über einzelne Genehmigungsentscheidungen

Niederlande:
Verpflichtender öffentlicher Bericht von der Genehmigungsbehörde

Die niederländische TIB-Kommission ist rechtlich verpflichtet, einen öffentlichen, jährlichen Bericht zu veröffentlichen.[72]

USA:
Möglichkeit, die Veröffentlichung einer Entscheidung oder Stellungnahme des Foreign Intelligence Surveillance Court zu beantragen

Jede/r Richter/in kann aus eigenem Antrieb oder auf Antrag einer beteiligten Partei die Veröffentlichung von Beschlüssen, Stellungnahmen oder anderen Entscheidung beantragen. Auf diesen Antrag hin kann der/die vorsitzende Richter/in nach Anhörung anderer Richter/innen des Gerichtshofs beschließen, dass das betreffende Dokument veröffentlicht wird.[73]

Wie eingangs erwähnt, führen wir ganz bewusst einige Ideen aus dem Bereich der gezielten Überwachung auf, wenn wir der Meinung sind, dass sich einige der spezifischen Praktiken oder Bestimmungen auch auf den Bereich der strategischen Überwachung anwenden lassen. In diesem Fall eröffnet die Veröffentlichung von Gerichtsentscheidungen Raum für Diskussionen und eine bessere öffentliche Untersuchung der Überwachungspraxis und der Auslegungen des Nachrichtendienstrechts.

72 Eijkman, Eijk und Schaik, 2018, 41.

73 United States Foreign Intelligence Surveillance Court (FISC): «Rules of Procedure», 1. November 2010, Rule 62, http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

USA:
Veröffentlichung neuer Rechtsauslegungen

Section 602(a) des USA Freedom Act beinhaltet eine Deklassifizierungspflicht. Demnach führt der Director of National Intelligence in Absprache mit dem Attorney General eine «Deklassifizierungsprüfung aller Entscheidungen, Anordnungen oder Stellungnahmen durch, die vom Foreign Intelligence Surveillance Court oder dem Foreign Intelligence Surveillance Court of Review (wie in Section 601(e) definiert) ausgegeben wurden und eine wesentliche Konstruktion oder Auslegung einer Rechtsvorschrift, einschließlich jeder neuen oder wesentlichen Konstruktion oder Auslegung des Begriffs «special selection term» (spezifischer Suchbegriff), beinhalten, und macht – im Einklang mit dieser Überprüfung – jede dieser Entscheidungen, Anordnungen oder Stellungnahmen so weit wie möglich der Öffentlichkeit zugänglich.»[74]

Um den Anforderungen an den Schutz von Quellen und Methoden gerecht zu werden, können Dokumente auch in überarbeiteter Fassung veröffentlicht werden.

Kontradiktorische Verfahren bieten zusätzliche Input-Legitimation für den Genehmigungsprozess

USA:
Externe juristische Gutachten können im Zuge des Genehmigungsverfahren eingeholt werden

Der FISC kann eine Person ernennen, die als Amicus Curiae («Freund des Gerichts») bei der Prüfung von Anordnungen behilflich ist, die nach Ansicht des Gerichts eine neuartige oder bedeutsame Rechtsauslegung darstellen.[75] Das Gericht hat also die Möglichkeit, im Rahmen des Genehmigungsprozesses für Auslandsüberwachung, ein kontradiktorisches Verfahren einzuleiten. Das Gesetz fordert ausdrücklich, dass die/der ernannte Gutachter/in «rechtliche Argumente vorbringt, die den Schutz der persönlichen Privatsphäre und der bürgerlichen Freiheiten fördern.»[76]

74 Section 602 des USA Freedom Act, https://www.congress.gov/bill/114th-congress/house-bill/2048/text, eigene Übersetzung.

75 50 U.S. Code § 1803 (i)(2)(A); Cook: «The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty», 2017, 543, http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1960&context=aulr.

76 50 U.S. Code § 1803(i)(4)(A), eigene Übersetzung.

Die Entscheidung über die Genehmigung einer Überwachungsmaßnahme profitiert davon, wenn dem genehmigenden Kontrollgremium zum Zeitpunkt der Entscheidung eine unabhängige gutachterliche Stellungnahme zur Verfügung gestellt wird. Wenn bei den Prüfungen der Anordnungen nur eine Sichtweise auf die jeweiligen Rechtsfragen vertreten ist, besteht die Gefahr der Voreingenommenheit und einseitiger Entscheidungen. Daher unterhält der FISC einen Pool designierter Rechtsgutachter/innen, aus dem das Gericht für einen spezifischen Fall einen Amicus Curiae auswählen kann. Die externe Expertise eines solchen «Freunds des Gerichts» ermöglicht einen frischen Blick auf wichtige oder neue Rechtsfragen und hilft, einen Tunnelblick zu verhindern. Gleichzeitig wird die Input-Legitimation des Verfahrens ausgeweitet. Ähnlich verfährt Schweden: Bei allen Verfahren vor dem schwedischen Gericht für Auslandsaufklärung [*Försvarsunderrättelsedomstolen*] muss ein/e Datenschutzbeauftragte/r [*Integritetsskyddsombud*] anwesend sein, es sei denn die Operation würde dadurch verzögert oder gefährdet.[77] Diese/r Beauftragte wird von der Regierung ernannt.

Allein der Hinweis, dass der FISC beabsichtigt, einen Amicus Curiae zu benennen, hat nachweislich eine abschreckende Wirkung auf die Exekutive. Laut dem FISA-Jahresbericht 2017[78] wurde in diesem Jahr kein Amicus Curiae ernannt. Zwar hatte das Gericht dreimal erwogen, eine Person zu ernennen, in allen drei Fällen hat die Regierung jedoch den vorgelegten Antrag letztendlich nicht weiterverfolgt oder die endgültigen Anordnung so abgeändert, dass sie «keine neuartige oder bedeutsame Rechtsfrage beinhaltete, wodurch die Anforderung zur Benennung des Amicus Curiae entfällt».[79] Allerdings müssen die Stellungnahmen, die ein Amicus Curiae vorbringt, nicht notwendigerweise «kontradiktorisch» sein. Sie können auch der Argumentation der Regierung folgen, beispielsweise bei technischen Aspekten, statt eine der Regierung entgegengesetzte Position einzunehmen.[80]

77 Lubin, 2018.

78 Administrative Office of the United States Courts: «Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017», 25. April 2018, http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf.

79 Ebd., 4, eigene Übersetzung.

80 Neben den rechtlichen Amici Curiae sollte es auch technische Amici Curiae geben, die dem Gericht mit Fachwissen in technologischen Fragen zur Seite stehen. Bisher wurde kein technischer Amicus Curiae ernannt, um zu einem Verfahren beizutragen.

Frankreich:
Quoten für spezifische Datenerfassungsmethoden

Das französische Nachrichtendienstgesetz legt quantitative Grenzen für den Einsatz bestimmter Überwachungsinstrumente fest, um verzichtbare, bereits genehmigte Maßnahmen zu beenden, bevor neue genehmigt werden. Die zulässige Anzahl gleichzeitig laufender Maßnahmen ist auf ein Kontingent begrenzt, das vom Premierminister auf Empfehlung der französischen Kontrollbehörde, der Commission nationale de contrôle des techniques de renseignement (CNCTR), festgesetzt wird.[81]

Das französische Quotensystem begrenzt die Nutzung bestimmter gezielter Erfassungsmethoden. Die zugrundeliegende Logik – die Dienste dazu zu zwingen, bestehende genehmigte Anordnungen einzusetzen bzw. zu verwerfen, statt einfach neue Maßnahmen zu beantragen – scheint ein adäquates Mittel zu sein, um die Nutzung spezifischer Instrumente zu begrenzen. Solche Quoten haben zudem das Potenzial, jährliche, öffentliche Diskussionen über die festgelegte Obergrenze anzustoßen. Natürlich hängt die Wirksamkeit dieses Ansatzes sowohl von dem dazugehörigen Prozess als auch von dem tatsächlich genutzten Kontingent ab. Im Idealfall sollte die Festlegung der Quoten auf einem transparenten und überprüfbaren Verfahren basieren, das die jeweilige Notwendigkeit eines bestimmten Kontingents darlegt.

Das Quotensystem gilt in Frankreich für drei Arten der Datenerfassung: erstens für das gezielte Erfassen elektronischer Kommunikation[82] mit einem Kontingent von maximal 3.040 Anordnungen im Jahr 2017, zweitens für die Nutzung von sogenannten IMSI-Catchern, mit einem Gesamtkontingent von 60 Stück und drittens für die Echtzeiterfassung von Verbindungsdaten. Hier beträgt das Kontingent 500 Anordnungen.[83] Den verschiedenen zuständigen Ministerien wird jeweils eine Teilmenge der Gesamtquote zugewiesen (z. B. Teilkontingente für Innen-, Verteidigungs- und andere Ministerien), und ihre Einhaltung wird täglich vom GIC (Groupement interministeriel de control) überprüft.[84]

---

81 Commission nationale de contrôle des techniques de renseignement (CNCTR): «Deuxième Rapport d'activité 2017», 2018, 37ff., https://www.cnctr.fr/_downloads/NP_CNCTR_2018_rapport_annuel_2017.pdf.

82 Artikel L. 852-1 des französischen Gesetzbuchs zur inneren Sicherheit (*Code de la sécurité intérieure*)

83 CNCTR, 2018, 37ff.

84 In Frankreich ist eine spezifische Behörde, das Groupement interministeriel de control (GIC), für Sammlung von Kommunikationsdaten zuständig. Das GIC zentralisiert die Weiterleitung genehmigter Anordnungen an die jeweiligen Anbieter, die die Daten besitzen. Die Behörde untersteht dem Premierminister und ist auch für die Kontrolle der Quoteneinhaltung zuständig.

Explizite, praktische Standards für die Beurteilung der Verhältnismäßigkeit bei der Genehmigung von SIGINT-Anordnungen

Eine genaue Erklärung, wie die Notwendigkeits- und Verhältnismäßigkeitsprüfung einer Anordnungen durchgeführt wird, ist für die Bewertung der Gründlichkeit und Legitimität des Verfahrens entscheidend. Das britische Investigatory Powers Commissioner's Office (IPCO) hat eine «Advisory Notice» veröffentlicht, die Behörden und die Öffentlichkeit darüber informiert, welchen allgemeinen Ansatz die Judicial Commissioners bei der Entscheidung über die Genehmigung von Anordnungen nach dem IP Act verfolgen.

Vereinigtes Königreich: IPCO Advisory Notice 01/2018

Die Judicial Commissioners, die für die Genehmigung aller Überwachungs-Anordnungen zuständig sind, müssen sich fragen, ob das, was mit der jeweiligen Anordnung erzielt werden soll, auch vernünftigerweise mit anderen, weniger grundrechtseinschränkenden Mitteln erreicht werden kann. Bei der Ausübung dieser gesetzlichen Pflicht müssen die Judicial Commissioners insbesondere Folgendes berücksichtigen:

- ob das Schutzniveau, das bei der Informationsbeschaffung anzuwenden ist, aufgrund der besonderen Sensibilität dieser Informationen erhöht ist;
- das öffentliche Interesse an der Integrität und Sicherheit von Telekommunikationssystemen und Postdiensten;
- alle sonstigen Aspekte des öffentlichen Interesses am Schutz der Privatsphäre;
- zusätzliche Schutzmaßnahmen für Angelegenheiten von Berufsgeheimnisträger/innen, wie das anwaltliche Berufsgeheimnis und journalistische Quellen;
- die Notwendigkeits- und Verhältnismäßigkeitsprüfungen, entsprechend dem Human Rights Act von 1998 und dem Recht der Europäischen Union, soweit sie auf die beantragten Befugnisse/Tätigkeiten anwendbar sind.[85]

85 IPCO: Advisory Notice 1/2018. Approval of Warrants, Authorisations and Notices by Judicial Commissioners», 2018, 4, https://www.ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf.

Diese Advisory Notice ist nicht bindend und kann sich theoretisch jederzeit ändern. Daher repräsentiert sie nur die Meinung der derzeitigen Judicial Commissioners, denn zudem besteht keine Pflicht, die Öffentlichkeit darüber zu informieren, ob die Richtlinien überarbeitet wurden. Der höchste Transparenz-Standard ist nach wie vor, solche Verfahrensregeln im Gesetz festzuhalten. Einige Kritiker/innen haben angemerkt, dass die Advisory Notice nicht hervorhebt, wie «wichtig eine aktuelle und relevante Begründung der nachrichtendienstlichen Notwendigkeit ist, um die Entscheidung zur Ausstellung von Anordnungen zu rechtfertigen»[86], insbesondere in Fällen, die die nationale Sicherheit berühren, bei denen die Advisory Notice zu einem größeren Ermessensspielraum tendiert.

Vereinigtes Königreich: Offener Dialog zwischen Kontrollgremium und der Zivilgesellschaft über Kriterien für Verhältnismäßigkeitsprüfungen von Überwachungsmaßnahmen

Nach der Veröffentlichung der Advisory Notice im Januar 2018 hat IPCO die Grundsätze für die Prüfung der Verhältnismäßigkeit im Mai 2018 ausgeweitet. Dazu hat die Kontrollbehörde öffentlich dazu aufgerufen, Ideen und Vorschläge einzureichen, die für die Verhältnismäßigkeitsprüfung von (Massen-)Überwachungsbefugnissen relevant scheinen. IPCO bat NGOs und andere Interessierte um Hilfe beim Identifizieren der vielfältigen Faktoren, die die Judicial Commissioners bei der Bewertung der Verhältnismäßigkeit von Anordnungen berücksichtigen sollten. Die Fragen dafür lauteten:

- Welche Faktoren sollten die Judicial Commissioners bei der Prüfung der Verhältnismäßigkeit einer vorgeschlagenen Maßnahme berücksichtigen?
- Gibt es einen bestimmten Ansatz, den die Prüfer/innen bei der Bewertung dieser zum Teil widersprüchlichen Faktoren verfolgen sollten?[87]

86 The Chambers of Simon McKay: «Judicial Approval of Warrants, Authorisations and Notices under the Investigatory Powers Act 2016: A Review of the Investigatory Powers Commissioner's Office First Advisory Note», 2018, https://simonmckay.co.uk/judicial-approval-of-warrants-authorisations-and-notices-under-the-investigatory-powers-act-2016-a-review-of-the-investigatory-powers-commissioners-office-first-advisory-note/, eigene Übersetzung.

87 IPCO: «IPC Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers», 23. Mai 2018, https://www.ipco.org.uk/docs/IPC_Submissions_on_bulk_powers.pdf; die Einreichungen sind hier zu finden: https://www.ipco.org.uk/Default.aspx?mid=4.13.

Die unabhängige Genehmigung wird zu einem noch stärkeren demokratischen Schutzmechanismus, wenn das Verfahren völlig transparent ist und die Prüfer/innen mit einem klaren Mandat und ausreichendem Ermessensspielraum ausgestattet sind, um Anordnungen unter Vorbehalt zu genehmigen. Im Idealfall sieht das Gesetz eine verbindliche Überprüfung der Einstufung vor, mit dem Ziel, möglichst viele Informationen, z. B. über kritische, neue Rechtsauslegungen, zu veröffentlichen.

Kontradiktorische Verfahren sind ein wesentliches Merkmal eines starken, unabhängigen Genehmigungsverfahrens. Weitere vielversprechende Beispiele sind explizite Standards für die Beurteilung der Verhältnismäßigkeit bei der Genehmigung von Anordnungen, wie z. B. die Advisory Notice des IPCO zusammen mit dem anschließenden Dialog mit der Zivilgesellschaft und andere Expert/innen. Wir freuen uns über Hinweise zu weiteren spezifische Standards, die von anderen Aufsichtsbehörden eingesetzt werden, um externe Beratung einzuholen oder die Verhältnismäßigkeit von SIGINT-Maßnahmen zu beurteilen. Dasselbe gilt für konkrete Prüfkriterien, mit denen die unabhängigen Kontrolleur/innen verifizieren können oder sollten, inwiefern eine beantragte Maßnahme rechtzeitig relevante Informationen liefern kann.

Eine erweiterte Zuständigkeit der Aufsichtsbehörden sollte insbesondere erwogen werden, wenn es um die Genehmigung des (internationalen) Informationsaustauschs geht.

Phase 4: Erfassung und Filterung

Sobald eine Anordnung genehmigt ist, kann der Nachrichtendienst mit der Durchführung der Überwachungsmaßnahme fortfahren. Dazu fängt er die relevanten Signale ab, beispielsweise indem er Daten bei einem Telekommunikationsanbieter oder bei einem Internet Exchange Point ausleitet. Anschließend müssen die gesammelten Daten aus zwei Gründen gefiltert werden: Erstens werden aufgrund der großen Datenmengen, die für eine langfristige Speicherung entschieden zu viel wären, unnötige Daten ohne nachrichtendienstlichen Wert herausgefiltert (z. B. alle Daten aus öffentlichen Video-Feeds); zweitens muss der Strom der erfassten Daten gefiltert werden, um den gesetzlichen Anforderungen zu entsprechen. Die Kommunikation bestimmter Personengruppen – wie alle inländische Kommunikation oder die Kommunikation von Anwält/innen oder anderen Berufsgruppen, die durch ihre Verschwiegenheitsverpflichtungen besonders auf das Fernmeldegeheimnis vertrauen (müssen) – können in den nationalen Überwachungsgesetzen ein höheres Schutzniveau genießen.[88]

88 Wie schon erwähnt, ist es technisch nicht immer möglich, geschützte Kategorien wie bestimmte Berufe herauszufiltern. Betroffene Personen oder Personenverbände könnten ihre Telefonnummern an Nachrichtendienste und Strafverfolgungsbehörden übermitteln. Bei der Internetkommunikation ist das eindeutige Filtern aber sehr viel komplizierter.

Erfassung

Relevante Aspekte

Bezüglich der Datenerfassung muss klar definiert werden, wer für die Datenausleitung zuständig ist und wo und wie die Geräte zur Datenerfassung installiert werden dürfen. Wird die Erfassung vom Nachrichtendienst abgewickelt oder erledigen private Stellen (z. B. die Internetanbieter) dies im Auftrag der Nachrichtendienste? Diese Unterscheidung ist relevant, da die Scharnierfunktion von Providern ein wichtiger Schutz vor einer zu weit gefassten staatlichen Datenerfassung sein kann. Im Prinzip sollten Nachrichtendienste keinen direkten Zugriff auf die Einrichtungen von Telekommunikationsanbietern haben. Es sind aber Fälle bekannt geworden, in denen Internetunternehmen sich bereit erklärt haben, Daten, die sie verwalten, im Auftrag einer Behörde zu durchsuchen. So hat die Firma Yahoo heimlich alle E-Mail-Konten nach von US-Nachrichtendiensten bereitgestellten Informationen durchsucht.[89] Ein Rechtsrahmen muss deshalb genau festlegen, wie (private) Unternehmen zur Zusammenarbeit verpflichtet werden können und welche Mittel Betreiber haben, um bestimmte Vorgaben anzufechten.

Gute gesetzliche Vorgaben

Intermediär für die zentrale Datenerfassung

Frankreich: Spezialisiertes Exekutivorgan fungiert als Datenerfassungszentrum

Im französischen Nachrichtendienstwesen werden die meisten von Dritten (Internetanbieter oder Kommunikationsdienstleister wie Google oder Facebook) gesammelten Daten durch das GIC verwaltet.[90] Prinzipiell gehört diese Behörde nicht zu den Nachrichtendiensten. Vielmehr fungiert es als zentraler Knotenpunkt, der alle Erfassungen unter der Aufsicht des Premierministers abwickelt und koordiniert.

Es empfiehlt sich, dass zwischengeschaltete Stellen wie das GIC für den ersten Filter-/Auswahlprozess verantwortlich sind, da so weniger Mitarbeiter/innen der Dienste

89 Menn: «Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources», 5. Oktober 2016, https://www.reuters.com/article/us-yahoo-nsa-exclusive/yahoo-secretly-scanned-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT.

90 Französische Regierung, «Groupement Interministériel de Contrôle (GIC)», http://www.gouvernement.fr/groupement-interministeriel-de-controle-gic; «Le Groupement interministériel de contrôle va beaucoup donner», http://defense.blogs.lavoixdunord.fr/archive/2016/02/01/groupement-interministeriel-de-controle-14495.html.

Zugang zu den gesammelten Daten haben. Ein ähnliches, spezialisiertes Datenerfassungszentrum gibt es in der Schweiz.[91] Das kann auch aus Kostengründen vorteilhaft sein: Statt über alle Nachrichtendienste hinweg technische Expert/innen zu unterhalten, kann die Bündelung von Fachwissen und Kompetenzen in einer zentralen Behörde die bessere Nutzung der verfügbaren Beschäftigten und Ressourcen ermöglichen. Zudem vereinfacht dies die Zuordnung von Verantwortlichkeiten.

Die Zentralisierung des Datenzugriffs kann auch dazu dienen, die ganzheitliche Kontrolle aller erfassten Daten zu erleichtern. Das GIC gewährt Analyst/innen nur Zugriff auf Daten, die sie für einen bestimmten Auftrag benötigen. Diese Gatekeeper-Funktion kann dazu beitragen, die Geheimhaltung zu wahren. Allerdings birgt die Zentralisierung der Datenspeicherung auch das Risiko eines zentralen Angriffspunkts (z. B. für Hacker-Angriffe usw.). Die französische Aufsichtsbehörde CNCTR bezeichnet das GIC jedoch auch als wirksamen Schutz vor missbräuchlichem Datenzugriff, da eine zwischengeschaltete Instanz – und nicht die Nachrichtendienste selbst – die Datenerfassung implementiert und verwaltet.[92]

USA:
Möglichkeiten der Telekommunikationsunternehmen, Einspruch gegen Überwachungsanordnungen zu erheben

Private Anbieter, wie z.B. Internetanbieter oder Betreiber von Internetknoten, die eine FISA-Überwachungsanordnung erhalten, können diese vor dem FISC anfechten.[93]

Ein gut dokumentierter, wenn auch erfolgloser Einspruch ist der Yahoo-Fall von 2007. Der Serviceprovider hatte die Verfassungsmäßigkeit einer Anordnung zur Weitergabe von Benutzerinformationen gemäß dem *Protect America Act* angefochten. Nachdem Yahoo die erste Klage vor dem FISC verloren hatte, legte der Anbieter gegen die Entscheidung Berufung beim FISC ein.[94]

91 Die schweizer Koordinierungsstelle heißt «Zentrum für elektronische Operationen» (ZEO). Siehe: Führungsunterstützungsbasis FUB: «ZEO (Elektronische Operationen)», https://www.vtg.admin.ch/de/organisation/fub.html.

92 CNCTR, 2018, 16.

93 Ein solches Verfahren ist hier (in geschwärzter Form) veröffentlicht: https://www.aclu.org/2014-fisc-opinion-internet-service-providers-challenge-section-702-surveillance.

94 Electronic Frontier Foundation: «Yahoo's Challenge to the Protect America Act in the Foreign Intelligence Court of Review,» 22. Oktober 2013, https://www.eff.org/cases/yahoos-challenge-protect-america-act-foreign-intelligence-court-review; zu den weiteren, aktuelleren Herausforderungen: Conger: «An Unknown Tech Company Tried (and Failed) to Stop the NSA's Warrantless Spying», 14. Juni 2017, https://gizmodo.com/an-unknown-tech-company-tried-and-failed-to-stop-the-1796111752.

USA:
Allein Internetanbieter sind für die Installation von Splittern und Selektorenlisten verantwortlich

Gemäß FISA Section 702 haben private Internetanbieter – und nicht die Sicherheitsbehörden – die genehmigten, vorgeschalteten Erfassungssysteme zu implementieren. «Die Regierung identifiziert oder weist bestimmte «Selektoren» zu, etwa Telefonnummern oder E-Mail-Adressen, die mit Zielpersonen in Verbindung gebracht werden, und sendet diese Selektoren an Anbieter elektronischer Kommunikationsdienste, damit diese mit der Datenerhebung beginnen.»[95] Daraufhin ist der Anbieter verpflichtet, die an diesen oder von diesem Selektor gesendeten Nachrichten an die Regierung weiterzugeben.[96] Wären die Dienste selbst für die Aktivierung der Selektoren zuständig, könnte dies zu einer größeren Datenerfassung führen.[97]

Die Installation und Wartung von Abhörtechnik durch einen privaten Vermittler stellt eine Schutzmaßnahme dar, weil die Nachrichtendienste die Geräte nicht eigenhändig anderweitig verwenden oder zu anderen Zwecken missbrauchen können. Vermittlungsinstanzen, die zur Zusammenarbeit verpflichtet sind, haben einen gewissen Anreiz, jede staatliche Anfrage genau nach den einschlägigen gesetzlichen Anforderungen zu beurteilen. Die Aktivierung eines weitreichenden Zugriffs auf ihre Kundendaten kann hohe Reputationskosten für Internetunternehmen nach sich ziehen. Daher erlauben sie im Zweifel nur, was unbedingt nötig ist. Diese zusätzliche Kontrollebene fehlt, wenn Länder ihren Nachrichtendiensten den direkten Zugriff auf Systeme oder Kommunikationsinfrastrukturen gewähren, ohne dass ein Provider zwischengeschaltet ist.[98]

95 Privacy and Civil Liberties Oversight Board (PCLOB): «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act», 2. Juli 2014, 7, https://www.pclob.gov/library/702-Report.pdf.

96 Ebd.

97 Eine E-Mail der Deutschen Telekom an den BND, die veröffentlicht wurde, liefert der Öffentlichkeit weitere Einblicke in die Zusammenarbeit zwischen Behörden und Internetanbietern: https://de-de.facebook.com/peterpilz/photos/902029969840817.

98 Eine Reihe von EU-Ländern (Schweden, Ungarn, Rumänien, Estland, Lettland und Litauen) beispielsweise haben direkten Zugriff; auch Finnland plant zurzeit die Zulassung eines Direktzugriffs. Weitere Informationen dazu finden Sie in der entsprechenden Abhandlung des Center for Democracy and Technology zu diesem Thema, die demnächst veröffentlicht wird.

Technische Schnittstellen für den direkten Datenbankzugriff der Kontrolleur/innen
Eine Reihe europäischer Länder (siehe Tabelle 4) hat Schnittstellen installiert, die Aufsichtsbehörden einen direkten Zugriff auf erfasste Daten ermöglichen. Ein solcher Direktzugang könnte eine wichtige Innovation für die Aufsicht sein, birgt aber auch Risiken.

Tabelle 4: Technische Kontrollschnittstellen

Land	Art des Zugriffs
Frankreich	«Das CNCTR hat permanenten, vollständigen und direkten Zugriff auf die Durchführungsberichte und Register der Überwachungstechniken, auf die gesammelten Informationen sowie auf die Transkriptionen und Extraktionen, die von den Nachrichtendiensten durchgeführt werden.»[99] Dies basiert auf den direkten technischen Schnittstellen der Aufsichtsbehörden mit dem GIC.
Niederlande	«Zur Durchführung ihrer Prüfungen hat die Aufsichtsabteilung der CTIVD direkten (digitalen) Zugang zu klassifizierten Informationen des AIVD (Algemene Inlichtingen- en Veiligheidsdienst, Allgemeiner Nachrichten- und Sicherheitsdienst) und des MIVD.»[100]
Norwegen	«Der Ausschuss kann die meisten seiner Inspektionen direkt in den elektronischen Systemen der Dienste ohne deren Mitwirken durchführen.»[101]
Schweiz	Die unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten hat direkten Zugriff auf die beim Nachrichtendienst des Bundes (NDB) gespeicherten Daten, einschließlich besonders schützenswerter Personendaten. Dieser Zugriff ist nicht dauerhaft, sondern gilt nur bis zum Abschluss einer konkreten Überprüfung und muss vom Inhaber der jeweiligen Datensammlung protokolliert werden.[102]

Der direkte Zugriff auf Datenbanken hat den Vorteil, dass die Kontrollbehörde Stichproben, unangekündigte Inspektionen und möglicherweise auch automatisierte Kontrollen der Datenverarbeitung durch die Nachrichtendienste durchführen kann. Üblicherweise ist der Zugang der Kontrollgremien zu Informationen in hohem Maße von der Kooperation der Exekutive und der Nachrichtendienste abhängig. Schon

99 Artikel L. 854-9 des Gesetzes Nr. 2015-1556; siehe auch: Agentur der Europäischen Union für Grundrechte: «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update», 2017, 79, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf, eigene Übersetzung; siehe auch: Französisches Gesetzbuch zur inneren Sicherheit (*Code de la sécurité intérieure*), Artikel L. 833-2.

100 Eijkman, Eijk und Schaik, 2018, 38, eigene Übersetzung.

101 Norwegisches parlamentarisches Aufsichtsgremium der Nachrichtendienste (EOS-Ausschuss): «Annual Report 2017 - Document 7:1 (2017-2018)», 22. Februar 2018, 10, https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf, eigene Übersetzung.

102 Artikel 78 (4–5) des Schweizer Nachrichtendienstgesetzes: «Aufgaben, Informationsrechte und Empfehlungen der Aufsichtsbehörde».

allein die Möglichkeit der Kontrolleur/innen direkt auf die Informationen und IT-Systeme der Nachrichtendienste zuzugreifen kann zu mehr Gesetzestreue führen. Wenn Mitarbeiter/innen der Nachrichtendienste nicht wissen können, ob ihr Handeln einer unabhängigen Prüfung – möglicherweise sogar in Echtzeit – unterliegt, kann das zu erhöhter Sorgfalt führen. Darüber hinaus ermöglichen technische Schnittstellen den Kontrollgremien, statistische Auffälligkeiten in den Datenbanken zu identifizieren. Das eröffnet neue Anwendungsmöglichkeiten für (automatisierte) Kontrolltechniken, die das Aufsichtspersonal dabei unterstützen, ihre begrenzten Ressourcen effektiv an den entscheidenden Stellen einzusetzen. Ein solcher Ansatz – also der Einsatz von Analysetechniken zur Identifizierung potenzieller Verstöße – stellt gewissermaßen eine «vorhersagende Aufsicht» dar und wird bereits bei Wirtschaftsprüfungen im Bankensektor angewandt.

Der direkte und ungehinderte Zugang von Kontrollbehörden auf die Datenbanken der Nachrichtendienste kann sie jedoch zu attraktiven Zielen für Spionage- und Hackerangriffe machen. Daher ist es wichtig, nur entsprechend geschultem Aufsichtspersonal einen derartigen Zugang zu gewähren und den Aufsichtsbehörden ein Höchstmaß an IT-Sicherheit zu bieten.

Die Interpretation nachrichtendienstlicher Rohdaten und Protokolldateien ist keine einfache Aufgabe. Ein bloßer Zugriff auf die Daten ist für die Kontrolle nicht zwingend förderlich, erst die Auswertung der Daten liefert einen Informationsvorteil. Mit anderen Worten: Aufsichtsbehörden müssen sich mit den Daten, auf die sie nun zugreifen dürfen, auch genau auseinandersetzen. Die Beschäftigten von Kontrollgremien könnten dabei etwa von Institutionen aus der Finanzaufsicht lernen und benötigen ggf. spezielle Schulungen. Außerdem könnten sie die Entwicklung und die Implementierung von Kontrollalgorithmen in Auftrag geben.

Filterung

Nachdem die Daten erfasst wurden, müssen sie – je nach Regelung im nationalen Nachrichtendienstrecht – zusätzlich nach verschiedenen Kriterien gefiltert werden.

Relevante Aspekte

Die Datenminimierungs- und Filterprozesse sollten dahingehend kritisch überprüft werden, inwieweit sie verfassungs- und menschenrechtliche Standards einhalten. Einige Nachrichtendienstgesetze gewähren beispielsweise einen höheren Datenschutz für Berufe, die der Geheimhaltungspflicht unterliegen. Dazu gehört die Kommunikation von und mit Pastor/innen, Rechtsanwält/innen, Journalist/innen und Ärzt/innen. Ob und inwiefern Tools zur Datenminimierung und -filterung solchen Berufsgeheimnisträger/innen in der Praxis gerecht werden können, sollte von Interesse für Kontrollgremien sein. Das gilt unter Umständen auch für die Prüfung geschützter Gesundheitsdaten und DNA-bezogener Informationen.

Darüber hinaus stellen sich technische Fragen. Denn auch sie können interessante Informationen über die Unabhängigkeit von Aufsichtsbehörden und das

Ausmaß, in dem die Datenminimierung tatsächlich eine Priorität der Nachrichtendienste ist, zutage fördern. Wie wird beispielsweise «Beifang» bei der Erfassung und Filterung behandelt? Unterliegen Datenfiltersysteme wie die Massive Volume Reduction (VRE)-Systeme des britischen Government Communications Headquarters (GCHQ) einer unabhängigen Kontrolle? Oder präziser: Werden die technischen Gerätschaften und die Filterprogramme regelmäßig unabhängig verifiziert? Oder verlassen sich die Kontrollbehörden lediglich auf die Zusicherungen der Nachrichtendienste, dass die Datenminimierungs- und Filterprozesse zweckmäßig funktionieren?

Gute gesetzliche Vorgaben

Löschung von ausgefiltertem Datenmaterial

Niederlande:
Alle herausgefilterten Rohdaten (einschließlich Inhalts- und Verkehrsdaten) können von den Nachrichtendiensten nicht mehr abgerufen werden.

Während in den Niederlanden Inhalts- und Verkehrsdaten bis zu drei Jahre lang gespeichert werden können (standardmäßig ein Jahr, zwei mögliche Verlängerungen um jeweils ein Jahr), müssen Daten, die ausgefiltert oder als nicht relevant für weitere nachrichtendienstliche Untersuchungen klassifiziert werden, umgehend und unwiderrufbar vernichtet werden.[103]

Die Nachrichtendienste sind verpflichtet, die Relevanz der erfassten Daten zu beurteilen (siehe Abschnitt «Datenpflege»).

Gute Kontrollpraxis

Prüfung der Compliance-Audits

USA:
Das Bundesgericht FISC prüft von den Nachrichtendiensten durchgeführte Compliance-Audits.

Moderne Nachrichtendienste sollten über dediziertes Personal für interne

103 Niederländisches Gesetz über Nachrichten- und Sicherheitsdienste 2017, Artikel 48 (5). Siehe auch: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Niederländisches Innenministerium): «Bijlage bij brief Wiv 2017 en regeerakkoord (Anlage zum Schreiben des Innenministers über das niederländische Gesetz über die Nachrichten- und Sicherheitsdienste)», 2017, 3.

Compliance-Audits verfügen. Die Möglichkeit, dass ein unabhängiges Gremium wie der FISC interne Audits überprüfen kann, stärkt die Wirkung dieser Kontrollen. Der FISC kann jedoch nur die von den Nachrichtendiensten bereitgestellten Audit-Daten nutzen und führt keine eigenen Inspektionen durch. Im Idealfall führt ein Kontrollgremium auch eigene Stichprobenprüfungen durch, um die Gründlichkeit und Vollständigkeit dieser Compliance-Audits zu gewährleisten.

Zusammenfassung der Ergebnisse und Reformagenda

Die zunehmende Verfügbarkeit von technischen Kontrollschnittstellen in verschiedenen europäischen Ländern ist eine beachtenswerte Praxis. Auch ist die Einbindung von privaten Akteuren (z. B. Internetanbieter) und öffentlichen Vermittlungsstellen (z. B. dem GIC in Frankreich), die die Datenerfassung vereinfachen und zentralisieren können, weiter zu erörtern. Ob sich die Zentralisierung der Datenverwaltung und der Echtzeitzugriff auf Datenbanken der Nachrichtendienste zu einem Mehrwert für die Aufsicht und die demokratische Regierungsführung entwickeln können, bleibt jedoch eine offene Frage. Der effektive Einsatz solcher Instrumente für verschiedene Kontrollfunktionen muss weiter untersucht werden.

Telekommunikationsanbieter gehören zu den zentralen Stakeholdern im Bereich der Überwachung und müssen deshalb eine starke Stimme haben. Die Möglichkeit, Überwachungsanordnungen anfechten zu können, ist in diesem Zusammenhang eine wichtige Praxis.

Die unabhängige Überprüfung von Datenfiltertechnik verdient eine größere Aufmerksamkeit seitens der Aufsichtsbehörden. Sie sollten die technische Umsetzung des Filtervorgangs und die unabhängige Prüfung der Filtereffektivität genauer untersuchen. Auch die Löschung von Daten gehört zu den laufenden Herausforderungen für Aufsichtsbehörden, der sich viele Kontrollinstitutionen gerade erst bewusst werden. Hier sollten das gegenseitige Lernen aus dem regelmäßigen Austausch mit anderen Kontrollbehörden in anderen Ländern sowie die Förderung eines systematischen Dialogs mit externen Fachleuten intensiviert werden.

Phase 5: Datenverarbeitung

Nach der Erfassung und Filterung müssen die Daten gespeichert, gekennzeichnet und später gelöscht oder vollständig vernichtet werden. Diese Phase des SIGINT-Prozesses ist besonders relevant für Aufsichtsbehörden und Nachrichtendienste, da ein gesetzeskonformes und effizientes Datenmanagement die Grundlage für eine aussagekräftige Datenanalyse liefert. Der Übersichtlichkeit halber ist diese Phase in vier Unterkategorien unterteilt, die die verschiedenen Aspekte der Datenverarbeitung widerspiegeln: Speicherung, Pflege, Austausch und Löschung.

Datenspeicherung

Relevante Aspekte

Aufgrund unterschiedlicher Speicherfristen müssen unter Umständen separate Datenbanken unterhalten werden, z. B. für verschlüsselte Daten, Verkehrs- und Inhaltsdaten oder um Datenpools nach ihrer Rechtsgrundlage oder ihren Zwecken zu unterscheiden. Das heißt, es kann durchaus relevant sein, ob es getrennte Datenspeicherorte gibt. Die Steuerung der Massenüberwachung beruht zunehmend auf der nachweisbaren technischen oder institutionellen Trennung zwischen der Datenerfassung und der Datenanalyse. Im Sinne der Datenschutzprinzipien sollte ein Überwachungsgesetz die Verknüpfung oder Vermischung von Datenbanken einschränken.

Länderübergreifende Bedrohungen führen zu einer engeren grenzüberschreitenden Zusammenarbeit zwischen den Nachrichtendiensten, vor allem zwischen Nachbarländern. Nachrichtendienstdaten – sowohl unausgewertete als auch ausgewertete – werden daher nicht nur bilateral ausgetauscht, sondern auch in *gemeinsamen Datenbanken* für unterschiedliche Bedrohungen und Zwecke gespeichert. Mit gemeinsamen Datenbanken meinen wir einen multilateralen Datenaustausch, der entweder im In- oder im Ausland gehostet werden kann. In der Regel werden gemeinsame Datenbanken multilateral betrieben, wobei alle beteiligten Dienste Daten hinzufügen und Daten abfragen können.

Die europäische Counter Terrorism Group (CTG) betreibt beispielsweise eine Datenbank, die den multilateralen Austausch von ausgewerteten Daten über Personen erleichtert, die in bestimmte Konfliktgebiete gereist und aus diesen zurückgekehrt sind.[104] Diese Datenbank wurde im Juli 2016 in Betrieb genommen. Sie wird auf Servern in den Niederlanden verwaltet und stellt den 30 teilnehmenden Diensten der CTG Informationen (nahezu) in Echtzeit zur Verfügung. Interessanterweise können auch Rohdaten innerhalb der CTG ausgetauscht werden, allerdings nicht über die gemeinsame Datenbank, sondern im Rahmen internationaler SIGINT-Kooperationen.[105]

Die niederländische Kontrollbehörde CTIVD kommt in ihrem Bericht über die CTG-Datenbank zu dem Schluss, dass Maßnahmen für den Schutz von Grundrechten derzeit nicht ausreichend berücksichtigt werden, und empfiehlt die Einrichtung zusätzlicher Schutzmaßnahmen und multilateraler Kontrollen.

Datenspeicherfristen für «ausländische» Daten

Die folgende Tabelle zeigt exemplarische Speicherfristen für erfasste Auslandskommunikation in drei Ländern. Nicht aufgeführt sind die vielen Optionen zur Fristverlängerung, die in den jeweiligen Gesetzen vorgesehen sind.

---

104 CTIVD: «Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD», 2018, 10, https://english.ctivd.nl/documents/review-reports/2018/04/24/index. Siehe auch: van Eijk und Ryngaert. «Expert Opinion – Legal Basis for Multilateral Exchange of Information», Anhang IV des CTIVD-Berichts Nr. 56 zum Prüfbericht über den multilateralen Austausch von Daten zu (vermeintlichen) Dschihadisten durch den AIVD, 2017, https://english.ctivd.nl/documents/review-reports/2018/04/24/appendix-iv.

105 CTIVD, 2018, 9.

Tabelle 5: Datenspeicherfristen

Land	Speicherdauer	Rechtsgrundlage
Deutschland	Verkehrsdaten: 6 Monate Inhaltsdaten: 10 Jahre (außerordentliche Verlängerung möglich)	§ 6 (6) BND-Gesetz § 20 (1–2) BND-Gesetz, § 12 (3) BVerfSch-Gesetz
Frankreich	Verkehrsdaten: 6 Jahre (ab Erfassung) Inhaltsdaten: 12 Monate ab dem Zeitpunkt der ersten Auswertung Nicht ausgewertete Inhaltsdaten können 4 Jahre nach Datum der Erfassung gespeichert werden Verschlüsselte Daten: 8 Jahre	Artikel L. 854-5 des Gesetzes Nr. 2015-1556 zur internationalen Kommunikationsüberwachung
Niederlande	Verkehrs- und Inhaltsdaten nach dem Filtervorgang: 3 Jahre ab der Entschlüsselung Verschlüsselte Daten: 3 Jahre mit unbegrenzten Verlängerungsmöglichkeiten für weitere 3 Jahre	Artikel 48 (5–6) des niederländischen Gesetzes über Nachrichten- und Sicherheitsdienste 2017

Gute gesetzliche Vorgaben

Schutz aller Datenkategorien

Niederlande:

Keine Unterscheidung zwischen Inhalts- und Verkehrsdaten bei der Datenspeicherung

Verkehrsdaten alleine, also beispielsweise Informationen über Anrufe und E-Mails, können genauso viel oder sogar noch mehr über eine Person oder Gruppe aussagen als Inhaltsdaten. Sie sind in keiner Weise weniger sensibel oder schützenswert als Kommunikationsinhalte.[106]

106 Carey: «Stanford Computer Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information», 16. Mai 2016, https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/, and Bradford Franklin, «Carpenter and the End of Bulk Surveillance of Americans,» 25. Juli 2018, https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans.

Auf technischer Ebene ist die Grenze zwischen Inhalts- und Verkehrsdaten ebenfalls verschwommen und schafft rechtliche Unsicherheiten.[107]

Während sich Kommunikationsinhalte relativ einfach von Nutzer/innen verschlüsseln lassen, sind Verkehrsdaten wie Anrufprotokolle und Informationen über Sender/in und Empfänger/in einer Nachricht technisch sehr viel schwieriger zu verschleiern. Aufgrund der großen Menge an Daten die im SIGINT-Bereich anfallen, sind die meisten von den Nachrichtendiensten verarbeiteten Informationen Verkehrsdaten. Infolgedessen greifen viele rechtliche Schutzmechanismen, die sich lediglich auf Inhalte beziehen, zu kurz. Die Abschaffung der Unterscheidung zwischen Inhalts- und Verkehrsdaten im Gesetz scheint daher ein lobenswerter Schritt hin zu einem besseren Schutz der Privatsphäre zu sein.

Verpflichtungen bezüglich gemeinsamer Datenbanken mit ausländischen Nachrichtendiensten

Deutschland:
Verpflichtung zur Bestimmung von Dateianordnungen

Der BND muss für jede gemeinsam mit ausländischen öffentlichen Stellen genutzte Datei, für die er verantwortlich ist, eine separate Dateianordnung treffen (§ 28 BND-Gesetz). Darin müssen die Bezeichnung der Datei, ihr Zweck, die Voraussetzungen der Speicherung, Übermittlung und Nutzung, die Anlieferung und der Zugriff, die Überprüfungsfristen und die Speicherdauer sowie die Rechtsgrundlage für die Datei aufgeführt sein. Außerdem muss die Anordnung explizit diejenigen ausländischen öffentlichen Stellen nennen, die zur Eingabe und zum Abruf befugt sind. Die Dateianordnung bedarf der Zustimmung des Bundeskanzleramtes, und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist vor Erlass einer Dateianordnung anzuhören.

Eine Einschränkung dieser Regelung ist, dass das Kontrollmandat der deutschen Datenschutzbehörde laut Gesetz nur die Erstellung der gemeinsamen Datei und die Datenübertragung vom BND zu einer solchen abdeckt.

Wenn sich der BND an einer von ausländischen öffentlichen Stellen geführten, gemeinsamen Datei beteiligt, muss das Bundeskanzleramt dem ebenfalls zustimmen

107 Bellovin, Blaze, Landau und Pell: «It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law», 2016, https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf.

(§ 30 BND-Gesetz). Außerdem kann der BND nur personenbezogene Daten in gemeinsame Datenbanken eintragen, wenn er derartige Daten auch in seinen eigenen Dateien speichern darf. Das ist relevant, weil die lokale Datenschutzbehörde oder das Kontrollgremium dann prüfen können, inwiefern die Dateneingaben des nationalen Nachrichtendienstes an eine gemeinsame, im Ausland verwaltete Datenbank mit den im Inland gespeicherten Daten übereinstimmen.[108]

Deutschland:
Gebot der Zweckbindung für gemeinsame Dateien

Damit deutsche Dienste sich an gemeinsamen Datenbanken beteiligen können (unabhängig davon, ob eine solche Datenbank im In- oder Ausland gehostet wird), bedarf es einer schriftlichen Absichtserklärung, die den Zweck der Datei festlegt und ein Gebot der Zweckbindung enthält. Letztere verlangt von allen Unterzeichner/innen die Bestätigung, dass die Daten nicht für andere als die in der Absichtserklärung formulierten Zwecke verwendet werden dürfen (§ 26 (4) BND-Gesetz).

USA:
Angleichung der Speicherfristen für SIGINT-Informationen über Personen mit und ohne US-Staatsbürgerschaft

Section 4 (a) der PPD 28 besagt, dass personenbezogene Informationen nur dann gespeichert werden dürfen, wenn die Speicherung vergleichbarer Daten von Staatsangehörigen der USA nach Section 2.3 der Executive Order 12333 zulässig wäre. Die Speicherung muss denselben Speicherfristen unterliegen wie bei vergleichbaren Daten über US-Bürger/innen. Die allgemeine Speicherdauer beträgt fünf Jahre, kann aber vom DNI verlängert werden.

108 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): «Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041)», 21. September 2016, https://www.bundestag.de/blob/459634/a09df397dff6584a83a43a334f3936a3/18-4-660-data.pdf.

Niederlande:
«Oversight 3.0-Projekt» zu künftigen Herausforderungen von Kontrollbehörden

Die CTIVD hat ein mehrjähriges Forschungsprojekt ins Leben gerufen, um die technischen Herausforderungen der Nachrichtendienstkontrolle im digitalen Zeitalter besser verstehen und angehen zu können.[109] Dazu gehören neue Überwachungstechnologien, die wirksame Löschung von irrelevanten oder veralteten Daten und die automatisierte Datenanalyse. Indem die CTIVD aktiv Zeit und Geld in die Erforschung neuer Möglichkeiten zur Überwachung von digitalen Datenerfassungsmethoden investiert und Wissenschaftler/innen und andere unabhängige Experten/innen in den Prozess einbezieht, schafft sie wichtige Grundlagen für die zukünftige Entwicklung der Aufsicht.

Deutschland:
Gemeinsame Kontrollen von G10-Kommission und Bundesdatenschutzbeauftragtem[110]

Je höher die Anzahl der Kontrollgremien ist, desto höher die Gefahr, dass wichtige Informationen bei der Prüfung übergangen oder nicht ausreichend untersucht werden. Vor diesem Hintergrund haben die deutsche Datenschutzbehörde und Mitglieder der G10-Kommission begonnen, gemeinsame Inspektionen durchzuführen.

Je nach nationaler Gesetzgebung übernehmen mehrere Gremien oder Behörden unterschiedliche Kontrollfunktionen. So gibt es in den Niederlanden die TIB-Kommission, die CTIVD und das parlamentarische Aufsichtsgremium. In Deutschland wiederum wird die Fernmeldeaufklärung von der G10-Kommission und dem Unabhängigen Gremium geprüft, gleichzeitig spielen jedoch auch die oder der Bundesbeauftragte für den Datenschutz und das Parlamentarische Kontrollgremium eine Rolle in der demokratischen Kontrolle der Massenüberwachung.

109 CTIVD: «Start project Toezicht 3.0.», 25. April 2017, https://www.ctivd.nl/actueel/nieuws/2017/04/25/index-2.

110 BfDI: «26. Tätigkeitsbericht 2015–2016», 2017, 134, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.pdf?__blob=publicationFile&v=7.

Datenpflege

Dies umfasst sämtliche Vorgänge, die die Kennzeichnung und Registrierung nachrichtendienstlicher Daten und Dateien betreffen. Die Datenpflege ist nicht nur aus datenschutzrechtlicher Sicht geboten, sondern dient auch einem praktischen Zweck: Sie gewährleistet, dass die Dienste nur relevante und korrekte Daten aufbewahren.

Relevante Aspekte

Wie werden massenhaft erfasste Daten gekennzeichnet? Welche Befugnisse hat die Datenschutzbehörde, um die ordnungsgemäße Führung von Dateien zu untersuchen? Um eine solche Prüfung überhaupt zu ermöglichen, müssen sämtliche Informationen über Zugang zu und Verwendung von Daten nachverfolgbar sein. Wichtig ist außerdem, dass die Daten so weit wie möglich anonymisiert werden. Die Sicherheit und Qualität der Dateien müssen gewährleistet werden, um die sensiblen Informationen vor Diebstahl oder Missbrauch zu schützen.

Eine angemessene Datenpflege baut auch auf klaren Beschränkungen des Datenzugriffs auf. Ist der Zugriff auf die gespeicherten Daten gesetzlich geregelt und auf bestimmte Personen beschränkt? Oder wird der Datenzugriff durch eine Anordnung zur Datenauswertung gesteuert und begrenzt (siehe Phase 2)?

Gute gesetzliche Vorgaben

Niederlande:
Sorgfaltspflicht bei der Datenverarbeitung, einschließlich der Verwendung von Algorithmen

Das niederländische Nachrichtendienstgesetz erlegt den Leiter/innen der Sicherheits- und Nachrichtendienste eine allgemeine *Sorgfaltspflicht* auf (Paragraf 24). Diese umfasst angemessene Maßnahmen gegen Datenschutzverletzungen und die Verpflichtung, die Gültigkeit und Richtigkeit der verarbeiteten Daten zu gewährleisten. Die niederländischen Dienste sind außerdem verpflichtet, «geeignete Maßnahmen zu ergreifen, um die Qualität der Datenverarbeitung sicherzustellen, einschließlich der verwendeten Algorithmen und (Verhaltens-) Modelle. Durch die Berücksichtigung von Algorithmen und Modellen verfolgt der Gesetzgeber einen technologieneutralen Ansatz».[111]

111 Eijkman, Eijk und Schaik, 2018, 29, eigene Übersetzung.

Das niederländische Gesetz sieht vor, dass alle Daten so schnell wie möglich auf ihre Relevanz für die vorgesehenen Ziele (wie sie in der ursprünglichen Anordnung festgehalten wurden) geprüft werden (Artikel 48). Daten, die als nicht relevant eingestuft wurden, müssen umgehend vernichtet werden. Nach einem Jahr müssen auch sämtliche noch nicht auf Relevanz geprüfte Daten vernichtet werden.

Zusammengenommen schaffen diese Bestimmungen einen rechtlichen Rahmen, der Qualität und Schutz der Daten gewährleistet. Die CTIVD ist befugt, die zu diesen Zwecken ergriffenen Maßnahmen hinsichtlich ihrer Gestaltung und Anwendung zu kontrollieren.

Deutschland:
Kennzeichnungspflicht aller massenhaft erfassten SIGINT-Daten

Das BND-Gesetz verlangt von den Diensten, alle erfassten Daten zu kennzeichnen (§ 10 (1)). Dies ist eine wichtige Voraussetzung für sinnvolle Datenschutzkontrollen.

Gute Kontrollpraxis

Pflicht zur regelmäßigen Kontrolle der Datenverarbeitung

Frankreich:
Zwingende Vorab-Stellungnahme der Kontrollbehörde zur Ausgestaltung der Datenkennzeichnung

Das Abfangen und Verwerten von Kommunikationsdaten unterliegt Kennzeichnungsmechanismen, die die spätere Datenhandhabung nachverfolgbar machen. Die CNCTR muss hierzu dem Premierminister eine Vorab-Stellungnahme zukommen lassen.[112] In der Vergangenheit beinhaltete diese Stellungnahmen zum Beispiel Empfehlungen zur Erfassung von Verkehrsdaten, Speicherfristen, Speicherbedingungen und zur Erstellung von Log-Dateien.[113] Obwohl die Stellungnahmen nicht bindend sind, kann eine frühe und verpflichtende Einbindung der Kontrollbehörde die Dienste darin bestärken, die Anforderungen der Kontrolle bei der Gestaltung des Kennzeichnungsverfahrens zu berücksichtigen.

112 Siehe: Artikel L. 854-4. des französischen Gesetzes Nr. 2015-1556 zur internationalen Kommunikationsüberwachung.

113 Siehe: CNCTR, 2018, 16.

Die norwegische Aufsichtsbehörde der Nachrichtendienste, EOS, hat einen Vorschlag zur regelmäßigen Prüfung von Datenbanken gemacht: «Aus Sicht des Gremiums sollten Datenbankeinträge regelmäßig von der Person oder den Personen geprüft werden, die für die Eintragung zuständig sind. So soll sichergestellt werden, dass die Datenbank aktuelle, korrekte, erforderliche und relevante Informationen enthält.»[114] Ein Mitglied der G10-Kommission formulierte eine ähnliche Forderung nach obligatorischen Datenschutzprüfungen durch die G10-Kommission mindestens alle zwei Jahre.[115]

Datenaustausch

Relevante Aspekte

Der Austausch von Daten mit ausländischen Nachrichtendiensten bringt die Verantwortung mit sich, das Risiko eines Missbrauchs der geteilten Daten zu bewerten und zu minimieren. Da im SIGINT-Bereich das Prinzip der Aufgabenteilung unter Partnerdiensten gängige Praxis ist, stellt sich die Frage, welche Regeln und Verfahren es gibt, um die Datenqualität der Partnerdienste zu bewerten. Die Aufsicht und die Rechenschaftspflicht im Rahmen von Datenübermittlungen und gemeinsamen Datenbanken muss garantiert sein. Und schließlich gilt es zu untersuchen, wie die Aufsichtsbehörden international zusammenarbeiten (sollten), um die rechtmäßige Nutzung internationaler Datenbestände zu kontrollieren.

Gute gesetzliche Vorgaben

Verschiedene Grundsätze für den Zugang der Kontrollbehörden zu gemeinsamen Daten

Unsere vergleichende Perspektive zeigt, dass Kontrollbehörden unterschiedliche Antworten auf die Frage nach dem Umgang mit dem Prinzip der «Third-Party-Rule» gefunden haben, welche als Grundlage der Kooperation von Nachrichtendiensten gilt. Die Bundesregierung begreift die Third-Party-Rule nicht als absolutes Verbot, Informationen weiterzugeben, sondern vielmehr als ein «Verbot mit Zustimmungsvorbehalt», wobei sich die Informationen beschaffende Stelle das «Informationsbeherrschungsrecht» vorbehält.

114 EOS-Gremium, 2018, 19, eigene Übersetzung.

115 Huber: «Kontrolle der Nachrichtendienste des Bundes – Dargestellt am Beispiel der Tätigkeit der G10-Kommission», 2017, 15, https://beck-online.beck.de/Dokument?vpath=bibdata%5Czeits%5CGSZ%5C2017%5Ccont%5CGSZ.2017.H01.gl2.htm.

Tabelle 6: Zugriff auf geteilte Daten

Aufsichtsbehörde als «Dritte» Allgemeine Praxis, Kontrollbehörden keinen Zugriff auf Daten von Dritten zu gewähren	**Aufsichtsbehörde mit größerem Zugriff auf Daten von Dritten** Allgemeine Erlaubnis unter Vorbehalt der Zugriffsbeschränkung in Ausnahmefällen	**Aufsichtsbehörde mit uneingeschränktem Zugriff auf Daten von Dritten** Uneingeschränkter Zugriff auf Daten von Dritten
Beispielland: Deutschland Daten, die von einem anderen Nachrichtendienst geteilt werden, dürfen standardmäßig nicht an die Kontrollbehörden weitergegeben werden. Die Regierung ist jedoch verpflichtet, sich um die Erlaubnis zur Freigabe durch den Partnerdienst zu bemühen.[116]	**Beispielland: Norwegen** Grundsätzlich hat die Aufsichtsbehörde Zugang zu allen Daten, die der norwegische Nachrichtendienst besitzt – auch von Dritten. Ausnahmen gelten nur für «besonders sensible Informationen».[117]	**Beispielländer: Dänemark und die Niederlande** Die Aufsichtsbehörden in diesen Ländern werden nicht durch Drittpartei-Regelungen behindert und können alle Daten einsehen, die der nationale Nachrichtendienst besitzt.

Norwegen: Standardmäßig größerer Zugriff auf Informationen Dritter durch das Kontrollgremium

Laut Gesetz hat das EOS-Gremium Zugang zu allen Informationen innerhalb des Nachrichtendienstes, die das Gremium für seine Kontrolltätigkeit für relevant hält. Nur in Ausnahmefällen hat die Leitung des Nachrichtendienstes das Recht und die Pflicht, von der Übermittlung «besonders sensibler Informationen» abzusehen und sich stattdessen an das Verteidigungsministerium zu wenden, damit weiter geprüft wird, ob die Einsicht gewährt werden soll.[118]

Folgende Ausnahmen können als besonders sensible Informationen gelten:

- die Identität der Informant/innen und V-Personen des norwegischen Nachrichtendienstes und seiner ausländischen Partner;
- die Identität besonders schützenswerter Bediensteter ausländischer Partner;

116 Wissenschaftlicher Dienst des Bundestags: «Kontrolle von Nachrichtendiensten bei Zusammenarbeit mit anderen Nachrichtendiensten im Ausland», März 2017, 6, https://www.bundestag.de/blob/508038/5a79b26ee2205e08171ee396ef87ae45/wd-3-072-17-pdf-data.pdf.

117 EOS-Gremium: «Dokument 16 (2015–2016). Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)», 29. Februar 2016, 71 (Punkt 19.5, eigene Übersetzung), https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf, eigene Übersetzung.

118 Ebd.

- Personen mit Aufgaben im Bereich der Bereitschaft im Falle einer Besatzung;
- besonders sensible nachrichtendienstliche Operationen ausländischer Partner im Ausland, die, wenn sie kompromittiert würden,
  - das Verhältnis zu einer ausländischen Macht aufgrund des mit der Operation verbundenen politischen Risikos ernsthaft beeinträchtigen oder
  - zu schweren Verletzungen oder zum Tod von Beschäftigten oder Dritten führen könnten.[119]

Dieses Vorgehen schränkt die Einsicht des EOS-Gremiums in Informationen über norwegische und ausländische Quellen nicht per se ein. In der Regel hat das EOS-Gremium Zugang zu den Auslandsaktivitäten der norwegischen Nachrichtendienste und ihrer Kooperationspartner.

Verglichen mit anderen Ländern wie Deutschland, das eine eher strenge Auslegung der «Third-Party-Rule» gegenüber seinen Aufsichtsbehörden anwendet, bietet das norwegische Modell den Aufsichtsbehörden größere Kontrollmöglichkeiten. Wie die Tabelle oben zeigt, gibt es aber auch Länder wie die Niederlande und Dänemark, die ihren Aufsichtsbehörden einen gänzlich uneingeschränkten Zugang zu Informationen von Dritten gewähren.[120]

Gute Kontrollpraxis

Deutschland: Stichprobenartige Kontrollen bei der automatischen Übermittlung von personenbezogenen Daten an ausländische Nachrichtendienste[121]

Hinsichtlich der automatischen Übermittlung personenbezogener Daten an ausländische Nachrichtendienste ist das Unabhängige Gremium befugt, stichprobenartig zu überprüfen, ob keine Daten, die gegen das Verbot der Wirtschaftsspionage verstoßen (§ 6 (5) BND-Gesetz), und keine anderen Daten, die dem nationalen Interesse Deutschlands zuwiderlaufen könnten, weitergegeben werden (§ 15 (3) BND-Gesetz). Darüber hinaus kann das Gremium auch stichprobenartig die Suchbegriffe kontrollieren, die zur Überwachung von EU-Mitgliedstaaten oder EU-Institutionen verwendet werden (§ 9 (5) BND-Gesetz). Da es technisch schwierig ist, sicherzustellen, dass keine inländischen Daten weitergegeben werden (siehe Phase 1), wird ein ausgeweitetes Kontrollmandat für die Kontrollgremien zur Überprüfung solcher Datenübertragungen noch wichtiger.

119 EOS-Gremium, 2018, 54, eigene Übersetzung.

120 Informationen aus dem Workshop des Europäischen Netzwerks Nachrichtendienstkontrolle (EION) am 14. Mai 2018.

121 § 15 (3) BND-Gesetz.

Datenlöschung

Daten ordnungsgemäß zu löschen, ist eine enorme Herausforderung und technisch nicht so einfach, wie man denken könnte. Denn beim «Löschen» einer Datei wird in der Regel nur der von dieser Datei eingenommene Speicherplatz als wieder nutzbar markiert. Daten sind so lange wiederherstellbar, bis ein Speicher überschrieben wird. Um sicherzustellen, dass gelöschte Daten nicht mehr wiederhergestellt werden können, muss der physische Speicherplatz auf einem Speichermedium mehrmals mit anderen Daten überschrieben werden (gemäß den Richtlinien der US-Bundesregierung mindestens sieben Mal).[122] Doch durch einfaches Überschreiben des Speicherplatzes durch neue Daten kann nicht garantiert werden, dass alle alten Daten endgültig entfernt wurden. Obwohl es technische Mittel gibt, um sicherzustellen, dass gelöschte Daten auch wirklich nicht wiederhergestellt werden können,[123] scheint es notwendig, detailliertere Standards für die Löschung von Daten zu entwickeln. Fehler in diesem Prozess könnten dazu führen, dass Millionen von Datensätzen jahrelang fälschlicherweise gespeichert bleiben.

Darüber hinaus ist es mittlerweile «teurer, Daten zu löschen, als sie zu speichern».[124] Daher haben sich Gesetzgeber schwer getan, rechtliche Definitionen oder öffentliche Standards für die «Löschung» oder «Vernichtung» von Daten in das Nachrichtendienstrecht aufzunehmen.[125] Infolgedessen wird die Datenlöschung dann auch zu einer echten Herausforderung für die Aufsicht. Der Grund: Aufsichtsbehörden benötigen genaue Protokolldateien, um die Einhaltung der Regeln zur Datenlöschung durch die Nachrichtendienste kontrollieren zu können. Das umfasst auch die automatisierte Datenvernichtung nach Ablauf der gesetzlichen Speicherfristen.

Zudem braucht es bessere Richtlinien bezüglich der Frage, welche Daten zu welchem Zeitpunkt gelöscht werden sollten. Speicherfristen (siehe Teil 1 von Phase 5) legen fest, wie lange Daten maximal aufbewahrt werden dürfen. Mit passenden, normativen Kriterien könnten die Dienste oder die zuständigen Kontrollgremien theoretisch auch verkürzte Speicherfristen bestimmen. Wenn beispielsweise das Datenbanksystem bestimmte Daten kennzeichnet, die für einen gewissen Zeitraum nicht verwendet wurden, sollte überprüft werden müssen, ob dieser bestimmte Datensatz noch benötigt wird.

---

122 Dorion: «Data Deletion or Data Destruction?», Juli 2008, https://searchdatabackup.techtarget.com/tip/Data-deletion-or-data-destruction.

123 Informationen zu einem auf Verschlüsselung basierenden Ansatz finden Sie hier: Reardon, Ritzdorf, Basin und Capkun: «Secure Data Deletion from Persistent Media», 2013, https://doi.org/10.1145/2508859.2516699.

124 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD): «The OECD Privacy Framework», 2013, 100, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, eigene Übersetzung.

125 Wir danken Professor Nico van Eijk, der bei unserem Workshop am 14. Mai 2018 wichtige Informationen zu den rechtlichen und technischen Herausforderungen der Datenlöschung präsentierte.

Relevante Aspekte

Das Nachrichtendienstrecht sollte möglichst spezifische und kurze Speicherfristen festlegen, nach deren Ablauf die Daten dauerhaft und unmissverständlich vernichtet werden müssen. Für die Löschung großer Datenmengen kann es besondere Anforderungen geben. So soll beispielsweise das XKeyscore-System der NSA über einen großen Zwischenspeicher verfügen, in dem alte Daten automatisch und kontinuierlich durch neue überschrieben werden.

Weiterhin ist relevant, wie die Datenvernichtung dokumentiert und von der zuständigen Gremien kontrolliert wird. Sind die gespeicherten Daten beispielsweise mit bestimmten genehmigten Anordnungen verknüpft und haben sie rückverfolgbare Zeitstempel für eine vollständige und ordnungsgemäße Löschung? Auch für mögliche Benachrichtigungen von Betroffenen sind angemessene Aufzeichnungen über die Datenvernichtung wichtig.

Wie wird das Speichern und Löschen in der Praxis umgesetzt? Sollten von Nachrichtendiensten abgefangene Daten in «Clouds» gespeichert werden? Selbst im Bereich der nationalen Sicherheit erleben wir eine enge Zusammenarbeit staatlicher Stellen mit kommerziellen Drittanbietern, wie z. B. private Anbieter von Cloud-Speicherlösungen.[126] Wie kann sichergestellt werden, dass eine solche Auslagerung die demokratische Rechenschaftspflicht und Kontrolle nicht beeinträchtigt – ist sie doch mit der Gefahr verbunden, die Verantwortung für eine entscheidende Phase der Datenverarbeitung an private Unternehmen zu übertragen?

Gute gesetzliche Vorgaben

Deutschland:
Verpflichtung zur sofortigen Löschung von unrechtmäßig erhobenen Daten

Wird eine bereits bestehende Anordnung nachträglich aufgehoben, so sieht das BND-Gesetz (§ 10 (2)) vor, dass alle in diesem Zusammenhang erhobenen Daten sofort gelöscht werden. Stellt sich nachträglich heraus, dass eine SIGINT-Maßnahme Suchbegriffe beinhaltet, die sich unrechtmäßig gegen EU-Organe oder Institutionen der EU-Mitgliedstaaten richtet, muss das Unabhängige Gremium informiert werden, und die in diesem Rahmen gewonnenen Daten sind unverzüglich zu löschen (§ 10 (3) BND-Gesetz).

126 Konkel: «The Details About the CIA's Deal With Amazon», 17. Juli 2014, https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

Niederlande:
Verpflichtung zur Vernichtung von Daten aus der Massenerfassung, die als irrelevant erachtet werden

Das niederländische Nachrichtendienstrecht verlangt, dass massenhaft erfasste Daten vernichtet werden müssen, sobald festgestellt wurde, dass sie für eine nachrichtendienstliche Untersuchung irrelevant sind.

Frankreich:
Verpflichtung zur Protokollierung von Datenlöschung

Abschnitt 854-6 des französischen Gesetzes zur Überwachung internationaler Kommunikation verlangt, dass «die Vernichtung von erfassten Daten, Abschriften und Auszügen von einzeln benannten und autorisierten Mitarbeiter/innen durchgeführt und protokolliert werden muss.»[127]

Kanada:
Verpflichtung zur Löschung von Gesundheitsdaten in ausländischen Datensätzen

Abschnitt 11.1 (1 a) von Bill C-59 besagt, dass die Dienste verpflichtet sind, in kanadischen oder ausländischen Datensätzen alle Informationen zu löschen, die vertrauliche Informationen über die körperliche oder geistige Gesundheit einer Person enthalten.

Gute Kontrollpraxis

Schweden:
Statistische Musteranalysen von Datenlöschungen

Die schwedischen Aufsichtsbehörde SIUN (Statens inspektion för försvarsunderrättelseverksamheten) muss kontrollieren, wie die Regeln der Löschungspflicht

127 Artikel L. 854-6 des französischen Gesetzes Nr. 2015-1556 zur internationalen Kommunikationsüberwachung, eigene Übersetzung.

von den Diensten angewendet werden. «Ein Ausgangspunkt für die Überprüfung ist die statistische Kontrolle der Menge des zerstörten Materials, um auf Abweichungen aufmerksam zu werden.»[128]

Es ist nicht möglich, sämtliche gelöschten Daten zu überprüfen. Deshalb scheint die Orientierung an statistischen Abweichungen als Auslöser für tiefergehende Kontrollen ein wirksames Mittel zu sein, um die knappen Ressourcen der Kontrolleur/innen effizient einzusetzen. Eine solche Abweichung könnte zum Beispiel ein ungewöhnlicher Ausreißer bei den Löschaktivitäten an einem bestimmten Tag sein. Um Muster in der Datenvernichtung sichtbar zu machen, müssen die Prüfprotokolle der Datenlöschung über lange Zeiträume verfügbar bleiben.

Norwegen:
Unabhängige Prüfung der Einhaltung der Löschpflichten

Das EOS-Gremium ist in seinem Jahresbericht von 2018 auf die Problematik der Datenlöschung eingegangen und hat gefordert, dass der Nachrichtendienst «in Kürze eine Lösung finden muss, um die Verarbeitung von Informationen zu verhindern, für die keine rechtliche Grundlage mehr existiert».[129]

Zusammenfassung der Ergebnisse und Reformagenda

Die massenhafte Datenverarbeitung birgt eine Reihe komplexer Herausforderungen für die Nachrichtendienstkontrolle, die die Aufsichtsbehörden noch viele Jahre lang beschäftigen werden. Um es vorsichtig auszudrücken: Im Aufsichtsbereich besteht viel Innovationspotenzial. Dieses Kapitel hat einige lobenswerte Praktiken vorgestellt, die diesbezüglich in jüngerer Vergangenheit initiiert wurden. Natürlich gibt es in vielen Ländern noch Lücken, insbesondere wenn es um Regeln und Verfahren für die Datenvernichtung und die Datenspeicherung ausländischer Daten geht.

Bei der Ausarbeitung von Nachrichtendienstgesetzen ist der Gesetzgeber möglicherweise nicht ausreichend auf die Bedeutung und Intensität der multilateralen Zusammenarbeit im Bereich der Nachrichtendienste eingegangen. Nachrichtendienste tauschen mit ihren ausländischen Partnern enorme Mengen von Primär- und Sekundärdaten aus und führen gemeinsam eine Reihe von Datenbanken. Die rechtlichen Rahmenwerke sollten die gemeinsame Verantwortung der Regierungen für

128 Schwedische Staatsinspektion für Verteidigungsnachrichtendienste (SIUN): «Årsredovisning för 2017», 22. Februar 2018, Abschnitt 4.1, http://www.siun.se/dokument/Arsredovisning_2017.pdf, eigene Übersetzung

129 EOS-Gremium, 2018, 20, eigene Übersetzung.

gemeinsame Datenbanken berücksichtigen, selbst wenn diese Datenbanken nicht auf ihrem Hoheitsgebiet gehostet werden. Außerdem ist es – wie die niederländische Regierung klargemacht hat – dringend erforderlich, eine wirksame Aufsicht über gemeinsame Datenbanken sicherzustellen, möglicherweise in Form einer multilateralen Aufsicht.

Viele Aufsichtsorgane scheinen der Ansicht zu sein, dass noch viel getan werden muss, um unabhängig zu prüfen, ob die Nachrichtendienste ihren Pflichten bezüglich der Datenlöschung nachkommen. Die Ausarbeitung von Standards, wie eine ordnungsgemäße Datenlöschung aussehen könnte, wäre ein erster wichtiger Schritt in diese Richtung. Genauso interessant fanden wir die unterschiedlichen Standards, die verschiedenen Staaten im Hinblick auf die «Third-Party-Rule» anwenden. Hier sind weitere Untersuchungen notwendig. Was wir bisher festgestellt haben, scheint darauf hinzudeuten, dass Aufsichtsbehörden erfolgreich von der «Third-Party-Rule» ausgenommen werden können, ohne dass sich dies negativ auf die Sicherheit oder hemmend auf den Datenaustausch zwischen Nachrichtendiensten auswirkt.

Phase 6: Analyse

In dieser Phase sind viele verschiedene Formen der Datennutzung relevant. Natürlich gibt es Überschneidungen zwischen der Datenverarbeitung und der Datenanalyse. Während sich die Datenverarbeitung auf die Dateneingabe und -pflege sowie andere formale oder technische Aspekte des Datenmanagements bezieht, werden Daten in dieser Phase zu Informationen, die für die politische Entscheidungsfindung relevant sind. Unterschiedliche (automatisierte) Datenanalysemethoden dienen unterschiedlichen Zwecken und unterliegen jeweils eigenen Regeln. Sehr große Datensätze werden sowohl verwendet, um Verbindungen zwischen bekannten Zielgruppen zu erkennen, als auch um «nach Spuren von Aktivitäten von Einzelpersonen zu suchen, die möglicherweise noch nicht bekannt sind, aber im Laufe einer Untersuchung auftauchen, oder um Aktivitätsmuster zu identifizieren, die auf eine Bedrohung hinweisen könnten.»[130] Das sogenannte Contact Chaining etwa ist eine häufig genutzte Methode zur Zielerfassung: Mithilfe eines (möglicherweise durch HUMINT – also durch menschliche Quellen erlangten) Ausgangs-Selektors («seed selector») beginnt der/die Auswerter/in den mühsamen Prozess, Informationen über eine Terrorzelle oder ein Terrornetzwerk zusammenzutragen, indem er/sie die Personen untersucht, mit denen die Ausgangsperson kommuniziert, und die Personen, mit denen diese wiederum kommunizieren (die nächsten zwei Kommunikationsebenen).[131]

Die Verfahren der automatisierten Musteranalyse und die Erkennung von Anomalien setzen zunehmend Methoden der sogenannten künstlichen Intelligenz (KI)

130 UK Home Office: «Interception of Communications. Draft Code of Practice», Dezember 2017, 52, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668941/Draft_code_-_Interception_of_Communications.pdf, eigene Übersetzung.

131 Government Communications Headquarters (GCHQ): «HIMR Data Mining Research Problem Book», 20. September 2011, 12, https://www.documentcloud.org/documents/2702948-Problem-Book-Redacted.html.

wie maschinelles Lernen und vorhersagende Analysen ein. «Aufgrund der großen Datenmengen, über die Nachrichtendienste verfügen, werden die Methoden der KI in diesem Anwendungsbereich vermutlich einen sehr hohen Nutzen haben.»[132] Die Risiken und Nutzen, die allgemein mit KI verbunden sind, stellen auch die bisherigen Kontrollmethoden in Frage und drängen Gesetzgeber und Aufsichtsbehörden dazu, sich kreativ mit künstlicher Intelligenz als Dual-Use-Technologie auseinanderzusetzen. Im Nachrichtendienstsektor soll KI die Arbeit von menschlichen Analysten/innen automatisieren, die zurzeit Stunden damit verbringen, Daten auf nutzbare Informationen zu sichten. Die künstliche Intelligenz könnte sie entlasten, damit sie effizienter und zeitnaher Entscheidungen auf Grundlage von Daten treffen können.[133] Andererseits schafft der Missbrauch von KI neue Sicherheitsbedrohungen, die abgewehrt werden müssen.[134]

Relevante Aspekte

Welche Arten der Datennutzung sind in einem spezifischen Rechtsrahmen zulässig? Und gibt es bestimmte Regeln für die unterschiedlichen Formen der Datennutzung, zum Beispiel Verfahren für jede Nutzungsart, die die genauen Umstände definieren, unter denen die jeweilige Nutzung zulässig ist?

Außerdem sollte es eine unabhängige Kontrolle (intern und extern) von Analysetechniken für Massendaten geben, einschließlich Regeln und Schutzmaßnahmen zum Einsatz von KI. Wie wird gemessen, ob und wie stark spezifische Werkzeuge der Datenanalyse den Datenschutz verletzen? Und welche Art von Material wird in durchsuchbare Datenbanken eingepflegt?

Wie wird die Konvergenz unterschiedlicher Datenbanken/Datenquellen reguliert? Dürfen Massenkommunikationsdaten mit anderen vorhandenen Daten (z.B. Daten, die über Sensoren oder Hacking-Operationen erlangt wurden) sowie öffentlich verfügbaren Daten abgeglichen werden? Falls ja, geschieht eine solche Datenanreicherung automatisch?

---

132 Hoadley und Lucas, 2018, 13, eigene Übersetzung.

133 Die Central Intelligence Agency (CIA) entwickelt zurzeit 137 Projekte, die KI auf unterschiedliche Weise einsetzen, z. B. die Integration von Bilderkennung und maschinellem Lernen in nachrichtendienstlichen Systemen, die Material durchkämmen und automatisch feindliche Aktivitäten für die Zielerfassung identifizieren; Bilderkennung oder -kennzeichnung zur Vorhersage von Ereignissen wie Terroranschläge oder Unruhen, basierend auf einer umfassenden Analyse von Open-Source-Informationen; Entwicklung von Algorithmen zur mehrsprachigen Spracherkennung und -übersetzung in lauten Umgebungen; Geolokalisierung von Bildern ohne zugehörige Metadaten; Verschmelzen von 2D-Bildern zu 3D-Modellen; und Werkzeuge zur Funktionsermittlung von Gebäuden auf der Grundlage von Analysen von alltäglichen Verhaltensmustern. Siehe Hoadley und Lucas, 2018, 9.

134 Brundage et al.: «The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Migration», Februar 2018, https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.

Niederlande:
Human-in-the-Loop (HITL)-Schutzmaßnahme bei der automatisierten Datenanalyse

Die Nachrichtendienste dürfen allein aufgrund der Ergebnisse automatisierter Datenanalysen keine Maßnahmen gegen eine Person fordern oder ergreifen. Wenn Datenanalyse-Algorithmen etwa darauf hinweisen, dass eine bestimmte Person einen Terrorangriff plant, darf ein Nachrichtendienst nicht alleine auf der Grundlage der Ergebnisse dieses Algorithmus handeln.[135]

Zwar können Analysefehler durch die Einbeziehung eines Menschen nicht unbedingt verhindert werden,[136] doch die Verpflichtung, vor dem Handeln andere Beweisformen vorzulegen, kann dazu beitragen, Fehler und falsche Schlussfolgerungen zu verhindern. Das niederländische Gesetz stellt außerdem klar, was unter den Begriff «automatisierte Datenanalyse» fällt. Dazu gehören der automatisierte Vergleich von Datensätzen miteinander sowie die Suche auf der Basis von Profilen, um bestimmte Muster zu finden.[137]

Niederlande:
Verpflichtende Schulungen für Analyst/innen

Das niederländische Gesetz schreibt eine Trennung des Datenzugangs vor und verlangt, dass nur Fachpersonal auf durch Anordnungen abgedeckte Datensätze zugreifen und diese analysieren darf.[138]

Auch im Vereinigten Königreich müssen entsprechende Vorkehrungen getroffen werden, die die Anzahl der Personen, denen bestimmte Materialien offengelegt werden

135 Eijkman, Eijk und Schaik, 2018, 19.

136 Cranor: «A Framework for Reasoning About the Human in the Loop», 2008, http://dl.acm.org/citation.cfm?id=1387649.1387650.

137 Niederländisches Gesetz über Nachrichten- und Sicherheitsdienste 2017, Artikel 60 (2).

138 Erläuterndes Memorandum zur Änderung des Gesetzes über Nachrichten- und Sicherheitsdienste (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Memorie van Toelichting inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten) 2016, 48f., https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten.

dürfen, begrenzen und das Vervielfältigen bestimmter Datensätze auf das erforderliche Minimum beschränken.[139]

Gute Kontrollpraxis

Vereinigtes Königreich: Automatische interne Kontrollsysteme für die Datenanalyse

«Es gibt computergestützte Systeme für das Prüfen und Suchen nach einer möglicherweise unzulässigen Nutzung der Systeme und Geräte des Government Communications Headquarters (GCHQ). Wählt beispielsweise eine autorisierte Person einen bestimmten Verkehr zur Untersuchung aus, muss die Person nachweisen, dass die Auswahl notwendig und verhältnismäßig ist. Dieses Verfahren unterliegt der internen Prüfung.»[140]

Frankreich: Vorab-Prüfung von KI-Experimenten und Datenanalysetechniken

Der französische Premierminister genehmigt automatisierte Datenanalysen auf Grundlage bestimmter Parameter, nachdem die CNCTR eine «nicht bindende Stellungnahme zu der automatischen Verarbeitung sowie den Parametern eingereicht hat. Die Aufsichtsbehörde wird über jede Änderung während der laufenden Operation informiert und hat permanenten, umfassenden und direkten Einblick in diese Auswertung und die gesammelten Erkenntnisse».[141]

Wenn der Nachrichtendienst die automatisierte Analyse erneut genehmigen lassen möchte, sollte der Verlängerungsantrag an den Premierminister eine Bewertung der Relevanz früherer automatisierter Analysen und die Anzahl der gewonnen Ziele bzw. Zielpersonen enthalten. Als der französische Nachrichtendienst 2016 plante, «Algorithmen» einzusetzen, um terroristische Bedrohungen auf Grundlage von «Verbindungsdaten» zu ermitteln, reichte die CNCTR zwei Stellungnahmen beim

139 Abschnitt 150 (1(a)) und (2), United Kingdom, IP Act 2016.

140 Agentur der Europäischen Union für Grundrechte, 2017, 59; siehe auch: UK Home Office: «Interception of Communications. Draft Code of Practice», Februar 2017, 6.14, eigene Übersetzung.

141 Agentur der Europäischen Union für Grundrechte, 2017, 97, eigene Übersetzung.

Premierminister ein – sowohl zur Gestaltung der Algorithmen als auch zur Bedeutung der Verbindungsdaten.[142]

Zusammenfassung der Ergebnisse und Reformagenda

Die Aufsicht der Nachrichtendienste kämpft bereits seit geraumer Zeit für eine wirksame Kontrolle des bislang als «Black Box» geltenden Bereichs der Datenanalyse. Die zunehmende Bedeutung von KI ist die in dieser Hinsicht jüngste Entwicklung – mit möglicherweise weitreichenden Konsequenzen für die Durchführung von Datenanalysen. Selbst wenn sich KI in der Überwachung lediglich in einem experimentellen Stadium befindet, kann das Risiko von Missbrauch und Fehlern bereits reale Auswirkungen haben. Wie kann sichergestellt werden, dass es eine Rechenschaftspflicht für die Fehler solcher Algorithmen gibt?

Die Kontrolle muss dafür sorgen, dass sie mit diesen Entwicklungen Schritt hält. Vielversprechende Praktiken wie das niederländische «Oversight 3.0»-Projekt oder die Einführung von Anordnungen für Eignungsprüfungen in Neuseeland sind auf diesem Gebiet hervorhebenswert. Kontrollgremien benötigen jedoch definitiv zusätzliche Ressourcen und Kontrollinstrumente, um die Rechenschaftspflicht von KI-gestützten Überwachungsaktivitäten zu gewährleisten.

Phase 7: Überprüfung und Evaluation

Die Einhaltung rechtlicher Schutzmaßnahmen muss durch eine umfassende und regelmäßige gerichtliche Kontrolle sichergestellt werden. Ebenso wichtig ist es, die Wirksamkeit von Überwachungsmaßnahmen zu untersuchen. Aufsichtspersonal muss sich dessen bewusst sein, um den politischen Wert, die Kosteneffizienz und die Notwendigkeit einer Verlängerung von Anordnungen bewerten zu können. Die Identifizierung geeigneter Kriterien und Methoden dafür bleibt eine große Herausforderung. Wenn beispielsweise Daten aus einer bestimmten Quelle oder Erfassungsmaßnahme nie in nachrichtendienstliche Berichte einfließen, bedeutet dies dann, dass die jeweilige Datenerhebung überflüssig ist und eine unnötige Belastung für die begrenzten Ressourcen der Nachrichtendienste darstellt? Oder wäre das im Gegenteil vergleichbar mit einem Szenario, in dem eine Feuerversicherung gekündigt wird, nur weil das Haus bisher nie gebrannt hat?

Relevante Aspekte

Der Umfang des Kontrollmandats der Aufsichtsbehörden ist ein wesentlicher Faktor. Eine effektive Prüfung setzt voraus, dass es im Kontrollmandat keine Lücken gibt. Die

142 Ebd., 45; CNCTR: «Premier rapport d'activité 2015/2016», 2016, 39f., https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf.

Kontrollaufgaben sollten funktional definiert werden und – wie vom Europarat empfohlen – alle Aspekte der Datenerfassung abdecken.[143]

Hat die zuständige Kontrollbehörde genügend Ressourcen (Personal, Zeit, Geld, technische Expertise), um aussagekräftige Prüfungen durchzuführen? Auch sollte das Nachrichtendienstgesetz festlegen, welche Rolle der Aufsicht bei der Beurteilung der politischen Relevanz abgeschlossener Nachrichtendienstoperationen zukommt. Und es sollte der Exekutive die Aufgabe übertragen, die Notwendigkeit und Effizienz massenhafter Datenerfassung nachzuweisen, gerade angesichts wachsender Verfügbarkeit von Open-Source-Informationen.

Gute gesetzliche Vorgaben

Ausweitung des Kontrollmandats

Kanada:
Ganzheitliche und behördenübergreifende Prüfung von SIGINT-Aktivitäten[144]

Nachrichtendienste führen ihre Untersuchungen oft in enger Zusammenarbeit mit anderen Sicherheitsbehörden durch (etwa mit Polizei, Militär, Zoll- und Grenzschutzbehörden). Wenn ein Kontrollgremium nur die Aktivitäten eines bestimmten Nachrichtendienstes überprüft, ist diese Prüfung unvollständig, ignoriert sie doch den Beitrag kooperierender Behörden.[145]

Vor diesem Hintergrund wäre die National Security and Intelligence Review Agency (NSIRA) – die in Bill C-59 vorgesehene neue Kontrollbehörde – ein integriertes Kontrollgremium mit Zuständigkeit für Tätigkeiten des Canadian Security Intelligence Service (CSIS), des CSE sowie für alle nationale Sicherheits- oder Nachrichtendienste anderer Ministerien, soweit diese sich auf die nationale Sicherheit oder nachrichtendienstliche Tätigkeiten beziehen.

Die neue britische Kontrollbehörde IPCO hat die Aufgabe, den Einsatz von Ermittlungsbefugnissen, nicht nur durch Nachrichtendienste, sondern auch durch Strafverfolgungsbehörden, Gefängnisse, lokale Behörden und andere Regierungsbehörden, zu kontrollieren. Eine solche Bündelung der Prüfkompetenzen in einer zentralen Kontrollinstitution ist sinnvoll, da die Polizei beispielsweise zunehmend elektronische Werkzeuge für Ermittlungszwecke einsetzt, die für ein genehmigendes Gremium

143 Europarat: «Democratic and Effective Oversight of National Security Services», Mai 2015, 11, https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb.

144 National Security and Intelligence Review Agency Act (NSIRA Act, in Planung als Teil von Bill C-59), Abschnitt 8.

145 Parsons et al., 2017, 35.

(z.B. auch ein Gericht) weniger nachvollziehbar und kontrollierbar sind als klassische Instrumente der Strafverfolgung. Die zunehmende Intransparenz erfordert zusätzliches technisches Fachwissen, um digitale Überwachungsmaßnahmen zu überprüfen.

In den USA ist das Privacy and Civil Liberties Oversight Board (PCLOB) für alle Aktivitäten der Terrorismusbekämpfung zuständig, die von einer Bundesbehörde betrieben werden – auch für solche außerhalb der Nachrichtendienste (z. B. beim Heimatschutz-Ministerium). Wenn auch auf den Bereich der Terrorismusabwehr beschränkt, erstreckt sich der Zuständigkeitsbereich der Kontrolle damit über ein breiteres Spektrum von Sicherheitsbehörden.

Regelmäßige Verlängerung

Sogenannte «Sunset»-Vorbehalte («sunset clauses»), wie sie beispielsweise im US-Recht üblich sind, sind ein wirksames Instrument, um die regelmäßige Evaluierungen und Anpassungen von Nachrichtendienstgesetzen anzustoßen. Der Zeitraum für ein solches gesetzlich festgelegtes Ablaufdatum kann variieren.

Niederlande:
Wirksamkeitsprüfung vor der Verlängerung einer Anordnung

Die Pflicht, bei der Beantragung einer Genehmigungsverlängerung für eine bestimmte Überwachungsmaßnahme die erforderlichen Informationen schriftlich vorzulegen, ist die Grundlage für jegliche Wirksamkeitsprüfung. Die genaue Kennzeichnung von Informationen ist unter anderem wichtig, um den ursprünglich abgefangenen Datenstrom nachverfolgen zu können, der einem bestimmten nachrichtendienstlichen (End-)Bericht zugrunde liegt. Damit kann dann bewertet werden, ob die Erfassung jenes Datenstroms notwendig und nützlich war.

Das niederländische MIVD unterhält ein kleines Büro, das als «advocatus diaboli» fungiert und einen konträren Blick auf (ausgewählte) Nachrichtendienstberichte und interne Verfahren liefert.

Norwegen:
Strafrechtliche Verantwortlichkeit bei Missachtung von Anfragen von Kontrollgremien

Jede/r amtierende oder ehemalige Beschäftigte eines norwegischen Nachrichtendienstes ist verpflichtet, Anfragen zu beantworten und allen Aufforderungen der Kontrollbehörde nachzukommen (z. B. Zeugenaussagen vor dem Gremium

tätigen) – und zwar unabhängig vom Geheimhaltungsgrad. «Vorsätzliche oder grob fahrlässige Verstöße» gegen diese Pflicht führen dazu, dass «eine Geldstrafe oder eine Freiheitsstrafe von höchstens einem Jahr verhängt wird, sofern nicht strengere strafrechtliche Bestimmungen gelten».[146]

Gute Kontrollpraxis

Frühe und systematische Einbindung der Kontrolle

USA:
Kein Anspruch auf das «deliberative privilege» gegenüber dem PCLOB

Das Privacy and Civil Liberties Oversight Board ist eine unabhängige Behörde innerhalb der Exekutive.[147] Da es in die Exekutive eingebunden ist, hat das PCLOB vollständigen Zugriff auf Informationen, insbesondere auf Materialien in der Beratungsphase. Die Regierung kann sich daher gegenüber dem PCLOB nicht auf ihr «deliberative privilege» berufen. Dabei handelt es sich um das Prinzip, wonach die internen Prozesse der Exekutive von Offenlegungsanforderungen ausgenommen werden können, etwa in Zivilprozessen oder bei Anträgen nach dem Informationsfreiheitsgesetz. Außerdem erhalten PCLOB-Mitglieder die höchste Sicherheitsüberprüfung. Der ungehinderte Zugang zu Informationen ist eine wichtige Voraussetzung, um die von der Regierung vorgebrachten Argumente kritisch hinterfragen zu können.

Der offizielle Bericht zu Überwachungsmaßnahmen nach «Section 215»[148] ist ein Beispiel für die Fähigkeit des PCLOB, die Argumentation der Regierung und den Anspruch auf die Wirksamkeit bestimmter Maßnahmen erfolgreich in Frage zu stellen und zu widerlegen.

---

146 Norwegisches EOS-Kontrollgesetz, Abschnitt 21, https://lovdata.no/dokument/NL/lov/1995-02-03-7; englische Übersetzung: EOS-Gremium, 2018, 60, https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf, eigene Übersetzung.

147 Obwohl das PCLOB nicht finanziell unabhängig ist, d. h. es kann nicht öffentlich mehr Mittel für seine Aktivitäten fordern, ergibt sich die Unabhängigkeit des Mandats aus der Möglichkeit, dem Weißen Haus und seinen Abteilungen zu widersprechen und eine abweichende Haltung einzunehmen.

148 PCLOB: «Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court», 23. Januar 2014, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

Neuseeland:
Verpflichtende vierteljährliche Vorfallsmeldung beim Generalinspekteur (Inspector General)

Seit 2016 müssen alle operativen Compliance-Verstöße registriert und an den Inspector General der Nachrichtendienste gemeldet werden. Davor galt dies lediglich für irrtümliche Datenerfassungen. Zu diesen Vorfällen gehören u. a.:

- Erfassen von falschen Nummern, Leitungen, Datensätzen oder Geräten (z. B. durch die versehentliche Verwendung einer falschen Telefonnummer);
- Anschlüsse, die erfolgreich erfasst wurden, aber anschließend von der Zielperson aufgegeben und/oder von einer Nicht-Zielperson übernommen wurden;
- sowie Fälle, von Organisationen, die den NZSIS [New Zealand Security Intelligence Service] unterstützen und denen nicht die richtigen oder aktuellen Dokumente zu einer bestimmten Anordnung vorlagen; und die Nichteinhaltung interner Richtlinien oder Verfahren.[149]

Internationale Zusammenarbeit von Kontrollbehörden

Europa:
Gemeinsame Prüfungen und Austauschtreffen

Seit einigen Jahren arbeiten die Nachrichtendienst-Kontrollbehörden von Belgien, den Niederlanden, der Schweiz, Norwegen und Dänemark zusammen.[150] Die teilnehmenden Gremien haben vereinbart, in «allen teilnehmenden Ländern eine vergleichbare Untersuchung der internationalen Zusammenarbeit der

149 Büro der Generalinspekteurin für Nachrichtendienste und Sicherheit, Cheryl Gwyn: «Annual Report for the Year Ended 30 June 2017», 1. Dezember 2017, 31f., http://www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2017.pdf, eigene Übersetzung.

150 Bisher beteiligen sich folgende Behörden: Der belgische Ständige Kontrollausschuss für Nachrichten- und Sicherheitsdienste (Comiteri), die niederländische Kontrollbehörde für Nachrichten- und Sicherheitsdienste (CTIVD), die Schweizer Unabhängige Aufsichtsbehörde des Nachrichtendienstes sowie Delegationen aus Schweden (Sicherheits- und Datenschutzausschuss *Säkerhets- och integritetsskyddsnämnden*), Norwegen (Parlamentarisches Aufsichtsgremium der Nachrichtendienste EOS) und Dänemark (Nachrichtendienst-Aufsichtsbehörde); siehe hierzu: Belgischer Ständiger Kontrollausschuss für Nachrichten- und Sicherheitsdienste (Comiteri): «Rapport d'activité 2015», 16. September 2016, 80f., http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2015.pdf.

verschiedenen Nachrichtendienste mit Fokus auf den Kampf gegen «Foreign Terrorist Fighters» durchzuführen.»[151]

Ziel der Zusammenarbeit ist es, das Thema aus unterschiedlichen Blickwinkeln, jedoch auf Grundlage eines vergleichbaren Ansatzes zu beleuchten. Ein solche Vorgehensweise ermöglicht, sich ein ganzheitliches Bild von den Anstrengungen der internationalen nachrichtendienstlichen Zusammenarbeit zu machen, die für ein Kontrollgremium allein viel schwieriger zu untersuchen wären. Zudem fördert diese Herangehensweise einen sehr viel intensiveren Dialog über die Rolle von und die Verbesserungsmöglichkeiten für Kontrollinstrumente, um die tatsächlichen Herausforderungen der Kontrolle besser zu bewältigen.

Five Eyes:
Five Eyes Intelligence Oversight and Review Council (FIORC)

Dieser gemeinsame Rat wurde im September 2016 gegründet und setzt sich aus Mitgliedern aus Australien, Kanada, Neuseeland, dem Vereinigten Königreich und den USA zusammen.[152] Ziel des Forums ist es, die Beziehungen zwischen den Five-Eyes-Kontrollgremien zu intensivieren, den Meinungsaustausch über Themen von gemeinsamem Interesse zu ermöglichen, einen Raum für den Vergleich von Kontrollmethoden zu schaffen und Bereiche zu identifizieren, in denen die Zusammenarbeit die Leistungsfähigkeit der Kontrolle fördern kann.[153]

---

151 Comiteri: «Activity Report 2016. Review Investigations, Control of Special Intelligence Methods and Recommendations», 2018, 82f., http://www.comiteri.be/images/pdf/Jaarverslagen/Vast-Comit-I--Activity-Report-2016.PDF; EOS Committee, 2018, 12, eigene Übersetzung.

152 Diese Kontrollgremien nehmen am FIORC teil: Office of the Inspector General of Intelligence and Security of Australia, Office of the Communications Security Establishment Commissioner and the Security and Intelligence Review Committee of Canada, Commissioner of Security Warrants und Office of the Inspector General of Intelligence and Security of New Zealand, Office of the Investigatory Powers Commissioner of the United Kingdom, Office of the Intelligence Community Inspector General of the United States, siehe hierzu: Office of the Inspector General National Security Agency, «Semiannual Report to Congress. 1 October 2017 to 31 March 2018», 2018, https://www.dni.gov/files/documents/FOIA/OCT2017-MAR-2018_SAR_FINAL.PDF; ebenso Barker, Petrie, Dawson, Godec, Purser und Porteous: «Oversight of Intelligence Agencies: A Comparison of the ‹Five Eyes› Nations», 2017, 9, http://apo.org.au/system/files/123831/apo-nid123831-515251.pdf.

153 Die erste FIORC-Konferenz, an der Vertreter/innen der Aufsichtsbehörden aller Five Eyes-Nationen teilnahmen, fand im Oktober 2017 in Ottawa, Kanada, statt. Siehe Security Intelligence Review Committee: «SIRC Annual Report 2017–2018: Building For Tomorrow: The Future Of Security Intelligence Accountability In Canada», 2018, http://www.sirc-csars.gc.ca/anrran/2017-2018/index-eng.html.

Beratungsgremien für Kontrollbehörden

Im Dezember 2014 hat die CTIVD einen «Expertenkreis» ins Leben gerufen, der aus Expert/innen und Wissenschaftler/innen besteht und die Aufsichtsbehörde zu wichtigen Entwicklungen berät. Einige dieser Expert/innen beraten die CTIVD darüber hinaus bezüglich der Auswahl von Themenfeldern für Inspektionen und Prüfungen.[154] Das IPCO hat einen Technologie-Beratungsausschuss (TAP) aus wissenschaftlichen Gutachter/innen unter Leitung des Statistikers Bernard Silverman zusammengestellt.[155] Auch der neuseeländische Generalinspekteur für Nachrichtendienste und Sicherheit hat ein gesetzliches Beratungsgremium, bestehend aus zwei Personen, ernannt.[156]

Zusammenfassung der Ergebnisse und Reformagenda

Angesichts hochkomplexer moderner Sicherheitseinsätze, an denen meist verschiedene Behörden mit ähnlichen Mitteln beteiligt sind, haben einige Gesetzgeber den Aufgabenbereich der Kontrollbehörden über Nachrichtendienste hinaus ausgeweitet. Dadurch werden die Aufsichtsbehörden sichtbarer und auch als Arbeitgeber attraktiver, was wiederum technische Expertise anlocken kann. Eine weitere gute Praxis, die wir in dieser Phase erörtert haben, ist der wachsende Trend zu regelmäßigem und substantiellem Austausch unter Kontrollgremien. In Europa sollten weitere Länder, etwa Frankreich und Deutschland, darüber nachdenken, bestehenden Plattformen für die Zusammenarbeit von Kontrollgremien beizutreten.

Außerdem haben wir in diesem Kapitel die Notwendigkeit beleuchtet, die Wirksamkeit von Massenüberwachungsmaßnahmen weiter zu untersuchen. In einer Zeit, in der die Nachrichtendienste auch auf eine Vielzahl von Open-Source-Informationen zurückgreifen können, sollten Regierungen zeigen, welchen anhaltenden Mehrwert SIGINT-Operationen haben. Jedoch stellt sich die Frage, anhand welcher Kriterien und Methoden die Effektivität nachrichtendienstlicher Tätigkeiten gemessen werden kann.

Phase 8: Berichterstattung

In der letzten Phase des Prozesses der strategischen Fernmeldeaufklärung müssen sowohl Regierungen als auch Kontrollgremien transparent sein und angemessene Informationen über die staatlichen Überwachungsaktivitäten sowie die entsprechenden Kontrolltätigkeiten bereitstellen. Um das Vertrauen der Öffentlichkeit zu stärken, sollten die Nachrichtendienste wichtige rechtliche Dokumente, die im öffentlichen

154 CTIVD: «Kenniskring en tegenspraak CTIVD», 20. September 2017, https://www.ctivd.nl/over-ctivd/kenniskring--en-tegenspraak.

155 IPCO: «A Message from the Commissioner By Sir Adrian Fulford», 17. Mai 2018, https://www.ipco.org.uk/Default.aspx?mid=16.1; Investigatory Powers Commissioner's Office, Twitter-Nachricht, 15. Dezember 2017, https://twitter.com/IPCOffice/status/941722822405013506.

156 Inspector General of Intelligence and Security of New Zealand: «About: The Intelligence and Security Agencies», http://www.igis.govt.nz/about/.

Interesse liegen, proaktiv veröffentlichen.[157] Durch Veröffentlichungen dieser Art konnten beispielsweise Einblicke in sonst nur selten öffentlich zugängliche und recht umfassende Berichte zu den unterschiedlichen Arten und Mustern von Regelverstößen bei der Überwachung auf Basis der Section 702 des *Foreign Intelligence Surveilance Acts* gewährt werden.[158]

Obwohl vollständige Transparenz der Aufsichtsaktivitäten aufgrund von Geheimhaltungsanforderungen nicht immer möglich ist, ist die regelmäßige Berichterstattung durch die Kontrollbehörden ein entscheidendes Mittel, um das Vertrauen der Öffentlichkeit zu gewinnen und der Rechenschaftspflicht nachzukommen. Daher sollte eine solche Berichterstattung so umfassend und zeitnah wie möglich geschehen.

Relevante Aspekte

Welche Regeln gibt es bezüglich einer verpflichtenden, regelmäßigen und öffentlichen Berichterstattung über Überwachungsmaßnahmen und ihre demokratische Kontrolle? Informationen über Kontrollmethoden und -fähigkeiten, insbesondere im Hinblick auf die massenhafte Überwachung von Kommunikationsdaten, sollten so weit irgend möglich bereitgestellt werden. Die Berichte sollten ein ganzheitliches Bild der nachrichtendienstlichen Aktivitäten liefern. Welche Hintergrundinformationen und Statistiken werden der Öffentlichkeit zur Verfügung gestellt? Und wie kommunizieren die Kontrollgremien mit der Öffentlichkeit?

Gute gesetzliche Vorgaben

Option, sich aus der Geheimhaltung zu lösen

Standardmäßig unterliegen alle vom Parlamentarischen Kontrollgremium (PKGr) erörterten Angelegenheiten strikter Geheimhaltung. Einzelne Vorgänge der Arbeit des Gremiums können jedoch öffentlich bewertet werden, wenn zwei Drittel der Mitglieder diesen Schritt unterstützen. In diesem Fall können einzelne Mitglieder des PKGr eine abweichende Stellungnahme – ein sogenanntes *Sondervotum* – zum jeweiligen Fall veröffentlichen.[159] Eine solche Regelung, die Abweichungen von der normalen

157 Die US-Nachrichtendienste haben einige offizielle Dokumente über ihre Aktivitäten und Vorgehensweisen veröffentlicht, wie zum Beispiel deklassifizierte FISC-Stellungnahmen, vierteljährliche und halbjährliche Prüfberichte. Viele dieser Dokumente sind unter http://www.icontherecord.tumblr.com einsehbar. Einen Leitfaden zu den veröffentlichten Dokumenten findet man hier: https://www.dni.gov/files/CLPT/documents/Guide_to_Posted_Documents.pdf. Eine durchsuchbare Datenbank aller Dokumente steht unter https://www.intel.gov/ic-on-the-record-database zur Verfügung.

158 Robyn Greene hat ein informatives Dokument zusammengestellt, das die Öffentlichkeit darüber informiert, wie unbeabsichtigte Fehler den Zugriff auf geschützte Kommunikationen ermöglichen können – und zwar «mit signifikanten und nachhaltigen Auswirkungen». Eine Zusammenfassung der Compliance-Verletzungen von Section 702 des FISA-Gesetzes findet man hier: Greene: «A History of FISA Section 702 Compliance Violations», 28. September 2017, https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/.

159 § 10 (2) Parlamentarisches Kontrollgremiumgesetz, 29. Juli 2009.

Einstufung ausdrücklich erlaubt und die Veröffentlichung bestimmter Fälle oder Aktivitäten unterstützt, kann ein nützliches Aufsichtsinstrument sein. Auch in den USA besteht durch Executive Order 13526 die Möglichkeit, Informationen, die die nationale Sicherheit betreffen, bei besonderem öffentlichem Interesse zu veröffentlichen. Die Durchführungsverordnung besagt, dass «in Ausnahmefällen die Notwendigkeit, derartige Informationen zu schützen, durch das öffentliche Interesse an der Offenlegung der Informationen aufgehoben wird».[160]

Verpflichtung zur Offenlegung von Fehlern

Der britische IP Act verpflichtet die Kontrollbehörde IPCO, eine Person über jeden relevanten Fehler der in Bezug auf sie gemacht wurde, zu informieren, wenn es im öffentlichen Interesse liegt, dass die Person über den Fehler informiert wird (Section 231 (1) IP Act). Dass sich diese Fehlermeldepflicht auf einzelne, konkrete Personen bezieht, legt nahe, dass hauptsächlich gezielte Überwachungsmaßnahmen von dieser Bestimmung abgedeckt werden. Es wäre aber auch denkbar, die Bevölkerung über Fehler bei Massenüberwachungsmaßnahmen in Kenntnis zu setzen. In ihrem Anwendungsbereich ist die Bestimmung allerdings deutlich beschnitten: Der IP Act enthält nämlich auch eine Bestimmung, wonach eine Verletzung der Rechte einer Person unter dem Menschenrechtsgesetz von 1998 nicht ausreicht, um die Meldung eines Fehlers zu rechtfertigen (Section 231 (3) IP Act). Wenn Menschenrechtsverletzungen nicht genügen, um eine Berichterstattung zu begründen, bleibt abzuwarten, welche Arten von Fehlern dann tatsächlich gemeldet werden.

Gute Kontrollpraxis

Mehr Transparenz bei Kontrollmethoden

Norwegen:
Berichterstattung zu fehlerhaften Selektoren/Suchbegriffen

Das EOS hat kürzlich «die Nichtkonformität der technischen Datenerfassung des Dienstes» öffentlich bekannt gegeben, «die zur unbeabsichtigten Erfassung von Informationen aus Kommunikationsmitteln (im Folgenden als ‹Selektoren› bezeichnet) geführt hat, die in Wirklichkeit norwegisch waren».[161]

Obwohl der zitierte Bericht keine weiteren Angaben dazu enthält, ist es bemerkenswert, dass eine Aufsichtsbehörde öffentlich auf solche Unregelmäßigkeiten hinweist.

160 U.S. Government Publishing Office, Executive Order 13526, 2009, Section 3.1(d), https://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf, eigene Übersetzung.

161 EOS-Gremium, 2018, 43f, eigene Übersetzung.

USA:
PCLOBs Bemühungen um Offenlegung

Im PCLOB-Bericht zu Section 702[162] konnte die Aufsichtsbehörde die Deklassifizierung eines Großteils der Informationen über das Programm durchsetzen.[163]

Da Anträge auf Veröffentlichung von ehemals eingestuften Informationen in der Regel entweder von oben – sprich vom Präsidenten – oder aus der Öffentlichkeit kommen, stellt dieser Vorgang eine echte Neuerung dar. Es handelte sich dabei um einen «lateralen» Antrag eines unabhängigen Aufsichtsorgans des Bundes.

Viele Aufsichtsbehörden haben begonnen, mehr Ressourcen für die Öffentlichkeitsarbeit aufzuwenden, und kommunizieren zum Beispiel über öffentliche Info-Websites und Twitter. Wichtiger ist aber, dass es verbindliche Standards für mehr Transparenz sowie genaue und zeitnahe Kontrollberichte gibt. Vor diesem Hintergrund ist es lobenswert, dass die Aufsichtsbehörden von Belgien, Dänemark, den Niederlanden und Norwegen ihre jährlichen Berichte jetzt auch auf Englisch veröffentlichen. Damit liefern sie eine wertvolle Ressource für Vergleichsstudien.

Institutionelle Unterstützung für Whistleblower/innen

USA:
Ausdrückliches Bekenntnis zum Schutz von Whistleblowern

Im Juli 2018 hat der Inspector General der NSA eine Version seines Halbjahresberichts für den US-Kongress veröffentlicht, der über Prüfungen und Untersuchungen von Oktober 2017 bis März 2018 informiert. Der Bericht besagt: «Wir erkennen an, dass Behörden wie die NSA einfach zu groß und ihre Tätigkeiten zu vielfältig sind, als dass das OIG [Office of the Inspector General] wissen könnte, was in der gesamten Organisation passiert, wenn sich nicht Personen zu Wort melden, wenn sie etwas sehen, von dem sie glauben, dass es falsch ist. Und das kann nicht erwartet werden, wenn diese Personen Vergeltungsmaßnahmen zu befürchten haben. Whistleblower/innen spielen bei der Förderung einer effektiven Kontrolle eine wichtige Rolle, vor allem in einer Behörde wie der NSA, wo ein Großteil der Arbeit außerhalb der Öffentlichkeit stattfinden muss, um wirksam zu sein.»[164]

162 PCLOB, 2014.

163 Federation of American Scientists: «Secrecy News 07/28/14», 28. Juli 2014, https://fas.org/sgp/news/secrecy/2014/07/072814.html.

164 Office of the Inspector General National Security Agency, 2018, iii, eigene Übersetzung.

Gleichzeitig hat der Inspector General die Einrichtung einer Schutzseite für Hinweisgeber/innen auf der eingestuften OIG-Website und die Einrichtung einer Koordinationsstelle für Whistleblower/innen angekündigt.[165]

Zusammenfassung der Ergebnisse und Reformagenda

Die Nachrichtendienstführung profitiert von einem größeren Wissen der Öffentlichkeit über die Kontrollmaßnahmen sowie von detaillierten Möglichkeiten, Einblicke in die Durchführung von Überwachungsmaßnahmen zu gewinnen. Unsere Vergleichsstudie nationaler Kontrollsysteme zeigt, dass der Bereich der Transparenzberichterstattung noch ausbaufähig ist. Dazu gehören sowohl mehr Informationen über die Anwendung von Überwachungsbefugnissen in der Praxis als auch über die Dynamiken innerhalb der Aufsicht (z. B. wie unterschiedliche Kontrollinstrumente eingesetzt wurden). Künftige Vergleichsanalysen zu Standards der öffentlichen Berichterstattung, beispielsweise zu verfügbaren Statistiken zum Genehmigungsprozess (d. h. die Gesamtzahl der genehmigten und abgewiesenen Anträge, die Anzahl von Genehmigungen unter Vorbehalt usw.) sind ratsam. Sie können darlegen, wie es Kontrollgremien möglich ist, das öffentliche Vertrauen zurückzugewinnen. Eine systematische Berichterstattung zu Fehlern bei der Massenüberwachung sollte ebenfalls in Betracht gezogen werden.

Während der wirksame Schutz von Whistleblower/innen – nicht zuletzt in SIGINT-Diensten – entscheidend bleibt, könnte die Ausarbeitung strukturierter Berichte über Erfolge und Fehlschläge ebenfalls das öffentliche Vertrauen in die Dienste stärken.

In Systemen gezielter Überwachung sollten Personen, deren private Kommunikation abgefangen wurde, darüber informiert werden, um ihnen die Möglichkeit wirksamer Rechtsmittel zu geben. Auch wenn dies im Kontext der massenhaften Auslandsüberwachung nicht immer umsetzbar sein mag, gibt es möglicherweise Optionen, eine Verpflichtung einzuführen, nach der EU-Bürger/innen informiert werden müssen, wenn ihre Daten bei der Erfassung ausländischer Kommunikationsdaten durch ein anderes europäisches Land abgegriffen wurden.

165 Clark: «NSA Watchdog Breaks Precedent By Releasing Semi-Annual Report», 27. Juli 2018, https://www.govexec.com/management/2018/07/nsa-watchdog-breaks-precedent-releasing-semi-annual-report/150105/; weitere Informationen zum Schutz für Whistleblower in den USA findet man unter https://fas.org/sgp/crs/intel/R43765.pdf.

IV Diskussion

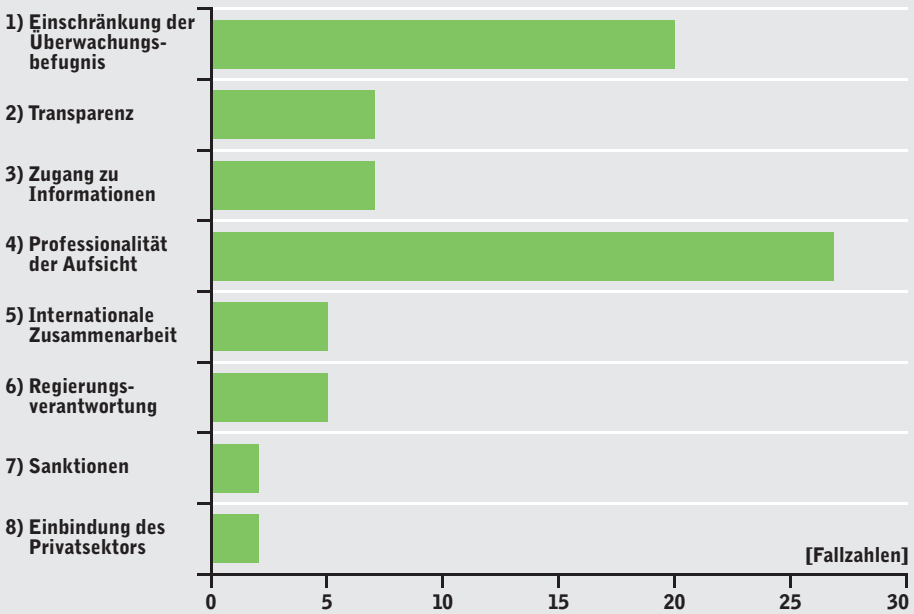
Unsere Suche nach guten rechtlichen Vorgaben und innovativer Kontrollpraxis in den verschiedenen Phasen der Steuerung und Kontrolle der Fernmeldeaufklärung umfasst 64 gute Praktiken. Diese reichen von der Abschaffung der Diskriminierung nach Staatsangehörigkeit über verbesserte Genehmigungsverfahren bis hin zu zusätzlichen Schutzmaßnahmen bei der gesetzlichen Ausgestaltung der internationalen Zusammenarbeit von Nachrichtendiensten. Die in diesem Kompendium hervorgehobenen Praxisbeispiele beziehen sich jeweils auf unterschiedliche Dimensionen. Hierzu gehören:

- Einschränkung der Überwachungsbefugnis
- Transparenz
- Zugang zu Informationen
- Professionalität der Aufsicht
- Internationale Zusammenarbeit
- Regierungsverantwortung
- Sanktionen
- Einbindung des Privatsektors

Diese Kategorien dienen zur Orientierung und schließen sich nicht gegenseitig aus. Beispielsweise lässt sich die Vorgabe, die Verlässlichkeit ausländischer Kooperationspartner sorgfältig zu prüfen, sowohl der Regulierungsdimension «Internationale Zusammenarbeit» als auch «Professionalität der Aufsicht» zuordnen. Eine vollständige Übersicht der 64 Empfehlungen und der ihnen zugewiesenen Kategorien findet sich im Anhang.

Was können wir von der Verteilung der Beispiele in den verschiedenen Kategorien lernen? Die folgende Abbildung zeigt, dass ein Großteil der Empfehlungen entweder die Überwachungsbefugnis weiter einschränkt oder die Aufsichtsprofessionalität fördert. Für uns ist das ein klares Zeichen, dass die Gesetzgeber in den verschiedenen Demokratien versucht haben, einen Mangel an Legitimation in diesen beiden Bereichen zu überwinden. Gleichzeitig zeigen unsere Ergebnisse, dass andere wichtige Bereiche in den jüngsten Reformen weniger im Vordergrund standen – insbesondere die direkte Regierungsverantwortung für die Steuerung von Überwachungsmaßnahmen hätte vielerorts noch konkreter gefasst werden können. Wir konnten für diese Regulierungsdimension insgesamt nur fünf Empfehlungen aufzeigen. In der jüngeren Geschichte lassen sich genügend Beispiele aufführen, in denen unlautere Motive der

Abbildung 3: Regulierungsdimensionen der Praxisbeispiele

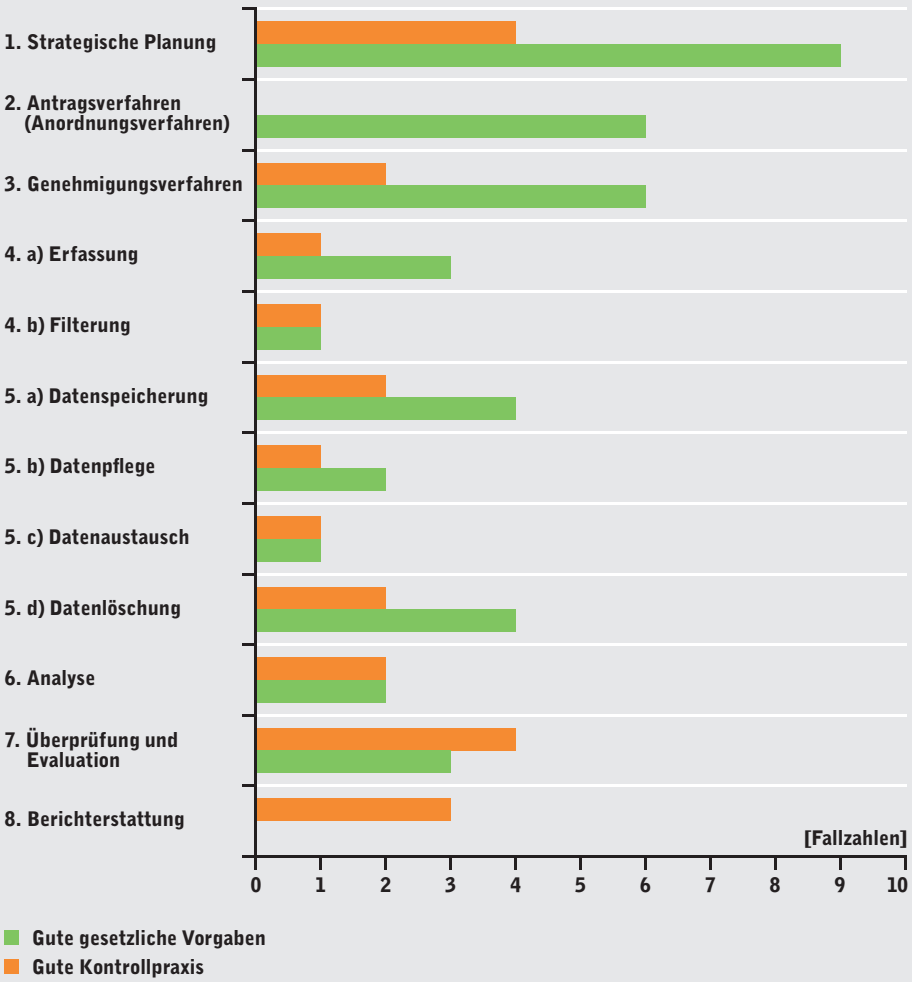


Exekutive die Steuerung von Überwachungsaktivitäten beeinflußt haben.[166] Deshalb ist es wichtig, klare Verantwortlichkeiten für die wichtige Rolle der Exekutive in diesem Politikfeld gesetzlich festzulegen. Auch im Bereich der Sanktionen, zu denen die Strafbarkeit des Missbrauchs von Überwachungsbefugnissen zählt, konnten wir nur zwei Beispiele ausmachen. Zusätzliche Möglichkeiten, Gesetzesverstöße wirksam zu ahnden, würden die Durchsetzungsfähigkeit der Aufsichtsbehörden gegenüber den Diensten stärken.

Wir haben zudem sieben Beispiele für verbesserte Transparenzvorgaben identifiziert, die in unseren Augen mehr Aufmerksamkeit verdienen. Darunter fällt das amerikanische Beispiel, wonach die Geheimhaltungspflicht von Genehmigungsverfahren aufgehoben wird, wenn neue rechtliche Auslegungen von Nachrichtendienstgesetzen darin enthalten sind. Allerdings bleibt auch hier deutlicher Spielraum für weitere Verbesserungen. Die Bereitstellung von genaueren Informationen über den tatsächlichen Umfang der genehmigten Überwachungsmaßnahmen (Anzahl und Formen der Genehmigungen, mit oder ohne Auflagen) und Benachrichtigungen sowie detaillierte Angaben über die eingesetzten Kontrollinstrumente sollten ebenfalls in öffentlichen Berichten enthalten sein. Mehr Transparenz in Bezug auf die tatsächliche Umsetzung

166 Tréguer: «French Constitutional Council Strikes Down «Blank Check» Provision in the 2015 Intelligence Act», Verfassungsblog.de, 26. Oktober 2016.

Abbildung 4: Gute Praxisbeispiele pro Phase



von Maßnahmen der Fernmeldeaufklärung würden das Vertrauen der Bevölkerung in die Arbeit der Dienste stärken.

Interessanterweise enthalten nur sehr wenige Gesetze Regeln, die klar definieren, wer für die Ausleitung und Erfassung von Daten zuständig ist und wie Anbieter gegen staatliche Forderungen nach einem Datenzugriff Einspruch einlegen können. Ohne die Einbindung des Privatsektors wären die meisten Erhebungen nicht umsetzbar. Die Zwischenschaltung von Providern kann einen Schutzraum vor Übergriffen der Exekutive bieten. Im Allgemeinen sollte der Dialog zwischen Netzbetreibern und Kontrollgremien aufgenommen werden.

Mit Blick auf die Verteilung der 64 Praxisbeispiele auf die acht aufeinanderfolgenden Phasen unseres Analyseschemas (siehe Abbildung 4), stellen wir zudem

fest: Parlamentarier neigen im Allgemeinen dazu, den Rechtsrahmen zu verbessern, anstatt Innovationen im Bereich der Kontrollpraxis einzuführen. Ein Grund dafür könnte sein, dass Veränderungen der Kontrolldynamik in der praktischen Umsetzung aufwändiger sind. Nichtsdestotrotz sind sie aber gleichermaßen wichtig, denn selbst die besten gesetzlichen Vorgaben bieten nur bedingt Schutz, wenn deren Einhaltung nicht wirksam überprüft wird. Gerade in diesem Bereich müssen Aufsichtsbehörden künftig noch intensiver daran arbeiten, mit dem technologischen Wandel Schritt zu halten. Parlamente auf der ganzen Welt sind gut beraten, nicht nur in die neueste Überwachungstechnologie zu investieren, sondern auch in neue Kontrolinstrumente für moderne Aufsichtsbehörden.

Technische Schnittstellen für den direkten Datenbankzugriff gehören hier zu den wichtigsten Innovationen in der Aufsichtspraxis. Der ungehinderte und vollständige Zugang der Kontrolleur/innen zu allen relevanten Informationen in den IT-Systemen der Nachrichtendienste ist für eine wirksame Kontrolle unabdingbar. In Bezug auf diese Dimension sind viele Reformbemühungen eher unzureichend – ganz zu schweigen von der sich rasant weiterentwickelnden Zusammenarbeit von Nachrichtendiensten. Hier müssen nationale Kontrollbehörden am Ball bleiben. Einige Aufsichtsgremien in Europa haben nun einen neuen Weg beschritten, diese enorme Aufgabe in Angriff zu nehmen. Dabei profitieren sie nicht nur vom gegenseitigen Lernen durch engeren Austausch. In Zukunft könnten sie auch kreative Lösungen finden, um einige der aktuellen Kontrolldefizite zu beheben, die mit der internationalen Nachrichtendienstkooperation einhergehen.[167] Wie kürzlich von der niederländischen CTIVD vorgeschlagen, sollte man zum Beispiel die institutionelle Gestaltung einer multilateralen Aufsicht über die europäische CTG-Datenbank kreativ angehen.

Einige Aufsichtsgremien haben es mittlerweile geschafft, in der Öffentlichkeit als unabhängige Stimme wahrgenommen zu werden. Etwaige Vereinnahmungen durch die Regierung (regulatory capture) können sie besser zurückdrängen und ihre Unabhängigkeit bekräftigen. Viele Gremien sind gestärkt aus den jüngsten Reformen der Nachrichtendienstgesetze hervorgegangen. Um im «goldenen Zeitalter der Überwachung» die Grundprinzipien der demokratischen Rechtsstaatlichkeit wirksam durchzusetzen, brauchen wir mehr denn je einflussreiche und eigenständige Kontrolleur/innen.

167 Siehe hierzu die gemeinsame Stellungnahme der Aufsichtsgremien aus Belgien, Dänemark, Niederlande, Norwegen und der Schweiz: «Stärkung der Aufsicht über den internationalen Datenaustausch zwischen Nachrichten- und Sicherheitsdiensten», 2018.

V Fazit

Die zahlreichen Nachrichtendienstreformen, die im Nachgang der Enthüllungen des Whistleblowers Edward Snowden in einigen Ländern verabschiedet wurden, sind in den Augen vieler Beobachter/innen ungenügend und enttäuschend. Die Diskussion über grundrechtsbasierte und demokratisch kontrollierte staatliche Überwachung von Kommunikation ist mit der Verabschiedung neuer Gesetze ohnehin noch nicht beendet. Gerichte wie der Europäische Gerichtshof für Menschenrechte haben den nationalen Regierungen tendenziell einen großen Spielraum bei der Umsetzung von Massenüberwachung eingeräumt, gleichwohl bestehen sie konsequent auf einen geeigneten Rechtsrahmen und eine effektive Kontrolle. Was dies letztlich in der Praxis bedeutet, wird jedoch nicht von Gerichten vorgegeben, sondern muss durch den Gesetzgeber entschieden werden. Auch wenn die Mühlen der demokratischen Institutionen langsam mahlen: Die Parlamente stehen hier in der Pflicht, aus den Fehlern mangelhafter Nachrichtendienstkontrolle zu lernen und wirksamere Schutzmaßnahmen einzuführen. Das mag nicht das Snowden-Erbe sein, das einige erwartet haben, aber genau das ist die schwierige und gleichwohl notwendige Aufgabe demokratischer Regierungskontrolle.

Wir hoffen, dass das vorliegende Kompendium an dieser Stelle einen Beitrag leisten kann, und freuen uns über Feedback und Ideen zu den von uns zusammengetragenen Empfehlungen. Jede Reform des Nachrichtendienstrechts birgt Aspekte, die im internationalen Vergleich herausstechen und weiterer Diskussion bedürfen. Natürlich garantieren auch die dargestellten guten Praktiken für sich genommen keine einwandfreie Steuerung und Kontrolle von Nachrichtendiensten, aber wir glauben, dass deren Übernahme die demokratischen Standards verbessern.

Bessere Kontrolle bedeutet auch bessere Sicherheitsvorsorge. Im digitalen Zeitalter erwarten die Bürger/innen zurecht verantwortungsbewusste und effektive Formen der Steuerung von Überwachungsmaßnahmen. Dazu gehören sowohl rechtliche Schutzmechanismen als auch eine effektive Kontrollpraxis, da beide Dimensionen eine wesentliche Rolle bei der Gewährleistung der Sicherheit spielen. Eine wirksame Kontrolle bringt Regierungen dazu, ihre Ressourcen so effektiv wie möglich einzusetzen und ihre Ziele so sorgfältig wie möglich auszuwählen. Das Verfolgen klarer und rechtskonformer Ziele (Phase 1) sowie spezifische und robuste Anordnungs- und Genehmigungsverfahren (Phase 2 und 3) sind dafür entscheidend. Ebenso wichtig ist ein sorgfältiger Datenumgang der Nachrichtendienste bei der Erfassung, Verarbeitung und Analyse (Phase 4, 5 und 6). Es gibt viele mögliche Formen des Missbrauchs in diesen Phasen. Deshalb müssen sowohl der gesetzliche Rahmen als auch die Kontrollpraxis über die Genehmigung hinaus detaillierte Vorgaben beinhalten. Im Hinblick auf institutionelle Lernprozesse und das Vertrauen der Öffentlichkeit

in die Nachrichtendienstführung sind außerdem die professionelle, unabhängige Überprüfung der Wirksamkeit genehmigter Maßnahmen und eine verstärkte öffentliche Berichterstattung über moderne Überwachungsaktivitäten (Phase 7 und 8) von grundlegender Bedeutung.

Natürlich wird auch weiterhin nach einer besseren demokratischen Kontrolle und Steuerung der Massenüberwachung gesucht werden müssen. Gerichte, parlamentarische Gremien, exekutive Fachaufsicht und unabhängige Kontrollbehörden spielen alle dabei eine wichtige Rolle: Ihr Zusammenspiel kann das Vertrauen der Öffentlichkeit in Nachrichtendienstaktivitäten zurückgewinnen und fördern. Die große Aufgabe, für ausreichende Transparenz zu sorgen und die Einhaltung der Gesetze nachzuweisen, nimmt selbstverständlich auch die Nachrichtendienste selbst in die Pflicht. Wie einige Beispiele in diesem Kompendium zeigen, haben die Nachrichtendienste in einigen Ländern bereits mehr dafür getan als andere, um beispielsweise die Öffentlichkeit ausreichend über ihrer Arbeitsweisen zu informieren.

Wir hoffen, dass unsere Empfehlungen die notwendige Debatte darüber entfachen, wie die Befugnisse der Massenüberwachung besser eingegrenzt und wirksamer kontrolliert werden können. Doch positive Veränderungen entstehen nicht allein durch das Identifizieren guter Praktiken. Sie müssen diskutiert und Teil einer umfassenderen nationalen Reformagenda werden, die auch neue technologische Entwicklungen in den Blick nimmt. Gesetzgeber sollten diese Praktiken jetzt ernsthaft mit zivilgesellschaftlichen Organisationen und der Regierung diskutieren, um einige der bewährten Kontroll- und Regulierungsbeispiele aus anderen Ländern zu bewerten und zu übernehmen. Wir sind gerne bereit, diese Debatte zu unterstützen, um gemeinsam die Gewährleistung unserer Sicherheit und den Schutz unserer Privatsphäre voranzubringen.

VI Anhang

Liste der Workshop-Teilnehmerinnen und -Teilnehmer

Viele Menschen haben uns im Rahmen dieser Studie mit Ratschlägen und Expertise unterstützt. Im Rahmen zahlreicher Interviews und zweier Fachworkshops haben wir konstruktives Feedback und zusätzliche Informationen erhalten.

Wir sind sehr dankbar für die Hilfe, das Interesse und die Zeit, die unterschiedlichste Gruppen in unser Projekt investiert haben.

Die folgenden Expertinnen und Experten haben während eines Workshops am 14. und 15. Juni 2018 in Berlin wertvolle Anregungen zu früheren Entwürfen dieses Berichts gegeben.

- Sharon Bradford Franklin, Director of Surveillance and Cybersecurity Policy, New America's Open Technology Institute
- Iain Cameron, Professor am Institut für Rechtswissenschaft, Universität Uppsala, schwedisches Mitglied der Venedig-Kommission im Europarat
- Joan Feigenbaum, Grace Murray Hopper Professorin für Informatik, Yale University
- Giles Herdale, Policy Advisor und Ko-Vorsitzender, Independent Digital Ethics Panel for Policing
- Eric Kind, Dozent an der Queen Mary University of London
- Ronja Kniep, wissenschaftliche Mitarbeiterin, Wissenschaftszentrum Berlin für Sozialforschung (WZB)
- Klaus Landefeld, Stellv. Vorstandsvorsitzender, Vorstand Infrastruktur und Netze eco - Verband der Internetwirtschaft e.V. und Mitglied des Aufsichtsrats bei DE-CIX International
- Greg Nojeim, Senior Counsel und Director, Freedom, Security and Technology Project, Center for Democracy & Technology
- Jörg Pohle, Postdoc, Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG)
- Volker Roth, Professor für Informatik, Freie Universität Berlin
- Graham Smith, Partner, Bird & Bird LLP
- Eric Töpfer, Wissenschaftlicher Mitarbeiter, Deutsches Institut für Menschenrechte
- Nico van Eijk, Professor für Medien- und Telekommunikationsrecht und Direktor des Instituts für Informationsrecht, Universität Amsterdam
- Njord Wegge, Senior Research Fellow, Norwegisches Institut für internationale Beziehungen (NUPI)

Die folgenden Expert/innen für Nachrichtendienstkontrolle haben während eines Workshops am 14. Mai 2018 in Berlin wertvolle Anregungen zu früheren Versionen dieses Berichts gegeben. Da nicht alle Teilnehmenden namentlich genannt werden möchten, ist diese Liste nicht vollständig.

- Frank Brasz, stellvertretender Generalsekretär, CTIVD, Niederlande
- Wouter de Ridder, Ständiger Kontrollausschuss für Nachrichten- und Sicherheitsdienste Comiteri, Belgien
- Arild Færaas, Sekretariat des EOS-Gremiums, Norwegen
- Emil Bock Greve, Nachrichtendienst-Aufsichtsbehörde TET, Dänemark
- Bertold Huber, stellvertretender Vorsitzender, G10-Kommission, Deutschland
- Rune Odgaard Jensen, Nachrichtendienst-Aufsichtsbehörde TET, Dänemark
- Jantine Kervel-de Goei, Generalsekretärin, CTIVD, Niederlande
- Charles Miller, Investigatory Powers Commissioner's Office, UK
- Dominic Volken, stellvertretender Leiter, Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten, Schweiz

Interview- und Gesprächspartner/innen

Nicht alle Befragten haben der Nennung ihrer Namen zugestimmt. Daher sind an dieser Stelle nicht alle durchgeführten Interviews aufgeführt.

- Marie-Laure Basilien-Gainche, Professorin der Rechtswissenschaften, Université Jean Moulin Lyon 3, Ehrenmitglied des Institut Universitaire de France
- Susan Decker, Senior Research Advisor, Security Intelligence Review Committee, Kanada
- Craig Forcese, Professor der Rechtswissenschaften, University of Ottawa
- Lex Gill, wissenschaftliche Mitarbeiterin, Citizen Lab, University of Toronto
- Elspeth Guild, Professorin der Rechtswissenschaften, Queen Mary University of London
- Lotte Houwing, File Coordinator, Public Interest Litigation Project
- Peter Koop, Electrospaces.net
- Sébastien-Yves Laurent, Professor an der Université de Bordeaux – Fakultät für Rechts- und Politikwissenschaften
- Evan Light, Communications Program, Glendon College, York University
- Simon McKay, Anwalt für Bürger- und Menschenrechte
- Brenda McPhail, Director, Privacy, Technology & Surveillance Project, Canadian Civil Liberties Association
- David Medine, ehemaliger Vorsitzender des US Privacy and Civil Liberties Oversight Board
- Mario Oetheimer, Leiter des Bereichs «Information Society, Privacy and Data Protection», Agentur der Europäischen Union für Grundrechte
- Jonathan Obar, Department of Communication Studies, York University
- Félix Tréguer, Post-Doc, Sciences Po Paris

Übersicht der guten Praktiken

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
1	Keine Unterscheidung zwischen aus- und inländischen Daten bei der Datenerfassung	Strategische Planung	Gesetzliche Vorgaben	NL	Einschränkung der Überwachungsbefugnis 
2	Zusätzliche Bändigung von Massenüberwachungsbefugnissen	Strategische Planung	Gesetzliche Vorgaben	USA	Einschränkung der Überwachungsbefugnis 
3	Transparenz über die Akteur/innen die an der Formulierung des Auftragsprofils des BND beteiligt sind	Strategische Planung	Gesetzliche Vorgaben	D	Transparenz 
4	Jährliche Revision aller Aufklärungsschwerpunkte durch die Abteilungsleiter/innen	Strategische Planung	Gesetzliche Vorgaben	USA	Regierungsverantwortung 
5	Eignungsprüfung für ausländische Kooperationspartner	Strategische Planung	Gesetzliche Vorgaben	NL	Internationale Zusammenarbeit  Professionalität der Aufsicht 
6	Schriftliche Vereinbarungen zu den Zielen, der Art und der Dauer der internationalen Zusammenarbeit müssen vom Kanzleramt genehmigt werden	Strategische Planung	Gesetzliche Vorgaben	D	Internationale Zusammenarbeit  Regierungsverantwortung 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
7	Verbot der Wirtschaftsspionage	Strategische Planung	Gesetzliche Vorgaben	D	Einschränkung der Überwachungsbefugnis 
8	Verbot der Diskriminierung von geschützten Gruppen durch Massenüberwachung	Strategische Planung	Gesetzliche Vorgaben	USA	Einschränkung der Überwachungsbefugnis 
9	Strafrechtliche Haftung für Missbrauch von Überwachungsbefugnissen	Strategische Planung	Gesetzliche Vorgaben	USA	Sanktionen 
10	Der parlamentarische Kontrollausschuss muss regelmäßig über die operativen Zwecke informiert werden	Strategische Planung	Kontrollpraxis	UK	Transparenz 
11	Vollständiger Zugriff auf die Dokumentation von Kooperationsvereinbarungen	Strategische Planung	Kontrollpraxis	CA	Internationale Zusammenarbeit  Zugang zu Informationen 
12	CTIVD kann die Prüfvermerke kontrollieren	Strategische Planung	Kontrollpraxis	NL	Internationale Zusammenarbeit  Zugang zu Informationen 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
13	Das parlamentarische Kontrollgremium muss über alle Absichtserklärungen (MoU) informiert werden	Strategische Planung	Kontrollpraxis	D	Internationale Zusammenarbeit  Zugang zu Informationen 
14	Beschränkung der Anzahl der Dienste, die erfasste Daten nutzen dürfen	Antragsverfahren	Gesetzliche Vorgaben	F	Einschränkung der Überwachungsbefugnis 
15	Nennung der automatisierten Auswertungsmethoden in den Anordnungen	Antragsverfahren	Gesetzliche Vorgaben	F	Professionalität der Aufsicht 
16	Spezifische Anforderung, den nachrichtendienstlichen Mehrwert in einer SIGINT-Anordnung zu begründen	Antragsverfahren	Gesetzliche Vorgaben	CA	Einschränkung der Überwachungsbefugnis  Professionalität der Aufsicht 
17	Auflistung der Suchbegriffe in Anordnungen für die Ausland-Ausland-Fernmeldeaufklärung	Antragsverfahren	Gesetzliche Vorgaben	D	Einschränkung der Überwachungsbefugnis  Professionalität der Aufsicht 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
18	Bestimmung konkreter Glas-faserkabel für die Erfassung	Antragsver-fahren	Gesetzliche Vor-gaben	NL	Einschränkung der Überwa-chungsbefugnis 
19	Direkte ministe-rielle Verantwor-tung für die Akti-vierung bestimm-ter Suchbegriffe	Antragsver-fahren	Gesetzliche Vor-gaben	D	Regierungsver-antwortung 
20	Anordnungen können unter Vor-behalt genehmigt werden	Genehmi-gungsver-fahren	Gesetzliche Vor-gaben	CA	Professionalität der Aufsicht 
21	Verpflichtender öffentlicher Bericht von der Genehmigungsbe-hörde	Genehmi-gungsver-fahren	Gesetzliche Vor-gaben	NL	Transparenz 
22	Möglichkeit, die Veröffentlichung einer Entschei-dung oder Stel-lungnahme des Foreign Intelligen-ce Surveillance Court zu bean-tragen	Genehmi-gungsver-fahren	Gesetzliche Vor-gaben	USA	Transparenz 
23	Veröffentlichung neuer Rechtsausle-gungen	Genehmi-gungsver-fahren	Gesetzliche Vor-gaben	USA	Transparenz 
24	Externe juristische Gutachten kön-nen im Zuge des Genehmigungsver-fahren eingeholt werden	Genehmi-gungsver-fahren	Gesetzliche Vor-gaben	USA	Professionalität der Aufsicht 
25	Quoten für spezi-fische Datenerfas-sungsmethoden	Genehmi-gungsver-fahren	Gesetzliche Vor-gaben	F	Einschränkung der Überwa-chungsbefugnis 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
26	IPCO Advisory Notice 01/2018	Genehmi-gungsver-fahren	Kontrollpraxis	UK	Professionalität der Aufsicht 
27	Offener Dialog zwischen Kon-trollgremium und der Zivilge-sellschaft über Kriterien für Verhältnismäßig-keitsprüfungen von Überwachungs-maßnahmen	Genehmi-gungsver-fahren	Kontrollpraxis	UK	Professionalität der Aufsicht 
28	Spezialisiertes Exekutivorgan als Datenerfassungs-zentrum	Erfassung	Gesetzliche Vor-gaben	F	Regierungsver-antwortung 
29	Möglichkeiten der Telekommunikati-onsunternehmen, Einspruch gegen Überwachungs-anordnungen zu erheben	Erfassung	Gesetzliche Vor-gaben	USA	Einbindung des Privatsektors 
30	Allein Internet-anbieter sind für die Installation von Splittern und Selektorenlisten verantwortlich	Erfassung	Gesetzliche Vor-gaben	USA	Einbindung des Privatsektors 
31	Technische Schnittstellen für den direkten Datenbank-zugriff der Kontrolleur/innen	Erfassung	Kontrollpraxis	F NL NOR CH	Professionalität der Aufsicht 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
32	Alle ausgefilterten Rohdaten (einschließlich Inhalts- und Verkehrsdaten) können von den Nachrichtendiensten nicht mehr abgerufen werden	Filterung	Gesetzliche Vorgaben	NL	Einschränkung der Überwachungsbefugnis 
33	Das Bundesgericht FISC prüft von den Nachrichtendiensten durchgeführte Compliance-Audits	Filterung	Kontrollpraxis	USA	Zugang zu Informationen 
34	Keine Unterscheidung zwischen Inhalts- und Verkehrsdaten bei der Datenspeicherung	Datenspeicherung	Gesetzliche Vorgaben	NL	Einschränkung der Überwachungsbefugnis 
35	Verpflichtung zur Bestimmung von Dateianordnungen	Datenspeicherung	Gesetzliche Vorgaben	D	Professionalität der Aufsicht 
36	Gebot der Zweckbindung für gemeinsame Dateien	Datenspeicherung	Gesetzliche Vorgaben	D	Professionalität der Aufsicht 
37	Angleichung der Speicherfristen für SIGINT-Informationen über Personen mit und ohne US-Staatsbürgerschaft	Datenspeicherung	Gesetzliche Vorgaben	USA	Einschränkung der Überwachungsbefugnis 
38	«Oversight 3.0-Projekt» zu künftigen Herausforderungen von Kontrollbehörden	Datenspeicherung	Kontrollpraxis	NL	Professionalität der Aufsicht 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
39	Gemeinsame Kontrollen von G10-Kommission und Bundesdaten-schutzbeauftrag-tem	Datenspei-cherung	Kontrollpraxis	D	Professionalität der Aufsicht 
40	Sorgfaltspflicht bei der Daten-verarbeitung, einschließlich der Verwendung von Algorithmen	Datenpflege	Gesetzliche Vor-gaben	NL	Regierungsver-antwortung 
41	Kennzeichnungs-pflicht aller mas-senhaft erfassten SIGINT-Daten	Datenpflege	Gesetzliche Vor-gaben	D	Einschränkung der Überwa-chungsbefugnis  Professionalität der Aufsicht 
42	Zwingende Vorab-Stellungnahme der Kontrollbehörde zur Ausgestaltung der Datenkenn-zeichnung	Datenpflege	Kontrollpraxis	F	Einschränkung der Überwach-ungsbefugnis  Professionalität der Aufsicht 
43	Standardmäßig größerer Zugriff auf Informationen Dritter durch das Kontrollgremium	Datenaus-tausch	Gesetzliche Vor-gaben	NOR	Zugang zu Infor-mationen 
44	Stichprobenartige Kontrollen bei der automatischen Übermittlung von personenbezoge-nen Daten an aus-ländische Nach-richtendienste	Datenaus-tausch	Kontrollpraxis	D	Professionalität der Aufsicht 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
45	Verpflichtung zur sofortigen Löschung von unrechtmäßig erhobenen Daten	Datenlö-schung	Gesetzliche Vor-gaben	D	Einschränkung der Überwach-ungsbefugnis 
46	Verpflichtung zur Vernichtung von Daten aus der Massenerfassung, die als irrelevant erachtet werden	Datenlö-schung	Gesetzliche Vor-gaben	NL	Einschränkung der Überwach-ungsbefugnis 
47	Verpflichtung zur Protokollierung von Datenlöschung	Datenlö-schung	Gesetzliche Vor-gaben	F	Professionalität der Aufsicht  Einschränkung der Überwach-ungsbefugnis 
48	Verpflichtung zur Löschung von Gesundheitsdaten in ausländischen Datensätzen	Datenlö-schung	Gesetzliche Vor-gaben	CA	Einschränkung der Überwach-ungsbefugnis 
49	Statistische Mus-teranalysen von Datenlöschungen	Datenlö-schung	Kontrollpraxis	SWE	Professionalität der Aufsicht 
50	Unabhängige Prüfung der Ein-haltung der Lösch-pflichten	Datenlö-schung	Kontrollpraxis	NOR	Professionalität der Aufsicht 
51	Human-in-the-Lo-op (HITL)-Schutz-maßnahme bei der automatisierten Datenanalyse	Analyse	Gesetzliche Vor-gaben	NL	Professionalität der Aufsicht 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
52	Verpflichtende Schulungen für Analyst/innen	Analyse	Gesetzliche Vor-gaben	NL	Professionalität der Aufsicht 
53	Automatische interne Kontroll-systeme für die Datenanalyse	Analyse	Kontrollpraxis	UK	Professionalität der Aufsicht  Einschränkung der Überwach-ungsbefugnis 
54	Vorab-Prüfung von KI-Experi-menten und Daten-analysetechniken	Analyse	Kontrollpraxis	F	Professionalität der Aufsicht 
55	Ganzheitliche und behördenübergrei-fende Prüfung von SIGINT-Praktiken	Überprü-fung und Evaluation	Gesetzliche Vor-gaben	CA	Zugang zu Infor-mationen  Professionalität der Aufsicht 
56	Wirksamkeitsprü-fung vor der Ver-längerung einer Anordnung	Überprü-fung und Evaluation	Gesetzliche Vor-gaben	NL	Einschränkung der Überwach-ungsbefugnis 
57	Strafrechtliche Verantwortlichkeit bei Missachtung von Anfragen von Kontrollgremien	Überprü-fung und Evaluation	Gesetzliche Vor-gaben	NOR	Sanktionen 

Nr.	Beispiel	Phase	Untersuchungs-ebene	Land*	Regulierungs-dimension
58	Kein Anspruch auf das deliberative Privileg («deliberative privilege», Gewohnheitsrecht) gegenüber dem PCLOB	Überprüfung und Evaluation	Kontrollpraxis	USA	Zugang zu Informationen 
59	Verpflichtende vierteljährliche Vorfallsmeldung beim Generalinspekteur (Inspector General)	Überprüfung und Evaluation	Kontrollpraxis	NZ	Professionalität der Aufsicht 
60	Gemeinsame Prüfungen und Austauschtreffen	Überprüfung und Evaluation	Kontrollpraxis	BE NL CH NOR DK	Professionalität der Aufsicht 
61	Five Eyes Intelligence Oversight and Review Council (FIORC)	Überprüfung und Evaluation	Kontrollpraxis	AUS CA NZ UK USA	Professionalität der Aufsicht 
62	Berichterstattung zu fehlerhaften Selektoren/Suchbegriffen	Berichterstattung	Kontrollpraxis	NOR	Transparenz 
63	PCLOBs Bemühungen um Offenlegung	Berichterstattung	Kontrollpraxis	USA	Transparenz 
64	Ausdrückliches Bekenntnis zum Schutz von Whistleblowern	Berichterstattung	Kontrollpraxis	USA	Transparenz 

*BE = Belgien; CA = Kanada; CH = Schweiz; D = Deutschland; DK = Dänemark; F = Frankreich; NL = Niederlande; NOR = Norwegen; NZ = Neuseeland; SWE = Schweden; UK = Vereinigtes Königreich; USA = Vereinigte Staaten von Amerika

Abkürzungsverzeichnis

Abkürzung	Name	Erklärung
AB-ND	Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten (Schweiz)	
AIVD	Algemene Inlichtingen en Veiligheids-dienst	Allgemeiner Nachrichten- und Sicherheitsdienst (Niederlande)
BND	Bundesnachrichtendienst (Deutschland)	
BND-Gesetz	Gesetz über den Bundesnachrichten-dienst (Deutschland)	
BVerfG	Bundesverfassungsgericht (Deutschland)	
BVerfSchG	Bundesverfassungsschutzgesetz (Deutschland)	
EuGH	Gerichtshof der Europäischen Union	
CNCTR	Commission nationale de contrôle des techniques de renseignement	Nationale Kontrollkommission für technische Überwachungsmethoden (Frankreich)
COMINT	Communication Intelligence	Fernmeldeaufklärung
CSE	Communications Security Establishment (Kanada)	Nachrichtendienst Kanadas, zuständig für Fernmelde- und elektronische Aufklärung
CSIS	Canadian Security Intelligence Service	Sicherheits- und Nachrichtendienst Kanadas, vorrangig Inlandsnachrichtendienst mit gewissen Aufgaben der Auslandsaufklärung, wie Terrorismusbekämpfung
CTG	Counter Terrorism Group	Informelles Gremium zur Terrorismusbekämpfung der Nachrichtendienste der Mitgliedstaaten der Europäischen Union sowie der Dienste Norwegens und der Schweiz
CTIVD	De Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten	Kontrollbehörde für die Nachrichten- und Sicherheitsdienste der Niederlande
DNI	Director of National Intelligence (USA)	Direktor der nationalen Nachrichtendienste der USA
DPA	Data Protection Authority	Datenschutzbehörde
EGMR	Europäischer Gerichtshof für Menschenrechte	

Abkürzung	Name	Erklärung
EOS	Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste	Parlamentarisches Aufsichtsgremium der Nachrichtendienste (Norwegen)
FIORC	Five Eyes Intelligence Oversight and Review Council	Gemeinsamer Ausschuss der Kontrollgremien der Five Eyes-Allianz (nachrichtendienstlicher Zusammenschluss von USA, Vereinigtem Königreich, Kanada, Australien und Neuseeland)
FISA	Foreign Intelligence Surveillance Act	Gesetz über nachrichtendienstliche Überwachung im Ausland (USA)
FISC	United States Foreign Intelligence Surveillance Court	Bundesgericht der Vereinigten Staaten, das Maßnahmen der Auslands-Fernmeldeaufklärung prüft und genehmigt
G10-Gesetz	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz, Deutschland)	
G10-Kommission		Unabhängiges Organ, das über die Notwendigkeit und Zulässigkeit von nachrichtendienstlichen Überwachungsmaßnahmen entscheidet, die in den Schutzbereich des Artikel 10 GG eingreifen
GCHQ	Government Communications Headquarters	Nachrichtendienst des Vereinigten Königreichs, zuständig für Fernmelde- und elektronische Aufklärung
GIC	Groupement interministériel de contrôle	Behörde unter der Leitung des französischen Premierministers, zuständig für die zentrale Koordinierung der Datenbeschaffung bei privaten Intermediären (z.B. Netzbetreibern)
HUMINT	Human Intelligence	Informationsgewinnung durch menschliche Quellen
IP Act	Investigatory Power Act (UK)	Gesetz über elektronische Überwachung durch Polizei und Nachrichtendienste im Vereinigten Königreich
IPCO	Investigatory Powers Commissioner's Office (UK)	Kontrollbehörde, zuständig für die Kontrolle elektronischer Überwachung durch Polizei und Nachrichtendienste im Vereinigten Königreich
MIVD	Militaire Inlichtingen- en Veiligheidsdienst	Militärischer Nachrichten- und Sicherheitsdienst (Niederlande)
MoU	Memorandum of Understanding	Abkommen

Abkürzung	Name	Erklärung
ND-Gesetz	Nachrichtendienstgesetz (Schweiz)	
NDB	Nachrichtendienst des Bundes (Schweiz)	
NSA	National Security Agency (USA)	Technischer Nachrichtendienst der Vereinigten Staaten
NSIRA	National Security and Intelligence Review Agency (Kanada)	Geplantes Aufsichtsgremium aller kanadischen Nachrichtendienste (abhängig von der Verabschiedung von Bill C-59)
NZSIS	New Zealand Security Intelligence Service (Neuseeland)	Neuseeländischer Nachrichtendienst
PCLOB	The Privacy and Civil Liberties Oversight Board (USA)	Aufsichtsgremium innerhalb der Exekutive der USA
PKGr	Parlamentarisches Kontrollgremium	In Deutschland
PPD 28	Presidential Policy Directive 28 on Signals Intelligence Activities (USA)	Präsidentielle Durchführungsverordnung zur Kommunikationsüberwachung
SIGINT	Signals Intelligence	Fernmeldeaufklärung
SIUN	Statens inspektion för försvarsunderrättelseverksamheten	Schwedische Kontrollbehörde für die Nachrichtendienste
TAP	Technology Advisory Panel (UK)	Technischer Beirat der britischen Kontrollbehörde (IPCO)
TIB	Toetsingscommissie Inzet Bevoegdheden	Niederländisches Kontrollgremium, das den Einsatz von Überwachungsmaßnahmen prüft und genehmigt

Literatur

Administrative Office of the United States Courts. 2018. «Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017». http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf.

Agentur der Europäischen Union für Grundrechte. 2015. «Surveillance by Intelligence Services - Volume I: Member States' Legal Frameworks». http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services.

——.2017. «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update». http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega.

Anderson, David. 2015. «A Question of Trust: Report of the Investigatory Powers Review». London: Independent Reviewer. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

——.2016. «Report of the Bulk Powers Review». London: Independent Reviewer. https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review-report/.

——.2018. «New Approaches to Intelligence Oversight in the U.K.». *Lawfare* . 2. Januar 2018. https://www.lawfareblog.com/new-approaches-intelligence-oversight-uk.

Barker, Cat, Claire Petrie, Joanna Dawson, Samantha Godec, Pleasance Purser, und Holly Porteous. 2017. «Oversight of Intelligence Agencies: A Comparison of the 'Five Eyes' Nations». Parliamentary Library, Research Paper Series 2017-18. Parliament of Australia. Department of Parliamentary Services. http://apo.org.au/system/files/123831/apo-nid123831-515251.pdf.

Belgian Standing Intelligence Agencies Review Committee (Comiteri), Tilsynet med Efterretningstjenesterne (TET), Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), EOS-utvalget (EOS Gremium), Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND. 2016. «Rapport d'activité 2015». http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2015.pdf.

——.2018a. «Stärkung der Aufsicht über den internationalen Datenaustausch zwischen Nachrichten- und Sicherheitsdiensten». https://www.ab-nd.admin.ch/content/dam/ab-nd-internet/de/publications/2018-11-14%20Joint%20statement%20final%20DE.pdf.

——.2018b. «Activity Report 2016. Review Investigations, Control of Special Intelligence Methods and Recommendations». Brussels. http://www.comiteri.be/images/pdf/Jaarverslagen/Vast-Comit-I--Activity-Report-2016.PDF.

Bellovin, Steven M., Matt Blaze, Susan Landau, und Stephanie K. Pell. 2016. «It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law». *Harvard Journal of Law & Technology* 30 (1). https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf.

Bos-Ollermann, Hilde. 2017. «Mass Surveillance and Oversight». In: *Surveillance, Privacy and Trans-Atlantic Relations*, herausgegeben von David D. Cole, Federico Fabbrini, und Stephen J. Schulhofer. Hart Studies in Security and Justice, Volume 1. Oxford: Hart Publishing.

Bradford Franklin, Sharon. 2018. «Carpenter and the End of Bulk Surveillance of Americans». *Lawfare*. 25. Juli 2018. https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans.

Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, u. a. 2018. «The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Migration». https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf.

Bundesverfassungsgericht. 2005. «Leitsätze zum Urteil des Zweiten Senats vom 12. April 2005 (2 BvR 581/01)». https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2005/04/rs20050412_2bvr058101.pdf;jsessionid=969575C316AC611F8F71AAB2F6C75D6F.1_cid394?__blob=publicationFile&v=1.

Carey, Bjorn. 2016. «Stanford Computer Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information». *Stanford News*, 16. Mai 2016. https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/.

Chopin, Olivier. 2017. «Intelligence Reform and the Transformation of the State: The End of a French Exception». *Journal of Strategic Studies* 40 (4): 532–53. https://doi.org/10.1080/01402390.2017.1326100.

Clark, Charles S. 2018. «NSA Watchdog Breaks Precedent By Releasing Semi-Annual Report». *Government Executive*. 27. Juli 2018. https://www.govexec.com/management/2018/07/nsa-watchdog-breaks-precedent-releasing-semi-annual-report/150105/.

Commissie van Toezicht op de Inlichtingen-en Veiligheidsdiensten (CTIVD). 2015. «Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX». https://www.ctivd.nl/documenten/publicaties/2015/08/26/reactie-ctivd-conceptwetsvoorstel.

——.2016. «Review Report on the Implementation of Cooperation Criteria by the AIVD and the MIVD». CTIVD no. 48. https://english.ctivd.nl/documents/review-reports/2016/12/22/index48.

——.2017. «Kenniskring en tegenspraak CTIVD - Over CTIVD». 20. September 2017. https://www.ctivd.nl/over-ctivd/kenniskring--en-tegenspraak.

——.2018. «Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD». CTIVD No. 56. https://english.ctivd.nl/documents/review-reports/2018/04/24/index.

Commission nationale de contrôle des techniques de renseignement (CNCTR). 2016. «Premier rapport d'activité 2015/2016». https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf.

——.2018. «Deuxième Rapport d'activité 2017». https://www.cnctr.fr/_downloads/NP_CNCTR_2018_rapport_annuel_2017.pdf.

Conger, Kate. 2017. «An Unknown Tech Company Tried (and Failed) to Stop the NSA's Warrantless Spying». *Gizmodo*. 14. Juni 2017. https://gizmodo.com/an-unknown-tech-company-tried-and-failed-to-stop-the-1796111752.

Cook, Ben. 2017. «The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty». *American University Law Review* 66 (2, Article 5). http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1960&context=aulr.

Cranor, Lorrie Faith. 2008. «A Framework for Reasoning About the Human in the Loop». In *Proceedings of the 1st Conference on Usability, Psychology, and Security*. UPSEC'08. Berkeley, CA, USA: USENIX Association. http://dl.acm.org/citation.cfm?id=1387649.1387650.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). 2016. «Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041)». Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. https://www.bundestag.de/blob/459634/a09df397df-f6584a83a43a334f3936a3/18-4-660-data.pdf.

——.2017. «26. Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016». Bonn. https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.pdf?__blob=publicationFile&v=3.

Donohue, Laura K. 2017. «The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law». https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law.

Dorion, Pierre. 2008. «Data Deletion or Data Destruction?» *SearchDataBackup*. Juli 2008. https://searchdatabackup.techtarget.com/tip/Data-deletion-or-data-destruction.

Dreo Rodosek, Gabi. 2016. «Sachverständigengutachten. Beweisbeschluss SV-13, 1. Untersuchungsausschuss der 18. Wahlperiode», September, https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisation_rodosek.pdf.

Eijk, Nico van, und Cedric Ryngaert. 2017. «Expert Opinion - Legal basis for multilateral exchange of information». Appendix IV bij CTIVD rapport no. 56 to the review report on the multilateral exchange of data on (alleged) jihadists by the AIVD. Utrecht/Amsterdam. https://english.ctivd.nl/documents/review-reports/2018/04/24/appendix-iv.

Eijkman, Quirine, Nico van Eijk, und Robert van Schaik. 2018. «Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?» Institute for Information Law (IViR, University of Amsterdam). https://www.ivir.nl/publicaties/download/Wiv_2017.pdf.

Electronic Frontier Foundation. 2013. «Yahoo's Challenge to the Protect America Act in the Foreign Intelligence Court of Review». 22. Oktober 2013. https://www.eff.org/cases/yahoos-challenge-protect-america-act-foreign-intelligence-court-review.

Electrospaces.net. 2018. «Collection of Domestic Phone Records under the USA Freedom Act». 14. Juli 2018, https://electrospaces.blogspot.com/2018/07/collection-of-domestic-phone-records.html

EOS-utvalget Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS Gremium). 2016. «Dokument 16 (2015–2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)». Oslo. https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf

——.2018. «Annual Report 2017 - Document 7:1 (2017-2018)». Oslo. https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf.

Europäischer Gerichtshof. 2016. «C-203/15 Tele2 Sverige AB v Post-Och Telestyrelsen und C-698/15 SSHD v Tom Watson & Others». 16. Dezember 2016. http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=186492&occ=first&dir=&cid=406338.

Europäischer Gerichtshof für Menschenrechte. 2010. «Case of Kennedy v. The United Kingdom (Application No. 26839/05)». Straßburg.

——.2015. «Case of Roman Zakharov v. Russia (Application No. 47143/06)». Urteil. Straßburg. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]}.

——.2016. «Case of Szabó and Vissy v. Hungary (v. 37138/14)».12. Januar 2016. Straßburg. http://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf.

——.2018a. «Case of Paul Popescu v. Romania (Application No. 64162/10)». Straßburg. https://www.juridice.ro/wp-content/uploads/2018/02/CASE-OF-PAUL-POPESCU-v.-ROMANIA.pdf.

——.2018b. «Case of Centrum För Rättvisa v. Sweden (Application No. 35252/08)». Straßburg. http://www.statewatch.org/news/2018/jun/echr-sweden-Judgment-bulk-interception-communications-FULL.pdf.

Europäischer Gerichtshof für Menschenrechte und Europarat. 1978. «Case of Klass and Others v. Germany (Application No. 5029/71).» Straßburg. 6. September 1978. https://stewartroom.co.uk/wp-content/uploads/2014/07/Cases-ECHR-Klass.pdf.

——.2009. «Case of Iordachi and Others v. Moldova (Application No. 25198/02)». Straßburg. https://rm.coe.int/168067d212.

Europarat, Europäischer Menschenrechtskommissar 2015. «Democratic and Effective Oversight of National Security Services». Straßburg. https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb.

Farrell, Henry. 2016. «America's Founders Hated General Warrants. So Why Has the Government Resurrected Them?» *Washington Post*. 14. Juni 2016. https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/.

Federation of American Scientists. «Secrecy News 07/28/14», 28. Juli 2014, https://fas.org/sgp/news/secrecy/2014/07/072814.html.

Forcese, Craig. 2018. «Bill C-59 and the Judicalization of Intelligence Collection. Draft Working Paper 04-06-18». *Ottawa Faculty of Law Working Paper No. 2018-13*., 13.

Führungsunterstützungsbasis FUB. o. J. «Die Organisation der FUB - ZEO (Elektronische Operationen)». https://www.vtg.admin.ch/de/organisation/fub.html.

Gallagher, Ryan. 2016. «Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure». The Intercept. 7. Juni 2016. https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/.

Goldman, Zachary K., und Samuel J. Rascoff, Hrsg. 2016. *Global Intelligence Oversight. Governing Security in the Twenty-First Century*. Oxford: Oxford University Press.

Government Communications Headquarters (GCHQ). 2011. «HIMR Data Mining Research Problem Book». https://www.documentcloud.org/documents/2702948-Problem-Book-Redacted.html.

Government of France. o. J. «Groupement Interministériel de Contrôle (GIC)». *Gouvernement.fr*. Zugegriffen 20. Juni 2018. https://www.gouvernement.fr/groupement-interministeriel-de-controle-gic.

Graulich, Kurt. 2017. «Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und internationale Datenkooperation». *Kriminalpolitische Zeitschrift* 1: 43–52.

Greene, Robin. 2017. «A History of FISA Section 702 Compliance Violations». *New America*. 28. September 2017. https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/.

Hoadley, Daniel S., und Nathan J. Lucas. 2018. «Artificial Intelligence and National Security». Congressional Research Service. https://fas.org/sgp/crs/natsec/R45178.pdf.

Houwing, Lotte. 2018. «The Wiv 2017. A critical contemplation of the Act in an international context». https://www.burojansen.nl/pdf/2018-LotteHouwing-WivCriticalContemplation_final.pdf.

Huber, Berthold. 2017. «Kontrolle der Nachrichtendienste des Bundes - dargestellt am Beispiel der Tätigkeit der G10-Kommission». *Zeitschrift für das Gesamte Sicherheitsrecht*, Nr. 01. https://beck-online.beck.de/Dokument?vpath=bibdata%5Czeits%5CGSZ%5C2017%5Ccont-%5CGSZ.2017.H01.gl2.htm.

Human Rights Watch. 2017. «Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act». Human Rights Watch. 14. September 2017. https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance.

Inspector-General of Intelligence and Security of New Zealand. o. J. «About: The Intelligence and security agencies». Zugegriffen 21. August 2018. http://www.igis.govt.nz/about/.

International Network of Civil Liberties Organizations. 2018. «Unanswered questions - International Intelligence Sharing». https://www.inclo.net/pdf/iisp/unanswered_questions.pdf.

Investigatory Powers Commissioner's Office. 2018a. «IPCO Advisory Notice: Approval of Warrants, Authorisations and Notices by Judicial Commissioners». 01/2018. London. https://www.ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf.

——.2018b. «A message from the Commissioner By Sir Adrian Fulford». *IPCO Blog*. 17. Mai 2018. https://www.ipco.org.uk/Default.aspx?mid=16.1.

——.2018c. «IPC Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers», 23. Mai 2018. https://www.ipco.org.uk/docs/IPC_Submissions_on_bulk_powers.pdf.

Konkel, Frank. 2014. «The Details About the CIA's Deal with Amazon». *The Atlantic*, 17. Juli 2014. https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

Kris, David S., und J. Douglas Wilson. 2012. *National Security Investigations & Prosecutions 2d*. National Security Investigations & Prosecutions 2d 1. West. https://books.google.de/books?id=THYfMwEACAAJ.

Laperruque, Jake. 2018. «After ‹Foreign Surveillance› Law, Congress Must Demand Answers from Intelligence Community».The Hill, Januar 2018. https://thehill.com/opinion/cybersecurity/370271-after-foreign-surveillance-law-congress-must-demand-answers-from.

«Le Groupement interministériel de contrôle va beaucoup donner». 2016. *Defense - La voix du nord*. 1. Februar 2016. http://defense.blogs.lavoixdunord.fr/archive/2016/02/01/groupement-interministeriel-de-controle-14495.html.

Leigh, Ian, und Njord Wegge, Hrsg. 2018. *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*. 1 edition. Routledge.

Lubin, Asaf. 2017. «‚We Only Spy on Foreigners‘: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance». SSRN Scholarly Paper ID 3008428. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=3008428.

——.2018. «Legitimizing Foreign Mass Surveillance in the European Court of Human Rights». *Just Security*. 2. August 2018. https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.

Malgieri, Gianclaudio, und Paul De Hert. 2017. «European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards ‚Good Enough‘ Oversight, Preferably But Not Necessarily by Judges». In *Cambridge Handbook of Surveillance Law, Forthcoming 2017*, herausgegeben von D. Gray und S. Henderson. Rochester, NY: Social Science Research Network. https://papers.ssrn.com/abstract=2948270.

McKay, Simon. 2018. Blackstone's Guide to the Investigatory Powers Act 2016. Oxford, New York: Oxford University Press.

McKay, Simon, und Clive Walker. 2017. «Legal regulation of intelligence services in the United Kingdom». In *Handbuch des Rechts der Nachrichtendienste*. Stuttgart: Richard Boorberg.

Menn, Joseph. 2016. «Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources». *Reuters*, 5. Oktober 2016. https://www.reuters.com/article/us-yahoo-nsa-exclusive/yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 2016. «Memorie van Toelichting inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten». Kamerstuk. 28.

Oktober 2016. https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten.

——.2017. «Bijlage bij brief Wiv 2017 en regeerakkoord», 2017. https://www.aivd.nl/binaries/aivd_nl/documenten/kamerstukken/2017/12/15/kamerbrief-over-wiv-2017-en-het-regeerakkoord/20171215+Bijlage+bij+brief+minister+BZK+over+Wiv+2017+en+regeerakkoord.pdf.

Murray Daragh, Pete Fussey, und Maurice Sunkin. 2018. «Response to invitation for submissions on issues relevant to the proportionality of bulk powers». https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf.

National Security Agency/ Central Intelligence Agency. 2012. «(U)SIGINT Strategy 2012-2016». https://edwardsnowden.com/wp-content/uploads/2013/11/2012-2016-sigint-strategy-23-feb-12.pdf.

Necessary and Proportionate Coalition. 2014. «Necessary & Proportionate. International Principles on the Application of Human Rights to Communications Surveillance». https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.

Nyst, Carly. 2018. «Regulation of Big Data Surveillance by Police and Intelligence Agencies». The Human Rights, Big Data and Technology Project, University of Essex. https://1ing2s14id7e20wtc8xsceyr-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/Regulation-of-Big-Data-Surveillance-by-Police-and-Intelligence-Agencies.pdf.

Office of the Inspector-General of Intelligence and Security (Cheryl Gwyn). 2017. «Annual Report for the Year Ended 30 June 2017». Wellington. http://www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2017.pdf.

Office of the Inspector General National Security Agency (Wayne A. Stone). 2018. «Semiannual report to Congress. 1 October 2017 to 31 March 2018». https://www.dni.gov/files/documents/FOIA/OCT2017-MAR-2018_SAR_FINAL.PDF.

Ohm, Paul. 2010. «The Argument against Technology-Neutral Surveillance Laws», Nr. 88 Tex. L. Rev. 1685. https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr88&div=60&id=&page=.

Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). 2013. «The OECD Privacy Framework». https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, und Ronald Deibert. 2017. «Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017)». The Citizen Lab, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC). https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf.

Perry, Rodney M. 2014. «Intelligence Whistleblower Protections: In Brief». *Congressional Research Service*, Oktober. https://fas.org/sgp/crs/intel/R43765.pdf.

Privacy and Civil Liberties Oversight Board. 2014a. «Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court». https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

——.2014b. «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act».

Privacy International. 2018. «Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards». http://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global.

Reardon, Joel, Hubert Ritzdorf, David Basin, und Srdjan Capkun. 2013. «Secure Data Deletion from Persistent Media». In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13*, 271–84. Berlin, Germany: ACM Press. https://doi.org/10.1145/2508859.2516699.

Rechthien, Kay. 2016. «Sachverständigen-Gutachten gemäß Beweisbeschluss, 1. Untersuchungsausschuss (NSA-UA) der 18. Wahlperiode des Deutschen Bundestages», September. https://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf.

Renan, Daphna. 2016. «The Fourth Amendment as Administrative Governance». *Stanford Law Review*, Nr. 68 (Mai). http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2016/06/68_Renan_-_68_Stan._L._Rev._1039.pdf.

Richardson, Sophie, und Nicholas Gilmour. 2016. *Intelligence and Security Oversight. An Annotated Bibliography and Comparative Analysis*. Palgrave Macmillan. //www.palgrave.com/de/book/9783319302515.

Schaller, Christian. 2018. «Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden». *German Law Journal* 19 (4). https://static1.squarespace.com/static/56330ad3e4b0733dcc0c8495/t/5b5c85ff88251bab88673f2a/1532790273200/09+Vol_19_No_04_Schaller.pdf.

Security Intelligence Review Committee. 2018. «SIRC Annual Report 2017–2018: Building For Tomorrow: The Future Of Security Intelligence Accountability In Canada.» Ottawa. http://www.sirc-csars.gc.ca/anrran/2017-2018/index-eng.html.

Smith, Graham. 2016. «A Trim for Bulk Powers?» 7. September 2016. https://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html.

——.2018. «Illuminating the Investigatory Powers Act». *Cyberleagle*. 22. Februar 2018. https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html.

Statens inspektion för försvarsunderrättelseverksamheten (SIUN). 2018. «Årsredovisning för 2017». Stockholm. http://www.siun.se/dokument/Arsredovisning_2017.pdf.

Swire, Peter, Jesse Woo, und Deven R. Desai. 2018. «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft)».

The Chambers of Simon McKay. 2018. «Judical approval of warrants, authorisations and notices under the Investigatory Powers Act 2016: A review of the Investigatory Powers Commissioner's Office first Advisory Note». 2018. https://simonmckay.co.uk/judicial-approval-of-warrants-authorisations-and-notices-under-the-investigatory-powers-act-2016-a-review-of-the-investigatory-powers-commissioners-office-first-advisory-note/.

Tréguer, Félix. 2016a. «From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France», Oktober. https://halshs.archives-ouvertes.fr/halshs-01306332v11/document.

——.2016b. «French Constitutional Council Strikes Down “Blank Check" Provision in the 2015 Intelligence Act». *Verfassungsblog*. 26. Oktober. https://verfassungsblog.de/french-constitutional-council-strikes-down-blank-check-provision-in-the-2015-intelligence-act/.

UK Home Office. 2017. *Interception of Communications. Pursuant to Schedule 7 to the Investigatory Powers Act 2016. Draft Code of Practice*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf.

United States Foreign Intelligence Surveillance Court. 2010. «Rules of Procedure». Wahington D.C. http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

——.2014. «Memorandum opinion (Full title blackened)». https://www.aclu.org/sites/default/files/field_document/fisc_2014_opinion_re_702_provider_challenge.pdf.

Venedig-Kommission (Europäische Kommission für Demokratie durch Recht). 2015. «Report on the Democratic Oversight of Signals Intelligence Agencies.» http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e.

Wetzling, Thorsten, Hrsg. 2010. *Same myth, different celebration? Intelligence accountability in Germany and the United Kingdom*. Geneva: Graduate Institute of International and Development Studies.

——.2017a. «Options for More Effective Intelligence Oversight». *Discussion Paper*. https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.

——.2017b. «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficent Controls». Policy Brief. Berlin: Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

——.2017c. «New Rules for SIGINT Collection in Germany: A Look at the Recent Reform». *Lawfare*. 23. Juni 2017. https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform.

Wissenschaftlicher Dienst des Bundestags. 2017. «Kontrolle von Nachrichtendiensten bei Zusammenarbeit mit anderen Nachrichtendiensten im Ausland». WD 3-3000-072/17. Berlin: Deutscher Bundestag. https://www.bundestag.de/blob/508038/5a79b26ee2205e08171ee396ef87ae45/wd-3-072-17-pdf-data.pdf.

Wizner, Ben. 2017. «What changed after Snowden? A U.S. perspective». *International Journal of Communication* 11.

Zegart, Amy. 2011. «The Domestic Politics of Irrational Intelligence Oversight». *Political Science Quarterly* 126, no. 1: 1–25

Übersicht der zitierten Nachrichtendienstgesetze

Deutschland, *BND-Gesetz*, Gesetz über den Bundesnachrichtendienst, 20.12.1990 (letzte Änderung Juni 2017)

——, *Bundesverfassungsschutzgesetz*, Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, 20.12.1990 (letzte Änderung Juni 2017).

——, *Artikel 10-Gesetz*, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses 26.06. 2001 (letzte Änderung August 2017).

——, *Kontrollgremiumgesetz*, Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, 29.06.2009 (letzte Änderung Januar 2017).

Frankreich, Gesetz Nr. 2015-1556 zur internationalen Kommunikationsüberwachung (*loi n° 2015-1556 du 30 novembre 2015 relative au mesures de surveillance des communications électroniques internationales*), 30.11.2015.

——, Gesetzbuch zur inneren Sicherheit (*Code de la sécurité intérieure*), 2012 (letzte Änderung November 2018)

Großbritannien, Investigatory Powers Act 2016.

Kanada, Bill C-59: An Act respecting national security matters (2017), erste Lesung 20.06.2017 (derzeit im Antragsverfahren).

Neuseeland, Intelligence and Security Act 2017.

Niederlande, Gesetz über die Nachrichten- und Sicherheitsdienste 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*).

Norwegen, EOS-Kontrollgesetz (*Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrolloven)*), 03.02.1995 (letzte Änderung Juni 2017).

Schweiz, *Nachrichtendienstgesetz*, Bundesgesetz über den Nachrichtendienst, 25.09.2015 (letzte Änderung September 2017).

Vereinigte Staaten von Amerika, 50 U.S. Code § 1805 – Issuance of Order.

——, Executive Order 12333, 04.12.1981 (geändert 2003, 2004, 2008).

——, Executive Order 13526, 29.12.2009.

——, Foreign Intelligence Surveillance Act, 1978 (geändert 2008, 2011).

——, Foreign Intelligence Surveillance Court (FISC), Rules of Procedure, 01.11.2010.

——, Presidential Policy Directive/ PPD 28 - Signal Intelligence Activities, 17.01.2014.

——, *USA Freedom Act*, Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, 02.06.2015.

——, *US Patriot Act*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 26.10.2001.

——, *Wiretap Act*, 18 U.S. Code §§ 2510-2522

DEMOKRATIE
BAND 50

Massenüberwachung bändigen

Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich

Eine strenge Überwachungsgesetzgebung und eine wirksame Kontrolle der Nachrichtendienste könnten als Bollwerk gegen die Erosion der Grundrechte in unseren Demokratien dienen. Tatsächlich müssen die Regierungen aber regelmäßig von Gerichten wegen Fehlern in ihren Überwachungsgesetzen ermahnt werden. Zu Recht fordern die Gerichte strengere und wirksamere Schutz- und Kontrollmechanismen. Wie sollte eine effektive Aufsicht angesichts der raschen Entwicklung und der Komplexität der Überwachungstechnologie in der Praxis aussehen?

Diese Publikation von Thorsten Wetzling und Kilian Vieth fordert die Regierungen, die Kontrollbehörden und die Zivilgesellschaft auf, über die Landesgrenzen hinauszuschauen und sich von den in anderen Ländern bestehenden guten Praktiken, die hier präsentiert werden, inspirieren zu lassen.

ISBN 978-3-86928-195-7

Heinrich-Böll-Stiftung
Die grüne politische Stiftung

Schumannstraße 8, 10177 Berlin
030 285340 info@boell.de www.boell.de