

Überwachung durch Nachrichtendienste: Grundrechtsschutz und Rechtsbehelfe in der Europäischen Union

Zusammenfassung

Artikel 7 der Charta der Grundrechte der Europäischen Union gewährleistet allen Personen in der Europäischen Union (EU) das Recht auf Achtung ihres Privat- und Familienlebens, während Artikel 8 das Recht auf Schutz ihrer personenbezogenen Daten gewährleistet. Demnach dürfen diese Daten nur nach Treu und Glauben für festgelegte Zwecke verarbeitet werden. Außerdem hat jede Person das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. Ferner wird festgelegt, dass die Einhaltung dieser Vorschriften von einer unabhängigen Stelle überwacht wird. Artikel 47 sichert das Recht auf einen wirksamen Rechtsbehelf in einem fairen und öffentlichen Verfahren innerhalb einer angemessenen Frist.

Als die Medien im Juni 2013 weltweit begannen, die „Snowden-Dokumente“ zu veröffentlichen, wurde auch bekannt, dass Nachrichtendienste über umfangreiche globale Überwachungsprogramme verfügen. Die Snowden-Enthüllungen waren jedoch nicht die ersten Hinweise auf Programme zur groß angelegten Kommunikationsüberwachung, die nach den Anschlägen vom 11. September 2001 eingerichtet wurden. Das Ausmaß dieser Enthüllungen bleibt jedoch beispiellos und wirkt sich möglicherweise auf die Privatsphäre der Menschen auf der ganzen Welt aus. Die Überwachung zielt nicht mehr nur auf Staats- oder Geschäftsgeheimnisse ab, sondern erlaubt auch das umfassende Abhören privater Kommunikation. Dies verletzt sowohl das Recht auf Achtung des Privat- und Familienlebens der Personen als auch das Recht auf den Schutz personenbezogener Daten. Beide Rechte werden auf EU-Ebene durch die Charta der Grundrechte der Europäischen Union (EU-Grundrechtecharta) garantiert. Auch in

Bezug auf Überwachungstätigkeiten sind die EU und ihre Mitgliedstaaten zum Schutz dieser Rechte verpflichtet. Außerdem müssen betroffenen Menschen Rechtsbehelfe zur Anfechtung rechtswidriger Überwachung zur Verfügung gestellt werden.

„Eine solche massenhafte und ungezielte Überwachung ist naturgemäß unverhältnismäßig und stellt einen ungerechtfertigten Eingriff in die durch die Art. 7 und 8 der Charta garantierten Rechte dar.“

(EuGH, C-362/14, Maximilian Schrems gegen Data Protection Commissioner, Schlussanträge des Generalanwalts, 23. September 2015)

Die Snowden-Enthüllungen hatten eine Reihe von Reaktionen zur Folge. In der Welt der Nachrichtendienste, insbesondere in den für die Überwachung der Nachrichtendienste zuständigen Fachgremien, wurden die Auswirkungen der Enthüllungen in eingehenden Ermittlungen und Sonderberichten weiter untersucht. Die EU-Organe haben mit Entschlossenheit reagiert. Die Europäische Kommission, der Rat der Europäischen Union und das Europäische Parlament berichteten alle über die Enthüllungen, äußerten Besorgnis über die Massenüberwachungsprogramme, baten die US-Behörden um Klarstellung und arbeiteten an einer „Wiederherstellung des Vertrauens“ in den Beziehungen zwischen den Vereinigten Staaten und der EU. Auch wenn es für eine vollständige Beurteilung der Auswirkungen der Snowden-Enthüllungen noch zu früh ist, zeigten im Anschluss an die Enthüllungen in einigen EU-Mitgliedstaaten durchgeführte Untersuchungen, dass die derzeitigen nationalen Rechtsrahmen reformiert werden müssen. Das Europäische Parlament bekräftigte dies in seiner Entschließung vom März 2014 zu dem „Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren

Mitgliedstaaten und den entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres“ (2013/2188(INI), P7_TA (2014)0230), mit der ein *europäischer digitaler Habeas-Corpus-Grundsatz* eingeführt wurde.

„Die Snowden-Enthüllungen gaben uns die Gelegenheit, endlich zu handeln. Ich hoffe, wir werden daraus etwas Positives und Dauerhaftes machen, das auch in der nächsten Legislaturperiode Bestand haben wird – eine Datenschutz-Grundrechtecharta, auf die wir stolz sein können.“

(Claude Moraes, MdEP, Berichterstatter in der NSA-Untersuchung durch das EP, Pressemitteilung, 12. März 2014)

Überwachungsmaßnahmen: Überblick über die Rechtsrahmen der EU-Mitgliedstaaten

Im April 2014 forderte das Europäische Parlament die Agentur der Europäischen Union für Grundrechte (FRA) auf, eine eingehende Untersuchung zum Schutz der Grundrechte im Zusammenhang mit der Überwachung durchzuführen. Dieser Aufforderung kam die FRA nach und stellte einen Überblick über die gültigen Rechtsrahmen von Überwachungstätigkeiten in den 28 EU-Mitgliedstaaten zusammen sowie eine Übersicht über die bestehenden Grundrechtsnormen. Die FRA-Studie konzentrierte sich auf vorhandene Aufsichtsmechanismen und Rechtsbehelfen, die Personen, die Verletzungen ihrer Privatsphäre vermuten, zur Verfügung stehen.

Die Überwachungstechniken als solche wurden im Rahmen dieser Studie nicht überprüft, nur inwieweit die derzeitigen Rechtsrahmen die Anwendung solcher Techniken erlauben. Weiterhin wurde die Rolle von Fachgremien bei der Überwachung der Tätigkeiten der Nachrichtendienste untersucht und geprüft, inwieweit die entsprechenden Schutzbestimmungen

in den 28 EU-Mitgliedstaaten zum Schutz von Privatsphäre und Daten beitragen.

„Nachrichtendienste“ haben einen außenpolitischen Auftrag und konzentrieren sich auf externe Bedrohungen, während „Sicherheitsdienste“ einen innenpolitischen Auftrag haben und sich auf nationale Bedrohungen konzentrieren. Die FRA verwendet für beide Begriffe die Sammelbezeichnung „Nachrichtendienste.“

Diese Zusammenfassung stellt die wichtigsten Untersuchungsergebnisse der FRA dar. Der vollständige Bericht zum Grundrechtsschutz und zu Rechtsbehelfen hinsichtlich von Überwachungstätigkeiten wurde auf Englisch unter dem Titel *„Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States’ legal frameworks“* veröffentlicht (siehe Weitere Informationen).

Datenerhebung und Erfassungsbereich

Für diese Studie hat die FRA die gültigen Rechtsrahmen für Überwachungstätigkeiten in den 28 EU-Mitgliedstaaten untersucht sowie die Rechtsvorschriften und einschlägigen Grundrechtsnormen analysiert, um eine vergleichende Analyse der Rechtslage im Bereich der Überwachung für die gesamte EU vorzulegen.

Anhand der Antworten, die das multidisziplinäre Forschungsnetz der FRA, Franet, zur Verfügung stellte, wurden mittels Sekundärforschung Daten und Informationen in allen 28 EU-Mitgliedstaaten erhoben. Weitere Informationen wurden durch den

Austausch mit den wichtigen Partnern eingeholt, wie nationale Verbindungsbeamte und -beamtinnen der FRA in den Mitgliedstaaten, Fachgremien und einzelnen Datenschutzexperten. Die hier vorgelegten Ergebnisse basieren auf bestehenden Berichten und Veröffentlichungen, die nationale Gesetzgeber dabei unterstützen sollen, Rechtsrahmen für die Nachrichtendienste und deren demokratische Kontrolle zu schaffen.

Ein zweiter sozial- und rechtswissenschaftlicher Bericht mit Stellungnahmen der FRA, die auf empirischen Untersuchungen basieren, wird zu einem späteren Zeitpunkt veröffentlicht und sich eingehender mit den hier dargelegten Ergebnissen befassen.



Schutz der Grundrechte und EU-Recht

„Die bittere Wahrheit ist, dass die Verwendung von Massenüberwachungstechnologien das gesamte Recht auf Privatsphäre im Bereich von Kommunikationen im Internet effektiv beseitigt.“

(Vereinte Nationen (UN), Bericht des Sonderberichterstatters über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus (2014), Vierter Jahresbericht, der der Generalversammlung vorgelegt wurde, A/69/397, 23. September 2014)

Die EU-Mitgliedstaaten sind alle an internationale menschenrechtliche Mindeststandards gebunden, die von den Vereinten Nationen (UN) entwickelt wurden und allgemein verbindlich sind, wie beispielsweise die Resolution des Menschenrechtsrats zum Recht auf Privatsphäre im digitalen Zeitalter (Dok. A/HRC/28/L.27, 24. März 2015). Nach den Snowden-Enthüllungen wurden Massenüberwachungspraktiken von zahlreichen UN-Experten-gremien und Vertragsorganen verurteilt. Auch in den Standards des Europarats, einschließlich der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR), sind Mindeststandards enthalten. EU-Rechtsvorschriften, wie sie vom Gerichtshof der Europäischen Union (EuGH) ausgelegt werden, sind ebenfalls relevant. Letztendlich spielen in einem Bereich, in dem nur eingeschränkte internationale Verordnungen – mit Ausnahme von bestehenden internationalen Menschenrechten – unmittelbar angewendet werden, auch Selbstregulierungsmaßnahmen und unverbindliches Recht („soft law“) eine wichtige Rolle.

Der Bericht konzentriert sich auf die Rechte auf Privatsphäre und Datenschutz, die in Artikel 7 und 8 der EU-Grundrechtecharta verankert sind. Das Recht auf Datenschutz ist auch im Primär- und Sekundärrecht der EU festgelegt und gewährleistet, dass die Verarbeitung personenbezogener Daten in ihrem jeweiligen Anwendungsbereich rechtmäßig ist und nur soweit durchgeführt wird, wie sie zur Erfüllung des verfolgten legitimen Zwecks erforderlich ist. Diese Rechte gelten für alle Personen, unabhängig davon, ob es sich um Bürger der EU oder Drittstaatenangehörige handelt. Nach Artikel 52 Absatz 1 der EU-Grundrechtecharta muss jede Einschränkung notwendig und verhältnismäßig sein, den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen tatsächlich entsprechen, gesetzlich vorgeschrieben sein und den Wesensgehalt dieser Rechte achten.

Trotz bestehender internationaler Leitlinien wird „nationale Sicherheit“ in den verschiedenen EU-Mitgliedstaaten unterschiedlich ausgelegt. Dieses Konzept wird weder in der EU-Gesetzgebung noch in der Rechtsprechung des EuGH näher definiert, obwohl

laut EuGH Grundrechtseinschränkungen eng ausgelegt und gerechtfertigt sein müssen.

Diese unklare Beschreibung von „nationaler Sicherheit“ wirkt sich auf die Anwendbarkeit des EU-Rechts aus. Nach Artikel 4 Absatz 2 des Vertrages über die Europäische Union fällt „die nationale Sicherheit [...] in die alleinige Verantwortung der einzelnen Mitgliedstaaten.“ Dies bedeutet nicht, dass das EU-Recht im Falle von „nationaler Sicherheit“ gänzlich unanwendbar ist. Die Auslegung von „nationaler Sicherheit“ auf Ebene der Mitgliedstaaten und die Art und Weise wie Überwachungsprogramme durchgeführt werden, kann von den EU-Organen, insbesondere vom EuGH, bewertet werden.

Überwachungsarten: gezielte und ungezielte Überwachung

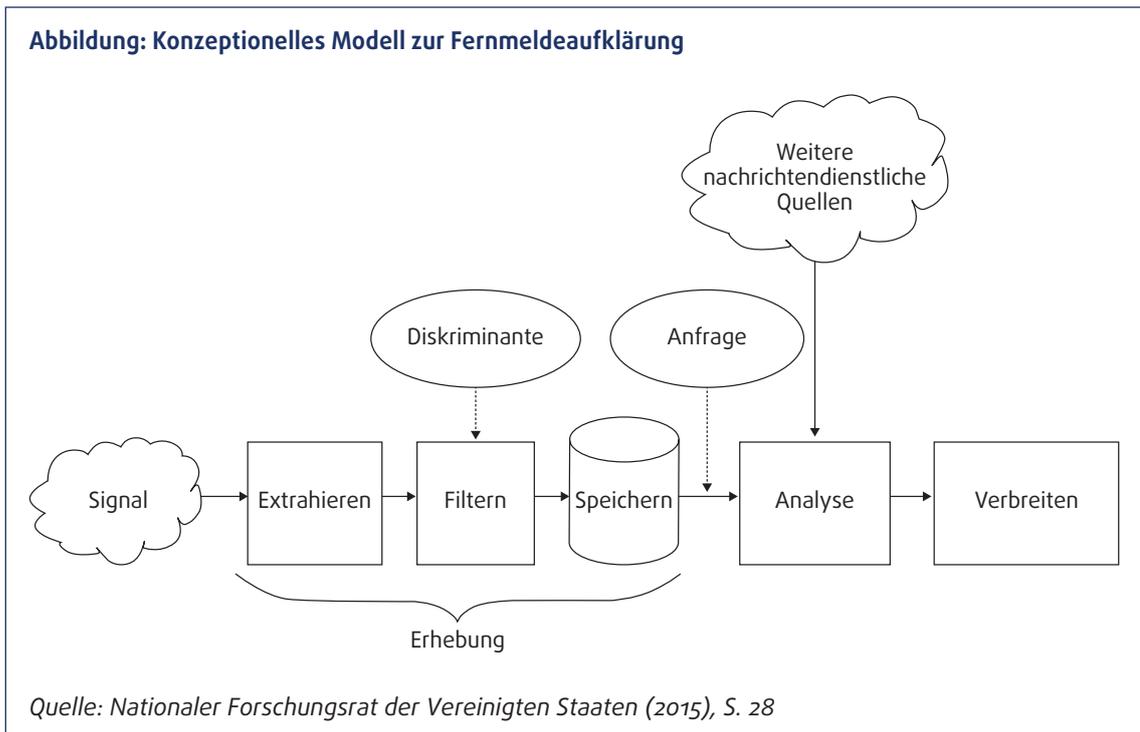
Die FRA-Studie geht darauf ein, wie gezielte und ungezielte Überwachung in den Rechtsrahmen der EU-Mitgliedstaaten organisiert ist.

Das niederländische Kontrollgremium für Nachrichten- und Sicherheitsdienste (CTIVD) definiert gezielte und ungezielte Überwachung wie folgt:

- Die gezielte Überwachung bezieht sich auf „eine Überwachung, bei der die Person, die Organisation oder die technischen Eigenschaften, über die Daten erhoben werden, im Voraus spezifiziert werden kann/können“;
- Die ungezielte Überwachung bezieht sich auf „eine Überwachung, bei der die Person, die Organisation oder die technischen Eigenschaften, über die Daten erhoben werden, nicht im Voraus spezifiziert werden kann/können.“

CTIVD, *Jahresbericht 2013-2014*, Den Haag, 31. März 2014, S. 45-46

Der enorme Umfang, der durch die bekannt gewordenen Überwachungsprogramme, wie beispielsweise PRISM, Xkeyscore und Upstream, erhobenen Daten, löste weitreichende Reaktionen aus. „Massenüberwachung“ (häufig als ungezielte Überwachung verstanden) umfasst die Erfassung von großen Mengen verschiedener Daten mit traditionellen, geheimen (gezielten) Überwachungsmethoden, wie beispielsweise mittels Telefonüberwachung. Letztere wird angewandt, wenn ein vorheriger Verdacht bezüglich einer bestimmten Person oder Organisation besteht. Diese Art von Überwachung ist in den



Gesetzen der EU-Mitgliedstaaten weit verbreitet und anerkannt. Innerhalb der meisten Rechtsrahmen der EU-Mitgliedstaaten ist die „Massenüberwachung“ weder reguliert, geschweige denn als solche bezeichnet. Lediglich in einigen EU-Mitgliedstaaten gibt es detaillierte Rechtsvorschriften zur Fernmelde- oder elektronischen Aufklärung (Signals Intelligence, SIGINT). Hierbei handelt es sich um den Oberbegriff, der verwendet wird, um das Abfangen von Signalen verschiedener Quellen durch die Nachrichtendienste zu beschreiben. FRA verwendet in der gesamten Analyse den Begriff Fernmelde- oder elektronische Aufklärung.

SIGINT stammt von den militärischen Nachrichtendiensten. Der Begriff bezieht sich auf das automatische Sammeln von Informationen durch die Überwachung und Erhebung digitaler Daten im Zusammenhang mit nachrichtendienstlichen Aktivitäten. Die Abbildung zeigt, dass die gesammelten Signale mithilfe von Diskriminanten oder Selektoren gefiltert werden. Hierbei handelt es sich um einen Satz an Parametern, der entweder a priori oder dynamisch in den Filterprozess eingesetzt wird, um die Kriterien zu definieren, nach denen bestimmt wird, welche Daten zum Erhalt der relevanten Informationen gespeichert werden müssen (zum Beispiel „alle E-Mail-Adressen, die bei der Kommunikation mit dem Jemen verwendet werden“).

Für den Nationalen Forschungsrat der Nationalen Akademien der Vereinigten Staaten ist Fernmelde- oder elektronische Aufklärung der Sammelbegriff

für alle Daten, die auf einem elektronischen Gerät gespeichert werden. Die Venedig-Kommission verwendet SIGINT als Sammelbegriff für Mittel und Methoden zur Überwachung und Analyse von Kommunikationen über Radio (einschließlich Satelliten- und Mobiltelefon) und Kabel.

Die FRA-Analyse der Rechtsrahmen, die die Überwachungsmethoden der Nachrichtendienste regeln, zeigt, dass die Rechtsvorschriften von fünf EU-Mitgliedstaaten (Deutschland, Frankreich, Niederlande, Schweden und das Vereinigte Königreich) die Bedingungen für die Verwendung gezielter und ungezielter Überwachung genau festlegen. Hierzu zählt auch die Fernmelde- oder elektronische Aufklärung. Andere Mitgliedstaaten legen diese Bestimmungen nur unzureichend fest, was eine rechtliche Analyse der genauen Vorgehensweise erschwert, mit der die Erhebung mittels Fernmelde- oder elektronischer Aufklärung durchgeführt wird. Obgleich sich die Rechtsvorschriften dieser Länder nicht konkret darauf beziehen, kann SIGINT dennoch durchgeführt werden. Da diese Vorgehensweise jedoch nur in den unveröffentlichten Regulierungsmaßnahmen dieser Länder vorgeschrieben ist, würde eine Analyse der anwendbaren Rechtsrahmen diesbezüglich keine Klarheit schaffen.

Wichtigste Ergebnisse

Nachrichtendienste und Überwachungsgesetze

Zielsetzung und Organisationsstruktur der Nachrichtendienste

Das Kernziel der Nachrichtendienste demokratischer Gesellschaften ist der Schutz der nationalen Sicherheit und der grundlegenden Werte einer offenen Gesellschaft unter Verwendung von nachrichtendienstlichen Instrumenten. Die Organisation der Nachrichtendienste in den einzelnen EU-Mitgliedstaaten ist eng mit den länderspezifischen geschichtlichen Entwicklungen verbunden und richtet sich nicht zwingend nach den Grundrechtsnormen. Infolgedessen sind die Nachrichtendienste der einzelnen EU-Mitgliedstaaten auf unterschiedlichste Art und Weise aufgebaut. In einigen Mitgliedstaaten wird die Arbeit von zwei Nachrichtendiensten durchgeführt, während in anderen Mitgliedstaaten fünf oder sechs Organe zuständig sind.

- In nahezu allen EU-Mitgliedstaaten wurden mindestens zwei verschiedene Nachrichtendienstorgane eingerichtet, wobei ein Organ für Zivilsachen und das andere für militärische Belange zuständig ist. Letzteres ist nicht Gegenstand dieses Berichts. Die zivilen Nachrichtendienste unterstehen gemeinhin den Innenministerien, gelegentlich aber auch dem Staatsoberhaupt (PremierministerIn oder PräsidentIn).
- In einigen Mitgliedstaaten sind die zivilen Nachrichtendienste weiter untergliedert in einen Dienst mit innenpolitischem und einen Dienst mit außenpolitischem Auftrag. Darüber hinaus haben manche Mitgliedstaaten staatliche Organe, die auf besondere Bedrohungen wie etwa organisiertes Verbrechen, Korruption oder Terrorismusbekämpfung spezialisiert sind, mit nachrichtendienstlichen Maßnahmen betraut.

Schutz der nationalen Sicherheit

Im Rahmen der FRA-Studie wird das Konzept der „nationalen Sicherheit“ im Zusammenhang mit dem Auftrag der Nachrichtendienste und den von ihnen möglicherweise ausgeführten Überwachungsmaßnahmen analysiert. Abermals zeigen die Ergebnisse, wie groß die Unterschiede zwischen den EU-Mitgliedstaaten sind.

- Nachrichtendienste befassen sich primär mit dem Schutz der nationalen Sicherheit, wobei die EU-Mitgliedstaaten darunter nicht alle dasselbe verstehen. Der Umfang dessen, was nationalen Sicherheit bedeutet, ist selten festgelegt, allerdings werden bisweilen ähnliche Begriffe verwendet. Manche Mitgliedstaaten verwenden den Begriff „nationale Sicherheit“ überhaupt nicht, sondern verweisen auf die „innere Sicherheit“ und/oder „äußere Sicherheit“ oder auch die „Sicherheit des Staates“.
- Die verschiedenen Aufgabenbereiche der Nachrichtendienste (d. h. ihres Auftrags) sind nicht identisch in allen EU-Mitgliedstaaten. Zusätzlich zu den herkömmlicheren Einsatzgebieten umfassen die Aufträge einiger Nachrichtendienste die Bekämpfung des organisierten Verbrechens und der Internetkriminalität. Diese Begriffe sind jedoch nicht einheitlich festgelegt.

Gesetzliche Regelung der Überwachung

Bisweilen gibt es keine eindeutige Abgrenzung zwischen den Aufgaben der Strafverfolgungsbehörden und den Aufgaben der Nachrichtendienste. Ausweitungen der Aufgaben dürfen nur vorgenommen werden, wenn ordnungsgemäß nachgewiesen wird, dass dies dem Schutz des Staates dient. Dies ist auch der eigentliche Grund für die Einrichtung von Nachrichtendiensten.

- In den meisten Mitgliedstaaten regulieren die Rechtsrahmen nur die gezielte Überwachung, entweder von Einzelpersonen oder von bestimmten Gruppen oder Organisationen. Neben der Regelung der gezielten Überwachung wurden von fünf Mitgliedstaaten detaillierte Gesetze über die Bedingungen der Verwendung der Fernmelde- oder elektronischen Aufklärung erlassen.
- Bei Betrachtung der geltenden Menschenrechtsstandards ist ersichtlich, dass den nationalen Rechtsrahmen klare Definitionen fehlen, in denen Personengruppen und Tätigkeitsbereiche aufgeführt werden, über die möglicherweise Informationen gesammelt werden.
- Die Organisation und Tätigkeiten der Nachrichtendienste sind in der überwiegenden Mehrzahl der Mitgliedstaaten gesetzlich geregelt (26 von 28). Rechtsvorschriften regeln die Organisation und Arbeitsweise der Nachrichtendienste der Länder. In einem Mitgliedstaat ist dem Nachrichtendienst laut Verfassung die Durchführung

von Überwachungsmaßnahmen untersagt. Ein weiterer Mitgliedstaat befindet sich im Gesetzgebungsprozess zur Reglementierung der Überwachungspraktiken seiner Nachrichtendienste.

- Die Analyse der FRA zeigt, dass die Rechtsgrundlage, die die Aufträge und Befugnisse nationaler Nachrichtendienste in den EU-Mitgliedstaaten festlegt stark variiert. Sie kann von einem einzigen Rechtsakt, der die Organisation und Mittel der nationalen Nachrichtendienste regelt, bis hin zu einem komplexen Rechtsrahmen bestehend aus verschiedenen Gesetzen und Verordnungen reichen. Diese wiederum regeln bestimmte Aspekte wie den Auftrag, die Organisation, die Kompetenzen und Mittel der Nachrichtendienste.
- In den meisten Mitgliedstaaten sind die Tätigkeiten der Nachrichtendienste durch zwei Gesetze reglementiert: ein Gesetz über den Auftrag und die Organisation des Nachrichtendienstes und ein Gesetz über die Handlungsmittel und die Bedingungen zu deren Verwendung.
- In den meisten EU-Mitgliedstaaten (23 von 28) sind die Nachrichtendienste und die Strafverfolgungsbehörden voneinander getrennt. Zwei Mitgliedstaaten haben sich vor kurzem von Systemen entfernt, in denen die Nachrichtendienste der Polizei oder ähnlichen Strafverfolgungsbehörden angehörten.

Kontrolle der Nachrichtendienste

In der Analyse der FRA werden die Mechanismen der Rechenschaftspflicht im Zusammenhang mit der Überwachung durch Nachrichtendienste untersucht. Insbesondere wird erläutert, wie von den EU-Mitgliedstaaten Aufsichtsmechanismen eingerichtet wurden. Die Kontrolle ist ein Mittel zur Gewährleistung der öffentlichen Rechenschaftspflicht für die Entscheidungen und Handlungen der Nachrichtendienste. Laut Experten ist das Ziel der Kontrolle, einen Missbrauch von Befugnissen zu vermeiden, die Ausübung von weitreichenderen Befugnissen zu legitimieren und ein verbessertes Ergebnis nach einer Evaluierung bestimmter Handlungen zu erzielen. Gemäß dem allgemeinen Konsens des Berichts der Venedig-Kommission und anderen wissenschaftlichen Untersuchungen, sollte die Kontrolle eine Kombination aus folgenden Punkten sein:

- Durchführungskontrolle;
- Parlamentarische Kontrolle;

- Expertengremien;
- Gerichtliche Überprüfung.

Durchführungskontrolle und Koordinierung zwischen Aufsichtsgremien

Die Exekutive kann die Nachrichtendienste auf verschiedene Weise kontrollieren: durch die Bestimmung ihrer strategischen Zielsetzungen und Prioritäten oder die Vorgabe von Leitlinien, durch die Nominierung und/oder Ernennung des Führungsstabs des Nachrichtendienstes, durch die Aufstellung des Haushaltsplans, über den das Parlament letztendlich abstimmen wird, oder durch die Genehmigung der Zusammenarbeit mit anderen Diensten. In manchen Mitgliedstaaten spielt die Exekutive zudem eine wichtige Rolle bei der Autorisierung von Überwachungsmaßnahmen.

Zur wirksamen Kontrolle ist eine gute Koordinierung zwischen den verschiedenen Aufsichtsgremien erforderlich, um die Abdeckung aller Aspekte der Tätigkeiten der Nachrichtendienste zu gewährleisten. Besitzen die Aufsichtsgremien kein klares, umfassendes Verständnis der Tätigkeiten aller nationalen Nachrichtendienste, zieht dies Kontrolllücken nach sich und die Wirksamkeit des Aufsichtssystems als Ganzes wird gehemmt.

- Aufgrund der unterschiedlichen Politik und Rechtssysteme in den EU-Mitgliedstaaten gibt es eine Vielzahl an Organen die für die Aufsicht der Nachrichtendienste zuständig sind. Die EU-Mitgliedstaaten verfügen über äußerst unterschiedliche Aufsichtssysteme. Auch wenn aus den bewährten Praktiken bestehender Systeme Nutzen gezogen werden kann, würden einzelne Bereiche von einer Rechtsreform, die die Befugnisse der Aufsichtsgremien erweitert, profitieren.
- Den unterschiedlichen Aufsichtsgremien wird eine große Vielfalt an Befugnissen zugesprochen, und auch der Umfang der Befugnisausübung variiert.
- Sieben Mitgliedstaaten verfügen über Aufsichtssysteme, die die Exekutive, das Parlament sowie die Justizbehörden (mittels vorherige Genehmigung) und Expertengremien vereinen. Zu diesen zählt jedoch keines der Länder mit einem Rechtsrahmen, das die Informationsbeschaffung durch Fernmelde- oder elektronische Aufklärung gestattet.

- Für eine wirksame Aufsicht sind nicht notwendigerweise alle vier Arten von Aufsichtsmechanismen erforderlich. Eine derartige Aufsicht kann erreicht werden, solange sich die vorhandenen Stellen ergänzen und in ihrer Gesamtheit ein starkes System bilden, das einschätzen kann, ob der Auftrag der Nachrichtendienste ordnungsgemäß ausgeführt wird. Dies ist dann der Fall, wenn die Aufsichtsbefugnisse alle Tätigkeitsbereiche eines Nachrichtendienstes abdecken. Ist der Auftrag selbst jedoch unklar oder unzureichend definiert, ist es den Aufsichtsgremien nicht möglich, Einfluss zu nehmen.
- Der Zugriff der Aufsichtsgremien auf Informationen und Dokumente ist unerlässlich. Während die von den Nachrichtendiensten gesammelten Informationen vertraulich sind und durch Sicherheitsvorkehrungen gewährleistet werden muss, dass sie dementsprechend behandelt werden, können die Aufsichtsgremien ihre Aufgaben nur ausführen, wenn sie zunächst Zugang zu allen relevanten Informationen haben. Das Gegenteil scheint jedoch die Norm zu sein.

Parlamentarische Kontrolle

Die parlamentarische Kontrolle ist angesichts der Aufgabe des Parlaments, die Regierung zur Verantwortung zu ziehen, von großer Bedeutung. Das Parlament als Gesetzgeber ist für den Erlass eindeutiger, zugänglicher Rechtsvorschriften zur Etablierung von Nachrichtendiensten und Festlegung ihrer Organisation, besonderen Befugnisse und Beschränkungen verantwortlich. Auch obliegt es der Verantwortung des Parlaments, den Haushaltsplan der Nachrichtendienste zu genehmigen, und in manchen Mitgliedstaaten zu prüfen, ob die Tätigkeiten der Nachrichtendienste dem Rechtsrahmen entsprechen.

- Die Ergebnisse der FRA zeigen, dass in 24 EU-Mitgliedstaaten eine parlamentarische Kontrolle erfolgt. In 21 dieser Mitgliedstaaten werden die Nachrichtendienste von Parlamentsfachausschüssen beaufsichtigt. Einige Mitgliedstaaten haben einen für unterschiedliche Sicherheits- und Nachrichtendienste zuständigen Parlamentsausschuss eingerichtet, während andere verschiedene Ausschüsse etabliert haben, die sich gesondert mit den Diensten befassen.
- Keinem Parlamentsausschuss eines Mitgliedstaates wird der uneingeschränkte Zugang zu nachrichtendienstlichen Informationen gewährt.
- Die verschiedenen Parlamentsausschüsse der Mitgliedstaaten haben unterschiedliche Aufträge: die meisten Ausschüsse besitzen die herkömmlichen Aufsichtsbefugnisse hinsichtlich

der Gesetzgebung, dem Haushaltsplan und dem Erhalt von Informationen über die Tätigkeit der Dienste, während nur wenige Ausschüsse Beschwerden untersuchen, verbindliche Entscheidungen zu den Nachrichtendiensten treffen oder Unterstützung bei der Genehmigung von Überwachungsmaßnahmen leisten dürfen.

- Hinsichtlich der Befugnis der Parlamentsausschüsse zur Einleitung von Ermittlungen sind diese Ausschüsse laut den Gesetzen der Mehrheit an EU Mitgliedsstaaten berechtigt, Nachrichtendienste oder die Exekutive um Informationen zu ersuchen. Sie haben jedoch nicht das Recht, deren Vorlage zu verlangen.

Aufsicht durch Expertengremien

Die Aufsicht durch Expertengremien ist besonders nützlich, da die mit der Materie vertrauten Einzelpersonen Zeit haben sich mit diesem Thema zu befassen und frei von politischen Affinitäten sind. Dies ermöglicht eine eingehende Prüfung der Tätigkeiten der Nachrichtendienste. Dem Menschenrechtskommissar des Europarates zufolge eignen sich solche Expertengremien häufig am besten, um die operativen Tätigkeiten der Sicherheits- und Nachrichtendienste zu beaufsichtigen.

- Wenn auch die parlamentarische Kontrolle äußerst wichtig ist, muss sie durch andere Aufsichtsgremien ergänzt werden, insbesondere durch starke Expertengremien, die die operativen Tätigkeiten überwachen können. Hierzu zählen unter anderem die Erhebung, der Austausch und die Nutzung personenbezogener Daten sowie die Achtung des Rechts auf Privatleben.
- Innerhalb der EU haben 15 Mitgliedstaaten ein oder mehrere Expertengremien, die sich ausschließlich der Beaufsichtigung der Nachrichtendienste widmen, eingerichtet. Ihre Kompetenzen umfassen die Autorisierung von Überwachungsmaßnahmen, Untersuchung von Beschwerden, Anforderung von Dokumenten und Informationen von den Nachrichtendiensten und Beratung der Exekutive und/oder des Parlaments. Um ihr Potenzial voll auszuschöpfen, muss ihnen eine angemessene Unabhängigkeit gewährt, Ressourcen bereitgestellt und Befugnisse erteilt werden.
- In manchen Mitgliedstaaten sind keine Institutionen, die von den Nachrichtendiensten und der Exekutive unabhängig sind, an der Autorisierung von Überwachungsmaßnahmen beteiligt.
- In Mitgliedstaaten, in denen eine unabhängige Behörde Überwachungsmaßnahmen autorisiert, ist für eine gezielte Überwachung meist eine

gerichtliche Zustimmung erforderlich, wobei die Genehmigung durch Expertengremien die alternative, bevorzugte Lösung ist. Es gibt keinen gemeinsamen Ansatz zur Kontrolle der Informationsbeschaffung durch Fernmelde- oder elektronische Aufklärung.

- Neben dem unerlässlichen Verständnis der rechtlichen Aspekte der Überwachung, müssen die Expertengremien auch über technische Kompetenzen verfügen. Manche Mitgliedstaaten stellen dies sicher, indem sie Experten verschiedener Fachrichtungen, einschließlich der Informations- und Kommunikationstechnologien (IKT), einbeziehen. Andere vertrauen in hohem Maße auf eine Kombination aus derzeitigen oder ehemaligen Richtern und Abgeordneten.

Die EU-Mitgliedstaaten haben den Datenschutzbehörden (Data Protection Authorities, DPA) – sogenannte Fachgremien zur Wahrung der Privatsphäre und Gewährleistung des Datenschutzes – eine entscheidende Rolle für den Schutz personenbezogener Daten zugewiesen. Diese Rolle ist im europäischen Primär- und Sekundärrecht verankert. Die auf die Überwachung von Nachrichtendiensten spezialisierten Expertengremien verfügen jedoch zweifellos über anerkanntes Fachwissen zum Schutz der Privatsphäre und Gewährleistung des Datenschutzes im nachrichtendienstlichen Bereich.

- Die Ergebnisse der FRA zeigen, dass die Datenschutzbehörden in sieben Mitgliedstaaten gegenüber den Nachrichtendiensten dieselben Befugnisse haben wie gegenüber allen anderen Verantwortlichen für die Verarbeitung von Daten. Dies gilt auch im Vergleich zu anderen Datenverarbeitungstätigkeiten und den für die Verarbeitung von Daten Verantwortlichen des öffentlichen und privaten Sektors. In 12 Mitgliedstaaten besitzen die Datenschutzbehörden keine Zuständigkeiten im Bereich der Nachrichtendienste. In neun Mitgliedstaaten sind ihre Befugnisse beschränkt.
- In Mitgliedstaaten, in denen sich die Datenschutzbehörden und andere sachkundige Aufsichtsgremien die Zuständigkeiten teilen, kann ein Mangel an Kooperation untereinander aufgrund der fragmentierten Zuständigkeiten zu Lücken führen. In Mitgliedstaaten, in denen die Datenschutzbehörden nicht über ausreichende Zuständigkeiten für die Nachrichtendienste verfügen, ist das Aufsichtsgremium für die ordnungsgemäße Wahrung der Privatsphäre und die Gewährleistung des Datenschutzes verantwortlich.
- In früheren Untersuchungen der FRA über den Zugang zu Rechtsbehelfen zum Datenschutz wird die Notwendigkeit der Stärkung der Kapazitäten

der DPA aufgezeigt. Dies ist besonders im Hinblick auf die Rolle, die die Datenschutzbehörden bei der Aufsicht von Nachrichtendiensten spielen können, von Bedeutung.

Rechtsbehelfe

Gemäß den geltenden internationalen Normen muss jede Person, die den Verdacht hat, von einer Verletzung von Privatsphäre und Datenschutzrechten betroffen zu sein, die Möglichkeit haben, mittels Rechtsbehelfen Abhilfe zu schaffen. Das Recht auf einen wirksamen Rechtsbehelf, der es Einzelpersonen ermöglicht, Beschwerde gegen eine Verletzung ihrer Rechte einzulegen, stellt einen wesentlichen Bestandteil des Zugangs zur Justiz dar. Ein Rechtsbehelf muss in der Praxis und in der Gesetzgebung „wirksam“ sein.

Wie aus früheren Untersuchungen der FRA über den Zugang zu Datenschutz-Rechtsbehelfen und den Zugang zur Justiz ersichtlich ist, stehen Betroffenen einer Verletzung ihrer Privatsphäre und Datenschutzrechte eine Reihe verschiedener Rechtsbehelfe zur Verfügung. Angesichts der praktischen Schwierigkeiten beim Zugang zu den ordentlichen Gerichten spielen die außergerichtlichen Organe eine wichtige Rolle bezüglich Rechtsbehelfen im Bereich der Überwachung. Zu den außergerichtlichen Organen in den 28 EU-Mitgliedstaaten zählen die Expertengremien (einschließlich der Datenschutzbehörden), Exekutivorgane und parlamentarische Organe sowie Bürgerbeauftragte. In einigen Mitgliedstaaten ist die Anzahl außergerichtlicher Organe, die für Rechtsbehelfe im Bereich der Überwachung zuständig sind, vielversprechend, jedoch sollte dies unter Berücksichtigung der folgenden Erkenntnisse betrachtet werden.

Weder die Komplexität der Rechtsbehelfe noch die Menge der Daten, die von den Nachrichtendiensten mit Hilfe der SIGINT erhoben wurden, erleichtern die Umsetzung wirksamer Rechtsbehelfe. Die Fragmentierung und Kompartimentierung verschiedener Zugänge zu Rechtsbehelfen haben es erschwert, Rechtsbehelfe einzulegen. Tatsächlich zeigen die erhobenen Daten, dass seit den Snowden-Enthüllungen nur eine begrenzte Anzahl von Fällen, bei denen Überwachungstätigkeiten angefochten wurden, auf nationaler Ebene entschieden wurde.

Informationspflicht und Auskunftsrecht

Das Recht auf Unterrichtung und den Zugang zu Informationen ist äußerst wichtig, um Einzelpersonen auf Überwachungsmaßnahmen aufmerksam zu machen und Abhilfemaßnahmen einzuleiten. Der Europäische Gerichtshof für Menschenrechte (EGMR)

hat jedoch akzeptiert, dass diese Rechte berechtigterweise eingeschränkt werden können (siehe EGMR, *Klass u. a. gegen Deutschland*, Nr. 5029/71, 6. September 1978). Die Ergebnisse der FRA zeigen, dass diese Rechte durch die Geheimhaltung der Tätigkeiten der Nachrichtendienste in der Tat eingeschränkt werden. Ein weiterer Faktor ist die schiere Menge der mit SIGINT erhobenen Daten im Vergleich zu den mit herkömmlicheren Formen der Überwachung erhobenen Daten.

- In acht Mitgliedstaaten sind Informationspflicht und Auskunftsrecht gesetzlich gar nicht vorgesehen. Es sind die für Verschlussachen oder Staatsgeheimnisse geltenden Vorschriften zu beachten. In den übrigen 20 Mitgliedstaaten sehen die Rechtsvorschriften Informationspflicht und Auskunftsrecht, in einigen Fällen innerhalb festgesetzter Zeitrahmen, vor, allerdings gelten Einschränkungen. Diese Einschränkungen umfassen verschiedene Elemente, z. B. die nationale Sicherheit, nationale Interessen oder den Zweck der Überwachungsmaßnahme an sich.
- Nur in zwei Mitgliedstaaten wurden Sonderbestimmungen zur Informationspflicht in Verbindung mit der Fernmelde- oder elektronischen Aufklärung festgelegt: in einem Mitgliedstaat wird die Einzelperson nicht darüber informiert, wenn die verwendeten Selektoren der Einzelperson nicht direkt zugeschrieben werden können, in dem anderen Mitgliedstaat wird die Einzelperson nicht informiert, wenn die erhobenen personenbezogenen Daten unmittelbar nach Erhebung gelöscht und nicht weiterverarbeitet werden.
- Die Aufsichtsgremien von 10 EU-Mitgliedstaaten, einschließlich sechs nationaler Datenschutzbehörden, überprüfen die Beschränkungen der Informationspflicht und des Rechts auf Auskunft über Informationen. Dabei wird untersucht, ob der Verdacht einer Bedrohung der nationalen Sicherheit begründet ist, und/oder das Auskunftsrecht der Einzelperson indirekt ausgeübt wird. Im letztgenannten Fall wird von den Gremien beurteilt, ob Auskunft über die Daten zu gewähren oder eine Auskunftsverweigerung berechtigt ist. Ebenso überprüfen sie die Rechtmäßigkeit der Datenverarbeitung. In einem Mitgliedstaat ist eine richterliche Anordnung erforderlich, die bescheinigt, dass eine Mitteilung die Ermittlungen gefährden oder andere Gründe gegen eine Mitteilung sprechen würden.
- Zwei weitere Mitgliedstaaten gewähren als solches kein Recht auf Auskunft über Informationen. Die Gesetzgebung sieht jedoch ein Recht vor, das dasselbe Ergebnis erzielt: eine Person kann verlangen, dass das Aufsichtsgremium überprüft, ob ihre Daten rechtswidrig überwacht werden.

- In einigen Mitgliedstaaten wird die Datenverarbeitung von dem Aufsichtsgremium, das indirekt das Recht einer Einzelperson, Auskunft über Daten zu fordern, ausübt, weder bestätigt noch dementiert. Die Rückmeldungen beschränken sich in der Regel auf die Erklärung, dass die Beschwerde bearbeitet und/oder geprüft wurde.

Gerichtliche Rechtsbehelfe

Jeder Mitgliedstaat ermöglicht Einzelpersonen gerichtliche Beschwerden über Verletzungen ihrer Privatsphäre einzureichen, unabhängig davon, ob diese im Rahmen einer gezielten Überwachung oder einer Fernmelde- oder elektronischen Aufklärung erfolgten. Gerichte sind für Einzelpersonen eine Möglichkeit, Beschwerde über eine Verletzung ihrer Privatsphäre einzulegen, einschließlich der Anfechtung einer Entscheidung des Aufsichtsgremiums über ihre behauptete Verletzung der Privatsphäre. Auch ermöglichen sie Einzelpersonen, Rechtsbehelfe einzulegen, unter anderem im Bereich der Überwachung.

- Frühere Untersuchungen der FRA haben gezeigt, dass der Mangel an auf Datenschutz spezialisierten RichterInnen ein ernstzunehmendes Problem für die wirksame Durchsetzung der Rechtsbehelfe bei Verletzungen des Rechts auf Datenschutz darstellt. Dieses Ergebnis ist auch für die Überwachungstätigkeiten relevant, bei der zusätzlich zur nötigen Geheimhaltung in Verbindung mit nachrichtendienstlichen Angelegenheiten eine entsprechende Sachkenntnis, z. B. im Bereich der Informations- und Kommunikationstechnologien oder der nachrichtendienstlichen Angelegenheiten, unabdingbar ist.
- Nur zwei Mitgliedstaaten haben den Mangel an Spezialisierung im Zusammenhang mit Rechtsbehelfen unter Einbeziehung von RichterInnen/Strafgerichten abgeschwächt, indem sie RichterInnen und Strafgerichte herangezogen haben, die sowohl über die erforderlichen Kenntnisse zum Beschluss über die (oftmals) technischen Angelegenheiten als auch über die Berechtigung zum Zugriff auf Verschlussmaterial verfügen.

Außergerichtliche Rechtsbehelfe

Außergerichtliche Rechtsbehelfe sind Einzelpersonen üblicherweise leichter zugänglich als der Gerichtsweg, da die Verfahrensregeln weniger streng sind, die Kosten für Beschwerden geringer ausfallen und die Dauer der Verfahren kürzer ist. Frühere Erkenntnisse der FRA bestätigen dies besonders im Bereich des Datenschutzes: hier wird gewöhnlich eine größere Anzahl an Beschwerden

bei den nationalen Datenschutzbehörden eingereicht und nur wenige BeschwerdeführerInnen streben Gerichtsverfahren an. Die Zahl der außergerichtlichen Organe – mit Ausnahme der Datenschutzbehörden – die Berichten zufolge im datenschutzrechtlichen Gebiet tätig sind, ist jedoch gering und viele außergerichtliche Organe können lediglich in begrenztem Maße Rechtsbehelfe anbieten.

- In den meisten Mitgliedstaaten handelt es sich bei den für Beschwerden zuständigen Aufsichtsgremien (einschließlich den Datenschutzbehörden) um unabhängige Einrichtungen.
- Die Frage der Unabhängigkeit stellt sich, wenn ein leitendes Aufsichtsgremium sowohl über Abhilfebefugnisse als auch über die Befugnis zur Überwachung verfügt. Parlamentarische Gremien und sachkundige Aufsichtsgremien haben autonomere Verwaltungsstrukturen. Autonomie garantiert jedoch keinen wirksamen Rechtsbehelf, es sei denn, dieser wird auch von ausreichend Wissen gestützt. Die Art und Weise, wie Mitglieder von Aufsichtsgremien ernannt werden, sowie deren Stellung in der administrativen Hierarchie, sind ebenfalls wichtige Aspekte, die bei der Beurteilung der Unabhängigkeit eines Gremiums berücksichtigt werden sollten.
- In 13 EU-Mitgliedstaaten haben die Datenschutzbehörden die Befugnis, einzelne Beschwerden zu untersuchen und verbindliche Entscheidungen zu treffen. Bei dreien ist das Recht auf Zugang zu Akten und Räumlichkeiten jedoch eingeschränkt. In fünf Mitgliedstaaten gelten weitere Anforderungen, die die Anwesenheit des Leiters/der Leiterin oder eines Mitglieds der Datenschutzbehörde während der Überprüfung auf dem Gelände des Nachrichtendienstes verlangen.
- Fünf von sieben Mitgliedstaaten betrauen ihre sachkundigen Aufsichtsgremien (mit Ausnahme der Datenschutzbehörden) mit besonderen Abhilfebefugnissen, indem sie diesen Gremien den Erlass verbindlicher Entscheidungen zugestehen. In zwei EU-Mitgliedstaaten verfügt ein leitendes Aufsichtsgremium auch über Abhilfebefugnisse. Parlamentsausschüsse in vier Mitgliedstaaten sind zur Anhörung von Einzelbeschwerden berechtigt, aber nur einer kann diesen mit verbindlichen Entscheidungen abhelfen.

- Bürgerbeauftragte, die es in allen 28 EU-Mitgliedstaaten gibt, kümmern sich zumeist um administrative Versäumnisse und weniger um die Frage, ob die Überwachung tatsächlich gerechtfertigt ist. Nur ein Mitgliedstaat statet seinen Bürgerbeauftragten im Rahmen der einschlägigen nachrichtendienstlichen Rechtsvorschriften mit Abhilfebefugnissen aus. Ferner können die Befugnisse der Bürgerbeauftragten relativ stark eingeschränkt werden und Verfahren enden zumeist mit unverbindlichen Empfehlungen, die darauf abzielen, die Dinge in Ordnung zu bringen, so dass diese als Grundlage für künftige Maßnahmen dienen können, anstatt mit einem rechtsverbindlichen und durchsetzbaren Urteil. Dies wirkt sich selbstverständlich auf die Wirksamkeit der Rechtsbehelfe aus, die sie zur Verfügung stellen können.
- Zu den weiteren Elementen, die den Zugang zu Datenschutz-Rechtsbehelfen für Personen erleichtern können, zählen lockerere Regelungen bei der Beweislast und Sammelklagen sowie ein effektiver Schutz der Hinweisgeber („Whistleblower“). Die Parlamentarische Versammlung des Europarats erachtet die Offenlegung von Missständen („wistleblowing“) als effektivstes Instrument, um den der Überwachung gesteckten Rahmen durchzusetzen.



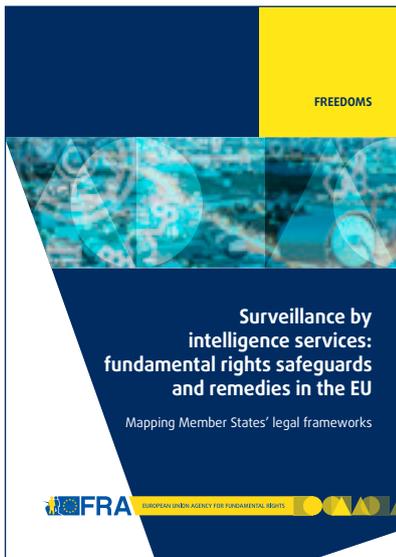
Schlussfolgerungen

Die FRA-Studie befasst sich mit einem Bereich, für den die EU nur einschränkt zuständig ist, und macht deutlich, wie unterschiedlich die Nachrichtendienste der Mitgliedstaaten organisiert sind und wie unterschiedlich sie ihre grundlegenden Tätigkeiten ausführen.

Überwachungsmaßnahmen greifen erheblich in die Rechte von Personen ein. Da die Überwachungsmaßnahmen geheim sind, müssen die Personen in gewissem Maße den Behörden vertrauen, die wiederum dazu verpflichtet sind, die Grundrechte der Personen zu schützen. Um das Vertrauen herzustellen, das eine Gesellschaft gegenüber ihren Nachrichtendiensten haben sollte, ist eine Rechenschaftspflicht erforderlich. Klare und verständliche Rechtsvorschriften, wirksame Aufsichtsmechanismen, angemessene Kontrollmechanismen und wirksame Rechtsbehelfe sind nur einige der Elemente, die unabdingbar sind, um diese Art Rechenschaftspflicht zu erzielen. Da die Nachrichtendienste zur Geheimhaltung verpflichtet sind, bleibt dies zweifelsfrei ein schwieriges Unterfangen. Die Einführung und Aufrechterhaltung klarer und verständlicher Rechtsvorschriften sowie wirksame Aufsichtsmechanismen auf Ebene der Mitgliedstaaten sind lediglich ein erster Schritt in Richtung eines transparenten

und grundrechtskonformen Systems. Die bei der Umsetzung auftretenden Schwierigkeiten deuten darauf hin, dass Hindernisse bestehen bleiben.

Die Reaktionen auf die Snowden-Enthüllungen haben die Notwendigkeit zum Vorschein gebracht, die einschlägigen Rechtsrahmen in der EU und ihren Mitgliedstaaten anzupassen und zu stärken. Wie die FRA-Studie zeigt, wurden bereits eine Reihe von rechtlichen Reformen durchgeführt. Regelmäßige Begutachtungen der Funktionsfähigkeit und Legitimität der Rechtsrahmen, die die Tätigkeit der Nachrichtendienste regeln, müssen zu einem wesentlichen Bestandteil der Aufsichtssysteme werden. Wie die Rechtsrahmen weiter reformiert werden sollen, um der fehlenden angemessenen Kontrolle entgegenzuwirken, ist ebenfalls eine Kernfrage. Außerdem müssen bei den Reformen in den EU-Mitgliedstaaten die neuesten technischen Entwicklungen in Betracht gezogen werden, um gewährleisten zu können, dass die Aufsichtsmechanismen mit den erforderlichen Instrumenten und dem nötigen Fachwissen ausgestattet sind. All dies zu verwirklichen, ist sicherlich eine Herausforderung – nichtsdestotrotz muss diese für die schwierige Aufgabe, die Sicherheit der Staaten zu schützen und gleichzeitig die Grundrechte zu wahren, angenommen werden.



Der Schutz der Öffentlichkeit vor Sicherheitsbedrohungen sowie der Schutz der Grundrechte sind ein Balanceakt. Brutale Terroranschläge und technologische Innovationen, die eine groß angelegte Überwachung von Kommunikationsdaten ermöglichen, haben die Angelegenheit noch komplizierter gemacht: Eingriffe in das Recht auf Privatsphäre und das auf Datenschutz im Namen des Schutzes der nationalen Sicherheit sind besorgniserregend. Die Snowden-Enthüllungen, die umfangreiche und willkürliche Überwachungsmaßnahmen weltweit aufgedeckt haben, verdeutlichen, dass für diese Rechte ein verbesserter Schutz erforderlich ist.

Dieser Bericht, der als Antwort auf die Forderung des Europäischen Parlaments nach einer eingehenden Untersuchung des Schutzes der Grundrechte im Kontext nachrichtendienstlicher Überwachung erarbeitet wurde, umreißt und analysiert die Rechtsrahmen der EU-Mitgliedstaaten zur Überwachung durch Nachrichtendienste. Sein Schwerpunkt liegt auf der sogenannten „Massenüberwachung“. Ferner werden auch die in den EU-Mitgliedsstaaten eingeführten Aufsichtsmechanismen der Nachrichtendienste dargestellt, die Tätigkeiten der Organe beschrieben, die mit der Kontrolle von Überwachungsmaßnahmen betraut sind, sowie die Rechtsbehelfe dargestellt, die den Personen zur Verfügung stehen, die solche nachrichtendienstlichen Tätigkeiten anfechten möchten. Der Bericht legt die damit verbundenen komplexen Überlegungen bloß und zeigt, wie schwierig es sein kann, häufig konkurrierende Prioritäten gleichermaßen zu berücksichtigen. Insofern leistet er einen Beitrag zur andauernden Diskussion, wie diese Prioritäten am besten miteinander in Einklang zu bringen sind.

Weitere Informationen:

Der vollständige Bericht der FRA zur „Überwachung durch Nachrichtendienste: Grundrechtsschutz und Rechtsbehelfe in der Europäischen Union“ (*Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States’ legal frameworks*) ist auf Englisch erhältlich unter <http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services>

Weitere Veröffentlichungen der FRA auf diesem Gebiet:

- FRA-Europarat (2014), *Handbuch zum europäischen Datenschutzrecht*, Luxemburg, Amt für Veröffentlichungen, <http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law> (verfügbar in den EU-Sprachen)
- FRA (2014), *Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten*, Luxemburg, Amt für Veröffentlichungen, <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states> und die Zusammenfassung des Berichts <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states-summary> (verfügbar in den EU-Sprachen)

Ein Überblick über die Tätigkeiten der FRA im Bereich des Datenschutzes ist abrufbar unter: <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection>



Amt für Veröffentlichungen

FRA - AGENTUR DER EUROPÄISCHEN UNION FÜR GRUNDRECHTE

Schwarzenbergplatz 11, 1040 Wien – Österreich
Tel.: +43 158030-0 - Fax: +43 158030-699
fra.europa.eu – info@fra.europa.eu
[facebook.com/fundamentalrights](https://www.facebook.com/fundamentalrights)
[linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency)
twitter.com/EURightsAgency

© Agentur der Europäischen Union für Grundrechte, 2015
Foto: © Shutterstock



Print: ISBN 978-92-9491-034-9, doi:10.2811/840869
PDF: ISBN 978-92-9491-017-2, doi:10.2811/6716