FAQ - Reform des Rechts der Nachrichtendienste (Stand 11.11.2026)

Koalitionsvertrag: „Wir stärken das Bundeskriminalamt und das Bundesamt für Verfassungsschutz, insbesondere in der Bekämpfung von Cyberkriminalität, Spionage und Sabotage. Wir vertrauen der Bundespolizei und schaffen für sie ein modernes Bundespolizeigesetz mit zeitgemäßen rechtlichen Grundlagen. (…) Zur Stärkung unserer nationalen Souveränität und der operativen Fähigkeiten unserer Nachrichtendienste, und um mit der Leistungsfähigkeit relevanter europäischer Partnerdienste wieder Schritt zu halten, streben wir eine grundlegende verfassungskonforme, systematische Novellierung des Rechts der Nachrichtendienste des Bundes an, einschließlich der rechtlichen Rahmenbedingungen für einen effektiven und effizienten Datenaustausch zwischen den Diensten und anderen Behörden (Ausweitung von Übermittlungsbefugnissen und Prüfung von Löschfristen). Wir sorgen für effektivere Kontrollstrukturen und zielgerichtetere Kontrollen nach den jeweiligen Maßgaben des Bundesverfassungsgerichts, auch durch den Deutschen Bundestag."

Warum brauchen wir eine große Reform der Nachrichtendienste?

Deutschland hat aktuell drei Nachrichtendienste: der Bundesnachrichtendienst (BND) ist der deutsche Auslands-Nachrichtendienst. Das Bundesamt für Verfassungsschutz (BfV) ist der Inlands-Nachrichtendienst und koordiniert darüber hinaus in seiner Funktion als Zentralstelle die 16 Landesämter für Verfassungsschutz. Das Bundesamt für den Militärischen Abschirmdienst (BAMAD) ist der Nachrichtendienst der Bundeswehr, das sich um die Abwehr von Gefahren für unsere Streitkräfte kümmert.

Im Koalitionsvertrag haben wir uns mit der Union darauf verständigt, unsere nationale Souveränität und die operativen Fähigkeiten unserer Nachrichtendienste zu stärken und diese „auf Augenhöhe mit unseren europäischen Partnern" weiterentwickeln zu wollen. Sehr oft sind wir auf Informationen aus dem Ausland angewiesen. Diesen Zustand wollen wir ändern.

Bereits im Zuge der Aufarbeitung des behördlichen Versagens bei der rechtsextremistischen Terrorgruppe NSU haben wir umfangreiche und nötige Reformen der Arbeit unserer Sicherheitsbehörden vorgenommen. Dies setzte sich auch nach der Aufdeckung des Skandals um den amerikanischen Nachrichtendienst NSA fort. Insbesondere wurde danach die parlamentarische Kontrolle der Nachrichtendienste ausgeweitet und personell spürbar verstärkt. Diesen Weg wollen wir weiter gehen.

Wir halten die Reform auch aus sozialdemokratischer Sicht zum Schutz unserer Bürgerinnen und Bürger für notwendig. Unsere Bundesjustizministerin Dr. Stefanie Hubig hat diesen Entwurf mit ihrem Haus in Vorbereitung auf den Kabinettsbeschluss sehr kritisch beraten und verfassungsrechtlich geprüft und viele wichtige Änderungen erreicht. Das wissen wir sehr zu schätzen und dafür möchten wir ausdrücklich danken.

Im parlamentarischen Verfahren haben wir die Beratungen in den Details fachlich kritisch geführt, da es sich um ein rechtlich und sicherheitspolitisch sensibles Thema handelt. Wir konnten noch zahlreiche weitere Verbesserungen erreichen (siehe auch unser Papier „Nachrichtendienstreform – zentrale Verbesserungen im parlamentarischen Verfahren" vom 9.11.2026).

Der Gesetzentwurf reagiert auf veränderte sicherheitspolitische Rahmenbedingungen und neue Bedrohungslagen. Ziel ist es, die rechtlichen Grundlagen der Nachrichtendienste an technische Entwicklungen anzupassen und bestehende Regelungslücken zu schließen. Es geht darum, unsere Freiheit, unsere Sicherheit und unsere Verfassung wirksam vor Angriffen zu

schützen. Da wir sehr offensichtlich mit neuen Arten von Bedrohungen konfrontiert sind, brauchen wir auch neue Antworten – und unsere Dienste Befugnisse, mit denen sie sich besser informieren und Angriffe im Notfall auch aktiv abwehren können. Russland bedroht Europa und vor allem Deutschland zunehmend und immer aggressiver durch hybride Bedrohungen. China verfolgt sein Ziel, bis 2049 globale Supermacht zu sein und nutzt Spionage, um seine Ziele planvoll, aber sehr aggressiv durchzusetzen. Insbesondere Rechtsextremismus, islamistischer Terrorismus aber auch zunehmend wieder Linksextremismus setzen unser Land von innen unter Druck. Das sind nur einige Entwicklungen von vielen, die wir in den letzten Jahren beobachten und die unsere Sicherheit, innen wie außen, vor große Herausforderungen stellen.

Wir haben uns auch vorgenommen, die rechtlichen Rahmenbedingungen für einen effektiven und effizienten Datenaustausch zwischen den Diensten und anderen Behörden anzupassen. Auch das BfV müssen wir insbesondere auch zur Bekämpfung von Cyberkriminalität, Spionage und Sabotage stärken.

Mit dem Ausbau der Befugnisse geht auch eine Stärkung der Kontrolle der Dienste einher. Das ist für uns ein absolutes Muss und wir haben die vorgesehenen Kontrollvorschriften im parlamentarischen Verfahren noch ausgebaut. Insgesamt ist dringend notwendig, dass wir unsere Nachrichtendienste modern und handlungsfähig aufstellen, um unser Land mit seiner freiheitlich demokratischen Grundordnung und der Freiheit, in der wir leben, zu schützen.

Darüber hinaus gilt es, bis Ende des Jahres ein Urteil des Bundesverfassungsgerichtes (BVerfG) umzusetzen, wonach wir vor allem die unabhängige Kontrolle eines Teils der strategischen Fernmeldeaufklärung neu regeln müssen. Die bisherige Ausgestaltung der G-10-Kommission genügt den verfassungsrechtlichen Anforderungen nicht mehr.

Das Gesetz über den Militärischen Abschirmdienst (MADG) hatten wir wegen des Ukrainekriegs und der dauerhaften Stationierung deutscher Soldaten in Litauen bereits vorgezogen und Anfang 2026 reformiert. Im Rahmen der jetzigen Reform werden nur noch kleine Anpassungen vorgenommen.

Welche neuen Befugnisse bekommen BND und BfV hauptsächlich?

Es sind neue digitale Befugnisse geplant (insbes. Auslesen technischer Spuren nach IT-Angriffen, Zugriff auf informationstechnische Systeme, Schutzmaßnahmen gegen Cyberangriffe). Darüber hinaus sind Befugnisse zur automatisierten Auswertung der Datenbestände sowie der Einsatz KI-gestützter Verfahren und selbstlernende Systeme vorgesehen. Ferner werden Auskunftsansprüche gegenüber Unternehmen ausgeweitet (z.B. zu Telemetriedaten von Fahrzeugen). Neu vorgesehen ist die Möglichkeit, in Sondersituationen sogenannter aktiver Maßnahmen zu ergreifen. Darunter fallen Eingriffe zur Abwehr schwerer Bedrohungen, die nach dem Gesetzentwurf nur unter engen gesetzlichen Voraussetzungen und unter unabhängiger Kontrolle zulässig sein sollen (z.B. Manipulation von Drohnenbauplänen, sodass die auf Grundlage dieser Pläne produzierten Drohnen keinen Schaden verursachen).

Wir schaffen für die neuen Befugnisse sehr hohe Eingriffsvoraussetzungen und auch eine klare Kontrolle der Maßnahmen.

Warum dürfen Nachrichtendienste künftig „aktive Maßnahmen“ ergreifen?

Bisher dürfen unsere Dienste nur Informationen sammeln. Mit den Regelungen über aktive Abwehrmaßnahmen wollen wir bisherige Regelungslücken schließen. Dabei geht es nicht um ein „Zurückschlagen“, also einen Gegenangriff, sondern um lediglich die Abwendung oder Einschränkung einer durch einen Angreifer zu verantwortende Gefährdung (§ 49 BNDG-E). Bisher durften die Dienste nur Informationen gewinnen und Gefahren oft nur beobachten, aber selbst nicht eingreifen – auch dann, wenn keine andere Behörde zuständig oder erreichbar war (siehe auch unten „Trennungsgebot“). Künftig dürfen die Dienste über die reine Gewinnung von Informationen hinaus in bestimmten streng kontrollierten Fällen auch aktive Maßnahmen ergreifen, wenn ein umgehendes Einschreiten erforderlich ist. Beispielsweise Sprengstoff kann so verfälscht werden, dass er nicht mehr zur Detonation gebracht werden kann. Der BND darf solche Maßnahmen grundsätzlich nur im Ausland durchführen, wo ein Rückgriff auf die Exekutive selbstverständlich nicht möglich ist.

Bei der Umsetzung haben wir in den Vorgesprächen zu dieser Reform auf abstrakt-generelle Regelungen hingewirkt mit einem Stufensystem hinsichtlich der Befugnisse. Alle Maßnahmen gegen eine fremde Macht müssen sich im Rahmen der Verhältnismäßigkeit bewegen – sie müssen insbesondere erforderlich sein, um einer Gefährdung durch die fremde Macht zu begegnen, und die etwaigen Folgen sind immer zu berücksichtigen.

Wichtig: Die grundsätzlichen Anordnungen, gegen welche Gefährdungen solche Maßnahmen durchgeführt werden dürfen (und ob – für den BND – eine spezifische Gefährdungslage überhaupt vorliegt), unterliegt der Vorabkontrolle durch den UKRat. Die jeweiligen Anordnungen müssen diesem zur Prüfung der Rechtmäßigkeit der Anordnung vorgelegt werden. Alle aktiven Maßnahmen müssen sich den Vorgaben dieser Anordnungen richten und unterliegen zudem auch der vollumfänglichen Kontrolle durch den UKRat.

Im parlamentarischen Verfahren haben wir die Kontrolle bezüglich des sensiblen Instruments der aktiven Maßnahmen weiter gestärkt: Das PKGr ist künftig jährlich über die durchgeführten aktiven Maßnahmen des BND und BfV zu unterrichten. Das PKGr kann zusätzlich jederzeit selbst Berichte anfordern.

Was ändert sich beim BND hinsichtlich des Zugriffs auf IT-Systeme?

Der BND verfügt bereits heute (§ 34 BNDG) über die Befugnis zum Zugriff auf IT-Systeme von Ausländern im Ausland (Computer Network Exploitation - CNE). Aufgrund der technologischen Entwicklungen in der Digitalisierung und der Verbreitung von Verschlüsselungstechnologien stehen kaum alternative Mittel zur Verfügung, die weniger eingriffsintensiv sind, um dem BND die Erfüllung seines Auftrags zu ermöglichen. Speziell CNE-Maßnahmen sind für den BND eine überaus wichtige Erkenntnisquelle, um Bedrohungen frühzeitig zu erkennen und gegenüber seinen Partnerdiensten kooperationsfähig zu sein.

Da sich ein Großteil des Lebens auf technischen Geräten abspielt, ist es unter hohen Voraussetzungen aber auch wichtig, Kenntnisse aus diesen zur Abwehr von Gefahren gewinnen zu können. Diese Vorschriften haben wir ausführlich besprochen und hart verhandelt.

Im ursprünglichen Gesetzentwurf war vorgesehen (§ 37 Absatz 3 BNDG-E), dass der Eingriff in private informationstechnische Systeme auch im Inland und bei deutschen Staatsangehörigen erfolgen darf. Dies stellt einen intensiven Grundrechtseingriff und einen Ausnahmefall dar, der an besondere Voraussetzungen geknüpft ist. Ziel ist immer die Früherkennung und Aufklärung von Bedrohungen aus dem Ausland. Es betrifft dabei nur Personen, bei denen ein besonderer Bezug zu einer aus solchen Bedrohungen erwachsenden konkretisierten Gefahr besteht. Auch Inländer:innen und deutsche Staatsangehörige im Ausland können in Sachverhalten agieren, die der Auslandsaufklärung durch den BND unterfallen. Dies ist z. B. der Fall bei Agenten fremder Mächte, die europäische Spionagenetzwerke unterhalten und sich im Bundesgebiet aufhalten oder durchreisen, deutsche Jihadisten im Ausland oder auch Deutsche, die in Tätigkeiten der Sanktionsumgehung verstrickt sind. Auch hier gilt, dass der Eingriff nur zulässig ist, wenn die zuständige Polizeibehörde nicht oder nicht rechtzeitig übernehmen kann oder die Third-Party-Rule gilt (s. o.). In diesen Fällen ist auch der UKRat für die Vorab-Kontrolle vor dem Eingriff zuständig. Dies ist die funktionale Entsprechung des Richtervorbehalts. Wir haben im Rahmen der Verhandlungen nun **für beide Dienste** festgelegt, dass **alle** Eingriffe in IT-Systeme mit Bezug zum Inland der Vorabkontrolle durch den UKRat unterliegen, nicht nur rein privat genutzte Systeme.

Durch die Erweiterung der Befugnis und damit Schließens einer Schutzlücke, ist der BND nicht mehr so abhängig von ausländischen Partnerdiensten, wenn es um den Schutz unseres Landes und das Abwenden von Bedrohungen geht.

Im Entwurf für das BND-Gesetz findet sich eine Regelung für einen abgestuften Zugriff auf IT-Systeme (§ 38 BNDG-E), bei der ein Zugriff nur auf bestimmte Teile des IT-Systems erfolgt (z.B.: Erhebung aller Chatnachrichten oder aller Fotos).

Warum braucht das BfV die Befugnis für den Zugriff auf fremde IT-Systeme?

Extremisten und ausländische Spione nutzen IT, um Anschläge auf kritische Infrastruktur vorzubereiten, Bauanleitungen für Waffen zu teilen oder Cyberangriffe zu steuern. Daher soll das Recht so angepasst werden, dass auch unser Inlandsnachrichtendienst auf bestimmte IT-Systeme (also z. B. Handys oder Festplatten von Computern) zugreifen darf, um Angriffe frühzeitig zu erkennen und abzuwehren. Dieser Zugriff auf informationstechnische Systeme ist an sehr hohe Voraussetzungen geknüpft und darf nur nach einer Vorabkontrolle durch den Unabhängigen Kontrollrat (UKRat) erfolgen. Dies werden wir im Folgenden auch noch näher ausführen.

Diese eingriffsintensive Befugnis ist aber an sehr hohe Hürden geknüpft. Es braucht konkrete Anhaltspunkte für eine schwere Gefahr: Zum einen muss eine mindestens konkretisierte Gefahr vorliegen und es muss sich um eine besonders erhebliche beobachtungsbedürftige Bedrohung handeln. Z. B. liegen konkrete Hinweise auf einen Anschlag auf Personen oder kritische Infrastruktur wie wichtige Stromleitungen vor. Bestimmte Tatsachen müssen also auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen hinweisen und darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität so viel bekannt sein muss, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt wird und weitgehend auf sie beschränkt werden kann. Das BfV darf diese Befugnis nur dann anwenden, wenn eine Maßnahme durch die Polizei nicht geeignet wäre oder nicht rechtzeitig käme. Die Polizei kann in beispielsweise in den Fällen nicht übernehmen, wenn die Hinweise von ausländischen Partnerdiensten stammen, die eine Weitergabe an die Polizei ausdrücklich untersagen (sog.

Third-Party-Rule). Die Polizei kann außerdem nicht tätig werden, wenn nur der Nachrichtendienst über die technische Fähigkeit verfügt, Schadsoftware auf dem Zielgerät zu platzieren.

Es gibt Bedenken, dass ein deutscher Nachrichtendienst seine Befugnis (Information wird abgerufen und verändert weitergeleitet, damit kein schädigendes Ereignis eintreten kann) missbrauchen könnte, um Bürgerinnen und Bürger zu belasten, indem er diskreditierendes Material auf ein IT-System aufspielt. Das ist in unserem Rechtsstaat aus guten Gründen verfassungsrechtlich nicht zulässig und wäre nach dem Gesetzentwurf nicht möglich. Schon die Tatbestandsvoraussetzung lassen ein solches Tun nicht zu, denn eine solche Schutzmaßnahme des BfV (§ 59 Absatz 1 BVerfSchG-E) ist nur zulässig, um eine von einer besonderen Bedrohung ausgehende Gefährdung für ein besonders gewichtiges Rechtsgut abzuwenden. Die Schutzmaßnahme ist zu dokumentieren. Darüber hinaus unterliegt diese Maßnahme wie dargestellt der Vorabkontrolle durch den UKRat. Klarstellend haben wir im parlamentarischen Verfahren zusätzlich einen Passus in § 59 Abs. 1 BVerfSchG aufgenommen, wonach aktive Maßnahmen nicht darauf ausgerichtet sein dürfen, Personen durch unwahre oder ehrverletzende Behauptungen in ihrem privaten oder beruflichen Umfeld zu beeinträchtigen. Wir haben für Eingriffe im digitalen Raum nunmehr auch noch einmal ausdrücklich klargestellt, dass für Mensch-Maschine-Kommunikation dieselben Vorgaben gelten wie für Mensch-Mensch-Kommunikation. Eine Differenzierung ist nicht mehr zeitgemäß.

Digitale Souveränität

Bei der Beschaffung von IT-Anwendungen, insbesondere KI-Tools durch die Dienste haben wir die Anforderungen im Rahmen der parlamentarischen Beratungen für die Beschaffung verschärft: es gilt ein weitreichender Vorrang für deutsche bzw. europäische Lösungen.

Was ändert sich bei der Fernmeldeaufklärung des BND (Strategische Aufklärung)?

Unter strategischer Aufklärung versteht man die Überwachung der Telekommunikationsströme durch den BND basierend auf bestimmten Suchbegriffen wie Telefonnummern oder E-Mailadressen. Es gibt nun einheitliche Regeln für die Erfassung von Daten im Ausland und Inland, die den Vorgaben des Grundgesetzes entsprechen. Die strategische Aufklärung erfolgt in zwei Stufen. In einem ersten Schritt werden nachrichtendienstliche relevante Datenströme erfasst und gespeichert. Inhaltsdaten dürfen künftig sechs Monate, Verkehrsdaten dreizehn Monate gespeichert werden. Bei Verkehrsdaten haben wir im parlamentarischen Verfahren die Speicherfrist von zwölf auf 13 Monate geändert. Der BND muss periodisch auftretende Ereignisse anhand der Metadaten vergleichend analysieren können. Viele nachrichtendienstlich relevante Ereignisse finden einmal jährlich statt, etwa militärische Übungen, internationale Konferenzen, politische Jahresversammlungen oder Jahrestage historischer Ereignisse in unterschiedlichen Staaten. Für einen Vergleich mit dem Vorjahr reicht eine Frist von genau zwölf Monaten nicht aus: Wiederholt sich das Ereignis, sind die Metadaten aus dem Zeitraum unmittelbar um das Vorjahresereignis nicht mehr vollständig verfügbar. Zudem verschieben sich jährlich wiederkehrende Ereignisse häufig um ein bis zwei Wochen; dann ist ein Vergleich gar nicht mehr möglich. Mit einer Frist von 13 Monaten kann der Bundesnachrichtendienst den Ablauf eines solchen Ereignisses nicht nur für sich, sondern im Vergleich zum Vorjahr betrachten. Gerade Veränderungen der Abläufe und der genutzten Kommunikation lassen Rückschlüsse auf nachrichtendienstlich relevante Veränderungen der Lage, der verfügbaren Mittel und Ressourcen oder des (militärischen) Vorgehens zu.

Insgesamt macht die strategische Aufklärung den BND bei unvorhergesehenen Krisen oder Anschlägen sofort auskunftsfähig ("kaltstartfähig"; „Gibt es Infos über Attentäter X?“). In der zweiten Stufe (Einsichtnahme) werden die Daten einer inhaltlichen Auswertung und Relevanzprüfung zugänglich gemacht und auf Suchbegriffe untersucht. Diese beiden Schritte sind rechtlich klar abgegrenzt und unterliegen unterschiedlichen Eingriffsvoraussetzungen.

Die Speicherung der Daten ist keine anlasslose Überwachung und keine Vorratsdatenspeicherung: Der BND darf weiterhin nur Leitungen anzapfen, bei denen es konkrete Hinweise auf nachrichtendienstlich relevante Verkehre gibt. Jede Maßnahme muss vorab vom UKRat genehmigt werden.

Die vorgesehenen Speichermöglichkeiten für die strategische Aufklärung unterscheiden sich: Die Speicherung erfolgt nur anlassbezogen, da sie nur aus ausgesuchten Telekommunikations-Strecken, die nachweislich relevante Verkehre enthalten, und im Rahmen einer vom UKRat kontrollierten strategischen Aufklärungsmaßnahme zulässig ist. Erfasst werden nur Auslandsverkehre (d.h. Ausland-Ausland und Inland-Ausland), reine Inlandsverkehre werden schon bei der Erhebung ausgefiltert, ihre Speicherung ist unzulässig. Eine Weiterverarbeitung ist nur bei nachgewiesener Relevanz für den auslandsbezogenen Aufklärungsauftrag des BND und erhöhten Eingriffsschwellen zulässig, eine Übermittlung an Gefahrenabwehr- oder Strafverfolgungsbehörden (mit der möglichen Folge, dass Anschlussmaßnahmen eingeleitet werden) ist nur in einem weiteren Schritt unter zusätzlichen hohen Schwellen zulässig.

Der gesamte Prozess von Erhebung bis Übermittlung unterliegt der Kontrolle durch den UKRat. Anders als bei der Vorratsdatenspeicherung erfolgt damit insbesondere auch eine vollständige datenschutzrechtliche Kontrolle der Speicherung sowie eine Protokollierung sämtlicher Zugriffe auf die Daten, die ebenfalls der Kontrolle unterliegen.

Wird durch die Reform das Trennungsgebot zwischen Polizei und Nachrichtendiensten aufgeweicht?

Die Trennung zwischen der Arbeit der Polizei und der Nachrichtendienste bleibt bestehen. Trotzdem stellt diese Reform einen Paradigmenwechsel dar. Aus diesem Grund werden wir auch die Kontrolle der Dienste neu aufstellen und erheblich stärken. Nachrichtendienste dürfen nur dann, in ganz bestimmten wenigen Fällen aktiv werden, wenn die Polizei oder andere Behörden die Gefahr nicht rechtzeitig oder nicht selbst abwehren können. Wenn befreundete ausländische Dienste Informationen an unsere Nachrichtendienste weitergeben, bestehen sie aus Gründen der Attributtierbarkeit oft darauf, dass diese Informationen nicht an andere Behörden, auch nicht Polizeibehörden weitergegeben werden dürfen (Third-Party-Rule). Im parlamentarischen Verfahren haben wir für das BfV noch einmal ausdrücklich textlich klargestellt und präzisiert, dass aktive Maßnahmen nur dann möglich sind, wenn die Polizei nicht rechtzeitig eingreifen kann. Aktive Maßnahmen durch das BfV kommen also nur da überhaupt in Frage, wo Schutzlücken bestehen, die anders nicht geschlossen werden können, da die Polizei z. B. wegen der third party rule nicht über entsprechende Informationen verfügt.

Dürfen die Nachrichtendienste in Zukunft einfach so Wohnungen von Bürgerinnen und Bürgern betreten?

Nein. Das heimliche Betreten von Wohnungen ist nur unter bestimmten hohen Voraussetzungen möglich und unterliegt einer Vorabkontrolle durch den UKRat. Diese Vorabkontrolle gibt es auch bei eingriffsintensiven Einsätzen von Vertrauenspersonen (V-Leuten) oder verdeckten Ermittlern, bei Eingriffen in das Post-/Telekommunikationsgeheimnis oder dem Auslesen informationstechnischer Systeme (BVerfSch-G §§16 Abs. 6, 34; BND-Gesetz §§ 18 Abs. 2, 97). Eine Wohnraumüberwachung dürfen BfV und BND mit Blick auf den Richtervorbehalt darüber hinaus erst dann durchführen, wenn das Bundesverwaltungsgericht die Rechtmäßigkeit dieser Maßnahme festgestellt hat. Hier braucht man sehr hohe Voraussetzungen. Wir haben in den parlamentarischen Beratungen klargestellt, dass der Richtervorbehalt zusätzlich auch beim Betreten von Wohnungen gilt.

Anwerbung von V-Leuten

BfV (§ 18 BVerfSchG-E) und BND (§ 23 BNDG-E) dürfen Vertrauenspersonen anwerben. Grundsätzlich bleibt auch im vorliegenden Gesetzentwurf die Anwerbung Minderjähriger als Vertrauenspersonen bzw. nachrichtendienstliche Verbindung (beim BND) ausgeschlossen. Künftig soll es jedoch laut des Regierungsentwurfes für die Dienste sehr eng begrenzte Ausnahmen für 16- und 17-Jährige geben [Ausnahme für BfV in § 18 I 3 und für BND in § 23 III 1, gilt nicht bei Ausländern im Ausland]. In den Verhandlungen mit unserem Koalitionspartner haben wir erreicht, dass hierbei entsprechend ausgebildetes Personal eingebunden sein und der Unabhängige Kontrollrat den Einsatz vorab genehmigen muss. Darüber hinaus ist der Einsatz nur mit dem Ziel zulässig, den Jugendlichen aus der Szene herauszuholen.

Könnte der Verfassungsschutz nach dem Entwurf meine Gesundheitsdaten einsehen?

Nein. Nach dem Gesetzentwurf unterfallen Informationen aus dem Kernbereich privater Lebensführung wie aus einem Arzt-Patienten-Verhältnis (gilt auch für Psychotherapeut:innen und Hebammen) besonderen Schutzvorgaben und dürfen grundsätzlich nicht erhoben werden. Sie sind ohne gesetzliche Regelung absolut geschützt und müssen daher nicht ausdrücklich genannt werden. Demgegenüber betreffen Daten, die im Mandatsverhältnis oder gegenüber Journalistinnen/Journalisten mitgeteilt werden, regelmäßig gerade nicht den Kernbereich privater Lebensführung, sodass diese Berufsgruppen in der Vorschrift über den Schutz von Vertraulichkeitsgruppen (§ 32 BVerfSchG-E, § 22 BNDG-E) explizit genannt sind. Wir haben in den Beratungen jedoch klargestellt, dass die Heilberufe im BNDG-E nun ausdrücklich in § 22 BNDG (Schutz von Vertraulichkeitsbeziehungen) aufgenommen werden. Für den Verfassungsschutz gelten die gleichen bewährten Regelungen wie auch im Strafverfahren (§ 160a StPO). . Für beide Dienste gilt also, dass Informationen, die den absolut geschützten Kernbereich betreffen, nicht zielgerichtet erfasst werden dürfen und falls sie dennoch erfasst wurden, sofort zu löschen sind.

Wie funktioniert die Kontrolle der Nachrichtendienste?

Wir stärken die Kontrolle und bauen sie im Vergleich zum Regierungsentwurf noch aus. Der seit 2022 bestehende UKRat wurde nach den Vorgaben des BVerfG eingerichtet. Er ist eine gerichtsähnliche oberste Bundesbehörde, die aber der Exekutive zugeordnet ist. Er agiert

unabhängig und weisungsfrei. Der UKRat besteht derzeit aus Richter:innen der obersten Bundesgerichte. Künftig sollen auch Bundesanwält:innen, Oberstaatsanwält:innen beim Generalbundesanwalt, vergleichbare Ministerialbeamt:innen mit mehrjähriger Erfahrung im Sicherheitsbereich sowie langjährig mit nachrichtendienstlichen Fragen befasste Abgeordnete in den UKRat gewählt werden können. Alle Mitglieder müssen über die Befähigung zum Richteramt verfügen. Die Mitglieder des UKRats sind nur dem Gesetz unterworfen und werden vom parlamentarischen Kontrollgremium auf 8 Jahre gewählt (ohne Wiederwahl).

Bisher war die Tätigkeit des UKRat im BND-Gesetz geregelt, mit dieser Reform erhält er ein eigenes Stammgesetz und umfangreiche weitere Zuständigkeiten. Seine Kontrollzuständigkeit beschränkte sich bisher auf die Rechtskontrolle über die strategische und technische Aufklärung des BND und wird nun erweitert auf die vollständige Kontrolle von BND und BfV. Der UKRat wird eine Vielzahl von Maßnahmen zukünftig vorab genehmigen müssen, ähnlich wie bei einer richterlichen Anordnung im polizeilichen Bereich. Damit läuft die Arbeit der G-10-Kommission aus, die bisher für die Genehmigung und Kontrolle bei Eingriffen der Nachrichtendienste in die Telekommunikation zuständig ist. Die bisher zersplitterte Kontrolle wird künftig beim UKRat gebündelt und dadurch auch vertieft. Das stärkt die Kontrolle, vermeidet Doppelstrukturen und verhindert widersprüchliche Entscheidungen.

Der UKRat darf die Dienste unangemeldet und anlasslos prüfen. Seine Prüfung erstreckt sich auf die gesamte Tätigkeit der Nachrichtendienste. Er hat bei Verstößen ein klares Anweisungsrecht. Betroffene können sich künftig proaktiv an den UKRat wenden, um etwaige Rechtsverstöße prüfen zu lassen. Dies gilt vom ersten Tag an, wobei der UKRat für seine Prüfungen zunächst eine Übergangszeit erhält.

Der Unabhängige Kontrollrat muss künftig in seinem öffentlichen Bericht grundsätzlich auch über Rechtsauslegung und Leitsätze aus seiner Entscheidungspraxis berichten. Dies haben wir ebenfalls im parlamentarischen Verfahren herausverhandelt. Diese Regelung sorgt für mehr Transparenz und ermöglicht einen Diskurs über die Rechtsanwendung und -fortbildung. Zusätzlich kann das PKGr jederzeit in einzelne Entscheidungen des Unabhängigen Kontrollrats Einsicht nehmen. Neben dieser richterlichen Kontrolle besteht weiterhin die parlamentarische Kontrolle, für die das PKGr verantwortlich ist. Diese kann bei seiner Tätigkeit künftig auch auf die Expertise des UKRats zugreifen. Im kommenden Jahr werden wir zusätzlich zu den bisher erreichten Regelungen zur Nachrichtendienstkontrolle aus der Mitte des Parlaments auch das PKGr-Gesetz reformieren. Dies erfolgt traditionell nicht über einen Regierungsentwurf. Zu entsprechenden Reformideen sind wir bereits im Austausch.

Neben UKRat und PKGr haben auch der Innenausschuss für das BfV und der Verteidigungsausschuss für das BAMAD Kontrollfunktionen. Das Vertrauensgremium prüft und bewilligt die Ausgaben der Nachrichtendienste.

Warum werden Maßnahmen nicht durch Gerichte kontrolliert, sondern den UKRat?

Der UKRat wurde aufgrund eines Urteils des BVerfG von 2020 geschaffen, um die technische Aufklärung des BND unabhängig und rechtsstaatlich zu kontrollieren. Gefordert wurde damals eine stärkere unabhängige Kontrolle.

In der internationalen Zusammenarbeit mit Partnerdiensten gilt meist die sog. „Third-Party-Rule“. Informationen, die unsere Dienste von Partnern bekommen, dürfen nicht mit Dritten geteilt werden, beispielsweise der Polizei oder Gerichten.

Da nachrichtendienstliche Maßnahmen teilweise eine erhebliche Eingriffsschwere (z.B. Quellen-TKÜ) aufweisen, bedarf es – wie bei polizeilichen Maßnahmen – an sich einer richterlichen Vorabkontrolle. Der UKRat übernimmt funktional die richterliche Kontrolle, ohne formal ein Gericht zu sein. Aufgrund dieser speziellen Konstruktion bezieht sich das Weitergabeverbot der Partnerdienste nicht auf den UKRat, so dass durch ihn eine effektive Kontrolle der Nachrichtendienste sichergestellt werden kann.

Neu ist, dass sich Bürger:innen künftig mit Beschwerden über mögliche Rechtsverletzungen durch Nachrichtendienste des Bundes unmittelbar an den UKRat wenden können. Dieser prüft die Eingaben.

Künftig wird der BfDI nicht mehr für die Datenschutzkontrolle der nachrichtendienstlichen Tätigkeit zuständig sein. Ist das nicht eine Schwächung?

Nein, die Einhaltung der datenschutzrechtlichen Vorgaben wird künftig einheitlich durch die administrative Kontrolle des UKRat überprüft. Dadurch werden Doppelstrukturen abgebaut, einheitliche Prüfergebnisse sichergestellt und mögliche Kontrolllücken geschlossen. Dies führt zu mehr Rechtsklarheit und Sicherheit in der Anwendung der Vorschriften und zu einer tieferen Kontrolle. Wir beseitigen dadurch auch das rechtsstaatlich nicht tragbare Risiko, dass durch unterschiedliche Kontrollorgane sich widersprechende Entscheidungen gefällt werden könnten. Der UKRat wird durch die Reform personell aufgestockt und damit weiter professionalisiert.

Wir haben durch das parlamentarische Verfahren eine Stärkung der Unabhängigkeit der administrativen Kontrolle im UKRat erreicht. Weisungen der Behördenleitung dürfen sich nicht auf die Prüftätigkeit beziehen, also bspw. keine Wertungen vorgeben. Die Leitung der administrativen Kontrolle erhält ein eigenständiges Vortragsrecht beim PKGr. Die Berichte des UKRats enthalten künftig einen vom Leiter der administrativen Kontrolle verantworteten eigenen Berichtsteil zur Tätigkeit dieser Kontrolle.

Die administrative Kontrolle wird ihre Prüftätigkeit nach einem risikobasierten Ansatz in Anlehnung an die MA-Risk (Rundschreiben der BaFin zu „Mindestanforderungen an das Risikomanagement“) durchführen. Gesetzlich festgelegte Pflichtprüfungen stellen zugleich sicher, dass besonders sensible Bereiche regelmäßig kontrolliert werden, u.a. muss jährlich geprüft werden, ob die Vorschriften über Mitteilungen an Betroffene nachrichtendienstlicher Maßnahmen eingehalten werden.

Führt der Wegfall der G10-Kommission zu einer Schwächung der parlamentarischen Kontrolle?

Die Mitglieder der G10-Kommission wurden zwar vom PKGr gewählt, da die Mitglieder keine Abgeordneten sein mussten, es handelte sich jedoch nicht um ein parlamentarisches Gremium. Verfassungsgerichtliche Vorgaben zur Professionalisierung der Kontrolle der nachrich-

tendienstlichen Tätigkeit haben vor einigen Jahren zur Schaffung des UKRats geführt. Die dortigen Kontrollbeauftragten arbeiten hauptamtlich und bringen langjährige Berufserfahrung in der obersten Gerichtsbarkeit des Bundes mit. Demgegenüber genügt die G-10-Kommission in ihrer aktuellen Struktur den Vorgaben des BVerfG nicht. Die Neuordnung und Erweiterung der Befugnisse der Nachrichtendienste erfordert eine Kontrolle, die den Vorgaben aus Karlsruhe entspricht. Eine Bündelung der Kontrolle beim UKRat ist daher zu befürworten.

Partnerdienste

Internationale Zusammenarbeit bleibt für deutsche Nachrichtendienste unverzichtbar. Gleichzeitig zielt die Reform darauf ab, eigene Fähigkeiten auszubauen und Abhängigkeiten zu reduzieren.

Die im Entwurf vorgesehenen Maßnahmen sehen wir jetzt schon bei Partnerdiensten. Teilweise haben diese sehr viel weitergehende Befugnisse. Wir haben vor dem parlamentarischen Verfahren schon darauf hingewirkt, dass die vorgesehen Maßnahmen des Entwurfs aufgrund unserer verfassungsrechtlichen Vorgaben sowie unserer Geschichte nicht weiter gehen als für die Erfüllung der Aufgaben der Dienste notwendig. Das würde für uns nicht in Frage kommen. Wir haben auch hier mit Input aus dem Parlament ebenso wie in der Bundesregierung durch Stefanie Hubig mit dem BMJV sehr verantwortungsbewusst verhandelt und dabei stets die Sicherheitslage im Blick gehabt und eine grundrechtsschonende Herangehensweise verfolgt.

Entscheidend bleibt für uns, dass die Befugnisse unserer Dienste verfassungskonform sind und die Arbeit der Dienste der Kontrolle durch UKRat und Parlament unterliegen.

Der Vergleich unserer Nachrichtendienste mit einer Geheimpolizei ist geschichtsvergessen und falsch

Unsere Nachrichtendienste unterliegen einer starken Kontrolle. Diese gestalten wir neu aus und vertiefen sie. Alle von den Diensten ergriffenen Maßnahmen fußen auf einer stringenten Legitimationskette. Die Arbeit unserer Dienste dient unserem Schutz und gerade auch dem Schutz unserer Freiheit.

Könnten die Neuregelungen durch eine rechte Regierung missbraucht werden?

Mit diesem Gesetz stärken wir auch unsere wehrhafte Demokratie. Denn die Regelungen sollen dafür sorgen, dass der Verfassungsschutz seinem Auftrag, verfassungsfeindlichen Bestrebungen entgegenzuwirken, besser nachkommen kann. Sollte dennoch auf Bundesebene jemals eine rechtsextreme Regierung an die Macht kommen, könnte diese mit ihrer Mehrheit ganz andere rechtliche Regelungen schaffen. Dies gilt es mit aller politischer Kraft zu verhindern.

Wir haben uns im Rahmen der parlamentarischen Beratungen dafür eingesetzt, das Verfassungsschutzgesetz um eine Resilienzklausel zu ergänzen. Danach gilt die Zusammenarbeitspflicht von Bund und Ländern im Verfassungsschutzverbund nur soweit dadurch keine Sicherheitsinteressen gefährdet werden. Künftig können insbesondere der Informationsaustausch beschränkt und unerwünschte Datenabflüsse verhindert werden.

Zusätzlicher Entschließungsantrag zur 2./3. Lesung: Strengere Anzeige- und Genehmigungspflichten

Wir fordern die Bundesregierung in einer Entschließung dazu auf, auch zu prüfen, inwieweit für ehemaliges Leitungspersonal sicherheitsrelevanter Bundesbehörden zusätzliche Transparenz-, Anzeige-, Genehmigungs- oder Karenzregelungen erforderlich sind.