Zusammenarbeit unter Vorbehalt

Zu einer Resilienzklausel bei der informationellen Zusammenarbeit im Verfassungsschutzverbund

Markus Thiel

26.11.2026 doi: 10.59704/051201abd1a13b0b

Am 13. November hat der Bundestag die Reform des Nachrichtendienstrechts verabschiedet. Die Erwartungen an die Novellen waren hoch. Man erhoffte sich u. a. gesetzliche Antworten auf die Frage, wie die Nachrichtendienste, namentlich die Verfassungsschutzbehörden, mit den Gefahren umgehen können, die ihnen selbst infolge einer Veränderung der politischen Kräfteverhältnisse drohen.

Es gehört zu den Schutzgütern der öffentlichen Sicherheit, die freiheitliche demokratische Grundordnung zu sichern, aber auch, die staatlichen Einrichtungen und Verfahren vor Versuchen einer schlagartigen Beseitigung oder einer schleichenden Aushöhlung zu schützen. Das präventive Gefahrenabwehrrecht zielt (auch) darauf ab, den Bestand und die Funktionsfähigkeit des Staates und anderer Träger hoheitlicher Gewalt zu gewährleisten. Extremistische Bestrebungen, die auf einen Umbau der staatlichen Ordnung unter Zurückdrängung wesentlicher verfassungsrechtlicher Grundsätze gerichtet sind, stellen sicherheitsrechtlich eine (abzuwehrende) Gefahr dar. Auch die drohende Missachtung gesetzlicher Vorgaben, ein diskriminierender Umgang mit bestimmten Bevölkerungsgruppen oder die systematische Verletzung von Grundrechten können, wenn ihr Eintritt hinreichend wahrscheinlich ist, eine komplexe Gefahrenlage begründen. Diese weitere, „präventive“ Dimension des sicherheitsrechtlichen Umgangs mit „Verfassungsfeinden“ blenden die aktuellen Diskussionen um Parteiverbotsverfahren und politische Bewältigung extremistischer Strömungen häufig aus.

Behördliches Vertrauen als „Achillesferse“ der Sicherheitsarchitektur

Die normativ konstruierte deutsche Sicherheitsarchitektur gründet auf den Postulaten von Verfassungstreue und Rechtsstaatskonformität aller beteiligten Ebenen und Behörden. Zugleich hat sie Vorkehrungen getroffen, dass sich Befugnisse und Informationen nicht bei einer Stelle „bündeln“. Das sog. Trennungsgebot scheidet etwa Polizei- und Nachrichtendienstbehörde nach Organisation, Beschäftigten, Befugnissen und Informationsbestand. So ist etwa der Datenaustausch zwischen Verfassungsschutz und Landespolizei an strenge Voraussetzungen geknüpft. Die verabschiedete Reform erlaubt zwar nun dem Bundesnachrichtendienst und dem Bundesamt für Verfassungsschutz vereinzelte „operative“ Maßnahmen. Das kann man ohne Weiteres als „Paradigmenwechsel“ bewerten (und im Detail auch recht kritisch sehen, wie etwa Johannes Buchheim und Paul Harnisch oder Matthias Bäcker). Unabhängig von der verfassungsrechtlichen Bewertung einer „Vernachrichtendienstlichung der Polizei“ (durch die Schaffung von Ermächtigungsgrundlagen für verdeckte polizeiliche Informationseingriffe) und einer „Verpolizeilichung der Nachrichtendienste“ (durch die Einräumung „operativer“ Befugnisse) stehen polizeiliche und nachrichtendienstliche Säule aber nach wie vor recht klar getrennt nebeneinander.

Während die Rechtsordnung diese Schnittstelle sorgfältig regelt, fehlt es hinsichtlich denkbarer Probleme innerhalb der polizeilichen bzw. nachrichtendienstlichen Säule bislang an Problembewusstsein. Die gesetzlichen Anforderungen an die Übermittlung von Informationen an andere Verfassungsschutz- bzw.

andere Polizeibehörden sind jeweils niedrigschwellig ausgestaltet. Auch die im Regierungsentwurf vorgesehenen Novellen von BVerfSchG, BNDG und MADG knüpfen an diese Konzeption an. So regelt etwa § 79 Abs. 1 BNDG-E, dass der Bundesnachrichtendienst personenbezogene Daten an das Bundesamt für Verfassungsschutz, an die Verfassungsschutzbehörden der Länder und an das Bundesamt für den Militärischen Abschirmdienst übermitteln darf, „wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung erforderlich ist 1. zur nachrichtendienstlichen Auslandsaufklärung oder 2. zur Erfüllung der Aufgaben der empfangenden Stelle“. Bei solchen „Einzelübermittlungen“ wird also zuvor jeweils noch überprüft, ob die Voraussetzungen für die Datenweitergabe vorliegen. Im Übrigen legt man die Idee einer Kooperationspflicht der Verfassungsschutzbehörden zugrunde, die auch verfassungsrechtlich in der Kompetenznorm des Art. 73 Abs. 1 Nr. 9 b) GG (ausschließliche Gesetzgebungskompetenz des Bundes) zum Ausdruck kommt.

Anders liegt es beim Austausch von Informationen über das gemeinsame nachrichtendienstliche Informationssystem. Gemäß § 6 Abs. 1 BVerfSchG-E übermitteln sich die Landesbehörden für Verfassungsschutz, das Bundesamt für Verfassungsschutz und der Militärische Abschirmdienst unverzüglich „die Informationen, die für ihre Verfassungsschutzaufgaben aufgrund tatsächlicher Anhaltspunkte zu bestimmten Bedrohungen relevant sind, einschließlich der Erkenntnisse ihrer Auswertungen“. Dies erfolgt nach § 6 Abs. 2 BVerfSchG-E technisch über das vom Bundesamt für Verfassungsschutz bereitgestellte (§ 5 Abs. 3 Nr. 1 BVerfSchG) gemeinsame nachrichtendienstliche Informationssystem. Die Bestimmungen enthalten eine Reihe von Schutzvorkehrungen, die jedoch im Wesentlichen denjenigen entsprechen, die schon der geltende § 6 BVerfSchG vorsieht: Die speichernde Stelle trägt die Verantwortung für die eingespeisten Daten; nur sie darf diese ändern, löschen oder ihre Verarbeitung einschränken. Die anderen Stellen dürfen die Daten wiederum nur dann abrufen, wenn sie diese für ihre Aufgabenerfüllung benötigen. Darüber hinaus finden sich Vorgaben zur Einschränkung von Zugriffsberechtigungen, die sich an der Art der Informationen bzw. am Aufgabenbereich des Zugreifenden orientieren. § 6 Abs. 3 BVerfSchG-E verpflichtet das Bundesamt für Verfassungsschutz dazu, technische und organisatorische Maßnahmen entsprechend § 64 Abs. 3 BDSG zu treffen. Dort geht es allerdings vorwiegend um Kontrollinstrumente hinsichtlich des Zugriffs und der Nutzung, der Zuverlässigkeit und der Datenintegrität. Dass nur die speichernde Stelle Daten verändern oder löschen darf, verhindert zwar eine gezielte Manipulation durch andere Verfassungsschutzbehörden. Diese Bestimmungen schützen aber nicht ausreichend davor, dass Beschäftigte einer Verfassungsschutzbehörde ohne sachlichen Grund auf den Datenbestand zugreifen, Informationen zu rechtswidrigen Zwecken nutzen oder an Unbefugte weitergeben. Keinen hinreichenden Schutz vermitteln die Bestimmungen indes für Konstellationen, in denen Beschäftigte einer Verfassungsschutzbehörde ohne sachlichen Grund auf den Datenbestand zugreifen, Informationen zu rechtswidrigen Zwecken nutzen oder an Unbefugte weitergeben.

Verfassungsschutzbehörden als Sicherheitsrisiko

In Sachsen-Anhalt könnte ein AfD-Mitglied künftig das Innenressort leiten – ein Mitglied einer Partei also, deren Landesverband von der Abteilung Verfassungsschutz im Innenministerium als gesichert rechtsextremistisch eingestuft wird. Damit könnte eine Behörde Zugriff auf den nachrichtendienstlichen Informationsverbund erlangen, deren Spitze (und nach und nach wahrscheinlich auch weiteres Personal) keineswegs mehr Garantin für eine rechtmäßige, verfassungskonforme und diskriminierungsfreie Verwendung dort verfügbarer Daten sowie für eine verlässliche Bereitstellung von Daten aus dem eigenen Zuständigkeitsbereich wäre. Auch ein beherztes Löschen eingespeister Informationen etwa über Parteifreunde wäre vorstellbar. Wie eine solchermaßen geleitete Verfassungsschutzbehörde zum „Systemsprenger im Sicherheitsföderalismus“ werden könnte, haben Lukas Maria Hohner und Till Stoye eindrücklich dargelegt. Ob die verfassungsrechtlich eingeräumten Optionen des Bundeszwangs als „Notfallreserve“ weiterhelfen

würden, lässt sich mit Heiko Meiertöns anzweifeln. Die Problematik betrifft nicht nur die Nachrichtendienste, sondern auch die Polizeibehörden, die sich in Verbundsystemen wechselseitig Informationen bereitstellen. Auch hier stellt sich die Frage nach einer zugleich rechtsstaatskonformen wie gefahrensensiblen Beschränkung von Zugriffsmöglichkeiten.

Der Ruf nach gesetzlichen Regelungen, um einzelne Behörden vorübergehend aus den Informationsverbünden ausschließen oder wenigstens die Zugriffsrechte wirksam begrenzen zu können, wird vernehmlicher. Diese Forderungen offenbaren ein gravierendes Dilemma: Die Verfassungsschutzbehörden sollen „zum Schutze der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes oder eines Landes“ zusammenwirken (Art. 73 Abs. 1 Nr. 9 b) GG) und sind schon verfassungsrechtlich aus Art. 20 Abs. 3 GG, aber auch nach § 3 Abs. 3 BVerfSchG an die allgemeinen Rechtsvorschriften gebunden. Zugleich kann es erforderlich sein, den Datenaustausch zu beschränken, und zwar in dem Fall, dass einzelne Verfassungsschutzbehörden keine zuverlässigen Kooperationspartner (mehr) sind. Das ist keineswegs Ausdruck eines generalisierten Misstrauens gegenüber diesen Behörden, sondern eine Präventivmaßnahme unter veränderten politisch-gesellschaftlichen Rahmenbedingungen. Sie wird umso wichtiger, je differenzierter man (aufgrund anderer tatsächlicher Entwicklungen und Bedrohungsszenarien) die behördlichen Befugnisse ausgestaltet und erweitert.

Anpassungen in der Zusammenarbeitspflicht

Der Regierungsentwurf des Gesetzes zur Reform der Nachrichtendienste hat diese Problematik nicht aufgegriffen. Erst der Änderungsantrag der Fraktionen der CDU/CSU und der SPD vom 6. November 2026 (Ausschussdrucksache 21(4)249 des Innenausschusses) regte u. a. an, § 1 Abs. 1 S. 1 BVerfSchG wie folgt zu fassen:

> *„Der Bund und die Länder sind verpflichtet, beim Schutz der freiheitlichen demokratischen Grundordnung sowie des Bestandes und der Sicherheit des Bundes und der Länder zusammenzuarbeiten, soweit dadurch nicht überragend wichtige Sicherheitsinteressen des Bundes oder eines Landes erheblich beeinträchtigt werden.“*

Laut Begründung soll damit die Zusammenarbeitspflicht z. B. bei erheblichen Geheimschutzrisiken begrenzt werden, wenn „in einem Landesamt für Verfassungsschutz Geheimschutz institutionell nicht umfassend gewährleistet wäre. Dies würde die Funktionsfähigkeit des gesamten Verfassungsschutzverbundes gefährden, wenn die Risikosituation nicht durch Anpassungen in der Zusammenarbeit begrenzt wird.“

Ohne konkretere Bestimmungen bliebe diese Norm ein „normativer Komparse“. Ergänzend sieht § 5 Abs. 2 S. 3 BVerfSchG-E daher bestimmte Konsequenzen einer erheblichen Beeinträchtigung überragend wichtiger Sicherheitsinteressen des Bundes oder eines Landes vor:

> *„Bestehen tatsächliche Anhaltspunkte, dass in der Zusammenarbeit überragend wichtige Sicherheitsinteressen des Bundes oder eines Landes erheblich beeinträchtigt werden, kann das Bundesamt für Verfassungsschutz, wenn dem die Mehrheit der Verfassungsschutzbehörden der Länder zustimmt, Anpassungen in der Zusammenarbeitspflicht, einschließlich der Verfügbarkeit des nachrichtendienstlichen Informationssystems, für die Verfassungsschutzbehörden bindend festlegen.“*

Nach Satz 4 kann das Bundesamt für Verfassungsschutz (allein) Anpassungen bindend festlegen. Die Anpassungen treten gemäß Satz 5 wieder außer Kraft, wenn entweder das Bundesamt sie aufhebt oder dies – bei einer Festlegung bei Gefahr im Verzug – wenigstens die Hälfte der Verfassungsschutzbehörden der Länder verlangt.

Der Innenausschuss ist dem Änderungsantrag in seiner Beschlussempfehlung vom 11. November 2026 (Drs. 21/9161 (neu)) gefolgt. Der Deutsche Bundestag hat in seiner Sitzung am 13. November 2026 dem Gesetzentwurf in der Fassung der Beschlussempfehlung mit der erforderlichen Mehrheit zugestimmt.

Damit ist die Zusammenarbeitspflicht von Bund und Ländern im Verfassungsschutzverbund nach der sog. Resilienzklausel unter den gesetzlichen Vorbehalt

gestellt, dass die Zusammenarbeit nicht überragend wichtige Sicherheitsinteressen des Bundes oder eines Landes erheblich beeinträchtigt. Der Zusatz in § 1 Abs. 1 S. 1 BVerfSchG-E dürfte es einzelnen Landesverfassungsschutzbehörden erleichtern, einen direkten Informationsaustausch mit einer anderen Verfassungsschutzbehörde im Einzelfall oder auch grundsätzlich zu verweigern.

Wesentlicher ist die Neuregelung in § 5 Abs. 2 S. 3 bis 5 BVerfSchG-E. Das Bundesamt für Verfassungsschutz erfüllt hier als Zentralstelle für die Zusammenarbeit eine wesentliche Funktion: Es darf (im Regelfall mit Zustimmung der Mehrheit der Landesverfassungsschutzbehörden) „Anpassungen in der Zusammenarbeitspflicht (…) für die Verfassungsschutzbehörden bindend festlegen“. Dies schließt ausdrücklich die Verfügbarkeit des nachrichtendienstlichen Informationssystems ein. Das Bundesamt für Verfassungsschutz wird dessen Bereitstellung unter Berufung auf § 1 Abs. 1 S. 1 und § 5 Abs. 2 S. 3, 4 BVerfSchG-E allerdings nicht gänzlich beenden dürfen, weil es dazu nach § 5 Abs. 3 Nr. 1 BVerfSchG-E unverändert im Rahmen seiner Zentralstellenaufgaben verpflichtet bleibt. Ob eine Landesverfassungsschutzbehörde von einer Mitwirkung im Informationsverbund unter Berufung auf § 1 Abs. 1 S. 1 BVerfSchG-E eigenständig Abstand nehmen dürfte (etwa auch gegen den Willen des Bundesamtes für Verfassungsschutz bzw. der Mehrheit der Landesverfassungsschutzbehörden), ist dagegen zweifelhaft. Die grundsätzliche Zusammenarbeitspflicht und das beim Bundesamt liegende „Initiativrecht“ sprechen gegen eine solche komplette „Ausscheroption“. Die Begründung der Beschlussempfehlung des Innenausschusses führt zwar aus:

> *„Die Möglichkeit jeder Verfassungsschutzbehörde für sich in ihrer Zusammenarbeit auch Belange ihrer Eigensicherung und operativen Sicherheit zu berücksichtigen, bleibt davon unberührt.“*

Es widerspräche aber dem Zweck der Kooperation im föderalen Verfassungsschutzgefüge, wenn sich gerade solche Verfassungsschutzbehörden aus dem Verbund zurückziehen könnten oder müssten, die ihrerseits verfassungskonform und rechtmäßig arbeiten. Dies würde den Verfassungsschutz insgesamt erheblich schwächen, anstatt den Abweichler gezielt zu isolieren.

Da sie weit gefasst sind, dürften § 5 Abs. 2 S. 3, 4 BVerfSchG-E allerdings ermöglichen, mit Zustimmung der Mehrheit der Landesbehörden bzw. bei Gefahr im Verzug einzelne Verfassungsschutzbehörden von der Nutzung des Informationssystems auszuschließen. Anpassungen hinsichtlich der Verfügbarkeit des Systems schließen auch Veränderungen des Kreises der Nutzungsberechtigten ein; sie beschränken sich begrifflich und angesichts des Zwecks der Regelung nicht auf bloße Modifikationen des Zugriffs bei fortbestehender Berechtigung „für alle“.

Materielle Anforderungen als „Schwachstelle“

Die hoch angesetzten materiellen Anforderungen sind eine Schwachstelle der Vorschriften. Es bedarf tatsächlicher Anhaltspunkte dafür, dass die Zusammenarbeit überragend wichtige Sicherheitsinteressen des Bundes oder eines Landes beeinträchtigt. Die „doppelte“ Qualifikation der überragend wichtigen Sicherheitsinteressen und der erheblichen Beeinträchtigung trägt der Funktionsfähigkeit des Verfassungsschutzverbundes Rechnung. Es bleibt aber fraglich, ob diese Voraussetzungen schon erfüllt wären, wenn eine andere Verfassungsschutzbehörde im Verbund etwa damit droht, verfügbare Informationen gezielt und systematisch zur Repression gegen bestimmte Bevölkerungsteile zu nutzen. Eine deviante Verfassungsschutzbehörde gefährdet regelmäßig nicht nur Bestand und Funktion des Bundes oder eines Landes, sondern bedroht und untergräbt den Menschen- und Grundrechtsschutz. Die „Resilienzklausel“ beruht auf der Sorge, der Geheimschutz könnte korrumpiert werden – die anderen Verfassungsschutzbehörden sollen keine weiteren Informationen in ein System einspeisen müssen, das ein „Leck“ aufweist. Diese „funktionszentrierte“ Perspektive sollte durch ein weites Verständnis der überragend wichtigen Sicherheitsinteressen um eine grundrechtliche Schutzdimension erweitert werden: Auch wenn überragend wichtige Rechtsgüter vieler Menschen verletzt zu werden drohen, sollte das

Bundesamt für Verfassungsschutz seine Anpassungsbefugnis ausüben können.

AUTOR*IN

Markus Thiel
Markus Thiel ist Professor für Öffentliches Recht mit Schwerpunkt Polizeirecht an der Deutschen Hochschule der Polizei in Münster.

EMPFOHLENE ZITATION

Thiel, Markus: Zusammenarbeit unter Vorbehalt: Zu einer Resilienzklausel bei der informationellen Zusammenarbeit im Verfassungsschutzverbund, Verfassungsblog, 26.11.2026, doi: 10.59704/051201abd1a13b0b.

Lizensiert unter CC BY-SA 4.0.