Informationsaustausch mit Extremist*innen

Auswirkungen einer AfD-geführten Landesregierung auf den Sicherheitsföderalismus

Markus Thiel

17.06.2026 doi: 10.59704/a635f75083e536c3

Seit heute Morgen tagt die Innenministerkonferenz in Hamburg. Eines ihrer Themen: Wie geht man damit um, wenn nach den Landtagswahlen im September die AfD einen Innenminister stellt? Und wie würde sich das auf die föderale Sicherheitsarchitektur auswirken? Im Sicherheitsföderalismus sind die Polizeibehörden von Bund und Ländern zur Erfüllung ihrer Aufgaben der Gefahrenabwehr und der Strafverfolgung auf eine enge und vertrauensvolle Kooperation angewiesen. Unverzichtbar ist dabei ein Austausch von Informationen, der wiederum strikten verfassungs- und datenschutzrechtlichen Bindungen unterliegt. Speist eine Behörde personenbezogene Daten in ein polizeiliches Informationssystem ein, treffen sie zwei Pflichten. Erstens muss sie selbst die Anforderungen des Bundesverfassungsgerichts beachten, vor allem das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Zweitens muss sie summarisch prüfen, was mit den Daten danach geschieht: Gewährleisten die abrufenden und weiterverwendenden Behörden zumindest einen hinreichenden Datenschutz und – allgemeiner – einen rechtsstaatlich einwandfreien Umgang mit den Daten?

Besteht im Einzelfall oder auch grundsätzlich die durch Tatsachen gestützte Befürchtung, dass dies nicht der Fall ist, darf die Behörde die Daten nicht in das Verbundsystem eingeben und auch nicht andersartig übermitteln. Bei einer generalisierten Besorgnis bezüglich einer Landespolizei ist das mit der geltenden Rechtslage kaum realisierbar. Dieser liegen in weiten Teilen nach wie vor der verfassungsstaatliche Homogenitätsgedanke des Art. 28 Abs. 1 S. 1 GG und die Annahme einer Verwaltung, die bundesweit rechtsstaatlich handelt, zugrunde. Diese Annahme aber trägt nicht mehr, sollte eine autoritär-populistische Partei auf Landesebene an die Regierung kommen. Die einfachgesetzlichen Schutzvorkehrungen des Datenschutzrechts sind auf punktuelle Einzelfälle zugeschnitten und greifen vor allem bei Zweifeln an einem rechtsstaatlichen Umgang mit übermittelten personenbezogenen Daten durch die empfangende Behörde. Bei Vorbehalten gegenüber einer Landespolizei im Ganzen versagen sie.

Austausch des Beamt*innenapparats nach einem Regierungswechsel?

Der Spitzenkandidat der AfD für die Landtagswahl in Sachsen-Anhalt, Ulrich Siegmund, hat angekündigt, im Fall einer Regierungsbildung 150 bis 200 Beamt*innenpositionen neu zu besetzen, nicht nur Stellen politischer Beamt*innen. Das Vorhaben ist evident verfassungswidrig. Art. 33 Abs. 2 GG schreibt die Bestenauslese nach Eignung, Befähigung und fachlicher Leistung vor, und das Lebenszeitprinzip (als hergebrachter Grundsatz des Berufsbeamtentums gemäß Art. 33 Abs. 5 GG) schützt insbesondere nichtpolitische Beamt*innen vor einer Entlassung ohne sachlichen Grund. Hinzu kommt: Der Landesverband der AfD ist seit 2023 als gesichert rechtsextremistische Bestrebung eingestuft. Jedenfalls nach den unmissverständlichen Äußerungen ihrer Funktionsträger*innen haben zahlreiche, vor allem vulnerable Personengruppen erhebliche Repressionen zu erwarten. Als Inhaberin des Gewaltmonopols läuft die Polizei Gefahr, dafür instrumentalisiert zu werden.

Drohende Veränderungen der polizeilichen Aufgabenerfüllung

Sollte sich das Szenario einer AfD-geführten Landesregierung in Sachsen-Anhalt realisieren, muss man wohl befürchten, dass die AfD Führungspositionen in den Sicherheitsbehörden mit Parteimitgliedern oder ande-

ren „Getreuen“ besetzt – möglicherweise auch unter Verletzung der dargestellten verfassungsrechtlichen Vorgaben. Wahrscheinlich ist, dass sich – auch bei unverändertem Normbestand – dann erhebliche Veränderungen z.B. in der polizeilichen Anwendungspraxis ergeben werden. Durch Verwaltungsvorschriften und Erlasse könnte die AfD die Ausübung von Beurteilungs- und Ermessensspielräumen lenken, den Polizeikräften eine intensivere Bestreifung und eine erhöhte Kontrollintensität auftragen, die Videoüberwachung des öffentlichen Raums ausweiten, Durchsuchungen und aufenthaltsbestimmende Maßnahmen verstärkt einsetzen usw. Auch die Nutzung des polizeilichen Informationsbestands dürfte sich wandeln. Zu befürchten sind namentlich eine diskriminierende Verwendung personenbezogener Daten und eine Überdehnung der Zweckbindung der vorhandenen Informationen. Die nachgeordneten Beamt*innen können zwar remonstrieren, wenn sie Bedenken gegen die Rechtmäßigkeit dienstlicher Anordnungen haben (§ 36 Abs. 2 BeamtStG), und sich – wird die Anordnung aufrechterhalten – an die bzw. den nächsthöhere*n Vorgesetzte*n wenden. Bestätigt diese*r die Anordnung, muss der*die Beamt*in sie dennoch ausführen, sofern das aufgetragene Verhalten nicht die Menschenwürde verletzt oder für die handelnde Person erkennbar strafbar oder ordnungswidrig ist. Es liegt auf der Hand, dass dieses Remonstrationsrecht für den „Normalbetrieb“ und punktuelle Rechtsverstöße konstruiert worden ist, einer parteipolitisch motivierten Besetzung der Führungspositionen und verfassungs- bzw. rechtswidrigen Anordnungen aber letztlich wenig entgegenzuhalten vermag.

Polizeilicher Datenaustausch und Datenverantwortung

Ist nun erkennbar, dass die Polizeibehörden eines Landes Informationen in größerem Umfang rechtsmissbräuchlich verwenden (könnten), muss dies Konsequenzen für die Polizeibehörden anderer Länder haben, die personenbezogene Daten in einen polizeilichen Informationsverbund einspeisen oder auf andere Weise übermitteln. Ein Beispiel ist das einheitliche Verbundsystem nach § 29 BKAG. Das Bundeskriminalamt stellt es als Zentralstelle für den polizeilichen Informationsverbund zwischen Bund und Ländern bereit. Teilnehmen dürfen u.a. das BKA, die Landeskriminalämter, die Bundespolizei und die sonstigen Polizeibehörden der Länder. Daneben steht die bilaterale Einzelübermittlung. Speist eine Behörde Daten in das Verbundsystem ein, gelten für diese Übermittlung die Datenschutzbestimmungen des jeweiligen Landes. Die gesetzlichen Regelungskonzepte verteilen die Verantwortung eindeutig: Für die Übermittlung und Einspeisung ist die übermittelnde Stelle verantwortlich, für den Abruf und die Weiterverwendung die abrufende Stelle (vgl. § 31 Abs. 2 BKAG).

Dass aber auch die übermittelnde Stelle nicht die Augen davor verschließen darf, dass die empfangende Stelle die Informationen in rechts- bzw. verfassungswidriger Weise verwenden könnte, ergibt sich unmittelbar aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG): Eine staatliche Stelle, die rechtmäßig über personenbezogene Daten verfügen darf, muss selbst gewährleisten, dass diese Daten nicht in einen normativ oder tatsächlich „rechtsfreien Raum“ geraten. Diese Datenverantwortung des Staates ergibt sich zum einen aus den grundrechtlichen Schutzpflichten, zum anderen aus der faktischen Dateninhaberschaft. Sie gebietet es, zu überprüfen, ob die empfangende und die datennutzende Stelle jedenfalls die grundlegenden Datenschutzstandards wahrt.

Dies darf sich auch nicht nur auf eine kursorische Missbrauchs- bzw. Willkürkontrolle beschränken. Das Bundesverfassungsgericht hat hohe verfassungsrechtliche Anforderungen für die sog. Speicherschwellen formuliert, also die Voraussetzungen, unter denen personenbezogene Daten in polizeilichen Informationsverbünden gespeichert werden dürfen. Das rechtsstaatlich fundierte Untermaßverbot verpflichtet den Staat dazu, grundrechtlich geschützte Rechtsgüter effektiv zu sichern. Dem widerspräche es, wenn die speichernde Stelle das Erfordernis einer rechtsstaatlichen Datennutzung auf Seiten der abrufenden Stelle schlechthin ausblenden dürfte. Es wäre absurd, wenn sich eine umfassend gesetzlich gebundene Behörde nach dem Prinzip „aus den Augen, aus dem Sinn“

durch die bloße Abgabe von Informationen jeglicher Verantwortung entäußern könnte.

Gestaffelte Verlässlichkeit

Die für die Polizeien geltenden Datenschutzbestimmungen gehen nun von einer Art gestaffelter Verlässlichkeit der Empfängerbehörden aus: Übermittlungen an andere Polizeibehörden sind daher weniger strikten Anforderungen unterworfen als Übermittlungen an andere innerstaatliche Behörden, öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union bzw. an Personen oder Stellen außerhalb des öffentlichen Bereichs. Insoweit besteht ein normativer Vertrauensvorschuss der Sicherheitsbehörden untereinander. Dieser liegt darin begründet, dass man sich wechselseitig auf die Bindung an Gesetz und Recht nach Art. 20 Abs. 3 GG verlässt. Vorgesehen sind allerdings normative Ausschlussgründe für die Datenübermittlung: § 26 Abs. 6 Nr. 4 PolG NRW etwa untersagt die Übermittlung, wenn tatsächliche Anhaltspunkte vorliegen, dass sie der EU-Grundrechtecharta widerspräche. Das gilt vor allem, wenn die Nutzung der Daten im Empfängerstaat elementare rechtsstaatliche Grundsätze oder Menschenrechte zu verletzen droht. Diesen Ansatz kann man verallgemeinern: Jede Behörde hat im Einzelfall zu überprüfen, ob sich aus tatsächlichen Anhaltspunkten ergibt, dass die an eine Polizeibehörde eines anderen Landes übermittelten Informationen zu rechtsstaats- bzw. menschenwürdewidrigen Zwecken verwendet werden.

Grundsatz der Zweckbindung

Besondere Bedeutung kommt außerdem dem datenschutzrechtlichen Grundsatz der Zweckbindung zu: Behörden dürfen personenbezogene Informationen – soweit eine Zweckänderung nicht gesetzlich gestattet ist – nur für diejenigen Zwecke verwenden, zu denen sie erhoben bzw. übermittelt worden sind. Bestehen eindeutige tatsächliche Anhaltspunkte für eine zweckwidrige Nutzung durch die empfangende Behörde, hat eine Übermittlung bzw. Einspeisung ebenfalls zu unterbleiben. Auch wird eine Behörde entscheiden können, bis auf Weiteres gar keine Informationen an Behörden eines anderen Landes zu übermitteln. Bei dieser Entscheidung wäre allerdings zu berücksichtigen, dass eine solche „Funkstille“ die Aufgabenerfüllung und damit die Funktionsfähigkeit der Polizeibehörden im Empfängerland erheblich beeinträchtigen kann. Das kann sich, etwa bei landesübergreifenden Gefährdungen, auch nachteilig auf die eigene Sicherheitsgewährleistung auswirken.

Besonderheiten des polizeilichen Informationsverbunds

Weitaus schwieriger zu lösen ist die Problematik, wenn und soweit polizeiliche Informationsverbundsysteme betroffen sind. Die Teilnahmeberechtigung der Landespolizeien ist gesetzlich niedergelegt (z.B. § 29 Abs. 3 BKAG). Ausschlusstatbestände für bislang berechtigte Behörden sind regelmäßig normativ nicht vorgesehen. Die anderen berechtigten Behörden könnten zwar mit Blick auf die verfassungsrechtliche Datenverantwortung gänzlich auf ein Einspeisen in das Verbundsystem verzichten. Damit würden sie es allerdings weitgehend obsolet machen, nur um die Behörden eines einzelnen Landes vorübergehend vom Empfang auszuschließen. Dann aber wären der Aufbau von Parallelstrukturen sowie der Umweg über eine jeweils bilaterale Informationsübermittlung äußerst kompliziert und unpraktikabel.

Die gesetzlichen Vorschriften z.B. des BKAG ließen sich aber durch die Möglichkeit ergänzen, bestimmte teilnahmeberechtigte Behörden für einen begrenzten, jeweils verlängerbaren Zeitraum vom Zugriff auf das Verbundsystem auszuschließen. Diese gravierende und als absolute ultima ratio auszugestaltende Entscheidung müsste ein gerichtsförmiges Gremium nach Anhörung des betroffenen Landes bzw. der betroffenen Behörde treffen. Die materiellen Anforderungen wären klar und hinreichend bestimmt zu fassen und sachgerecht von parteipolitischen Zuschreibungen loszulösen, um sie nicht schon bei bloßer politischer Missliebigkeit oder Unerwünschtheit greifen zu lassen. Entscheidend dürfte sein, dass in einem Land politische Mehrheitsverhältnisse herrschen, die begründete Besorgnis hinsichtlich eines verfassungs- und datenschutzrechtskonformen Umgangs mit den Daten wecken. Hinzukommen

müsste, dass tatsächliche Anhaltspunkte einen entsprechenden Einfluss dieser Mehrheiten auf die bislang teilnahmeberechtigten Sicherheitsbehörden nahelegen.

Vorkehrungen für den worst case?

Diese Erwägungen werfen zudem eine grundsätzliche Frage auf: Muss die Rechtsordnung Vorkehrungen für den voraussetzungsreichen *worst case* treffen? Dieser hätte mehrere Stufen: Regierungsübernahme einer rechtsextremistischen Partei, gegebenenfalls mit absoluter Mehrheit, verfassungswidriger Austausch zentraler Beamt*innen, polizeilicher „Kurswechsel“ über die Grenzen des rechtsstaatlich Zulässigen hinweg und schließlich ein drohender flächendeckender Missbrauch polizeilicher Informationen aus den Informationsverbünden. Man könnte darauf verweisen, dass Betroffenen die gängigen Rechtsschutzmöglichkeiten eröffnet bleiben. Allerdings erlangen diese von einer Verarbeitung ihrer personenbezogenen Daten in polizeilichen Informationssystemen oftmals keine Kenntnis oder erst zeitlich versetzt. Zudem steht ein solcher Verweis unter dem Vorbehalt einer funktionsfähigen und unabhängigen Rechtsprechung. Auch die Kontrollfunktionen der bzw. des Landesbeauftragten für den Datenschutz in Sachsen-Anhalt dürften unter einer autoritär-populistischen Regierung kaum noch Wirkung entfalten.

Die Rechtsordnung wird nur resilienter, wenn man das bislang Undenkbare denkt und die bisherigen, vor allem verfassungsrechtlichen Schutzvorkehrungen der „wehrhaften Demokratie“ durch einfachgesetzliche Bestimmungen ergänzt. Vereinzelt ist dies bereits geschehen. Im Polizeirecht ist das Vertrauen in die Funktionsfähigkeit des Rechtsstaates noch sehr hoch. Das Missbrauchspotenzial hinsichtlich personenbezogener Daten ist indes bereits im intakten Rechtsstaat beachtlich, und das Bundesverfassungsgericht hält das informationelle Trennungsprinzip zwischen Polizei- und Verfassungsschutzbehörden zu Recht hoch. Gänzlich ungeregelt ist ein Trennungsgebot in Richtung der Polizeibehörden eines Landes, das nachweislich erhebliche rechtsstaatliche Defizite aufweist. Verfassungsrechtlich ist es mit Blick auf die Bedeutung des Grundrechts der informationellen Selbstbestimmung und mit rechtsstaatlichen Grundsätzen ohne Weiteres zu begründen. Für eine auch einfachgesetzliche Niederlegung bedarf es des entsprechenden gesetzgeberischen Willens.

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: Informationsaustausch mit Extremist*innen: Auswirkungen einer AfD-geführten Landesregierung auf den Sicherheitsföderalismus, Verfassungsblog, 17.06.2026, doi: 10.59704/a635f75083e536c3.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260617-190655-0.