LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 8/4589**
8. Wahlperiode **05.03.2025**

KLEINE ANFRAGE

des Abgeordneten René Domke, Fraktion der FDP

Daten- und Informationsaustausch der Sicherheitsbehörden

und

ANTWORT

der Landesregierung

Vorbemerkung

Bei der nachfolgenden Beantwortung der Fragen geht die Landesregierung davon aus, dass mit der Fragestellung die Polizei und der Verfassungsschutz gemeint sind.

Die Rechtsordnung in Deutschland unterscheidet die Aufgabenfelder der Polizei, die primär auf die Verhütung, Verhinderung und Verfolgung von Straftaten sowie die Abwehr von sonstigen Gefahren für die öffentliche Sicherheit und Ordnung ausgerichtet sind, und die Aufgaben des in der Regel verdeckt arbeitenden Verfassungsschutzes, der im Schwerpunkt auf die Beobachtung und Aufklärung verfassungsfeindlicher Bestrebungen im Vorfeld ausgerichtet ist.
Sowohl die Frühwarnfunktion des Verfassungsschutzes als auch eine effektive Gefahrenabwehr und Strafverfolgung sind für die Gewährleistung der inneren Sicherheit unabdingbar. Dies setzt insbesondere eine enge und frühzeitige Zusammenarbeit zwischen Polizei und Verfassungsschutz voraus.

Daneben besteht das Trennungsgebot zwischen Polizei und Verfassungsschutz, demnach sind Verfassungsschutz und Polizeibehörden organisatorisch, befugnisrechtlich und informationell voneinander getrennt [vergleiche §§ 2, 8, 20 des Landesverfassungsschutzgesetzes (LVerfSchG M-V)].
Diesbezüglich wird ergänzend auf die drei Bundesverfassungsgerichtsentscheidungen [Urteil des Bundesverfassungsgerichts (BVerfG) vom 26. April 2022 zum Bayerischen Verfassungsschutzgesetz (BayVSG); Beschluss des BVerfG vom 28. September 2022 zu den Übermittlungsbefugnissen im Bundesverfassungsschutzgesetz (BVerfSchG); Beschluss des BVerfG vom 17. Juli 2024 zum Hessischen Verfassungsschutzgesetz (HVSG)] hingewiesen.

Der Minister für Inneres, Bau und Digitalisierung hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 5. März 2025 beantwortet.

Im Urteil zum BayVSG postulierte das Gericht zum einen, dass sich das Maß der Verhältnismäßigkeitsanforderungen an heimliche Überwachungsmaßnahmen des Verfassungsschutzes im Einzelnen am jeweiligen Eingriffsgewicht auszurichten hat. Zum anderen sieht das Gericht in der Übermittlung der aus den Überwachungsmaßnahmen des Verfassungsschutzes resultierenden personenbezogenen Daten und Informationen an eine andere Stelle einen erneuten Grundrechtseingriff.

Der Beschluss des BVerfG zu den Übermittlungsvorschriften des BVerfSchG konkretisiert die im Urteil zum BayVSG formulierten verfassungsrechtlichen Anforderungen an die Übermittlung von personenbezogenen Daten, die mit nachrichtendienstlichen Maßnahmen gewonnen wurden. Betont wird insbesondere, dass die aus der Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen.

Der Beschluss des BVerfG vom 17. Juli 2024 erging zum HVSG, das erst auf der Grundlage der vorstehend angeführten Entscheidungen des BVerfG aus dem Jahr 2022 überarbeitet worden war, kontrollierte sozusagen die Umsetzung der vorangegangenen Rechtsprechung. Im Ergebnis wurden Vorschriften zur Definition des Grades der Beobachtungsbedürftigkeit, zu einzelnen Maßnahmen wie der Ortung von Mobilfunkgeräten oder des Einsatzes von verdeckten Bediensteten, aber auch zur Übermittlung an Strafverfolgungsbehörden und sonstigen öffentlichen Stellen als verfassungswidrig erkannt.

Der effiziente und sichere Austausch von Daten und Informationen zwischen Sicherheitsbehörden ist eine wesentliche Voraussetzung für die Gewährleistung der inneren Sicherheit. Die Geschehnisse rund um Taleb A. und ähnliche Vorfälle in jüngster Vergangenheit lassen Rückschlüsse auf potenzielle Defizite im Daten- und Informationsaustausch zwischen den Sicherheitsbehörden in Deutschland und auch mit denen in Mecklenburg-Vorpommern zu.

1. Wie ist der Daten- und Informationsaustausch der Sicherheitsbehörden innerhalb des Landes Mecklenburg-Vorpommern organisiert?

   a) Wie ist dieser zwischen den Sicherheitsbehörden des Landes Mecklenburg-Vorpommern und denen anderer Bundesländer organisiert?
   b) Wie ist dieser zwischen den Sicherheitsbehörden des Landes Mecklenburg-Vorpommern und denen des Bundes organisiert?

Die Fragen 1, a) und b) werden zusammenhängend beantwortet.

Für den technischen Daten- und Informationsaustausch zwischen den Polizeien des Bundes und der Länder steht den Sicherheitsbehörden ein eigenes Corporate Network für die Erfüllung hoheitlicher Aufgaben zur Verfügung. Eine technische Unterscheidung beim Daten- und Informationsaustausch zwischen Bund und Ländern erfolgt aufgrund eines einheitlich abgestimmten Standards nicht. Innerhalb des Corporate Network werden Daten und Informationen in eigenen polizeilichen Fachverfahren miteinander ausgetauscht.

Darüber hinaus ist festzustellen, dass es einer Differenzierung zwischen der Datenübermittlung der Polizei an den Verfassungsschutz und umgekehrt bedarf. Die Polizei ist in weiten Teilen verpflichtet, dem Verfassungsschutz alle Informationen, die zur Erfüllung der Aufgaben der Verfassungsschutzbehörden erforderlich sind, zu übermitteln [vgl. § 24 des Landesverfassungsschutzgesetzes (LVerfSchG M-V)].
Die Datenübermittlung des Verfassungsschutzes an die Polizei unterliegt in Abhängigkeit des Informationsursprungs sowie des Verwendungszwecks und den damit zusammenhängenden Schutzbedarfen deutlich höheren rechtlichen Schwellen. Die jeweils geltenden Erhebungsschranken dürfen dabei nicht unterlaufen werden.
Im Rahmen der rechtlichen Voraussetzungen erfolgt der Informationsaustausch zwischen Polizei und Verfassungsschutz in Mecklenburg-Vorpommern anlassbezogen in schriftlicher Form bzw. in Form verschiedener Treffen, Besprechungen und Erörterungen.

Der Informationsaustausch in der alltäglichen Arbeit findet mit allen Sicherheitsbehörden von Bund und Ländern in zwei gemeinsamen Zentren statt. Für den Bereich des islamistischen Terrorismus gibt es seit dem Jahr 2004 das Gemeinsame Terrorismusmusabwehrzentrum in Berlin und für die Bereiche des Rechts- und Linksextremismus ist im Jahr 2012 das Gemeinsame Extremismus- und Terrorismusabwehrzentrum in Köln eingerichtet worden.

Die Verfassungsschutzbehörden des Bundes und der Länder nutzen darüber hinaus ein gemeinsames Datenbanksystem (NADIS = Nachrichtendienstliches Informationssystem), in dem grundsätzlich alle Daten gespeichert werden, für die die Speicherberechtigung nach den Verfassungsschutzgesetzen gegeben ist.

Neben den Systemen der Verfassungsschutzbehörden und denen der Polizeien existieren die Antiterrordatei und Rechtsextremismusdatei als gemeinsame Dateien. Sie finden ihre Rechtsgrundlage in den zugehörigen Gesetzen zur Errichtung dieser Dateien. In ihnen speichern sowohl die Verfassungsschutzbehörden als auch die Polizeien Daten.

2. Welche Regelungen begründen, gestalten oder beschränken jeweils diesen Daten- und Informationsaustausch?

Der Datenaustausch mit anderen Bundesländern sowie dem Bund richtet sich landesrechtlich zunächst nach den allgemeinen Weiterverarbeitungsregeln des Sicherheits- und Ordnungsgesetzes (SOG M-V), insbesondere den §§ 36 und 42 sowie § 39b SOG M-V für die Datenübermittlung. Danach dürfen personenbezogene Daten an andere Polizeien und Ordnungsbehörden des Bundes und der Länder übermittelt werden, soweit dies zur Erfüllung der polizeilichen oder ordnungsbehördlichen Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist.

Für das Verbundsystem INPOL gelten zusätzlich die §§ 29 ff. des Bundeskriminalamtgesetzes (BKAG). Danach nehmen alle Landespolizeibehörden sowie diverse Polizeibehörden des Bundes (§ 29 Absatz 3 Nummer 2 bis 6 BKAG) am polizeilichen Informationsverbund teil und stellen darin einander Daten zum Abruf und zur Verarbeitung zur Verfügung, soweit diese verbundrelevant (§ 30 BKAG) sind (§ 29 Absatz 2 Satz 2 BKAG).

Die Regelungen zum föderalen Informationsaustausch müssen sich ihrerseits am Grundrecht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes messen lassen. So hat das Bundesverfassungsgericht mit Urteil vom 1. Oktober 2024 (1 BvR 1160/19) entschieden, dass einige Normen des BKAG für die Speicherung im polizeilichen Informationsverbund in der damaligen Fassung nicht mit dem Grundgesetz vereinbar waren.
Weitere Regelungen sind in der Strafprozessordnung, den verschiedenen Verfassungsschutzgesetzen, den Bundes- und Landesdatenschutzgesetzen und den Richtlinien für die Führung der Polizeilichen Kriminalstatistik enthalten.
Zudem wird auf die zuvor genannten drei Bundesverfassungsgerichtsentscheidungen verwiesen, in deren Lichte die Informationsübermittlungsvorschriften auszulegen sind.

3. Welche technischen Systeme und Plattformen werden für den Daten- und Informationsaustausch genutzt?
   Welche Maßnahmen werden ergriffen, um die Datenintegrität und die Verfügbarkeit der Systeme sicherzustellen?

Auf die Antwort zu den Fragen 1, a) und b) wird verwiesen.

Aufgrund der Sicherheitseinstufungen für das Corporate Network der Polizeien des Bundes und der Länder wird auf die Vertraulichkeit der technischen Systeme verwiesen. Eine Auskunft über konkrete technische Systeme kann daher nicht gegeben werden.
Für den Daten- und Informationsaustausch über zentrale polizeiliche Fachverfahren werden die zentralen Fachverfahren: „Polizeiliche Informations- und Analyseverbund“ (PIAV), „einheitliche Fallbearbeitungssystem“ (eFBS), „PIAV Operativ Zentral“ (PIAV OZ), „Polizeiliche Information und Auswertung“ und „Informationssystem der Polizei“ (INPOL) genutzt. Die zentralen polizeilichen Fachverfahren wurden nach einheitlichen Sicherheitsstandards der Polizeien (Vertraulichkeit, Verfügbarkeit, Integrität) und zur Sicherstellung des Schutzbedarfes im Zusammenwirken mit den Datenschutzbeauftragten konzipiert.

Jede Behörde ist für die Datenintegrität und Verfügbarkeit selbst verantwortlich. Die konkreten Maßnahmen zur Sicherstellung der Datenintegrität und der Verfügbarkeit des Verfassungsschutzes Mecklenburg-Vorpommern unterliegen der Geheimhaltung. Die Landesregierung lehnt insofern im Hinblick auf Artikel 40 Absatz 3 der Verfassung des Landes Mecklenburg-Vorpommern eine Äußerung zu den geheimhaltungsbedürftigen Angelegenheiten des Verfassungsschutzes, insbesondere zu deren Arbeitsweise, Strategie und Erkenntnisstand, ab. Aus einer weiterführenden Bekanntgabe könnten Informationen zu konkreten Schutzmechanismen für die Gewährleistung der Datenintegrität offenbart werden. Dies wiederum könnte zur Ausnutzung möglicher Schwachstellen genutzt werden. Es wird auf die Zuständigkeit der Parlamentarischen Kontrollkommission gemäß § 27 LVerfSchG M-V und deren umfassendes Auskunftsrecht gemäß § 29 Absatz 2 LVerfSchG M-V sowie die Zuständigkeit des Landesbeauftragten für Datenschutz und Informationsfreiheit verwiesen.

4. Welche technischen Standards oder Vorgaben gibt es, um die Kompatibilität und Sicherheit der Systeme zu gewährleisten?
   Wie werden die Zugriffe auf ausgetauschte Daten dokumentiert und kontrolliert?

Der Daten- und Informationsaustausch erfolgt über einheitliche Standards der Polizeien. Dazu zählen das einheitliche Datenmodell Polizei, der abgestimmte „xPolizei Standard“, das Informationsmodell der Polizei und die technische Repräsentation XSP. Weiterhin gelten die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI)-Grundschutzes und das Inpol-Verbund-Manual als Voraussetzung. Eine Protokollierung erfolgt entsprechend den rechtlichen Vorgaben.

Für die Zusammenarbeit des Verfassungsschutzes Mecklenburg-Vorpommern mit den anderen Verfassungsschutzbehörden in Bund und Ländern ist durch den Einsatz von gemeinsamen Systemen die Kompatibilität per se gegeben.
Wie bereits in der Vorbemerkung sowie bei der Beantwortung von Frage 1 dargestellt, ist ein automatisierter Austausch von Daten zwischen dem Verfassungsschutz und den Polizeien nicht zulässig. Ein Zugriff von Polizeien auf Datensysteme der Verfassungsschutzbehörde oder umgekehrt existiert demzufolge nicht. Aus diesem Grund sind auch keine Abstimmungen zu technischen Standards erforderlich.
In den Systemen der Verfassungsschutzbehörden werden alle Zugriffe automatisiert protokolliert und können anlassbezogen kontrolliert werden.

5. Wie viele Anfragen zum Abruf von Informationen der Sicherheitsbehörden des Bundes wurden seit 2021 bis zum 31. Dezember 2024 durch Sicherheitsbehörden des Landes Mecklenburg-Vorpommern gestellt (bitte nach einzelnen Quartalen aufschlüsseln)?

   a) Wie viele Anfragen zum Abruf von Informationen der Sicherheitsbehörden anderer Bundesländer wurden seit 2021 bis zum 31. Dezember 2024 durch Sicherheitsbehörden des Landes Mecklenburg-Vorpommern gestellt (bitte nach einzelnen Quartalen aufschlüsseln)?
   b) Wie viele Anfragen zum Abruf von Informationen der Sicherheitsbehörden des Landes Mecklenburg-Vorpommern wurden seit 2021 bis zum 31. Dezember 2024 durch Sicherheitsbehörden des Bundes gestellt (bitte nach einzelnen Quartalen aufschlüsseln)?
   c) Wie viele Anfragen zum Abruf von Informationen der Sicherheitsbehörden des Landes Mecklenburg-Vorpommern wurden seit 2021 bis zum 31. Dezember 2024 durch Sicherheitsbehörden anderer Bundesländer gestellt (bitte nach einzelnen Quartalen aufschlüsseln)?

Die Fragen 5, a), b) und c) werden zusammenhängend beantwortet.

Sowohl im Bereich des Polizeilichen Staatsschutzes als auch beim Verfassungsschutz werden keine Statistiken zu Anzahl und Inhalt von Anfragen zum Abruf von Informationen geführt.
Es existieren keine auswertbaren Daten. Insofern liegen der Landesregierung diesbezüglich keine Erkenntnisse vor.

6. Wie bewertet die Landesregierung den aktuellen Stand sowohl der rechtlichen als auch der technischen Grundlagen für einen erfolgreichen Daten- und Informationsaustausch zwischen den Sicherheitsbehörden? Wie konkret erfolgt die Zusammenarbeit mit den Sicherheitsbehörden des Bundes und denen der anderen Bundesländer zur Verbesserung sowohl der rechtlichen als auch technischen Grundlagen?

In rechtlicher Hinsicht ist durch das Zusammenspiel aus landesrechtlichen Weiterverarbeitungs- und Übermittlungsnormen und den bundesrechtlichen Regelungen zum polizeilichen Informationsverbund grundsätzlich ein Rechtsrahmen geschaffen worden, der eine umfassende informationelle Kooperation der Landes- und Bundespolizeibehörden ermöglicht.

Es findet regelmäßig ein Austausch zu rechtlichen und technischen Verbesserungen über die Gremienstrukturen der Polizeien statt. Hierzu zählen u. a. der Unterausschuss Information und Kommunikation. Darüber hinaus wird im Zuge der digitalen Harmonisierung der Polizeien intensiv das Programm Polizei im Jahr 2020 für einen technischen Austausch genutzt.

Im Rahmen des Verfassungsschutzverbundes werden die technischen Voraussetzungen durch einheitliche Plattformen gewährleistet und entsprechen dem aktuellen Stand. Durch die in der Vorbemerkung genannten Bundesverfassungsgerichtsentscheidungen sind erhebliche rechtliche Konkretisierungen und damit verbundene Einschränkungen in Bezug auf den Informationsaustausch bzw. die Weitergabe vorgenommen worden. Diese zu bewerten, ist nicht Aufgabe der Landesregierung. Die Landesregierung wird noch in dieser Legislaturperiode eine Novellierung des Landesverfassungsschutzgesetzes, in welcher die Entscheidungen des Bundesverfassungsgerichtes berücksichtigt werden, vorlegen.

7. In welchen zeitlichen Abständen wird der erfolgte bzw. nicht erfolgte Daten- und Informationsaustausch evaluiert?

Die Evaluation des Daten- und Informationsaustausches erfolgt je nach Fachverfahren und/oder technischem System in unterschiedlichen Zeitabständen. So wird der bundesweite Datenaustausch im Rahmen des Programmes Polizei 2020 stetig optimiert.

Es erfolgt eine laufende Evaluation und permanente Kontrolle sowohl in Bezug auf den Umfang als auch die Qualität des Daten- und Informationsaustausches. Sofern anlassbezogen Defizite festgestellt werden, erfolgt intern aber auch im Austausch zwischen Polizei und Verfassungsschutz eine Erörterung. Festgestellte Optimierungspotenziale werden umgesetzt.

8. Wie hat sich die Gesamtzahl des erfolgten Daten- und Informationsaustausches unter Beteiligung der Sicherheitsbehörden des Landes in den letzten zehn Jahren entwickelt?

Zur Anzahl des Austausches erfolgt im Polizeibereich keine statistische Erhebung. Im Hinblick auf die Weiterentwicklung der Kommunikationstechnik wird jedoch eingeschätzt, dass sich die Anzahl innerhalb des Informationsaustausches erhöht hat.
U. a. nach Bekanntwerden der Taten des Nationalsozialistischen Untergrundes sowie dem terroristischen Anschlag auf dem Breitscheidplatz in Berlin im Jahr 2016 wurde der Daten- und Informationsaustausch in qualitativer und quantitativer Hinsicht deutlich verbessert. Vor dem Hintergrund der in der Vorbemerkung genannten Bundesverfassungsgerichtsentscheidungen ist davon auszugehen, dass der Umfang des Informationsaustausches zurückgeht.
Konkrete Statistiken werden nicht geführt. Es existieren somit keine Daten, die automatisiert ausgewertet werden könnten. Insofern ist eine detaillierte Beantwortung dieser Frage nicht möglich.

9. Welche Maßnahmen wurden in den letzten zehn Jahren seitens der Landesregierung ergriffen, um die rechtlichen und technischen Grundlagen für einen praktikablen Daten- und Informationsaustausch zwischen den Sicherheitsbehörden unseres Landes und denen der anderen Bundesländer sowie des Bundes zu schaffen oder diese zu verbessern (bitte getrennt nach Maßnahmen und Jahr aufschlüsseln)?

Mit der umfassenden Neufassung des SOG M-V, welche am 5. Juni 2020 in Kraft getreten ist, wurden auch die Normen zur Weiterverarbeitung und Übermittlung in §§ 36 und 39b SOG M-V an die Rechtsprechung des Bundesverfassungsgerichtes, insbesondere an dessen Urteil zum Bundeskriminalamtgesetz, angepasst.
Für die Verbesserung des Daten- und Informationsaustausches zwischen den Polizeien des Bundes und der Länder werden keine einzelnen Maßnahmen durch die Landespolizei geplant, da konkrete Anpassungen an fachliche und/oder technische und/oder rechtliche Anforderungen zum Daten- und Informationsaustausch im laufenden Prozess erfolgen.

Auf die aktuell anstehende Novellierung des Landesverfassungsschutzgesetzes wurde bereits bei der Beantwortung zu Frage 6 eingegangen. In Bezug auf die technischen Grundlagen stehen Haushaltsmittel zur Verfügung. Es ist davon auszugehen, dass vor dem Hintergrund der aktuell intensiv vorangetriebenen technischen Weiterentwicklungen im Verfassungsschutzverbund mit erheblichen Aufwendungen auch in den kommenden Jahren zu rechnen ist.

10. Welche Maßnahmen wurden in den letzten zehn Jahren durch den Bund oder andere Bundesländern ergriffen, um die rechtlichen und technischen Grundlagen anzupassen, damit ein erfolgreicher Daten- und Informationsaustausch zwischen den Sicherheitsbehörden gewährleistet wird (bitte getrennt nach Maßnahmen und Jahr aufschlüsseln)?

Maßnahmen des Bundes sind die Initiierung des Programms Polizei 2020 mit dem Beschluss der Saarbrücker Agenda im Jahr 2016. Das Programm Polizei 2020 ist im Bundesministerium des Innern und für Heimat angegliedert. Darüber hinaus wurde durch den Bund die Erweiterung des Polizeilichen Informations- und Analyseverbunds (PIAV) durch Ausbau der Datenanlieferung gemäß Kriminalitätsbereichen über verschiedene Stufen initiiert:

2016

Stufe 1 Waffen- und Sprengstoffkriminalität

2018

Stufe 2 Gewaltdelikte, gemeingefährliche Straftaten, Rauschgiftkriminalität

2020

Stufe 3 Cybercrime Eigentumskriminalität/Vermögensdelikte, Sexualdelikte
Stufe 4 Dokumentenkriminalität, Schleusung/Menschenhandel/Ausbeutung

2026

Stufe 5 Arzneimittelkriminalität, Falschgeldkriminalität, Geldwäsche, Korruption, Wirtschafts- und Umweltkriminalität, Umwelt- und Verbraucherschutzdelikte, Marken- und Produktpiraterie
Stufe 6 Politisch motivierte Kriminalität
Stufe 7 Organisierte Kriminalität

Seitens des Verfassungsschutzes wird auf die Vorbemerkung und die Antwort zu Frage 9 verwiesen.