Dr. Peter Schantz
Rechtsanwalt
Ministerialdirektor a.D.
peter.schantz@schantz-law.de

Berlin, den 19. Mai 2026

Verfassungsbeschwerde

1. des Herrn Henning Höne, MdL,
2. des Herrn Dietmar Brockes, MdL,
3. der Frau Angela Freimuth, MdL,
4. der Frau Staatsministerin a.D. Yvonne Gebauer, MdL,
5. des Herrn Marcel Hafke, MdL,
6. der Frau Franziska Müller-Rech, MdL,
7. des Herrn Thomas Nückel, MdL,
8. des Herrn Dr. Werner Pfeil, MdL ,
9. des Herrn Christof Rasche, MdL,
10. der Frau Susanne Schneider, MdL,
11. des Herrn Staatssekretär a.D. Dirk Wedel, MdL,
12. des Herrn Ralf Witzel, MdL,
13. der Frau Dr. Marie-Agnes Strack-Zimmermann, MdEP,
14. des Herrn Moritz Körner, MdEP,

– im Folgenden „**Beschwerdeführende**“ –

Die ladungsfähigen Privatanschriften der Beschwerdeführenden sind in der **Anlage 1** zusammengestellt mit der Bitte, sie vertraulich zu behandeln. Die Beschwerdeführenden zu 1 bis 12 sind zudem über den Landtag von Nordrhein-Westfalen, Platz des Landtages 1, 40221 Düsseldorf, aufgrund ihrer Tätigkeit als Landtagsabgeordnete erreichbar, die Beschwerdeführenden zu 13 und 14 über ihre Büros in Nordrhein-Westfalen, (…).

Bevollmächtigter: Dr. Peter Schantz

Die Beschwerdeführenden haben mich mit ihrer Vertretung in diesem Verfahren beauftragt. Die Vollmachten der Beschwerdeführenden zu 1 bis 12 für das Verfassungsbeschwerdeverfahren füge ich als **Anlage 2** bei. Die Vollmachten der Beschwerdeführenden zu 13 und 14 werde ich kurzfristig nachreichen, sobald sie mir im Original vorliegen.

Namens und im Auftrag der Beschwerdeführenden erhebe ich

Verfassungsbeschwerde

gegen § 6 Abs. 4 S. 1 und 2, § 9 Abs. 3, Abs. 4 und Abs. 8, § 11 Abs. 2 S. 1 Nr. 2, § 20, § 26, § 33 Abs. 3 und § 36 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutz-Gesetz Nordrhein-Westfalen – **VSG NRW**) in der durch Art. 1 des Gesetzes zur Neuverkündung des Verfassungsschutzgesetzes Nordrhein-Westfalen und zur Änderung weiterer Gesetze verkündeten Fassung (GV. NRW 2025, Nr. 46 v. 8.12.2025, S. 987 ff., beigefügt in **Anlage 3**).

Die Beschwerdeführenden rügen die Verletzung ihrer Grundrechte aus Art. 1 Abs. 1, Art. 2 i.V.m. Art. 1, Art. 4 Abs. 1, Art. 5 Abs. 1 S. 2 und Art. 12 Abs. 1 GG und beantragen,

1. § 6 Abs. 4 S. 1 und 2, § 9 Abs. 3, Abs. 4 und Abs. 8, § 11 Abs. 2 S. 1 Nr. 2, § 20, § 26, § 33 Abs. 3 und § 36 VSG NRW in der Fassung des Gesetzes zur Neuverkündung des Verfassungsschutzgesetzes Nordrhein-Westfalen (GV. NRW 2025, Nr. 46 v. 8.12.2025, S. 987 ff.) für nichtig, hilfsweise für unvereinbar mit dem Grundgesetz zu erklären und

2. einen angemessenen Gegenstandswert festzusetzen.

Zur besseren Übersicht stelle ich ein Inhaltsverzeichnis voran:

A. Einleitung

1 Die Verfassungsbeschwerde richtet sich gegen einzelne Regelungen des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG NRW). Das Gesetz ist im Jahr 2025 komplett novelliert sowie neu verkündet worden und am 1. April 2026 in Kraft getreten. Das Gericht hat in zahlreichen Entscheidungen Leitlinien für die Gefahrenabwehr durch die Polizei und die Arbeit der Nachrichtendienste aufgestellt. In der vorliegenden Verfassungsbeschwerde gegen Regelungen des VSG NRW geht es nicht nur um die Anwendung dieser Grundsätze. Sie wendet sich auch gegen Regelungen, die das Gericht bisher nicht beschäftigt haben oder zu denen es sich bisher nicht äußern musste. Das vorliegende Gesetz und damit dieses Verfahren könnte in verschiedener Hinsicht „Pilotfunktion“[1] für andere Bundesländer aber auch den Bund haben. Die Beschwerdeführenden wenden sich daher gegen die folgenden Regelungen.

I. Schutz von Berufsgeheimnisträgern (§ 9 Abs. 3 und 4 sowie Abs. 8 VSG NRW)

2 Unzureichend ausgestaltet ist der Schutz von Berufsgeheimnisträgern. Dies gilt für das Vertrauensverhältnis zwischen Abgeordneten und Bürgerinnen und Bürgern sowie zwischen Anwalt und Mandant. Der verfassungsrechtlich garantierte absolute Schutz besteht hier nicht, sondern ist von schwer prognostizierbaren Abwägungen des Verfassungsschutzes abhängig. Dies gilt auch für den Schutz von Journalistinnen und Journalisten, der allein durch das staatliche Aufklärungsinteresse begrenzt wird. Der verfassungsrechtlich absolute Schutz des Gesprächs mit Seelsorgern (z.B. des Beichtgesprächs) ist im Gesetzgebungsverfahren ganz gestrichen worden. Schließlich ist eine Verstrickungsregelung vorgesehen, die für Berufsgeheimnisträger, die an einer beobachtungsbedürftigen Bestrebung beteiligt sind, den Schutz unabhängig vom Kontext entfallen lassen. Dies erscheint zu weitgehend, ebenso der Wegfall des Schutzes für Nachrichtenmittler.

II. Kontaktpersonen

3 Zu weit reichen auch die Regelungen zu Kontaktpersonen. Diese erlauben es, auch gegen Personen, die selbst an keiner beobachtungsbedürftigen Bestrebung oder Tätigkeit beteiligt sind, nachrichtendienstliche Mittel anzuwenden. Sie machen sie also zu einer originären Zielpersonen – wie eine Person, die für solche beobachtungsbedürftigen Bestrebungen oder Tätigkeiten verantwortlich ist. Ausreichend ist dazu allein das Wissen darum,

[1] *Gusy*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2735, S. 5.

dass eine Person, mit der man mehr als nur flüchtig zu tun hat, an einer solchen Bestrebung oder Tätigkeit beteiligt ist – unabhängig vom Kontext. Alternativ kann es auch ausreichen, wenn die Zielperson sich der Kontaktperson zur Förderung der Tätigkeit oder Bestrebung bedient. Die Kontaktperson muss also gar nicht wissen, dass sie hier mit einer verfassungsfeindlichen Bestrebung oder Tätigkeit zu tun hat. Sie gerät aus ihrer Sicht rein zufällig schon bei neutralen Tätigkeiten in den Fokus des Verfassungsschutzes. Dies ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar.

III. Automatisierte Datenanalyse

4 Künstliche Intelligenz und maschinelles Lernen werden mit diesem Gesetz erstmals für die nachrichtendienstliche Zwecke eingesetzt. Ihr Ziel ist es teilweise, große Datenmengen durch Sortierung, Filterung und Priorisierung mit geringerem Aufwand zu erschließen (§ 26 Abs. 2 VSG NRW) oder überhaupt erst zu erheben (§ 6 Abs. 4 S. 2 VSG NRW). Teilweise sollen durch sie aber auch neue Erkenntnisse erlangt werden (§ 26 Abs. 3 und 4 VSG NRW). Hier stellen sich neue Fragestellungen. Für diese hat das Gericht vor allem im Bereich der Gefahrenabwehr zwar erste Maßstäbe aufgestellt.[2] Diese bedürften aber auch mit Blick auf die technischen Entwicklungen und Möglichkeiten weiterer Konkretisierung. Als Reaktion auf die Herausforderungen durch den Einsatz von KI hat der Europäische Gesetzgeber die KI-VO (VO (EU) 2024/1689) detaillierte Regelungen erlassen. Dabei verfolgt er das Ziel einer „sicheren, vertrauenswürdigen und ethisch vertretbaren KI“, bei deren Entwicklung die EU eine Führungsrolle einnehmen möchte (EG 8 KI-VO, siehe auch Art. 1 Abs. 1 KI-VO).

5 Die KI-VO findet auf den Bereich der nationalen Sicherheit jedoch keine Anwendung (Art. 2 Abs. 3 UAbs. 3 KI-VO). Die Herausforderungen der Technologie bleiben jedoch und müssen vom nationalen Gesetzgeber bewältigt werden, wenn er KI im nachrichtendienstlichen Bereich einsetzen möchte. Gewissermaßen muss er als Äquivalent eine „KI-VO für Nachrichtendienste“ schaffen. Aktuelle Berichte über die Nutzung von KI durch die US-amerikanischen Einwanderungsbehörde (*United States Immigration and Customs Enforcement (ICE)*) demonstrieren die Effektivität des Einsatzes von umfangreichen KI-basierten Datenanalysen im Bereich der öffentlichen Sicherheit.[3] Sie führen aber auch vor Augen, welche Risiken damit für die Grundrechte und die Demokratie einhergehen. Dies gilt erst

[2] BVerfGE 165, 363 Rn. 66 ff. – automatisierte Datenanalyse; zuvor schon BVerfGE 156, 11 Rn. 95 ff. – Antiterrordateigesetz II.
[3] Vgl. nur *Lindner*, „Weil wir eine hübsche kleine Datenbank haben – und Sie gelten jetzt als Terroristin“, FAZ v. 3.2.2026 **(Anlage 4)**.

recht in einer Zeit, in der nicht sicher ist, ob jede kommende Regierung vollständig auf dem Boden des Grundgesetzes stehen wird. Gerade mit diesen Konstellationen vor Augen muss die Verfassung staatlichen Befugnissen Grenzen setzen. Die Maßstäbe, die das Gericht aufstellt, gelten dabei über den vorliegenden Fall hinaus für alle Länder und den Bund.

6 Marktführer für entsprechende Software ist das US-Unternehmern *Palantir Technologies* (Palantir). Dessen Software befindet sich in verschiedenen Bundesländern bereits im Einsatz, u.a. in Bayern, Hessen, Hamburg, aber auch in Nordrhein-Westfalen im Bereich der Polizei. Die Sensibilität der Daten, die unvollständige Transparenz von Software sowie Datenströmen und die Notwendigkeit ständiger Verbesserung und Trainings verlangen eine sorgfältige Auswahl privater Unternehmen, zumal eine einmal getroffene Auswahl aufgrund der Investitionen und des Aufwandes einer Umstellung nur selten korrigiert werden wird. Wenn der Staat in einem so sensiblen Bereich KI einsetzen will, trifft ihn daher eine umfassende Gewährleistungsverantwortung – zum Schutz der Grundrechte, aber auch als Ausdruck **digitaler Souveränität**. Dieser Aspekt muss sich auch in gesetzlichen Regelungen widerspiegeln. Dies ist bisher nicht der Fall. Wie wichtig dies ist, zeigt ein Evaluationsbericht der schweizerischen Armee, dessen Autoren ausdrücklich von einer Kooperation mit Palantir abraten und Eigenentwicklungen empfehlen.[4] Auch die Bundeswehr hat eine Kooperation mit Palantir abgelehnt, weil sie es für unvorstellbar hält, Mitarbeitern von Industrieunternehmen Zugriff auf sensible Daten zu gewähren.[5]

7 Die verschiedenen Regelungen zum Einsatz von KI und maschinellem Lernen durch Durchführung automatisierter Datenanalyse (§§ 6 Abs. 4 S. 1 und 2 und § 26 VSG NRW) erfüllen aus Sicht der Beschwerdeführenden die verfassungsrechtlichen Anforderungen nicht. Sie sehen zu niedrige Eingriffsschwellen vor, obwohl es sich um schwerwiegende Eingriffe in die Privatsphäre handelt; dies gilt insbesondere für § 26 Abs. 3 VSG NRW, der auf die Gewinnung neuer Erkenntnisse abzielt. Darüber hinaus fehlen flankierende Regegelungen zum Schutz vor Diskriminierung, aber auch zur Qualitätssicherung, einschließlich der Auswahl der Software und des Kooperationspartners. Zudem werden Daten verwendet, die durch Eingriffe

---

[4] *Kurz*, „Palantir-Software hat verheerende Risiken“, netzpolitik v. 8.12.2025, abrufbar unter: https://netzpolitik.org/2025/schweiz-palantir-software-hat-verheerende-risiken/ m.w.N. **(Anlage 5)** (u.a. zum Evaluationsbericht, abrufbar hier: https://cdn.repub.ch/s3/republik-assets/repos/republik/article-wie-palantir-hartnaeckig-den-schweizer-staat-umwarb/files/505a33d5-adbd-49f8-baca-5864df625564/armeestaab-evaluation.pdf).

[5] *Jahn/Holtermann*, „Palantir für die Bundeswehr? „Sehe ich momentan überhaupt nicht“, Handelsblatt v. 27.4.2026, abrufbar unter: https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html **(Anlage 6)**.

in das IT-System-Grundrecht gewonnen worden sind. Diese Probleme setzen sich in der Übermittlungsregelung des § 33 Abs. 3 VSG NRW fort, die das Eingriffsgewicht durch die Analyse nicht berücksichtigt und eine Umgehung der hohen Eingriffshürden für andere Behörden erlaubt.

8 Den verfassungsrechtlichen Anforderungen entsprechen auch die Regelungen zum Training der IT-Produkte nicht. Hierbei bleibt unberücksichtigt, dass die Trainingsdaten Teil des abstrakten Wissens des KI-Modells werden. Es muss daher sichergestellt werden, dass es sich um ein spezielles KI-Modell handelt, das nur für die konkrete Behörde entwickelt und trainiert wird und auf das nur sie Zugriff hat. Besonders problematisch ist die Übermittlung von kompletten Datenbeständen des Verfassungsschutzes an Private zum Training von KI-Modellen. Zugespitzt: Palantir erhält die Akten des Verfassungsschutzes. Die flankierenden Regelungen bleiben sogar hinter dem zurück, was ein Auftragsdatenverbeiter nach Art. 28 DSGVO erfüllen muss. Unberücksichtigt bleibt, ob die Übermittlung auch in ein Drittland erfolgen könnte, in dem ausländische Sicherheitsbehörden Zugriff auf die als Trainingsdaten übermittelten Datenbestände hätten.[6]

IV. Zugriff auf private und staatliche Videoüberwachungseinrichtungen (§ 20 VSG NRW)

9 Das Gericht hat sich bisher noch nicht zum Zugriff auf private und staatliche Videoüberwachungsanlagen geäußert. Dieser Zugriff erlaubt die Live-Überwachung, die auch in Echtzeit an den Verfassungsschutz ausgeleitet werden soll, aber auch den Rückgriff auf Videoaufnahmen – rückwirkend bis zu einem Jahr. Erfasst werden dabei alle Videoüberwachungseinrichtungen – von der typischen Überwachungskamera, über Smartglasses, Smartphones, Dashcams in Autos, Drohnen etc. Schon aufgrund der Verbreitung von Videoüberwachungseinrichtungen ist das Überwachungspotenzial enorm. Dies hat auch Auswirkungen auf das „Gefühl des Überwachtwerdens“ in einer Gesellschaft und vor allem im öffentlichen Raum. Es macht einen erheblichen Unterschied, ob der Staat zur Abwehr einer Gefahr oder Aufklärung einer Straftat punktuell zugreift oder der Verfassungsschutz, dessen Aufgabenprofil viel weiter und losgelöst ist von bestimmten eingrenzenden Ereignissen wie einer Gefahr oder einer Straftat. Dieses Eingriffsgewicht spiegelt sich nicht in einer entsprechenden Eingriffsschwelle wider. Zudem verstößt die Regelung gegen das Doppeltürprinzip, weil es an einer Übermittlungsbefugnis der Betreiber der Einrichtungen nach dem BDSG fehlt.

---

[6] Vgl. 31. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, S. 40 (zum parallelen Regelung im PolG NRW).

B. Sachverhalt

I. Beschwerdegegenstand

10 Die Verfassungsbeschwerde richtet sich gegen die folgenden Regelungen:

§ 6 Informationserhebung

(…)

(4) Die Verfassungsschutzbehörde darf zu den in Absatz 1 genannten Zwecken personenbezogene Daten auch automatisiert erheben und zur Beobachtung mindestens erheblich beobachtungsbedürftiger Bestrebungen und Tätigkeiten elektronische Speichermedien durchsehen. Systeme im Sinne des § 26 Absatz 2 mit mathematisch-statistischen Verfahren wie maschinellem Lernen und künstlicher Intelligenz dürfen im Einzelfall zur Filterung, Sortierung und Priorisierung der nicht mit nachrichtendienstlichen Mitteln zu erhebenden personenbezogenen Daten eingesetzt werden, soweit dies zur Aufklärung bestimmter beobachtungsbedürftiger Bestrebungen oder Tätigkeiten im Sinne des § 3 Absatz 1 erforderlich ist. Der Einsatz selbst weiter lernender Systeme ist unzulässig. Eine Online-Durchsuchung ist ausgeschlossen.

§ 9 Schutz des Kernbereichs privater Lebensgestaltung und von Vertrauensbeziehungen (Vertrauensbereiche)

(…)

(3) Maßnahmen zur Erhebung von Daten, die

1. einem Mitglied des Deutschen Bundestags, der Bundesversammlung, des Europäischen Parlaments aus der Bundesrepublik Deutschland, eines Landesparlaments, der Bundesregierung, der Regierung eines Bundeslands oder eines Gerichts nach dem Deutschen Richtergesetz in der Fassung der Bekanntmachung vom 19. April 1972 (BGBl. I S. 713) in der jeweils geltenden Fassung in dieser Eigenschaft anvertraut wurden oder die es in dieser Eigenschaft einer anderen Person anvertraut hat, oder

2. Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken oder mitgewirkt haben, in Ausübung dieser Tätigkeit erlangt, vertraulich verarbeitet oder vertraulich weitergegeben haben,

sowie Maßnahmen zur Erlangung von Erkenntnissen über die Herkunft solcher Informationen sind unzulässig, soweit sie nicht zur Beobachtung mindestens erheblich beobachtungsbedürftiger Bestrebungen oder Tätigkeiten im Einzelfall zwingend erforderlich sind.

(4) Maßnahmen, die in das Vertrauensverhältnis einer Berufsgeheimnisträgerin oder eines Berufsgeheimnisträgers eingreifen und nicht von Absatz 3 erfasst sind, sind nur zulässig, wenn aufgrund bestimmter Tatsachen anzunehmen ist, dass das öffentliche Interesse an der Beobachtung das Interesse am Schutz des Vertrauensverhältnisses überwiegt. Berufsgeheimnisträgerinnen und Berufsgeheimnisträger in diesem Sinne sind die in § 203 des Strafgesetzbuches genannten Personen, die von Berufs wegen zur Wahrung fremder Geheimnisse, namentlich zum persönlichen Lebensbereich gehörender Geheimnisse oder von Betriebs- oder Geschäftsgeheimnissen verpflichtet sind. Bei der Abwägung sind insbesondere das öffentliche Interesse an der von der Berufsgeheimnisträgerin oder dem Berufsgeheimnisträger wahrgenommenen Aufgabe und das Interesse an der Geheimhaltung der ihr beziehungsweise ihm anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Das öffentliche Interesse an der Beobachtung überwiegt in der Regel, soweit die Maßnahme zur Beobachtung gesteigert beobachtungsbedürftiger Bestrebungen oder Tätigkeiten im Einzelfall erforderlich ist.

(…)

(8) Die Absätze 3 und 4 sind nicht auf Personen anzuwenden, bei denen bestimmte Tatsachen den Verdacht für Bestrebungen oder Tätigkeiten im Sinne des § 3 Absatz 1 bei ihnen selbst begründen oder sie diese durch Entgegennahme oder Weitergabe von Mitteilungen unterstützen. Überdies darf die G 10-Kommission in diesen Fällen die Auswertung von Brief- und Postsendungen sowie automatisiert erhobenen Daten nach einer Prüfung im Einzelfall auch im Hinblick auf das ansonsten geschützte Berufsgeheimnis zulassen. Bei Maßnahmen nach § 10 Absatz 1 Nummer 3 und 15 entscheidet das anordnende Gericht. Für erhobene Informationen, welche nicht die Verstrickung mit Bestrebungen oder Tätigkeiten gemäß § 3 Absatz 1 betreffen, gilt das Verfahren der Absätze 6 und 7.

§ 11 Erhebung personenbezogener Daten mit nachrichtendienstlichen Mitteln

(…)

(2) Ein nachrichtendienstliches Mittel zur systematischen Gewinnung von Daten darf sich nur gezielt gegen eine bestimmte Person richten, wenn tatsächliche Anhaltspunkte dafür bestehen, dass diese

1. (…)

2. mit einer Person nach Nummer 1 in Kontakt steht und

   a) von deren Bestrebungen oder Tätigkeiten Kenntnis hat oder

   b) die Person nach Nummer 1 sich ihrer zur Förderung der Bestrebungen oder Tätigkeiten bedient

und die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Überprüfung der Nachrichtenehrlichkeit und der Eignung von Vertrauenspersonen bleibt unberührt. Der Einsatz der nachrichtendienstlichen Mittel darf auch erfolgen, wenn Dritte unvermeidbar betroffen werden.

(…)

§ 20 Zugriff auf Videoüberwachungen des öffentlich zugänglichen Raums

(1) Die Verfassungsschutzbehörde darf zur Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebungen und Tätigkeiten verfügbare private und öffentliche Einrichtungen zur Videobeobachtung des öffentlich zugänglichen Raums in Echtzeit punktuell unentgeltlich mitnutzen. Die eine Einrichtung betreibenden oder verfügungsberechtigten Personen haben den Bediensteten der Verfassungsschutzbehörde auf Verlangen Zutritt zu den Räumlichkeiten, in denen sich die Einrichtung befindet, zu gewähren und die Mitbenutzung der Einrichtung zu dulden.

(2) Die Verfassungsschutzbehörde darf zur Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebungen und Tätigkeiten die Betreiberin oder den Betreiber einer Einrichtung zur Videoüberwachung des öffentlich zugänglichen Raums verpflichten, Bild- und Tonaufzeichnungen unentgeltlich in Echtzeit auszuleiten und Aufzeichnungen zu übermitteln. Die eine Einrichtung betreibenden oder verfügungsberechtigten Personen haben der Verfassungsschutzbehörde die relevanten Daten auf Verlangen und unentgeltlich zur Verfügung zu stellen. Die Verfassungsschutzbehörde hat die angeforderten Bild- und Tonaufzeichnungen sowie Ausleitungen soweit wie möglich nach Datum, Ort und Zeit einzugrenzen und dies den eine Einrichtung betreibenden oder verfügungsberechtigten Personen mitzuteilen. Die Verpflichtungen dürfen sich auch auf Daten beziehen, die bis zu einem Jahr vor dem Anordnungszeitpunkt liegen.

(3) Maßnahmen nach Absatz 1, welche die Grenzen des § 19 Absatz 2 Nummer 2 Buchstaben b und c überschreiten, sowie nach Absatz 2 bedürfen einer richterlichen Anordnung. Die Anordnung der Maßnahmen ist auf höchstens sechs Monate zu befristen. Verlängerungen um jeweils nicht mehr als sechs weitere Monate sind zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Über die Anordnung in den übrigen Fällen des Absatzes 1 entscheidet die Leitung der Verfassungsschutzabteilung oder ihre Vertretung in entsprechender Anwendung von § 13 Absatz 3.

(4) Die überlassenen Bild- und Tonaufzeichnungen sind nach der Auswertung unverzüglich zurückzugeben, zu löschen oder zu vernichten, soweit die Voraussetzungen in Absatz 2 nicht mehr vorliegen oder die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind.

(5) § 8 Absatz 4 Satz 1 und 2, Absatz 5, 6 und 7 Satz 1 und 2 gilt entsprechend.

§ 26 Einsatz automatisierter Verfahren zur Datenanalyse

(1) Die Verarbeitung personenbezogener Daten darf auch mittels automatisierter Verfahren erfolgen.

(2) Die Verfassungsschutzbehörde darf zur Filterung, Sortierung und Priorisierung bei ihr vorhandener personenbezogener Daten Systeme mit mathematisch-statistischen Verfahren, wie maschinellem Lernen und künstlicher Intelligenz, nutzen, wenn dies zur Aufklärung bestimmter beobachtungsbedürftiger Bestrebungen oder Tätigkeiten im Sinne des § 3 Absatz 1 im Einzelfall erforderlich ist. Der Einsatz selbst weiter lernender Systeme ist unzulässig. Eine Verknüpfung der Analysesysteme mit dem Internet erfolgt

nicht. Durch den Einsatz eines nachrichtendienstlichen Mittels gemäß § 10 Absatz 1 Nummer 15 gewonnene Daten dürfen nicht nach Satz 1 verarbeitet werden.

(3) Die Verfassungsschutzbehörde darf zur Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebungen und Tätigkeiten bei ihr vorhandene Daten, insbesondere im elektronischen Aktensystem oder im nachrichtendienstlichen Informationssystem gespeicherte personenbezogene Daten, mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, wenn dies zu den ursprünglichen Erhebungszwecken der betroffenen Daten nicht außer Verhältnis steht. Dabei dürfen auch Systeme mit mathematisch-statistischen Verfahren, wie maschinelles Lernen und künstliche Intelligenz, genutzt werden. Der Einsatz selbst weiter lernender Systeme ist unzulässig. Eine Verknüpfung der Analysesysteme mit dem Internet erfolgt nicht. Eine Kennzeichnung nach § 24 Absatz 5 ist aufrecht zu erhalten. Das Einbeziehen von polizeilichen Datenbanken oder von Daten, die durch den Einsatz eines nachrichtendienstlichen Mittels gemäß § 10 Absatz 1 Nummer 15 erhoben wurden, ist nicht zulässig.

(4) Im Rahmen der Verarbeitung nach Absatz 3 können insbesondere datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, Suchkriterien gewichtet, die eingehenden Erkenntnisse bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(5) Eingesetzte IT-Produkte sind regelmäßig zu überprüfen und auf dem Stand der Technik zu halten. Soweit wie technisch möglich, muss die Nachvollziehbarkeit der nach den Absätzen 1 bis 4 verwendeten Verfahren sichergestellt werden.

(6) Die Verfassungsschutzbehörde darf allgemein zugängliche und bei ihr vorhandene personenbezogene Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten weiterverarbeiten, soweit dies erforderlich ist, insbesondere, weil

1. unveränderte Daten benötigt werden oder

2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Soweit möglich, sollen dabei Daten aus allgemein zugänglichen Quellen genutzt werden. Die Daten sind so auszuwählen, dass statistische Verzerrungen und diskriminierende Verarbeitungsprozesse möglichst vermieden werden. Die Nutzung von Analyseergebnissen als Trainingsdaten ist nur zulässig, wenn die Analyseergebnisse durch qualifizierte Mitarbeiterinnen oder Mitarbeiter der Verfassungsschutzbehörde geprüft und nachvollzogen worden sind. Daten aus dem Einsatz eines nachrichtendienstlichen Mittels nach § 10 Absatz 1 Nummer 15 dürfen nicht nach Satz 1 verarbeitet werden.

(7) Personenbezogene und weitere Daten, die für Zwecke der Absätze 5 und 6 erforderlich sind, sind getrennt von den Akten und Dateien nach § 24 Absatz 1 Satz 2 vorzuhalten. Eine Verwendung dieser getrennt vorgehaltenen Daten zu anderen Zwecken ist unzulässig. Sie sind zum frühestmöglichen Zeitpunkt zu anonymisieren. Die Daten sind

zu löschen, sobald die Verfahren nicht mehr genutzt werden, zu deren Entwicklung, Überprüfung, Änderung oder Training sie verwendet wurden. Soweit Daten aus dem Einsatz nachrichtendienstlicher Mittel nach § 10 Absatz 1 Nummer 7 bis 14 eingeflossen sind, ist die Löschung gemäß § 21 Absatz 7 und 9 vorzunehmen. Soweit bei Datenverarbeitungen nach den Absätzen 1 bis 4 Daten Dritter verarbeitet werden, sind diese Daten nach der Verarbeitung zu löschen.

(8) Automatisierte Entscheidungen auf Basis der nach den Absätzen 1 bis 3 ermittelten Daten, insbesondere zum Einsatz nachrichtendienstlicher Mittel, sind ausgeschlossen. Die Letztbewertung der Analyseergebnisse obliegt einer Mitarbeiterin oder einem Mitarbeiter der Verfassungsschutzbehörde. Diese oder dieser steuert auch die aktenmäßige Erfassung der verarbeiteten Daten und Analyseergebnisse.

(9) Die Entscheidung über den Einsatz automatisierter Datenauswertungen gemäß der Absätze 2 und 3, bei denen auch mit nachrichtendienstlichen Mitteln erhobene Daten verarbeitet werden, trifft die Leitung der Verfassungsschutzabteilung oder ihre Vertretung. Diese entscheidet auch über die Entwicklung, Überprüfung, Änderung oder das Training entsprechender IT-Produkte. Die Entscheidung ist zu dokumentieren. In ihr sind das Ziel der Datenauswertung sowie die einzubeziehenden Daten darzustellen.

(10) Der Zugang zu und die Nutzung von automatisierten Verfahren sind mit einem Rechte- und Rollenkonzept zu regeln. Die Nutzerinnen und Nutzer sind besonders zu qualifizieren. In diesem ist die Zahl der Nutzerinnen und Nutzer angemessen zu begrenzen. Bei jeder Nutzung sind Zeitpunkt, Angaben, die die Feststellung der verarbeiteten Daten ermöglichen sowie Angaben zur Feststellung der Nutzerin oder des Nutzers zu protokollieren. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

(11) Das Nähere zur Entwicklung, Überprüfung, Änderung oder dem Training entsprechender IT-Produkte sowie zur Nutzung der automatisierten Verfahren nach den Absätzen 2 und 3 sowie zur Datenhaltung im Sinne des Absatzes 7 ist in einer Dienstanweisung zu regeln, die nach Anhörung des Parlamentarischen Kontrollgremiums erlassen wird. Vor jeder Änderung der Dienstanweisung ist das Parlamentarische Kontrollgremium zu hören.

§ 33 Weitere Bestimmungen

(…)

(3) Für die Übermittlung aus automatisierten Datenverarbeitungen gemäß § 26 Absatz 1 bis 4 gewonnener Erkenntnisse an Stellen außerhalb des Verfassungsschutzverbunds ist jeweils die Vorschrift anzuwenden, welche dem intensivsten Eingriffsgewicht der verarbeiteten Daten unter Betrachtung des jeweiligen Erhebungswegs entspricht.

§ 36 Übermittlung personenbezogener Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten

(1) Die Verfassungsschutzbehörde darf zum Zweck des § 26 Absatz 6 personenbezogene Daten an öffentliche oder nichtöffentliche Stellen übermitteln, soweit dies erforderlich ist, insbesondere weil

1. unveränderte Daten benötigt werden oder

2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Durch technische und organisatorische Maßnahmen hat die Verfassungsschutzbehörde bei der Übermittlung zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(2) Übermittlungen dürfen nur erfolgen an Amtsträgerinnen und Amtsträger, für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung Verpflichtete. § 1 Absatz 2, 3 und 4 Nummer 2 des Verpflichtungsgesetzes vom 2. März 1974 (BGBl. I S. 469, 547), das durch § 1 Nummer 4 des Gesetzes vom 15. August 1974 (BGBl. I S. 1942) geändert worden ist, findet auf die Verpflichtung zur Geheimhaltung entsprechende Anwendung. Durch technische und organisatorische Maßnahmen hat die empfangende Stelle zu gewährleisten, dass die personenbezogenen Daten gegen unbefugte Kenntnisnahme geschützt sind. Die empfangende Stelle darf die übermittelten Daten nur zu den Zwecken verwenden, zu denen sie übermittelt wurden, und hat die Daten nach der Verwendung zu löschen. Die Löschung ist gegenüber der Verfassungsschutzbehörde schriftlich zu bestätigen, die elektronische Form ist ausgeschlossen.

(3) Personenbezogene Daten, die mit nachrichtendienlichen Mitteln gemäß § 10 Absatz 1 nach richterlicher Anordnung oder Entscheidung der G 10-Kommission erhoben wurden, dürfen nicht übermittelt werden.

II. Beschwerdeführende

11 Die Beschwerdeführenden zu 1 bis 12 sind Abgeordnete des 18. Landtags von Nordrhein-Westfalen. Der Beschwerdeführenden zu 13 und 14 sind Mitglied des Europäischen Parlaments aus Deutschland, leben in Nordrhein-Westfalen und sind hier auch schwerpunkmäßig politisch aktiv. Die Beschwerdeführenden zu 3 und 8 sind zugleich als Rechtsanwälte tätig. Der Beschwerdeführende zu 7 ist von Beruf Journalist.

12 Die Beschwerdeführenden kommen auf vielerlei Art und Weise und bei verschiedensten Gelegenheiten mit Personen, Bestrebungen und Tätigkeiten in Berührung, die gemäß § 3 Abs. 1 VSG NRW mindestens beobachtungsbedürftig sind. Bereits aufgrund ihrer Tätigkeit als Abgeordnete kommen Sie regelmäßig in Kontakt mit Abgeordneten und anderen Mitgliedern der Alternative für Deutschland (AfD). Diese wird zwar selbst vom Verfassungsschutz in Nordrhein-Westfalen nicht beobachtet. Allerdings stuft der Verfassungsschutz den völkisch-nationalistischen Personenzusammenschluss als Verdachtsfall ein und bescheinigt ihm, einen „relevanten – jedoch nicht dominierenden – Faktor“ im Landesverband der

AfD darzustellen.[7] Auch die neu gegründete Jugendorganisation „Generation Deutschland“ ist nach Ansicht des Verfassungsschutzes ein Verdachtsfall.[8] Er sieht hier große personelle Kontinuitäten zu der Jungen Alternative NRW, der Vorgängerjugendorganisation. Diese ist aus Sicht des Verfassungsschutzes Bestandteil der rechtsextremistischen Strömung der Neuen Rechten.[9] Es ist daher mit einiger Wahrscheinlichkeit davon auszugehen, dass die Beschwerdeführenden im Rahmen ihrer parlamentarischen Tätigkeit sowie ihrer politischen Tätigkeit in Wahlkämpfen, im Wahlkreis und politischen Veranstaltungen im gesamten Bundesland mit Mitgliedern der AfD nicht nur flüchtig in Kontakt kommen, die einer dieser Organisationen angehören.

13 (…)

[7] Verfassungsschutzbericht des Landes Nordrhein-Westfalen 2024, S. 103.
[8] Pressemitteilung vom 6.3.2026, abrufbar unter: https://www.land.nrw/pressemitteilung/nordrhein-westfaelischer-verfassungsschutz-stuft-generation-deutschland-nrw-als.
[9] Verfassungsschutzbericht des Landes Nordrhein-Westfalen 2024, S. 103.

C. Zulässigkeit

14 Die Verfassungsbeschwerde ist zulässig.

I. Beschwerdefähigkeit

15 Die Beschwerdeführenden sind als natürliche Personen Grundrechtsträger und damit beschwerdefähig. Sie machen vorliegend nicht primär ihre Rechte als Abgeordnete geltend, sondern als Bürgerinnen und Bürger.

16 Eine Ausnahme besteht im Hinblick auf den unzureichenden Schutz des Mandatsgeheimnis, das den kommunikativen Austausch zwischen Bürgerinnen und Bürgern mit Abgeordneten schützt. Das Gericht hat nicht ausgeschlossen, dass sich Abgeordnete im Hinblick auf Eingriffe in ihre Privatsphäre auch auf Grundrechte berufen können.[10] Vor Eingriffen in die Vertraulichkeit ihrer Kommunikation in ihrer Funktion als Abgeordnete schützt sie aber in jedem Fall Art. 38 Abs.1 S. 2 i.V.m. Art. 47 S. 2 GG. Dies gilt für Landtagsabgeordnete nach Art. 28 Abs. 1 GG ebenso.[11] Ein Abgeordneter kann dieses Recht auch mittels einer Verfassungsbeschwerde geltend machen, da er anderenfalls schlechter als andere Grundrechtsträger behandelt werden würde und der Prüfungsumfang sich von einem Organstreit unterscheidet.[12]

17 Im Hinblick auf Landtagsabgeordnete hat das Gericht jedoch eine Einschränkung gemacht. So seien

> „Rechte, deren Geltung im Rahmen der verfassungsmäßigen Ordnung der Länder durch Art. 28 Abs. 1 GG gewährleistet ist, darum nicht ohne Weiteres auch vor dem Bundesverfassungsgericht einklagbar."[13]

Sie seien vor dem Bundesverfassungsgericht einklagbar, soweit es keinen „gleichwertigen Rechtsschutz" auf Landesebene gebe.[14] Dabei hat das Gericht sich aber offengezeigt, die Besonderheiten zu berücksichtigen, die sich aus der bundesstaatlichen Ordnung ergeben.[15]

18 Für die Beschwerdeführenden zu 1 bis 12 besteht – unabhängig von einer Verletzung ihrer Grundrechte – daher die Möglichkeit, diese Verletzung ihrer Abgeordnetenrechte als Verstoß gegen Art. 49 Abs. 1 Verfassung für das Land

---

[10] BVerfGE 118, 277 (320) – Verfassungsrechtlicher Status von Bundestagsabgeordneten; BVerfGE 99, 19 (29) – Gysi III.
[11] BVerfGE 134, 141 Rn. 103 ff. – Ramelow.
[12] BVerfGE 108, 251 (266 ff.) – Durchsuchung Abgeordnetenbüro.
[13] BVerfGE 134, 141 Rn. 106 – Ramelow.
[14] BVerfGE 134, 141 Rn. 105 – Ramelow.
[15] BVerfGE 134, 141 Rn. 106 – Ramelow.

Nordrhein-Westfalen, der insoweit Art. 47 S. 2 GG entspricht, vor dem Landesverfassungsgericht geltend zu machen.

19 Dieser Weg steht jedoch nicht den Beschwerdeführenden zu 13 und 14 zur Verfügung. Der Schutz ihrer Rechte als in Deutschland gewählte Mitglieder des Europäischen Parlaments ergibt sich aus § 6 EuAbgG; diese Regelung ist wortgleich mit Art. 47 GG. § 9 Abs. 3 S. 1 VSG NRW verstößt damit gemäß Art. 31 GG gegen Bundesrecht, so dass keine verfassungsgemäße Grundlage für einen Eingriff in die Grundrechte vorliegt, die den Beschwerdeführenden zu 13 und 14 auch als Mitglied des Europäischen Parlaments zustehen. Zudem können sie sich aber auch auf den Schutz berufen, der Mitgliedern des Deutschen Bundestages gemäß Art. 47 S. 2 GG zukommt. Nach Art. 9 Abs. 1 lit. a des Protokolls Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union,[16] das nach Art. 51 EUV Teil des Primärrechts der EU ist, gewährleistet ein Mitgliedstaat den Mitgliedern des Europäischen Parlaments, die aus diesem Mitgliedstaat kommen, die Unverletzlichkeit, die er nationalen Parlamentsmitgliedern zubilligt. Das BVerwG hat bereits für den Fall der Immunität entschieden, auf ein Mitglied des Europäischen Parlaments den Schutz des Art. 46 Abs. 2 GG entsprechend anzuwenden; dabei entschied es auch, dass die Sitzungsperioden durchgängig seien, so dass der Schutz zeitlich im Ergebnis nicht begrenzt sei.[17] Dies gilt auch für den Beschlagnahmeschutz, denn das Unionsrecht verweist zur Definition der Unverletzlichkeit nach Art. 9 Abs. 1 lit. a Protokoll Nr. 7 auf den Schutzumfang des nationalen Rechts für nationale Abgeordnete.[18] Für ein weites Verständnis, das auch Art. 47 S. 2 GG umfasst, spricht auch, dass Art. 9 Protokoll Nr. 7 wie Art. 47 S. 2 GG dem Schutz der Unabhängigkeit der Mandatsausübung dient.[19] Eine Erweiterung des Schutzes, den das Grundgesetz für inländische Sachverhalte gewähren, auf europäische Sachverhalte hat das Gericht auch im Fall der Grundrechtsberechtigung juristischer Personen aus einem anderen Mitgliedstaat angenommen und Art. 19 Abs. 3 GG im Lichte des Unionsrechts erweiternd ausgelegt.[20] So ist jetzt auch im Fall des Art. 47 S. 2 GG zu verfahren.

---

[16] Abl. C 202, S. 268 v. 7.6.2016.
[17] BVerwG, Beschluss v. 10.7.2018 - 2 WDB 2/18 – Rn. 6.
[18] EuGH v. 21.10.2008, C-200/07 und C-201/07, ECLI:EU:C:2008:579, Rn. 25 – Mara; EuGH v. 6.9.2011, C.-163/10, ECLI:EU:C:2011:543, Rn. 25 – Patriciello; EuG v. 17.1.2013, T-346/11 und T-347/11, ECLI:EU:T:2013:23, Rn. 43 – Gollnisch ./. EP.
[19] Zu diesem Zweck EuGH v. 21.10.2008, C-200/07 und C-201/07, ECLI:EU:C:2008:579, Rn. 26 – Mara; EuGH v. 6.9.2011, C.-163/10, ECLI:EU:C:2011:543, Rn. 26 – Patriciello.
[20] BVerfGE 129, 78 (93 f.) – Anwendungserweiterung.

II. Beschwerdegegenstand

20 Die Beschwerde richtet sich gegen ein Landesgesetz und damit gegen einen Akt öffentlicher Gewalt.

III. Beschwerdebefugnis und Subsidiarität

21 Die Beschwerdeführer sind beschwerdebefugt im Sinne von § 90 Abs. 1 BVerfGG. Sie sind durch die angegriffenen Vorschriften unmittelbar, selbst und gegenwärtig in ihren Rechten betroffen. Es ist zumindest möglich, dass Befugnisse nach dem VSG NRW die Beschwerdeführenden in ihren Grundrechten oder als Abgeordnete verletzen.

1. Unmittelbarkeit

22 Die Beschwerdeführenden sind unmittelbar durch die angegriffenen Vorschriften betroffen. Zwar bedürfen diese Vorschriften einer Umsetzung durch weitere Vollzugsakte. Eine unmittelbare Betroffenheit durch ein Gesetz ist nach der ständigen Rechtsprechung des Gerichts aber auch dann zu bejahen, wenn potenziell Betroffene den Rechtsweg nicht bestreiten können, weil die Maßnahme heimlich geschieht und sie von dem konkreten Vollzugsakt **keine Kenntnisse** erhalten. Dies gilt auch, wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, aber von ihr aufgrund **weitreichender Ausnahmebestände** auch langfristig abgesehen werden kann.[21]

a) Benachrichtigungspflicht

23 Dies ist hier der Fall. § 12 Abs. 1 S. 1 VSG NRW sieht zwar vor, dass die betroffenen Personen nach Beendigung des Einsatzes nachrichtendienstlicher Mittel zu benachrichtigen sind. Diese Regelung deckt zum einen aber nicht alle Fälle ab, weil sie nur nachrichtendienstliche Mittel erfasst, und erlaubt zum anderen zahlreiche Ausnahmen, die dazu führen, dass eine **Benachrichtigung in der Praxis weiterhin die absolute Ausnahme** bleibt.[22]

---

[21] BVerfGE 169, 130 – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 99 – Bayerisches Verfassungsschutzgesetz; BVerfGE 155, 119 Rn. 73 – Bestandsdatenauskunft II.

[22] Für das Land Nordrhein-Westfalen gibt es keine aussagekräftigen Statistiken hierzu (siehe etwa Landtag von Nordrhein-Westfalen, Drucksache 18/8594), obwohl das Gericht solche verlangt hat (vgl. BVerfGE 141, 220 Rn. 143 – BKA-Gesetz, auf diesen Mangel hinweisend *Max Planck Institut für zur Erforschung von Kriminalität, Sicherheit und Recht*, Überwachungsgesamtrechnung für Deutschland, Band I (2025), S. 18). Für Einzelbeschränkungen nach dem G-10-Gesetz siehe beispielhaft BT-Drucksache 20/9950, S. 1, wonach eine Mitteilung in 17 Prozent der Fälle erfolgte, die der G-10-Kommission vorgelegt worden sind.

24 So gilt § 12 Abs. 1 S. 1 VSG NRW generell **nur für den Einsatz nachrichtendienstlicher Mittel**. Was nachrichtendienstliche Mittel sind, definiert abschließend § 10 VSG NRW. Keine nachrichtendienstlichen Mittel sind aber etwa die Maßnahmen nach § 6 Abs. 4 VSG NRW oder die automatisierte Datenanalyse nach § 26 VSG NRW einschließlich der Übermittlung zu Zwecken des Trainings nach § 36 VSG NRW. Gegen diese Maßnahmen richtet sich aber gerade die Beschwerde.

25 Zudem sind die **Ausnahmen von der Benachrichtigungspflicht nach § 12 Abs. 3 VSG NRW** sehr weit. Sie geben die Möglichkeit, eine Benachrichtigung zurückzustellen und nach fünf Jahren unter Umständen vollständig von ihr abzusehen (§ 12 Abs. 4 VSG NRW). So erlaubt § 12 Abs. 3 Nr. 1 lit. b VSG NRW, eine Mitteilung bereits dann zurückzustellen, wenn die Aufgabenerfüllung der Verfassungsschutzbehörde, insbesondere durch Offenlegung ihres Erkenntnisstandes oder ihrer Arbeitsweise, gefährdet sein könnte. Dies wird in der Praxis sehr häufig der Fall sein. Auch Ausnahmen wie eine Gefährdung der öffentlichen Sicherheit oder der „Eintritt sonstiger übergreifender Nachteile für das Wohl des Bundes oder eines Landes“ sind sehr vage. Gleiches gilt für überwiegende schutzwürdige Interessen anderer Betroffener (§ 12 Abs. 3 Nr. 2 und 3 VSG NRW). Ein anderer Betroffene kann insbesondere die Zielperson nach § 11 Abs. 2 S. 1 Nr. 1 VSG NRW sein, wie die Gesetzesbegründung hervorhebt.[23] Dies ist im Falle der Beschwerdeführenden von ganz besonderer Relevanz, weil sie in der Regel nicht als Zielperson gemäß § 11 Abs. 2 S. 1 Nr. 1 VSG NRW in Betracht kommen werden, sondern als Kontaktpersonen oder Dritte.

26 Schließlich sieht § 12 Abs. 2 VSG NRW umfangreiche **Ausnahmen gegenüber Dritten** vor, gegen die sich eine Maßnahme nicht unmittelbar gerichtet hat oder deren Identität erst ermittelt werden muss. Diese Ausnahme könnte vielfach in Bezug auf die Beschwerdeführenden eine Rolle spielen, insbesondere im Hinblick auf Maßnahmen, die eine große Streubreite aufweisen und trotzdem aufgrund ihrer Intensität eine Benachrichtigung verfassungsrechtlich erfordern oder die Verarbeitung großer Datenmengen mit sich bringen; dies sind etwa § 6 Abs. 4, § 20, § 26 VSG NRW, gegen die sich die Beschwerdeführenden mit ihrer Beschwerde richten.

b) Auskunftsrecht

27 Von einer Kenntnis der betroffenen Personen ist auch nicht deshalb auszugehen, weil sie von ihrem datenschutzrechtlichen **Auskunftsrecht** gemäß § 30 Abs. 1 S. 1 VSG NRW hätten Gebrauch machen können. Erstens erlaubt § 30 Abs. 2 VSG NRW auch hier zahlreiche weitreichende

[23] Landtag von Nordrhein-Westfalen, Drucksache 18/14557. S. 152.

Ausnahmen, die § 12 Abs. 3 VSG NRW nachgebildet sind; auf die obigen Ausführungen dazu wird daher verwiesen. Nach Einschätzung von Sachverständigen wird daher die Auskunft auch in Zukunft die Ausnahme bleiben.[24] Zweitens erstreckt sich das Auskunftsrecht nach § 30 Abs. 1 S. 2 VSG NRW nur auf Vorgänge, die strukturiert zu der Person, die Auskunft verlangt, gespeichert worden sind. Ist sie daher nur Dritter oder Kontaktperson wird dies häufig nicht der Fall sein. Ob zusammengeführte Datenbestände nach § 26 Absatz 3 VSG NRW oder mit Datenbeständen des KI-Modelle als strukturierte Speicherung einzuordnen sind, ist zudem zweifelhaft. Drittens schließlich besteht kein Recht auf Auskunft über die Herkunft von personenbezogenen Daten (§ 30 Abs. 3 VSG NRW). Auch ein erfolgreiches Auskunftsersuchen würde daher nicht zwangsläufig dazu führen, dass die Beschwerdeführenden wüssten, wie Daten zu ihnen erhoben worden sind und sie damit Kenntnis von konkreten Vollzugsakten hätten.[25] Gleiches gilt für die Übermittlung von personenbezogenen Daten. Die betroffene Person erfährt hier nicht die Empfänger; diese sind aber für die verfassungsrechtliche Bewertung des Eingriffs durch die Übermittlung entscheidend.[26]

2. Eigene und gegenwärtige Betroffenheit

28 Es ist auch eine eigene und gegenwärtige Betroffenheit der Beschwerdeführenden gegeben.

a) Maßstab

29 Das Gericht hat in ständiger Rechtsprechung einen Maßstab entwickelt, wie Beschwerdeführer ihre eigene und gegenwärtige Betroffenheit nachweisen können, wenn sie von den konkreten Vollzugsakten typischerweise keine Kenntnis haben können. Das Gericht hat es für ausreichend gehalten, wenn die Beschwerdeführer die Möglichkeit darlegen, dass sie mit einiger Wahrscheinlichkeit durch die angegriffenen Rechtsnormen und die darauf beruhenden Maßnahmen in eigenen Grundrechten berührt werden.[27] Für eine Betroffenheit spricht regelmäßig eine große Streubereite, wenn also eine Maßnahme auch in großer Zahl unbeteiligte Personen in ihren Rechten berühren kann, während eine punktuelle, an hohe Anforderungen geknüpfte

---

[24] *Gusy*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2735, S. 16.
[25] Vgl. BVerfGE 169, 130 Rn. 46 – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 107 – Bayerisches Verfassungsschutzgesetz.
[26] Vgl. BVerfGE 162, 1 Rn. 120 – Bayerisches Verfassungsschutzgesetz.
[27] BVerfGE 169, 130 Rn. 38 – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 97 – Bayerisches Verfassungsschutzgesetz; BVerfGE 155, 119 Rn. 75 – Bestandsdatenauskunft II.

Maßnahme höhere Anforderungen an die Darlegung der Betroffenheit auslöst.[28]

30 Im vorliegenden Fall ist zu berücksichtigen, dass weder die Stellung als Abgeordnete noch als Berufsgeheimnisträger eine Verletzung eigener Grundrechte ausschließt. Wie dargelegt werden wird, ist der Schutz des Berufsgeheimnisses nach § 9 Abs. 3 und 4 VSG NRW unzureichend und verhindert eine Überwachung nicht in jedem Fall. Das Gesetz enthält für die Überwachung von Abgeordneten spezielle Regelungen; auch diese schließen einen Eingriff in die Rechte der Beschwerdeführenden nicht aus. So dürfen personenbezogene Daten eines Abgeordneten nach Maßgabe des § 24 Abs. 4 S. 1 VSG NRW gespeichert werden. Diese Regelung gilt jedoch nur für die Speicherung von Daten in Akten, die zu ihrer Person geführt werden, nicht aber für die Speicherung von personenbezogenen Daten über Abgeordnete in Akten zu anderen Personen. Zudem schließt die Regelung eine Speicherung der Daten von Abgeordneten zu ihrer Person nicht komplett aus, sondern lässt sie zu, wenn dies im Einzelfall zur Wahrnehmung einer Aufgabe gemäß § 3 Abs. 1 VSG NRW erforderlich ist. Soweit Daten für andere Aufgaben verarbeitet werden, etwa im Rahmen § 3 Abs. 4 VSG NRW (z.B. Sicherheitsüberprüfungen oder Regelanfragen für waffenrechtliche Erlaubnisse), gelten die Einschränkungen des § 24 Abs. 4 VSG NRW für Daten über Abgeordnete nicht.[29]

b) Eigene und gegenwärtige Beschwer durch die angegriffenen Regelungen

aa) § 9 Abs. 3, 4 und 8 VSG

31 Die Beschwerdeführenden können als Bürgerinnen und Bürger, als Abgeordnete sowie die Beschwerdeführenden zu 3 und 8 als Rechtsanwälte durch den unzureichenden Schutz des Berufsgeheimnisses bzw. der Vertrauensbeziehung zwischen Abgeordneten und Bürgerinnen und Bürgern in ihren Rechten berührt sein (Art. 12 Abs. 1 GG; Art. 47 i.V.m. Art. 38 Abs. 1 S.2, Art. 28 Abs. 1 S. 1 GG). Ferner sind die Beschwerdeführenden zu 5 und 10 durch den fehlenden Schutz des seelsorgerischen Gespräches in ihrer Religionsfreiheit (Art. 4 Abs. 1 GG) betroffen.

32 Als **Abgeordnete** haben die Beschwerdeführenden Kontakt zu zahlreichen Bürgerinnen und Bürgern. Darunter können sich auch solche Personen befinden, die Zielpersonen des Verfassungsschutzes sind, weil sie an einer

[28] BVerfGE 169, 130 Rn. 39 – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 98 – Bayerisches Verfassungsschutzgesetz.
[29] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 187.

beobachtungsbedürftigen Bestrebung oder Tätigkeit beteiligt sind. In diesem Fall ist es nicht auszuschließen, dass der Schutz der vertraulichen Kommunikation zwischen Abgeordneten und Bürgern nicht anwendbar ist. Der Verfassungsschutz könnte hier zu dem Ergebnis kommen, dass im Fall einer erheblich beobachtungsbedürftigen Tätigkeit oder Bestrebung das Aufklärungsinteresse eine Überwachung zwingend erfordert. Dann würde der Schutz nicht mehr greifen (vgl. § 9 Abs. 3 VSG NRW). Der Schutz könnte auch entfallen, wenn die Beschwerdeführenden als Nachrichtenmittler eingestuft werden würden (§ 9 Abs. 8 Satz 1 VSG NRW). Würden Sie zugleich als Kontaktpersonen nach § 11 Abs. 2 Nr. 2 VSG NRW eingestuft werden, könnten unmittelbar nachrichtendienstliche Mittel gegen sie eingesetzt werden. Auch im Übrigen könnten sie als Dritte betroffen sein, wenn ihr Kommunikationspartner mit nachrichtendienstlichen Mitteln überwacht wird.

33 Der unzureichende Schutz von **Rechtsanwältinnen und Rechtsanwälten** durch § 9 Abs. 4 VSG NRW betrifft zunächst die Beschwerdeführende zu 3 und den Beschwerdeführenden zu 8 in ihrer Berufsfreiheit. Als Rechtsanwältin und als Rechtsanwalt können sie nicht mehr von der vollständigen Vertraulichkeit der Kommunikation mit ihren Mandanten ausgehen. Wird ein Mandant vom Verfassungsschutz überwacht, muss das Berufsgeheimnis nach§ 9 Abs. 4 S. 1 VSG NRW zurücktreten, wenn das Aufklärungsinteresse überwiegt. Denkbar wäre es etwa, dass sich eine Person, die an einer Bestrebung oder Tätigkeit beteiligt ist, die nach § 3 Abs. 1 VSG NRW beobachtungsbedürftig ist, als Mandant an die Beschwerdeführende zu 3 oder den Beschwerdeführenden zu 8 wendet. Dies kann auch in einer Angelegenheit der Fall sein, die nichts mit der beobachtungsbedürftigen Tätigkeit oder Bestrebung zu tun hat (z.B. einer familienrechtlichen oder baurechtlichen Angelegenheit). Dies ist für den Verfassungsschutz von außen nicht erkennbar.

34 Die Einschränkung des Vertrauensverhältnisses zwischen Rechtsanwalt bzw. Rechtsanwältin und **Mandant bzw. Mandantin** betrifft jedoch alle Beschwerdeführenden, wenn Sie als Mandant oder Mandantin Rechtsrat suchen. Es ist nicht ausgeschlossen, dass der Rechtsanwalt, an den sie sich wenden, in einer verfassungsfeindlichen Bestrebung oder Tätigkeit engagiert ist; möglicherweise wissen die Beschwerdeführenden dies gar nicht, weil die Mandatierung einen vollkommen anderen Lebensbereich betrifft und sein Engagement nicht öffentlich ist. Dies allein kann bereits nach § 9 Abs. 8 Satz 1 VSG NRW zur Aufhebung des Schutzes des Berufsgeheimnisses führen. Zwar greifen dann Mechanismen wie zum Schutz des Kernbereichs privater Lebensgestaltung; diese ändern aber nichts daran, dass das Vertrauensverhältnis erst einmal beeinträchtigt wird.

35 (…)

bb) § 11 Abs. 2 Nr. 2 VSG NRW

36 Aufgrund der weiten Definition von Kontaktpersonen nach § 11 Abs. 2 Nr. 2 VSG NRW besteht auch die Möglichkeit, dass die Beschwerdeführenden mit einiger Wahrscheinlichkeit von Überwachungsmaßnahmen mit nachrichtendienstlichen Mitteln betroffen sein können. Es ist bereits ausreichend, um als Kontaktperson eingestuft zu werden, wenn eine Person weiß, dass jemand an einer Bestrebung oder Tätigkeit nach § 3 Abs. 1 VSG NRW beteiligt ist (§ 11 Abs. 2 Nr. 2 lit. b VSG NRW). Die Beschwerdeführenden gehen beispielsweise davon aus, dass dies wahrscheinlich auf Mitglieder und Angestellte der AfD-Fraktion im Landtag von Nordrhein-Westfalen zutrifft, weil sich unter ihnen Personen befinden, die Mitglieder der Jugendorganisation Generation Deutschland sind oder dem völkisch-nationalen Personenzusammenschluss in der AfD zuzurechnen sind.

37 Darüber hinaus ist § 11 Abs. 2 Nr. 2 lit. b VSG NRW so weit gefasst, dass darunter nahezu jede Tätigkeit fallen kann. Denn es muss noch nicht einmal der Kontaktperson bekannt sein, dass sie gerade eine erheblich beobachtungsbedürftige Bestrebung oder Tätigkeit fördert. Auch neutrale Handlungen können darunterfallen. Würde sich etwa ein Funktionär einer Bestrebung nach § 3 Abs. 1 VSG NRW an die Beschwerdeführende zu 3 oder den Beschwerdeführenden zu 8 in ihrer Funktion als Rechtsanwältin bzw. Rechtsanwalt wenden, um sich beim Abschluss eines Mietvertrags beraten zu lassen, könnte dies bereits ausreichen, wenn die angemieteten Räume für den Zweck der Tätigkeit oder Bestrebungen genutzt werden würden – auch wenn dieses Motiv nicht offengelegt werden würde.

cc) § 20 VSG NRW

38 Der Zugriff auf private und staatliche Videoüberwachungseinrichtungen nach § 20 VSG NRW berührt die Beschwerdeführenden gegenwärtig in ihren eigenen Grundrechten, vor allem ihrem allgemeinen Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Die Maßnahme weist eine hohe Streubreite auf und greift daher nicht nur in die Grundrechte von Zielpersonen ein, sondern auch im großen Umfang in die Grundrechte von Dritten. Dies hat

auch der Gesetzgeber in der Begründung selbst erkannt.[30] Zu diesen Dritten gehören, unabhängig von der Frage, ob sie auch Kontaktpersonen sein können, die Beschwerdeführenden. Sie bewegen sich privat, beruflich und politisch im öffentlichen Raum in Nordrhein-Westfalen, z.B. in Verkehrsmitteln, auf Bahnhöfen, öffentlichen Plätzen, Veranstaltungen und anderen Orten, an denen Videoüberwachung aus verschiedensten Gründen (z.B. wegen möglicher Kriminalität) erfolgt. Es bestehen daher vielfältige Gelegenheiten, bei denen sie als Dritte erfasst werden können.

39 Im Rahmen von Videoaufnahmen des öffentlichen Raumes werden Dritte typischerweise gleichzeitig mit den Zielpersonen erfasst, so dass die Informationen über sie und die Zielperson untrennbar miteinander verbunden sind. Eine Erhebung personenbezogener Daten über sie ist daher zulässig (§ 6 Abs. 7 S. 2 VSG NRW), ebenso eine Weiterverarbeitung (vgl. § 24 Abs. 3 S. 1 i.V.m. § 6 Abs. 7 S. 2 VSG NRW).

dd) Regelungen zur automatisierten Datenanalyse (§ 6 Abs. 4 S. 1 und 2, § 26, § 33 Abs. 3 und § 36 VSG NRW)

40 Die Beschwerdeführenden sind durch die verschiedenen Regelungen zur automatisierten Datenanalyse gegenwärtig in ihren Rechten betroffen. Ziel der automatisierten Datenanalyse ist es gerade, eine große Zahl von Informationen zusammenzuführen. Bereits darin liegt ein eigenständiger Grundrechtseingriff durch eine zweckändernde Weiterverarbeitung.[31] Die Streubreite ist zudem denkbar weit.

41 Für die Zulässigkeit der Beschwerde ist es unerheblich, ob die angegriffenen Befugnisse bereits genutzt werden.[32] Dies kann jederzeit geschehen, auch ohne Kenntnis der Öffentlichkeit von diesem Schritt.[33]

(1) § 26 Abs. 2, 3 und 6 und § 36 VSG NRW

42 § 26 Abs. 2, 3 und 6 VSG NRW erlauben die Verarbeitung aller beim Verfassungsschutz vorhandenen Daten. Darunter fallen auch Daten Dritter, aber auch personenbezogene Daten, die etwa im Rahmen von Sicherheitsüberprüfungen nach § 3 Abs. 4 VSG NRW erhoben worden sind; hierunter dürften sich auch Daten der Beschwerdeführenden befinden, weil viele Mitarbeiterinnen und Mitarbeiter, die im Landtag arbeiten,

---

[30] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 148.
[31] Vgl. BVerfGE 156, 11 Rn. 73 f. – Antiterrordateigesetz II; BVerfGE 165, 363 Rn. 50, 67 ff. – automatisierte Datenanalyse.
[32] Vgl. BVerfGE 165, 363 Rn. 15 – automatisierte Datenanalyse (die Freie und Hansestadt Hamburg hatte – anders als Hessen – noch nicht einmal ein Programm zur Nutzung der gesetzlichen Befugnis beschafft).
[33] Vgl. BVerfGE 156, 11 Rn. 59 – Antiterrordateigesetz II.

sicherheitsüberprüft werden müssten und die Beschwerdeführenden hier mit einiger Wahrscheinlichkeit als Auskunftspersonen benannt sein dürften.

43 (…)

44 § 26 Abs. 6 und § 36 Abs. 1 VSG NRW sehen zudem – sogar vorrangig – die Nutzung allgemein zugänglicher Daten zum Training sowie zur Entwicklung, Überprüfung und Änderung von IT-Produkten vor. Dies zielt auf das Training mit Daten aus dem Internet.[34] Die Streubreite ist auch hier sehr weit. Es bleibt vollkommen unklar, wie die allgemein zugängliche Datenmenge eingegrenzt wird. Die Menge der betroffenen Personen wird dadurch schwer überschaubar. Dies liegt jedoch in der Natur der Datenverarbeitung begründet. Da durch das Training das abstrakte Wissen des KI-Modells erzeugt wird, erscheint es sehr wahrscheinlich, dass das Modell auch Informationen über das politische System und Leben in NRW „lernt“ und damit auch Daten über die Beschwerdeführenden verarbeitet. § 6 Abs. 7 S. 3 VSG NRW schließt dabei nur die gezielte automatisierte Erhebung von Daten über Dritte aus.

45 Sind die personenbezogenen Daten erst einmal Teil des KI-Modells geworden, werden sie darin weiterverarbeitet. Dies begründet zusätzlich die Beschwer durch den Einsatz der IT-Produkte nach § 26 Abs. 2 und 3 sowie § 6 Abs. 4 S. 2 VSG NRW sowie die unzulängliche Regelung zur Löschung nach § 26 Abs. 7 VSG NRW.

46 Da mit einiger Wahrscheinlichkeit auch Daten der Beschwerdeführenden im Rahmen der Datenanalyse nach § 26 Abs. 2 und 3 VSG NRW verarbeitet werden, betreffen sie auch die unzulänglichen Regelungen zur Qualitätssicherung, Auswahl einer verlässlichen Software und Vertragspartners, zur Vermeidung von Diskriminierung und zur Gewährleistung der Nachvollziehbarkeit der Ergebnisse der Datenanalyse sowie die zu niedrige Eingriffsschwellen. Für sie besteht eine erhöhte Wahrscheinlichkeit, von den Risiken des Einsatzes von KI und maschinellem

[34] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 193.

Lernen betroffen zu werden (z.B. indem sie irrtümlich mit einer erheblich beobachtungsbedürftigen Bestrebung assoziiert werden).

(2) § 33 Abs. 3 VSG NRW

47 Die Beschwerdeführenden sind auch von den zu niedrigen Übermittlungsschwellen selbst und gegenwärtig betroffen. Wenn ihre Daten – sei es als Datenbestand des Verfassungsschutzes, als allgemein zugängliche Daten oder als Ergebnis eines Webcrawlings nach § 6 Abs. 4 S. 1 uns 2 VSG NRW, das dem Verfassungsschutz ebenfalls zur Verfügung steht – verarbeitet werden, können auch Ergebnisse der Analyse personenbezogene Daten über sie enthalten. Dementsprechend können sie durch eine Übermittlung dieser Analysen, bei der die verfassungsrechtlich vorgesehenen Voraussetzungen nicht eingehalten werden, in ihren Grundrechten verletzt werden.

(3) § 6 Abs. 4 S. 1 und 2 VSG NRW

48 § 6 Abs. 4 S. 1 und 2 VSG NRW erlaubt den Einsatz von KI und maschinellem Lernen zur automatisierten Erhebung von Daten und Verarbeitung (Filterung, Sortierung und Priorisierung). Dies zielt vor allem auf die Erhebung von öffentlich zugänglichen Daten aus dem Internet; die Gesetzesbegründung spricht hier von „Webcrawling“, also einem automatischen Durchkämen des Internets.[35] Hierin liegt – wie dargelegt werden wird (→Rn. 245 f.) – ein Grundrechtseingriff, denn der Verfassungsschutz erhebt hier systematisch Daten und führt keine „Online-Streife“ durch, bei der er sich einzelne Websites ansieht. Es verwirklichen sich vielmehr bei dieser Form der Datenerhebung und Aufbereitung die Risiken der modernen Datenverarbeitung, denen das Recht auf informationelle Selbstbestimmung gerade entgegenwirken soll.[36] Eine nähere tatbestandliche Eingrenzung nimmt § 6 Abs. 4 S. 1 und 2 VSG NRW nicht vor; die erhobenen Daten müssen lediglich zur Aufklärung bestimmter beobachtungsbedürftiger Bestrebungen erforderlich sein. Es wird lediglich die gezielte Erhebung von Daten Dritter ausgeschlossen (§ 6 Abs. 7 S. 3 VSG NRW). Eine Massendatenerhebung mittels Webcrawling ist damit gerade nicht ausgeschlossen. Aufgrund der Streubreite der Regelung und dem Ziel der Befugnis, große Datenmengen aus dem Internet zu verarbeiten, ist die Zahl der betroffenen Personen schwer einzugrenzen. Potenziell kann von einer solchen „Online-Rasterfahndung“[37] jeder betroffen sein.[38]

---

[35] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 117.
[36] BVerfGE 65, 1 (43) – Volkszählung; BVerfGE 152, 152 Rn. 84 f. – Recht auf Vergessen I.
[37] So der Sachverständige *Achelpöhler* (DAV) in der Anhörung, Landtag von Nordrhein-Westfalen, APr 18/974, S. 18
[38] Vgl. zur Rasterfahndung BVerfGE 165, 1 Rn. 73 – Polizeiliche Befugnisse nach SOG MV.

IV. Subsidiarität und Rechtswegerschöpfung

1. Maßstab

49 Die Beschwerde wahrt den Grundsatz der Subsidiarität. Das Gericht hat aus der Subsidiarität spezielle Zulässigkeitsanforderungen abgeleitet. Zwar steht gegen ein Gesetz kein Rechtsweg zur Verfügung. Es sind jedoch daneben alle zumutbaren Mittel zu nutzen, um der Grundrechtsverletzung zunächst anderweitig abzuhelfen. Dies kann nach der Rechtsprechung des Gerichts auch eine Feststellungs- und Unterlassungsklage sein. Zweck der Subsidiarität der Verfassungsbeschwerde ist, dass das Gericht seine Entscheidung nicht auf einer ungesicherten Tatsachen- und Rechtsgrundlage treffen muss, sondern sich auf verfassungsrechtliche Fragen konzentrieren kann.[39] Dies entspricht auch seiner Funktion als Verfassungsgericht. Auf eine fachgerichtliche Feststellungs- und Unterlassungsklage kann daher verzichtet werden, wenn diese Fragen ausreichend geklärt sind und die Beurteilung der angegriffenen Normen allein verfassungsrechtliche Fragen aufwirft.[40]

2. Spezifisch verfassungsrechtliche Fragen

50 Vorliegend kann auf eine fachgerichtliche Klärung verzichtet werden, weil die Verfassungsbeschwerde auf spezifisch verfassungsrechtliche Fragen zielt und keine fachgerichtliche Vorklärung erforderlich ist. Dies betrifft sowohl die Regelungen zum Schutz von Berufsgeheimnisträgern (§ 9 VSG NRW), als auch die Definition der Kontaktpersonen (§ 11 Abs. 2 Nr. 2 VSG NRW) sowie die Regelungen zum Zugriff auf private und staatliche Videoüberwachung (§ 20 VSG NRW) und die Regelungen zum Einsatz automatisierter Datenanalyse (§ 6 Abs. 4 S. 1 und 2, § 26, § 33 Abs. 3, § 36 VSG NRW). Diese Regelungen werfen im Kern verfassungsrechtliche Fragen auf, ohne dass es auf die Auslegung des Fachrechts ankäme oder eine Ermittlung des Sachverhalts durch ein Fachgericht die Entscheidungsfindung des Gerichts erleichtern würde. Die Anrufung eines Fachgerichts und eine anschließende konkrete Normenkontrolle nach Art. 100 Abs. 1 GG würden eine Klärung daher nur verzögern.

---

[39] Zum Ganzen BVerfGE 169, 130 Rn. 40 f. – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 100 ff. – Bayerisches Verfassungsschutzgesetz; BVerfGE 150, 309 Rn. 41 ff. – Kfz-Kennzeichenkontrolle II.

[40] BVerfGE 162, 1 Rn. 102 – Bayerisches Verfassungsschutzgesetz; BVerfGE 169, 130 Rn. 42 – Hessisches Verfassungsschutzgesetz; BVerfGE 115, 119 Rn. 77 – Bestandsdatenauskunft II; BVerfGE 150, 309 Rn. 44 – Kfz-Kennzeichenkontrolle II.

3. Möglichkeit fachgerichtlichen Rechtsschutzes

51 Zudem ist es sehr zweifelhaft, ob die Beschwerdeführenden fachgerichtlichen Rechtsschutz durch eine Feststellungs- und Unterlassungsklage erreichen könnten. Das Bundesverwaltungsgericht verlangt in ständiger Rechtsprechung für eine Unterlassungsklage:

> „Eine vorbeugende Unterlassungsklage, mit der ein drohendes tatsächliches Verwaltungshandeln abgewehrt werden soll, ist nur statthaft, wenn sich dieses Handeln hinreichend konkret abzeichnet, insbesondere die für eine Rechtmäßigkeitsprüfung erforderliche Bestimmtheit aufweist."[41]

Diesen Maßstab legt das Bundesverwaltungsgericht auch im Falle heimlicher Überwachungsmaßnahmen durch einen Nachrichtendienst an.[42] Da die konkreten Vollzugsakte heimlich erfolgen, die Beschwerdeführenden typischerweise nicht benachrichtigt werden und auch keine andere Möglichkeit haben, genauere Kenntnis von den Vollzugsakten zu erhalten, ist es ihnen nahezu unmöglich, diese Anforderungen des Bundesverwaltungsgerichts zu erfüllen.

4. Keine weiteren Abhilfemöglichkeiten

52 Neben einer Klage wäre es denkbar, dass sich die Beschwerdeführenden mit der Bitte um Abhilfe an die **nachrichtendienstlichen Kontrollgremien** wenden. Dies wäre jedoch zur Durchsetzung ihrer Rechte nicht effektiv. Erstens erlaubt § 56 Abs. 1 S. 1 VSG NRW zwar eine Eingabe an das Kontrollgremium. Diese Eingabe muss sich aber auf ein konkretes Verhalten des Verfassungsschutzes gegenüber dem Petenten beziehen. Wie bereits dargelegt kennen die Beschwerdeführenden die konkreten Vollzugsakte nicht. Zweitens kann das Kontrollgremium der Eingabe nicht mit einer verbindlichen Entscheidung abhelfen und auch keine konkrete Normenkontrolle initiieren, um eine verfassungswidrige gesetzliche Regelung aufheben zu lassen.

53 Die **G-10-Kommission** bietet keine Abhilfemöglichkeit. Sie ist nicht zuständig, denn sie überwacht nur bestimmte Maßnahmen, die nicht Gegenstand dieses Verfahrens sind (vgl. § 57 Abs. 1 VSG NRW).

V. Frist

54 Die Beschwerdefrist ist gewahrt. Es handelt sich um eine Verfassungsbeschwerde gegen ein Gesetz. Die Beschwerdefrist beträgt daher ein Jahr nach Inkrafttreten des Gesetzes (§ 93 Abs. 3 BVerfGG). Die

[41] BVerwGE 161, 76 Rn. 22 m.w.N.
[42] BVerwG, Urteil vom 25.01.2022 – 6 A 1.22 – Rn. 21 ff.

angegriffenen Regelungen sind am 1. April 2026 in Kraft getreten (vgl. Art. 5 des Gesetzes zur Neuverkündung des Verfassungsschutzgesetzes Nordrhein-Westfalen und zur Änderung weiterer Gesetze).

VI. Sonstige allgemeine Zulässigkeitsvoraussetzungen

55 Die Verfassungsbeschwerde ist nach § 93a Abs. 2 lit. a BVerfGG anzunehmen, weil ihr grundsätzliche verfassungsrechtliche Bedeutung zukommt.

56 Zudem ist sie zur Durchsetzung der Grundrechte der Beschwerdeführenden angezeigt (§ 93a Abs. 2 lit. b BVerfGG), weil sie in einem Bereich, der für die Demokratie und die Ausübung von Grundrechten besonders sensibel ist und zugleich weitgehend der Kontrolle durch Gerichte, politische Diskussion und Öffentlichkeit entzogen ist, in verfassungswidriger Weise tief in die Grundrechte der Bürgerinnen und Bürger eingreift. Der verfassungsgerichtlichen Kontrolle der zugrundeliegenden gesetzlichen Regelungen kommt hier eine besondere Bedeutung zu. Dies spiegelt sich auch in den detaillierten Anforderungen wider, die das Gericht für heimliche Überwachungsmaßnahmen aufgestellt hat.

VII. Zuständigkeit des Bundesverfassungsgerichts

57 Die Zuständigkeit des Bundesverfassungsgerichts ist gegeben und damit die Verfassungsbeschwerde zulässig, da keine unionsrechtlichen Regelungen anwendbar sind, welche die angegriffenen Regelungen erforderten oder gar abschließend regeln.[43] Es kann daher offenbleiben, inwieweit Art. 4 Abs. 2 S. 3 EUV grundsätzlich die Befugnisse der Nachrichtendienste vollständig erfasst[44] und aus dem Anwendungsbereich des Unionsrechts ausklammert.

58 Soweit § 20 Abs. 2 VSG NRW den Zugriff auf Daten erlaubt, die für private Zwecke erhoben worden sind, ist zwar der Anwendungsbereich des Unionsrechts eröffnet, so dass auch die europäischen Grundrechte als Mindeststandard zu berücksichtigen sind.[45] Wie der EuGH in der Rs. *Privacy International* für die E-Privacy-RL (2000/58/EG) klargestellt hat, ist die Offenlegung oder Übermittlung gegenüber einem Nachrichtendienst eine „Verarbeitung“ durch ein Telekommunikationsunternehmen. Art. 4 Abs. 2 S. 3 EUV steht dem nicht entgegen.[46] Diese Rechtsprechung lässt sich auf die

---

[43] BVerfGE 162, 1 Rn. 143 – Bayerisches Verfassungsschutzgesetz; BVerfGE 169, 130 Rn. 83 – Hessisches Verfassungsschutzgesetz.
[44] Für eine differenzierte Sichtweise siehe *Bäcker* in BeckOK, Datenschutzrecht, Art. 2 DSGVO Rn. 9a.
[45] BVerfGE 152, 152 Rn. 67 ff. – Recht auf Vergessen I.
[46] EuGH, Urteil vom 6.10.2020, C-623/17, ECLI:EU:C:200:790, Rn. 42 ff. – Privacy International.

Übermittlung oder Zugänglichmachung zu „Bild- und Tonaufnahmen“ durch Videoüberwachungseinrichtungen übertragen. Auch hierbei handelt es sich um eine „Verarbeitung“ personenbezogener Daten (Art. 4 Nr. 2 DSGVO), so dass die DSGVO und damit das Unionsrecht auf diese Verarbeitung durch den Betreiber der Videoüberwachung als Verantwortlichem anwendbar ist (vgl. Art. 2 Abs. 1 DSGVO).[47] Die Zuständigkeit des BVerfG ist trotzdem eröffnet, weil die DSGVO weder eine Befugnis nach § 20 VSG NRW erfordert, noch abschließende Regelungen hierzu vorsieht.

59 Die KI-VO ist auf den Bereich der nationalen Sicherheit nicht anwendbar (Art. 2 Abs. 3 UAbs. 3 KI-VO).

[47] Ständige Rechtsprechung des EuGH zur Videoüberwachung seit EuGH, Urteil vom 11.12.2014, C-212/13, ECLI:EU:C:2014:2428, Rn. 23, 25 – Ryneš, wonach bereits die Erhebung eine Verarbeitung personenbezogener Daten darstellt und damit auch deren Offenlegung, zumal dem Verfassungsschutz noch zusätzliche Erkenntnisquellen zur Verfügung stehen.

D. Begründetheit

60 Die Verfassungsbeschwerde ist begründet.

I. § 9 Abs. 3, 4 und 8 VSG (Schutz von Berufsgeheimnisträgern)

61 Die Regelungen zum Schutz von Berufsgeheimnisträgern in § 9 Abs. 3, 4 und 8 VSG NRW sind mit den verfassungsrechtlichen Vorgaben nicht vereinbar. Sie gewährleisten keinen strikten Schutz von Informationen, die dem anwaltlichen Berufsgeheimnis, dem Mandatsgeheimnis oder der Vertraulichkeit des seelsorgerischen Gesprächs unterliegen. Hierdurch verletzt die Regelung Art. 1 Abs. 1, Art. 2 i.V.m. Art. 1, Art. 4 Abs. 1 und 2, Art. 12 Abs. 1 und Art. 47 GG sowie Art. 31 GG i.V.m. § 6 EuAbgG. Darüber ist der Schutz von Journalisten unzureichend ausgestaltet und verletzt hierdurch Art. 5 Abs. 1 S. 2 GG.

62 Ein Eingriff in die Grundrechte der Berufsgeheimnisträger ergibt sich hierbei aufgrund der einzelnen Überwachungsbefugnisse.

1. Regelungsinhalt

63 Der Gesetzgeber hat in § 9 VSG eine sehr komplizierte Regelung geschaffen, die sowohl den Schutz des Kernbereichs privater Lebensgestaltung gewährleisten soll als auf den Schutz des Vertrauensverhältnisses verschiedener Berufsgruppen. Diesem Zweck dienen § 9 Abs. 3 und 4 VSG NRW, die zusätzlich durch § 9 Abs. 8 VSG NRW eingeschränkt werden.

64 Das Gesetz unterscheidet zwischen zwei Gruppen:

- **Journalisten und Mandatsträger** sind „als Personen mit institutioneller, verfassungsrechtlicher Bedeutung“[48] nach § 9 Abs. 3 VSG NRW geschützt. Die Regelung erfasst die Erhebung von Informationen, die dem Mandatsgeheimnis unterliegen oder aber der Vertraulichkeit der journalistischen Arbeit, einschließlich Informationen über Herkunft der Informationen (d.h. vor allem der Schutz journalistischer Quellen). Dieser Schutz ist jedoch **nicht absolut**. Er endet, wenn dies zur Beobachtung mindestens erheblich beobachtungsbedürftiger Bestrebungen im Einzelfall zwingend erforderlich ist. Es findet **keine Abwägung** mit den konkreten Vertraulichkeitserwartungen und Umständen des Einzelfalls statt.

[48] Landtag von Nordrhein-Westfalen, Drucksache 18/16212, S. 16 (Änderungsantrag der Fraktionen der CDU und Bündnis 90/Die Grünen).

– § 9 Abs. 4 VSG NRW schützt Informationen, die gemäß **§ 203 StGB** einem Berufsgeheimnis unterliegen (§ 9 Abs. 4 S. 2 VSG NRW). Im parlamentarischen Verfahren hat hier ein Systemwechsel stattgefunden. Der Gesetzentwurf der Landesregierung knüpfte noch an § 53, 53a StPO an. Durch die Änderung wurde der Kreis der geschützten Berufsgruppen erheblich erweitert (vgl. nur Tierärzte, Angestellte einer Versicherung); es entfiel aber der Schutz von Geistlichen nach § 53 Abs. 1 S. 1 Nr. 1 StPO. Der Schutz von Berufsgeheimnisträger steht **unter dem Vorbehalt der Abwägung**. Er greift nicht mehr, wenn das öffentliche Interesse an der Beobachtung das Interesse am Schutz des Vertrauensverhältnisses überwiegt (§ 9 Abs. 4 S. 1 VSG NRW). Das Gesetz hebt hervor, dass das öffentliche Interesse an der Aufgabe, die der Berufsgeheimnisträgers wahrnimmt und das Interesse an der Vertraulichkeit der Informationen dabei zu berücksichtigen sind (§ 9 Abs. 4 S. 3 VSG NRW). Zugleich stellt es die Regelvermutung auf, dass das öffentliche Interesse an den Informationen überwiegt, wenn sie zur Beobachtung einer gesteigert beobachtungsbedürftigen Bestrebung oder Tätigkeit im Einzelfall erforderlich sind (§ 9 Abs. 4 S. 4 VSG NRW).

Bereits hier zeigt sich eine **Unwucht**: Der Schutz eigentlich niedrigere Schutz nach § 9 Abs. 4 VSG NRW tritt erst im Falle einer gesteigert beobachtungsbedürftigen Bestrebung zurück – dies auch nur als abwägungsoffener Regelfall. Demgegenüber endet der Schutz der wegen ihrer verfassungsrechtlichen Fundierung als besonders schutzwürdig wahrgenommene Berufsgruppen ohne Abwägung im Einzelfall, wenn dies zwingend für die Beobachtung einer erheblich beobachtungsbedürftigen Bestrebung zwingend erforderlich ist, also schon sehr viel früher.

65 Ferner begrenzt § 9 Abs. 8 VSG NRW den Schutz nach § 9 Abs. 3 und 4 VSG NRW: Wenn bestimmte Tatsachen bei dem Mitglied der geschützten Berufsgruppen selbst den Verdacht für eine zumindest beobachtungsbedürftige Bestrebung nach § 3 Abs. 1 VSG NRW begründen oder es diese durch die Entgegennahme oder Weitergabe von Mitteilungen unterstützt (§ 9 Abs. 8 S. 1 VSG NRW). Mit anderen Worten: Sobald damit ein Mitglied einer geschützten Berufsgruppe der Bestrebung angehört, kann er sich damit nicht mehr auf den Schutz als Berufsgeheimnisträger berufen.

66 In diesen Fällen kann die G-10-Komission bzw. das Verwaltungsgericht die Auswertung von Brief und Postsendungen oder automatisiert erhobenen Daten bzw. den Zugriff auf Videoüberwachungseinrichtungen oder eine akustische oder optische Wohnraumüberwachung zulassen (§ 9 Abs. 8 S. 2 und 3 VSG NRW). Dies geschieht „auch im Hinblick auf das ansonsten

geschützte Berufsgeheimnis“. Diese Regelung ist kryptisch. Es spricht viel dafür, sie als spezielle Voraussetzung für die Anordnung der erwähnten nachrichtendienstlichen Mittel zu verstehen; so sah dies auch § 9 Abs. 5 VSG NRW-E des Regierungsentwurfs vor. Dies passt jedoch nicht zum Wortlaut („Überdies“). Zudem ist nach § 9 Abs. 8 S. 1 der Berufsgeheimnisschutz verstrickter Berufsgeheimnisträger bereits aufgehoben.

67 Schließlich erklärt § 9 Abs. 8 S. 4 VSG NRW die Regelungen zum Schutz von kernbereichsrelevanten Daten nach § 9 Abs. 6 und 8 VSG NRW für anwendbar, soweit sie nicht die Verstrickung betreffen. Gemeint sein dürften z.B. Mandatsinformationen unbeteiligter Dritter.

2. Rechtsanwälte

68 § 9 Abs. 4 und 8 VSG NRW verstößt gegen den verfassungsrechtlich verbürgten Schutz von Rechtsanwälten als Berufsgeheimnisträger nach Art. 12 Abs. 1 GG und des Schutzes des Kernbereichs privater Lebensgestaltung nach Art. 2 Abs. 1 i.V.m. Art. 1 GG.

a) Maßstab

69 Das Gericht hat bereits in seiner Entscheidung zum Großen Lauschangriff den Schutz der Vertrauensbeziehung zu einem **Strafverteidiger** dem Schutz des Kernbereichs privater Lebensgestaltung zugeordnet und damit einem **absoluten Schutz** unterstellt:

> „Auch dem Gespräch mit dem Strafverteidiger kommt die zur Wahrung der Menschenwürde wichtige Funktion zu, darauf hinwirken zu können, dass der Beschuldigte nicht zum bloßen Objekt im Strafverfahren wird.“[49]

70 Das Gericht hat sich in einer Reihe von Entscheidungen damit auseinandergesetzt, ob sich dieser Schutz auf **alle Rechtsanwälte erstreckt**. Zunächst hat es die Gleichbehandlung von Rechtsanwälten und Strafverteidigern für verfassungsgemäß gehalten, weil sich beide Tätigkeiten kaum voneinander trennen lassen:

> „Die genannten Personengruppen waren nach früherer Rechtslage nur dann von dem absoluten Schutz erfasst, wenn sie als Verteidiger im Sinne des § 138 Abs. 1 StPO aufgetreten sind. In diesem Fall kam die Erwägung zum Tragen, dass das Verhältnis zwischen Verteidiger und Beschuldigtem typischerweise Bezüge zur Menschenwürdegarantie aufweist, was für die mit Wirkung vom 1. Februar 2011 in § 160a Abs. 1 StPO aufgenommenen Berufsgeheimnisträger nicht ohne Weiteres der Fall ist. Allein die Stellung der Rechtsanwälte als unabhängige Organe der Rechtspflege und ihre Teilnahme an der Verwirklichung des Rechtsstaats (vgl. BTDrucks 17/2637, S. 6) heben sie noch nicht in einer Weise aus dem Kreis der lediglich von dem relativen Schutz

[49] BVerfGE 109, 279 (323) – Großer Lauschangriff; ähnlich in der Folge auch BVerfGE 125, 208 Rn. 259 – Neuregelung Telekommunikationsüberwachung.

des § 160a Abs. 2 StPO erfassten Berufsgeheimnisträger heraus, die einen Verzicht auf Ermittlungsmaßnahmen rechtfertigen könnte.

Eine hinreichende Rechtfertigung kann jedoch in dem Umstand gesehen werden, dass eine Differenzierung zwischen Anwälten und Verteidigern aufgrund der Nähe der Tätigkeitsfelder faktisch kaum möglich ist (vgl. auch BTDrucks 17/2637, S. 6 f.). Bei der Kontaktaufnahme eines von einer Ermittlungsmaßnahme Betroffenen mit einem Rechtsanwalt wird sich aus der Außenperspektive vielfach nicht feststellen lassen, ob der Betroffene allgemeinen rechtlichen Rat oder die Beratung durch einen Strafverteidiger sucht. Auch bei einem bereits bestehenden nicht strafrechtlichen Mandat ist der Übergang zur Strafverteidigung mitunter fließend. **Einem anwaltlichen Beratungsverhältnis ist - anders als dies etwa bei Steuerberatern der Fall ist - bei generalisierender Betrachtung die Option der Strafverteidigung immanent.** Daher ist es mit Blick auf den Menschenwürdebezug der Strafverteidigung vertretbar, auch die nunmehr neu von § 160a Abs. 1 StPO erfassten Berufsgruppen an dem dort normierten absoluten Schutz teilhaben zu lassen."[50] (Hervorhebungen hinzugefügt)

71 In seiner Entscheidung zum BKA-Gesetz hat das Gericht dann eine Unterscheidung von Rechtsanwälten und Strafverteidigern als ungeeignet verworfen. Dabei hat es besonders darauf verwiesen, dass im Bereich der Gefahrenabwehr Strafverteidigung nicht entscheidend sei; dieser Gedanke lässt sich auf den nachrichtendienstlichen Bereich übertragen:

„**Verfassungsrechtlich nicht tragfähig** ist insoweit allerdings die Ausgestaltung des Schutzes der Vertrauensverhältnisse von Rechtsanwälten zu ihren Mandanten. Die vom Gesetzgeber herangezogene Unterscheidung zwischen Strafverteidigern und den in anderen Mandatsverhältnissen tätigen Rechtsanwälten ist als Abgrenzungskriterium für einen unterschiedlichen Schutz schon deshalb ungeeignet, weil die in Frage stehenden Überwachungsmaßnahmen nicht der Strafverfolgung, sondern der Gefahrenabwehr dienen, die Strafverteidigung also hier gerade nicht entscheidend ist." [51]

72 Daraus folgt ein **absoluter Schutz** des Vertrauensverhältnisses zwischen Rechtsanwälten und ihren Mandaten und Mandantinnen. Dieser Schutz ist auch durch die Entscheidung zur nachrichtendienstlichen Ausland-Ausland-Überwachung **nicht relativiert** worden, an die sich der Gesetzgeber möglicherweise anlehnt:

„Gegenüber Berufs- und Personengruppen, deren Kommunikationsbeziehungen einen besonderen Schutz der Vertraulichkeit verlangen, ist zunächst deren gezielte Überwachung zu begrenzen. Die Nutzung von Suchbegriffen, die zu einer gezielten Erfassung der Telekommunikationsanschlüsse solcher Personen führen, kann nicht schon allein damit gerechtfertigt werden, dass hierdurch potenziell nachrichtendienstlich relevante Informationen erlangt werden können. Die journalistische Tätigkeit rechtfertigt nicht, Personen einem höheren Risiko der Überwachung auszusetzen als andere Grundrechtsträger und sie wegen ihrer Kontakte und Recherchen zum Objekt der Informationsabschöpfung zur Verfolgung von Sicherheitsinteressen zu machen (vgl. BVerfGE 107, 299 <336>). Entsprechendes gilt für Rechtsanwältinnen und

[50] BVerfGE 125, 208 Rn. 261 f. – Neuregelung Telekommunikationsüberwachung.
[51] BVerfGE 141, 220 Rn. 257 – BKA-Gesetz.

> Rechtsanwälte. Deren gezielte Überwachung als Nachrichtenmittler ist hier vielmehr auch im Rahmen der strategischen Überwachung an qualifizierte Eingriffsschwellen zu binden. Danach ist sicherzustellen, dass das Eindringen in Vertraulichkeitsbeziehungen nur zur Aufklärung von im Einzelfall schwerwiegenden Gefahren und besonders schweren Straftaten beziehungsweise zur Ergreifung bestimmter gefährlicher Straftäter zulässig ist. Es bedarf hierfür belastbarer Erkenntnisse. Im Übrigen ist eine Überwachung und Auswertung nur nach Maßgabe einer Abwägung zulässig, wonach das öffentliche Interesse an der Information das Interesse der Betroffenen an dem Schutz der Vertraulichkeit im Einzelfall überwiegt (vgl. BVerfGE 129, 208 <258 ff.>; 141, 220 <318 f. Rn. 255 ff.>). Der Gesetzgeber wird zu prüfen haben, ob und wieweit hier zwischen verschiedenen Vertraulichkeitsbeziehungen weiter zu differenzieren ist (vgl. § 160a StPO; dazu BVerfGE 129, 208 <259 f.>). Abzusichern ist ihr Schutz jedenfalls grundsätzlich durch eine gerichtsähnliche ex ante-Kontrolle.
>
> Soweit die Erfassung von besonders schutzwürdigen Vertraulichkeitsbeziehungen erst im Rahmen der Auswertung bemerkt wird, bedarf es auch insoweit einer Prüfung der Voraussetzungen und gegebenenfalls dann einer Abwägung, ob die entsprechende Kommunikation ausgewertet und genutzt werden darf (zutreffend Löffelmann, in: Dietrich/Gärditz/Graulich/Gusy/Warg [Hrsg.], Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, S. 33 <43 mit Fn. 41>; entgegen Gärditz, DVBl 2017, S. 525 <528>). Auch hier kommt es darauf an, ob zu erwarten ist, dass hierdurch Erkenntnisse über schwerwiegende und sich konkret abzeichnende Gefahren gewonnen werden und dem öffentlichen Interesse hieran gegenüber dem Schutz der Vertraulichkeit nach Maßgabe einer Abwägung im Einzelfall der Vorrang zukommt. Auch diese Entscheidung bedarf einer gerichtsähnlichen Kontrolle.“[52]

73 Diese Passage lässt sich auf die Tätigkeit eines Nachrichtendienstes im Inland und die ihm zur Verfügung stehenden Ermittlungsinstrumente jedoch nicht übertragen. Zum einen ist der Kontext dieser Passage zu betrachten. Gegenstand dieser Entscheidung war die strategische Überwachung des Telekommunikationsverkehrs zur Auslandsaufklärung. Dieser Zweck weist erhebliche Besonderheiten auf, die ihn von Inlandssachverhalten unterscheiden.[53] Das Gericht kommt daher zu dem Schluss:

> „Als anlasslose, im Wesentlichen allein final angeleitete und begrenzte Befugnis ist sie jedoch eine Ausnahmebefugnis, die auf die Auslandsaufklärung durch eine Behörde, welche selbst grundsätzlich keine operativen Befugnisse zur Gefahrenabwehr hat, begrenzt bleiben muss. Nur durch deren besonderes Aufgabenprofil ist sie gerechtfertigt.“[54]

Ein Verfassungsschutzbehörde hat demgegenüber eine andere Aufgabe, wie auch das Gericht festgestellt hat.[55] Dies erscheint auch sachgerecht. Denn eine Verfassungsschutzbehörde wird im Inland tätig. Ihre Tätigkeit hat daher eine

---

[52] BVerfGE 154, 152 Rn. 194 f. – nachrichtendienstliche Ausland-Ausland-Überwachung.
[53] BVerfGE 154, 152 Rn. 157 ff. – nachrichtendienstliche Ausland-Ausland-Überwachung.
[54] BVerfGE 154, 152 Rn. 166 – nachrichtendienstliche Ausland-Ausland-Überwachung; ähnlich auch BVerfGE 162, 1 Rn. 161 – Bayerisches Verfassungsschutzgesetz.
[55] BVerfGE 162, 1 Rn. 160 f. – Bayerisches Verfassungsschutzgesetz (im Kontext der Eingriffsschwellen).

sehr viel stärkere Auswirkung auf die demokratische Meinungsbildung und Grundrechtsausübung in Deutschland. Der Vertraulichkeitsschutz der Beziehung zwischen Mandant und Rechtsanwalt findet auch seine besondere Bedeutung darin, dass er einem Mandat erlaubt, sich zu Verfahren vor deutschen Gerichten und Behörden beraten zu lassen. Insoweit wirkt hier auch das gesellschaftliche Interesse an einem fairen Verfahren vor deutschen Gerichten voraus, das auch den grundrechtsgleichen Rechten nach Art. 103 Abs. 1 und Art. 101 Abs. 1 S. 2 GG zugrunde liegt.[56]

74 Zum anderen wäre es aber auch psychologisch fernliegend, für die Überwachung durch den Verfassungsschutz andere Maßstäbe anzunehmen als für Zwecke der Gefahrenabwehr oder der Strafverfolgung. Für die Frage der Vertraulichkeit ist es nicht entscheidend, welche Behörde ein Mandatsgespräch überwacht oder geschützte Unterlagen einsieht. Die Vertraulichkeit ist in jedem Fall zerstört. Ein Mandant kann sich damit nicht mehr frei offenbaren.

b) Subsumtion

aa) § 9 Abs. 4 VSG NRW

75 § 9 Abs. 4 VSG NRW verstößt gegen diese verfassungsrechtlichen Vorgaben. Die Vertrauensbeziehung zwischen Mandant und Rechtsanwalt ist nicht absolut gewährleistet, obwohl dies nach der Rechtsprechung des Gerichts – wie soeben dargelegt – verfassungsrechtlich geboten ist. Sie unterliegt einer Abwägung (§ 9 Abs. 4 S. 1 VSG NRW) und damit der Einschätzung einer staatlichen Stelle. Es ist damit nicht absehbar, ob eine Kommunikation zwischen Mandant und Rechtsanwalt vertraulich sein wird. Auf dieser Basis ist ein offener Austausch zwischen Rechtsanwalt und Mandant und damit eine möglichst effektive Rechtsberatung nicht möglich.

bb) § 9 Abs. 8 VSG NRW

76 Ebenfalls gegen die verfassungsrechtlichen Vorgaben verstößt § 9 Abs. 8 VSG NRW, indem der Schutz der anwaltlichen Vertrauensbeziehung zu weit beschränkt wird.

(1) Verstrickung

77 Der Schutz entfällt danach schon, sobald bestimmte Tatsachen den Verdacht begründen, dass der Rechtsanwalt selbst in eine Bestrebung oder Tätigkeit nach § 3 Abs. 1 VSG NRW verstrickt ist. Der Gedanke der Verstrickung als

[56] Vgl. BVerfGE 107, 395 (408 f.) – Rechtsschutz gegen den Richter.

Grenze des Schutzes von Berufsgeheimnisträgern ist nicht neu. Bisher ist er im Strafverfahren angewandt worden, wenn der Berufsgeheimnisträger in Verdacht steht, sich selbst strafbar gemacht zu haben und dadurch gewissermaßen „das Lager wechselt“ (vgl. etwa § 97 Abs. 2 S. 2, § 160a Abs.4 S. 1 StPO). Er soll dann nicht selbst vor Verfolgung geschützt sein.[57] Über eine entsprechende Regelung ist im nachrichtendienstlichen Bereich bisher – soweit ersichtlich – noch nicht in der Sache entschieden worden.

78 Es bestehen bereits grundlegende Unterschiede gegenüber der nachrichtendienstlichen Tätigkeit, die dazu führen, dass sich die Grundgedanken der strafprozessualen Regelungen nicht übertragen lassen. Während im Strafprozessrecht im Raum steht, dass sich der Berufsgeheimnisträger strafbar gemacht hat, handelt er im vorliegenden Kontext rechtmäßig. Dies bedeutet nicht, dass ein Berufsgeheimnisträger nicht Gegenstand der Beobachtung des Verfassungsschutzes sein kann. Soweit er aber als Rechtsanwalt tätig wird, muss etwas anderes gelten. Anderenfalls bestünden zwei Gefahren:

79 Erstens könnte er seinen Beruf faktisch nicht mehr ausüben, wenn sein Schutz als Berufsgeheimnisträger insgesamt entfallen würde. Die Regelung differenziert hier nicht zwischen nachrichtendienstlich relevanten Tätigkeiten und der normalen Berufstätigkeit (vgl. „nicht auf Personen anzuwenden“). Dies hätte auch Auswirkungen auf seine Mandanten, die möglicherweise nichts mit einer Bestrebung nach § 3 Abs. 1 VSG NRW zu tun haben oder davon auch nichts wissen. Der nachgelagerte Schutz des § 9 Abs. 8 S. 4 i.V.m. Abs. 6 und 7 VSG NRW dürfte die abschreckende Wirkung für mögliche Mandanten nicht entfallen lassen.

80 Zweitens aber besteht die Gefahr, dass sich eine Bestrebung nach § 3 Abs. 1 VSG NRW nicht mehr anwaltlich beraten lassen könnte. Gerade bei Verfahren mit einem politischen Hintergrund (z.B. Partei- oder Vereinsverbotsverfahren, Staatsschutzdelikt, § 130 StGB, Versammlungsverbote, Zugang zu öffentlichen Einrichtungen) wird eine solche Bestrebung (oder einzelne ihrer Mitglieder) sich an einen Anwalt wenden, der selbst ein Mitglied ist oder ihr nahesteht („Szeneanwalt“). Möglichweise muss sie dies sogar, weil sie sonst keine Rechtsberatung erhält. Damit bestände aber die Gefahr, dass auch die beobachtete Bestrebung keine Gelegenheit mehr hätte, sich vertraulich rechtlich beraten zu lassen. Dies ist aber in einem Rechtsstaat als Teil eines fairen Verfahrens unabdingbar, um die rechtliche Überprüfung staatlichen Handelns veranlassen zu können und seine eigene Rechtsposition vor Gericht zu verteidigen.

---

[57] BVerfGE 125, 208 Rn. 272 – Neuregelung Telekommunikationsüberwachung m.w.N.; BVerfG NJW 2015, 3430 Rn. 18.

(2) Nachrichtenmittler

81 Zudem endet der Berufsgeheimnisträgerschutz nach § 9 Abs. 8 S. 1 VSG NRW, wenn der Berufsgeheimnisträger die Bestrebung unterstützt, indem er Mitteilungen entgegennimmt oder weitergibt. Der Schutz entfällt damit automatisch, ohne dass eine Abwägung stattfindet. Dies widerspricht den verfassungsrechtlichen Vorgaben, die das Gericht sogar für den – tendenziell mit geringerem Schutz versehenen – Bereich der nachrichtendienstlichen Ausland-Ausland-Überwachung angenommen hat:

> „Die journalistische Tätigkeit rechtfertigt nicht, Personen einem höheren Risiko der Überwachung auszusetzen als andere Grundrechtsträger und sie wegen ihrer Kontakte und Recherchen zum Objekt der Informationsabschöpfung zur Verfolgung von Sicherheitsinteressen zu machen (vgl. BVerfGE 107, 299 <336>). **Entsprechendes gilt für Rechtsanwältinnen und Rechtsanwälte**. Deren **gezielte Überwachung als Nachrichtenmittler** ist hier vielmehr auch im Rahmen der strategischen Überwachung an **qualifizierte Eingriffsschwellen** zu binden. Danach ist sicherzustellen, dass das Eindringen in Vertraulichkeitsbeziehungen **nur zur Aufklärung von im Einzelfall schwerwiegenden Gefahren und besonders schweren Straftaten beziehungsweise zur Ergreifung bestimmter gefährlicher Straftäter** zulässig ist. Es bedarf hierfür **belastbarer Erkenntnisse**. Im Übrigen ist eine Überwachung und Auswertung nur nach Maßgabe einer **Abwägung** zulässig, wonach das öffentliche Interesse an der Information das Interesse der Betroffenen an dem Schutz der Vertraulichkeit im Einzelfall überwiegt.“[58] (Hervorhebungen hinzugefügt)

82 § 9 Abs. 8 S. 1 VSG NRW enthält weder eine Abwägung noch qualifizierte Eingriffsschwellen (es reicht die niedrigste Stufe nach § 3 Abs. 1 VSG NRW aus) oder Anforderungen an die Entscheidungsgrundlage.

3. Journalisten

83 Der Schutz von Journalisten nach § 9 Abs. 3 und Abs. 8 VSG NRW entspricht nicht den verfassungsrechtlichen Anforderungen und verstößt damit gegen Art. 5 Abs.1 S. 2 GG.

a) Maßstab

84 Nach der Rechtsprechung des Gerichts genießen Journalisten – anders als Rechtsanwälte – keinen absoluten Schutz. Das Gericht hat vielmehr in ständiger Rechtsprechung betont, dass ein derartiger Vorrang vor staatlichen Strafverfolgungsinteressen unzulässig wäre.[59] Zuletzt hat das Gericht eine Abwägung zwischen der Vertraulichkeit der journalistischen Arbeit und dem

---

[58] BVerfGE 154, 152 Rn. 194 – nachrichtendienstliche Ausland-Ausland-Überwachung.
[59] BVerfGE 125, 208 Rn. 267 f. – Neuregelung Telekommunikationsüberwachung; BVerfGE 141, 220 Rn. 256 – BKA-Gesetz; BVerfGE 107, 298 (332 f.) – Journalistische Verbindungsdaten.

betroffenen öffentlichen Interesse verlangt – sogar bei einer Überwachung im Ausland für Zwecke der Auslandsaufklärung.[60]

b) Subsumtion

aa) § 9 Abs. 3 VSG NRW

85 § 9 Abs. 3 VSG NRW genügt diesen Anforderungen nicht. Er nimmt pauschal einen Wegfall des Schutzes von Journalisten und Presseangehörigen an, wenn dies für die Beobachtung mindestens erheblich beobachtungsbedürftiger Bestrebungen im Einzelfall zwingend erforderlich ist. Die Regelung berücksichtigt das konkrete Vertraulichkeitsinteresse nicht, sondern stellt einseitig auf das staatliche Beobachtungsinteresse ab. Es droht damit, dass gerade Journalisten zum Beobachtungsobjekt werden, die im beobachtungsbedürftigen Milieu recherchieren und möglicherweise über bessere oder andere Informationszugänge verfügen als der Verfassungsschutz. Genau dies wollte das Gericht aber ausdrücklich verhindern:

> „Die journalistische Tätigkeit darf nicht zum Anlass genommen werden, Journalisten einem höheren Risiko auszusetzen als andere Grundrechtsträger, Objekt der Erhebung von Verbindungsdaten für Zwecke der Strafverfolgung Dritter zu werden. Insbesondere darf die Inanspruchnahme von Journalisten nicht allein auf den Erfahrungssatz gestützt werden, dass Journalisten auf Grund ihrer Recherchen häufig mehr über gesuchte Straftäter wissen als andere Bürger.“[61]

> „Die journalistische Tätigkeit rechtfertigt nicht, Personen einem höheren Risiko der Überwachung auszusetzen als andere Grundrechtsträger und sie wegen ihrer Kontakte und Recherchen zum Objekt der Informationsabschöpfung zur Verfolgung von Sicherheitsinteressen zu machen.“[62]

86 Eine verfassungskonforme Auslegung wäre mit den hohen Bestimmtheitsanforderungen im sicherheitsrechtlichen Bereich bei heimlichen Überwachungsmaßnahmen nicht vereinbar. Der Wortlaut und die systematische Auslegung durch Vergleich mit § 9 Abs. 4 VSG NRW legen klar ein Entscheidungsprogramm fest, das keine Abwägung vorsieht. Da eine Konkretisierung der Norm in der Praxis im Wechselspiel mit der Rechtsprechung faktisch ausscheidet, wäre es dann in der Hand des Verfassungsschutzes die Regelung verfassungskonform auszulegen. Es ist aber gerade die Aufgabe des Gesetzgebers, für den Verfassungsschutz begrenzende gesetzliche Regelungen zu schaffen.

---

[60] BVerfGE 154, 152 Rn. 194 – nachrichtendienstliche Ausland-Ausland-Überwachung.
[61] BVerfGE 107, 298 (336) – Journalistische Verbindungsdaten.
[62] BVerfGE 154, 152 Rn. 194 – nachrichtendienstliche Ausland-Ausland-Überwachung.

bb) § 9 Abs. 8 VSG NRW

87 Aus dem gleichen Grund hat das Gericht die Einstufung von Journalisten als Nachrichtenmittler kritisch gesehen und hierfür qualifizierte Anforderungen aufgestellt.[63] Diese sind – wie zu Rechtsanwälten ausgeführt (→Rn. 81) – hier nicht erfüllt.

4. Mandatsträger

88 Der Schutz von Mandatsträgern vor Überwachungsmaßnahmen durch den Verfassungsschutz nach § 9 Abs. 2 VSG genügt nicht den verfassungsrechtlichen Anforderungen und verstößt gegen Art. 47 GG sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Darüber hinaus liegt ein Verstoß gegen Bundesrecht vor (Art. 31 GG i.V.m. § 6 EuAbgG).

a) Maßstab

89 Nach der ständigen Rechtsprechung des Gerichts genießen Mandatsträger einen absoluten Schutz, der sich aus ihrer verfassungsrechtlichen Stellung ergibt. Diese folgt für Bundestagsabgeordnete aus Art. 47 GG i.V.m. Art. 38 Abs. 1 S. 2 GG und für Landtagsabgeordnete aus Art. 49 Abs. 1 Verfassung von Nordrhein-Westfalen sowie über Art. 28 Abs. 1 S. 1 GG ebenfalls aus dem Grundgesetz.[64] Für Mitglieder des Europäischen Parlaments gilt der Schutz des § 6 EuAbgG; darüber hinaus ist – wie dargelegt (→Rn. 19) – Art. 47 GG auch wie in unionsrechtskonformer Auslegung anzuwenden.

90 Aus diesem Grund hat das Gericht den besonderen Schutz nach § 160a Abs. 1 StPO für gerechtfertigt gehalten:

> „Die Einbeziehung der Abgeordneten in § 160a Abs. 1 StPO kann sich hingegen auf eine ausdrückliche verfassungsrechtliche Rechtfertigung stützen. Der Schutz der Abgeordneten dient zwar nicht dem Persönlichkeitsrecht der Beschuldigten, sondern wird den Abgeordneten um der Institution des Parlaments und seiner Funktionsfähigkeit willen gewährt (BVerfGE 109, 279 <323>). Deshalb ordnet das Grundgesetz für Bundestagsabgeordnete ein Zeugnisverweigerungsrecht und ein Beschlagnahmeverbot an (Art. 47 GG). Diese unmittelbar in der Verfassung normierten ausdrücklichen Verbote selbst offen durchgeführter Ermittlungsmaßnahmen **heben die Abgeordneten aus dem Kreis der anderen Zeugnisverweigerungsberechtigten heraus** und rechtfertigen insoweit auch einen **besonderen, weitergehenden Schutz**.“[65] (Hervorhebungen hinzugefügt)

---

[63] BVerfGE 107, 298 (336) – Journalistische Verbindungsdaten; BVerfGE 154, 152 Rn. 194 – nachrichtendienstliche Ausland-Ausland-Überwachung.
[64] BVerfGE 134, 141 Rn. 103 ff. – Ramelow.
[65] BVerfGE 125, 208 Rn. 263 – Neuregelung Telekommunikationsüberwachung.

91 Dieser Schutz umfasst nicht nur die Unterlagen des Abgeordneten, sondern auch die Vertraulichkeit der Kommunikation zwischen dem Abgeordneten und Bürgerinnen und Bürgern:

> „Der kommunikative Prozess, bei dem der Abgeordnete nicht nur Informationen weitergibt, sondern auch Informationen empfängt, ist vom Schutz des Art. 38 Abs. 1 Satz 2 GG umfasst. Das freie Mandat schließt die Rückkoppelung zwischen Parlamentariern und Wahlvolk ein und trägt dem Gedanken Rechnung, dass die parlamentarische Demokratie auf dem Vertrauen des Volkes beruht (vgl. BVerfGE 118, 277 <353>). Sie schützt daher – neben dem speziellen Schutz der vertraulichen Kommunikation des Abgeordneten durch das in Art. 47 GG gewährte Zeugnisverweigerungsrecht – die Kommunikationsbeziehungen des Abgeordneten als Bedingung seiner freien Willensbildung und gewährleistet dabei insbesondere, dass die von ihm zu vertretenden, in die politische Willensbildung des Deutschen Bundestages einzuspeisenden Meinungen und Interessen ihn unverzerrt und ohne staatliche Beeinflussung erreichen können.
>
> (…)
>
> Wird die Kommunikationsbeziehung zwischen Abgeordnetem und Bürgern gestört, so ist folglich die parlamentarische Willensbildung und infolgedessen die demokratische Repräsentationsfunktion des Parlaments berührt.“[66]

b) Subsumtion

aa) § 9 Abs. 3 Nr. 1 VSG NRW

92 § 9 Abs. 3 Nr. 1 VSG NRW erfüllt diese verfassungsrechtlichen Anforderungen nicht. Dabei kann offenbleiben, ob Art. 47 i.V.m. Art. 38 Abs. 1 S. 2 GG (ggf. i.V.m. Art. 28 Abs. 1 S. 1 GG) durch das Schutzgut der freiheitlichen demokratischen Grundordnung eingeschränkt werden kann. Dies hat das Gericht bisher nur für den Fall entschieden, dass der Abgeordnete selbst sein Mandat missbraucht, um diese zu bekämpfen.[67] Ist der Abgeordnete selbst Objekt der Beobachtung trifft das Gesetz Schutzregelungen, z.B. § 24 Abs. 4 VSG NRW.

93 Ist Gegenstand der Beobachtung jedoch eine Kommunikation zwischen dem Abgeordneten und einer Zielperson des Verfassungsschutzes, sieht das Gesetz nur einen lückenhaften Schutz in § 21 Abs. 2 S. 3 VSG NRW für Abgeordnetenpost vor, so dass die Vertraulichkeit der Kommunikation vor allem durch § 9 Abs. 3 Nr. 1 VSG NRW gewährleistet wird. Dieser Schutz ist aber zu stark eingeschränkt.

94 Zum einen stellt die Regelung einseitig auf das Beobachtungsinteresse des Verfassungsschutzes ab. Es findet gerade keine Abwägung mit den betroffenen Vertraulichkeitserwartungen und der Bedeutung des

---

[66] BVerfGE 134, 141 Rn. 97, 99 – Ramelow.
[67] BVerfGE 134, 141 Rn. 112 ff. – Ramelow.

Mandatsgeheimnisses für den demokratischen Prozess statt. Eine solche Abwägung wäre jedoch erforderlich, um im Einzelfall eine praktische Konkordanz zwischen dem Mandatsgeheimnis nach Art. 47 i.V.m. Art. 38 Abs. 1 S. 2 VSG NRW und dem Schutz der freiheitlichen demokratischen Grundordnung andererseits zu finden (sofern man eine Einschränkung von Art. 47 GG überhaupt annehmen will, wenn der Abgeordnete selbst sein Mandat nicht missbraucht).

95 § 9 Abs. 3 VSG NRW verwirklicht diese praktische Konkordanz zudem nur unzureichend. Der Schutz durch diese Regelung entfällt bereits, wenn dies für die Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit zwingend erforderlich ist. Dies erscheint zu wenig schwerwiegend, um ein unmittelbar durch verfassungsrechtliches Schutzgut einzuschränken. Der Schutz des Mandatsgeheimnisses bleibt damit sogar hinter dem verfassungswidrigen Schutz anderer Berufsgeheimnisträger nach § 9 Abs. 4 VSG NRW zurück, obwohl das Mandatsgeheimnis eine hohe Bedeutung für den demokratischen Prozess hat und verfassungsrechtlich verbürgt ist. Im Fall des § 9 Abs. 4 VSG NRW findet nicht nur eine Abwägung zwingend statt. Die Regelvermutung des § 9 Abs. 4 S. 4 VSG NRW gibt bereits vor, dass der Schutz des Berufsgeheimnisses im Falle einer besonders beobachtungsbedürftigen Bestrebung noch nicht einmal regelmäßig zurücktritt. Demgegenüber entfällt der Schutz nach § 9 Abs. 3 VSG NRW *immer* und knüpft dabei an die niedrigere Schwelle der erheblich beobachtungsbedürftigen Bestrebung an.

bb) § 9 Abs. 8 S. 1 VSG NRW

96 Auch § 9 Abs. 8 S. 1 VSG NRW entspricht nicht den verfassungsrechtlichen Anforderungen, soweit er das Mandatsgeheimnis entfallen lässt, wenn der Abgeordnete Mitteilung entgegennimmt. Als Kommunikationspartner wird ein Abgeordneter häufig Informationen entgegennehmen. Dies könnte es gerechtfertigt lassen, ihn als Nachrichtenmittler zu ordnen; Folge wäre ein Entfall des Schutzes nach § 9 Abs. 3 Nr. 1 VSG NRW. Ob eine Eingrenzung über das Merkmal der „Unterstützung“ erfolgen könnte, ist nicht klar. Dies wäre nur der Fall, wenn man es intentional und nicht objektiv auslegen würde.

5. Seelsorger

a) Maßstab

97 Der Gesetzgeber hat gegen Art. 4 Abs. 1 und 2 GG und Art. 3 Abs. 1 GG verstoßen, indem er es unterlassen hat, eine Regelung zum Schutz von Geistlichen und Seelsorgern vorzusehen.

98 Das Gericht hat einen absoluten Schutz der Vertrauensbeziehung zwischen Geistlichen und Seelsorgern angenommen und aus dem Menschenwürdegehalt der Religionsausübung gefolgert, zumindest in Bezug auf seelsorgerische Gespräche:

> „§ 53 StPO schützt zwar seinem Grundgedanken nach das Vertrauensverhältnis zwischen dem Zeugen und dem Beschuldigten. Jedoch erfolgt auch dieser Schutz nicht in allen Fällen des § 53 StPO um der **Menschenwürde des Beschuldigten** oder der Gesprächspartner willen. **Diese Annahme trifft allerdings auf das seelsorgerliche Gespräch mit einem Geistlichen zu**. So gehört der Schutz der Beichte oder der Gespräche mit Beichtcharakter zum verfassungsrechtlichen Menschenwürdegehalt der Religionsausübung im Sinne des Art. 4 Abs. 1 und 2 GG.“[68]

In der Folge hat es einen gegenüber anderen Berufsgeheimnisträgern weitergehenden Schutz mehrfach bestätigt.[69] Besonders deutlich wird dies in einer Entscheidung aus dem Jahr 2007, indem das seelsorgerische Gespräch dem Kernbereich privater Lebensgestaltung zugeordnet und damit absolut geschützt wird:

> „Das Bundesverfassungsgericht anerkennt einen Kernbereich privater Lebensgestaltung, in den einzugreifen dem Staat verwehrt ist (vgl. BVerfGE 6, 32 <41>; 27, 1 <6>; 32, 373 <379>; 34, 238 <245>; 80, 367 <373>; 109, 279 <313>). Der Schutz des Kernbereichs privater Lebensgestaltung umfasst auch bestimmte Formen der Kommunikation mit Personen des besonderen Vertrauens (vgl. BVerfGE 90, 255 <260>). Hierzu zählt unter anderem das seelsorgerische Gespräch mit einem Geistlichen. Der Schutz der Beichte und der Gespräche mit Beichtcharakter zählt zum verfassungsrechtlichen Menschenwürdegehalt der Religionsausübung (vgl. BVerfGE 109, 279 <322>).“[70]

b) Subsumtion

aa) Gesetzgeberisches Unterlassen

99 Das vorliegende Gesetz enthält keine Regelungen zum Schutz des seelsorgerischen Gesprächs mehr. Dieser Schutz ist durch die Annahme des Änderungsantrags der Fraktionen CDU und Bündnis 90/DIE Grünen entfallen. Während der Regierungsentwurf den Schutz der Berufsgeheimnisträger noch vorsah (§ 9 Abs. 1 VSG NRW-E), indem er an § 53 und § 53a StPO anknüpfte, ist dieser Schutz durch den Verweis auf § 203 StGB in § 9 Abs. 4 S. 2 VSG NRW entfallen. Seelsorger fallen nicht unter § 203 StGB.[71]

---

[68] BVerfGE 109, 279 (322) – Großer Lauschangriff.
[69] BVerfGE 141, 220 Rn. 256 – BKA-Gesetz; BVerfGE 125, 208 Rn. 259 – Neuregelung Telekommunikationsüberwachung.
[70] BVerfG NJW 2027, 1865 Rn. 18.
[71] BGH NStZ 2010, 646 Rn. 25.

100 Verfassungsrechtlich wäre der Gesetzgeber gehalten gewesen, eine Regelung zum Schutz des seelsorgerischen Gespräches vorzusehen. Diese Lücke kann auch nicht geschlossen werden, indem die besondere Schutzwürdigkeit des Vertrauensverhältnisses zwischen Gläubigem und Seelsorger im Rahmen der Verhältnismäßigkeit berücksichtigt wird. Der Schutz des seelsorgerischen Gesprächs als Teil des Kernbereichs absoluter Lebensgestaltung ist einer Abwägung nicht zugänglich und absolut. Dies muss sich schon aufgrund der Wesentlichkeit dieses Schutzes für die Grundrechte der betroffenen Personen in einer gesetzlichen Regelung niederschlagen und kann nicht der Verwaltung überlassen bleiben. Diese unterliegt gerade im vorliegenden Bereich einer nur eingeschränkten gerichtlichen Kontrolle, so dass eine Konkretisierung im Wechselspiel mit der Rechtsprechung ausscheidet.

101 Hiergegen ließe sich vorbringen, dass das seelsorgerische Gespräch durch die Regelungen zum Kernbereich privater Lebensgestaltung (Art. 9 Abs. 1 VSG NRW) geschützt sei. Dies ist jedoch alles andere als eindeutig und gibt damit der Exekutive einen Auslegungsspielraum. Dieser könnte sich auf die historische Auslegung stützen, weil der Gesetzgeber explizit einen Systemwechsel vollziehen wollte, indem er nicht mehr auf §§ 53, 53a StPO abstellte.[72] Er hat aber als Anknüpfungspunkt auch nicht – was durchaus naheliegender gewesen wäre – auf §160a StPO abgestellt, der spezifisch den Berufsgeheimnisträgerschutz gegenüber Überwachungsmaßnahmen und Seelsorger einbezieht (§ 160a Abs. 1 S. 1 i.V.m. § 53 Abs. 1 Nr. 1 StPO).

102 Würde man auf das Erfordernis einer gesetzlichen Regelung verzichten, wären ebenso alle anderen Regelungen zum Schutz von besonderen Vertrauensbeziehungen verzichtbar. Dies entspricht nicht der Rechtsprechung des Gerichts, das gesetzliche Regelungen zum Schutz von Vertrauensbeziehungen explizit als verfassungsrechtlich geboten angesehen hat.[73]

bb) Verstoß gegen den Gleichheitssatz

103 Selbst wenn man im Fehlen einer ausdrücklichen Regelung zum Schutz von seelsorgerischen Vertrauensverhältnissen kein verfassungsrechtlich relevantes Unterlassen sehen würde, läge hierin ein Verstoß gegen den Gleichheitssatz (Art. 3 Abs. 1 GG), weil der Gesetzgeber Regelungen zum Schutz anderer Vertrauensbeziehungen in § 9 Abs. 3, 4 und 9 VSG NRW geschaffen hat (auch wenn diese weitgehend verfassungswidrig sind).

---

[72] Landtag von Nordrhein-Westfalen, Drucksache 18/16212, S. 15 f.
[73] BVerfGE 154, 152 Rn. 194 – nachrichtendienstliche Ausland-Ausland-Überwachung.

II. § 11 Abs. 2 S. 1 Nr. 2 VSG NRW (Kontaktpersonen)

104 § 11 Abs. 2 S. 1 Nr. 2 i.V.m. § 10 VSG NRW verletzt Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG Es ist nicht verhältnismäßig, gegen Kontaktpersonen als Zielpersonen nachrichtendienstliche Mittel zu ergreifen, nur weil sie Kenntnis davon haben, dass eine Person, mit der sie in Kontakt stehen, an einer beobachtungsbedürftigen Bestrebung beteiligt ist oder sich diese Person ihrer zur Förderung einer solchen Bestrebung oder Tätigkeit bedient.[74]

1. Grundrechtseingriff

105 Ein Eingriff in die gerügten Grundrechte ergibt sich nicht unmittelbar aus § 11 Abs. 2 S. 1 Nr. 2 VSG NRW. Diese Regelung legt nur die Personen fest, gegen die nachrichtendienstliche Mittel **zur systematischen Gewinnung von Daten gezielt** eingesetzt werden dürfen. Es wäre also grundsätzlich möglich, diese Personen nach § 19 VSG NRW zu observieren, ggf. sogar langfristig, auf Videoaufnahmen nach § 20 VSG NRW zuzugreifen, Finanzermittlungen gegen sie durchzuführen, bei Post- und Telekommunikationsunternehmen Auskünfte einzuholen (§ 22 VSG NRW) und sogar verdeckte Ermittler, virtuelle Agenten und V-Personen einzusetzen (§§ 15 ff. VSG NRW). Hierbei handelt es sich um schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung. Maßnahmen gegen Kontaktpersonen können unter den gleichen Voraussetzungen angeordnet werden wie gegen Personen, die an einer beobachtungsbedürftigen Bestrebung oder Tätigkeit beteiligt sind. Anders als die Gesetzesbegründung nahelegt[75] bezieht sich die Subsidiaritätsklausel in der vom Landtag beschlossenen Fassung auf § 11 Abs. 2 S. 1 Nr. 1 und 2 VSG NRW und läuft damit faktisch leer.

2. Rechtfertigung

106 Derartige Eingriffe sind unter den weiten Voraussetzungen der Definition von Kontaktpersonen nicht gerechtfertigt.

a) Maßstäbe

107 Ausgangspunkt ist das Verantwortlichkeitsprinzip. In einem Rechtsstaat müssen sich präventive Maßnahmen in erster Linie gegen Personen richten, die für eine Gefahr verantwortlich sind, die eine Straftat vorbereiten oder – im Bereich des Verfassungsschutzes – an einer beobachtungsbedürftigen

[74] Wie hier siehe *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 13; *Zöller*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2838, S. 9 in Bezug auf §11 Abs. 2 S. 1 Nr. 2 lit. b VSG NRW.
[75] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 148.

Bestrebung oder Tätigkeit beteiligt sind.[76] Sie setzen damit den Anlass dafür, dass der Staat in ihre Grundrechte eingreift. Demgegenüber müssen Bürgerinnen und Bürger, die in keine dieser Aktivitäten verfangen sind, grundsätzlich unbehelligt bleiben. Dies gilt besonders in Bezug auf heimliche Überwachungsmaßnahmen, von denen sie typischerweise niemals etwas erfahren. In einem Rechtsstaat sollte eine Person, die sich an die Gesetze hält und durch ihr Handeln keinen Anlass gibt, prinzipiell davon ausgehen dürfen, dass sie nicht Ziel staatlicher Maßnahmen wird. Könnte sie eine staatliche Überwachung noch nicht einmal mehr vermeiden, indem er sich gesetzestreu verhält, würde dies ein Gefühl „ständigen Überwachtwerdens“[77] hervorrufen. Wenn der Staat trotzdem solche Bürgerinnen und Bürger überwacht, um Informationen über andere Bürgerinnen und Bürger zu erlangen, ist diese Inpflichtnahme zumindest in höchstem Maße rechtfertigungsbedürftig und kann nur unter engen Voraussetzungen zulässig sein. Dies muss vor allem im Bereich der Nachrichtendienste gelten, weil deren Eingriffsschwellen gering sind und sie weit im Vorfeld einer konkreten Gefahr tätig werden. In der Regel ist daher keine Dringlichkeit gegeben; dementsprechend stehen häufig auch andere Mittel der Informationsgewinnung zur Verfügung.

108 Das Gericht hat eine Überwachung Dritter nicht schlechthin ausgeschlossen. Bei Maßnahmen, die – wie die hier in Rede stehenden nachrichtendienstlichen Mittel –

> „stärker in Grundrechte eingreifen, reichen lose Zusammenhänge nicht aus (…). Es genügt nicht schon, dass Dritte mit einer Zielperson überhaupt in irgendeinem Austausch stehen. Vielmehr bedarf es zusätzlicher Anhaltspunkte, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Bestrebung dienlich sein wird.“[78]

Das Gericht verlangte an anderer Stelle eine „spezifische Nähe der Betroffenen zu der aufzuklärenden Gefahr oder Straftat“, damit ein solcher Eingriff verhältnismäßig sein kann.[79]

109 Art. 19a des Bayerischen Verfassungsschutzgesetzes enthielt eine Befugnis zur langfristigen Observation mit einem ähnlich gefassten Adressatenkreises. Das Gericht hat diese Norm jedoch aus anderen Gründen für verfassungswidrig erklärt und musste sich daher mit dem Adressatenkreis nicht näher auseinandersetzen.[80] Gleiches gilt für eine Regelung zum Einsatz von verdeckten Ermittlern im Hessischen Verfassungsschutzgesetz, die

---

[76] BVerfGE 141, 220 Rn. 104 – BKA-Gesetz.
[77] BVerfGE 125, 260 Rn. 241 – Vorratsdatenspeicherung.
[78] BVerfGE 162, 1 Rn. 212 – Bayerisches Verfassungsschutzgesetz; zuvor schon BVerfGE 141, 220 Rn. 116 – BKA-Gesetz.
[79] BVerfGE 141, 220 Rn. 116 – BKA-Gesetz.
[80] Vgl. BVerfGE 162, 1 Rn. 356 ff. – Bayerisches Verfassungsschutzgesetz

allerdings eine klare Subsidiarität von Kontaktpersonen als Zielpersonen enthielt.[81]

b) Subsumtion

110 § 11 Abs. 2 S. 1 Nr. 2 VSG erfüllt diese Maßstäbe nicht.

aa) Intensität der Verbindung

111 Nach dem Wortlaut der Regelung muss eine Person mit einer Zielperson nach § 11 Abs. 2 S. 1 Nr. 1 in Kontakt stehen. Was dies bedeutet, bleibt vage. Die Gesetzesbegründung führt zwar aus:

> „Dies meint ein stabiles Kontaktverhältnis, das sich durch einen regelmäßigen Austausch bzw. Kommunikation auszeichnet. Eine bloße flüchtige Verbindung ist nicht ausreichend."[82]

112 Diese Einschränkung findet sich jedoch nicht – auch nicht andeutungsweise – in der Norm selbst.[83] Daher ist die Regelung **entweder zu unbestimmt oder unverhältnismäßig.** Eine normenklare und bestimmte Regelung ist zudem bei der Inanspruchnahme Dritter von besonderer Bedeutung, wie das Gericht ausgeführt hat, um die „Entscheidung über die „Grenzen der Freiheit (…) nicht einseitig in das Ermessen der Verwaltung"[84] zu stellen und die Voraussehbarkeit eines möglichen Eingriffs auf Seiten der Bürger zu gewährleisten:

> „Die Anforderungen an die Bestimmtheit und Klarheit der Norm dienen ferner dazu, die Verwaltung zu binden und ihr Verhalten nach Inhalt, Zweck und Ausmaß zu begrenzen (vgl. BVerfGE 56, 1 [12]; 110, 33 [54]). Dies setzt voraus, dass hinreichend klare Maßstäbe bereitgestellt werden. Die Entscheidung über die Grenzen der Freiheit des Bürgers darf nicht einseitig in das Ermessen der Verwaltung gestellt sein (vgl. BVerfGE 78, 214 [226]). Dem Gesetz kommt im Hinblick auf den Handlungsspielraum der Exekutive eine begrenzende Funktion zu, die rechtmäßiges Handeln des Staates sichern und dadurch auch die Freiheit der Bürger schützen soll. Dieser Aspekt der Bindung der Verwaltung ist bei einer Überwachungsmaßnahme besonders wichtig, da der Betroffene von ihr nichts weiß und daher keine Möglichkeit hat, in einem vorgeschalteten Verfahren Einfluss auf das eingreifende Verhalten der Verwaltung zu nehmen. **Der Schutz durch begrenzende Maßstäbe erhält zusätzlich besondere Bedeutung dadurch, dass auch betroffene Dritte – hier die anderen Telekommunikationsteilnehmer, gegebenenfalls auch Kontakt- und Begleitpersonen – mit einer staatlichen Überwachung nicht rechnen und sich deshalb vor einem Einblick in ihren Privatbereich nicht schützen können**."[85] (Hervorhebungen hinzugefügt)

---

[81] BVerfGE 169, 130 Rn. 181 ff. – Hessisches Verfassungsschutzgesetz.
[82] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 148.
[83] *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 13 f.
[84] BVerfGE 113, 348 (376) – Präventive Telekommunikationsüberwachung
[85] BVerfGE 113, 348 (376) – Präventive Telekommunikationsüberwachung.

bb) Bezug zum Beobachtungsobjekt

113 Selbst wenn man den Konkretisierungsversuch in der Gesetzesbegründung zugrunde legen würden, wäre der Bezug zum Beobachtungsobjekt zu schwach, um heimliche Überwachungsmaßnahmen zu rechtfertigen. Das Gericht sieht eine Rechtfertigung darin, dass die Überwachung von Personen, auch wenn sie mit einer Bestrebung nicht verstrickt sind, zu deren Aufklärung beitragen kann. § 11 Abs. 2 S. 1 Nr. 2 VSG NRW knüpft jedoch an neutrale Sachverhalte an.

(1) Kenntnis

114 So reicht es nach § 11 Abs. 2 S. 1 Nr. 2 lit. a VSG NRW aus, dass jemand weiß, dass die Zielperson an einer beobachtungsbedürftigen Bestrebung beteiligt ist. Bereits dieser Kreis ist weit. Jemand erfüllt bereits die Voraussetzungen, wenn er – auch nur am Rande – mitbekommt, dass ein Kollege, ein Geschäftspartner, ein Nachbar oder ein Freund an einer beobachtungsbedürftigen Bestrebung beteiligt ist. Handelt es sich bei den beobachtungsbedürftigen Bestrebungen um große Organisationen wie Parteien oder deren Vorfeldorganisationen weitet sich der Kreis potenzieller Adressaten nachrichtendienstlicher Mittel schnell aus.

> **Beispiel**: Ein Kandidat einer verfassungsfeindlichen Partei tritt zu einer Wahl an. Sein Porträt ist auf Plakaten zu sehen. Damit weiß jede Person, die diese Plakate sieht, dass sie an einer Bestrebung nach § 3 Abs. 1 VSG NRW beteiligt ist und könnte als Kontaktperson Adressat von nachrichtendienstlichen Mitteln werden.

115 Die Weite des betroffenen Personenkreises zeigt, dass der Gesetzgeber nicht ausreichend sichergestellt hat, dass der Einsatz nachrichtendienstlicher Mittel gegen diese Person auch wirklich der Aufklärung der beobachtungsbedürftigen Bestrebungen dient.[86] Man mag natürlich argumentieren, dass viele dieser Kontaktpersonen für den Verfassungsschutz komplett uninteressant sind und damit gar nicht damit rechnen müssen, Ziel von Nachrichten dienstlich Mitteln zu werden. Dies mag zutreffen, legt die Entscheidung aber in verfassungsrechtlich unzulässiger Weise in das – weitgehend unkontrollierte – Ermessen der Verwaltung. Wenn sie aufgrund „tatsächlicher Anhaltspunkte“ meint, Erkenntnisse über eine Bestrebung zu gewinnen, reicht dies aus (§ 11 Abs. 1 Nr. 1 VSG NRW). Die genaue Umschreibung des potenziellen Adressatenkreis nachrichtendienstlicher Mittel hat daher – wie ausgeführt – auch in der Rechtsprechung des Gerichts eine besonders große Bedeutung, besonders wenn Dritte betroffen sind.[87]

---

[86] *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 13.
[87] BVerfGE 113, 348 (376) – Präventive Telekommunikationsüberwachung.

116 Die Grenzziehung, die der Gesetzgeber hier vornimmt, hat auch erhebliche **soziale Konsequenzen**: Wie wirkt sich die – möglicherweise nur entfernte – Möglichkeit aus, Adressat von Maßnahmen des Verfassungsschutzes zu werden, wenn man selbst mit einer Bestrebung nach § 3 Abs. 1 VSG NRW gar nichts zu tun hat? Allein aufgrund dieser Befürchtung könnten viele Menschen sich veranlasst sehen, den Kontakt mit Personen abzubrechen, von denen sie wissen, dass sie in solchen Bestrebungen engagiert sind. Und zwar auch dann, wenn sie mit Ihnen in ganz anderen Rollen zu tun haben, z.B. als Freunde, Kollegen, Geschäftspartner, Nachbarn, in Vereinen oder Familienmitglieder.

(2) Förderung der Bestrebung

117 Unverhältnismäßig ist auch die Anknüpfung daran, ob sich eine Zielperson einer anderen Person zur Förderung einer Beobachtung bedürftigen Bestrebung oder Tätigkeit bedient.[88] Die potenzielle Kontaktperson muss noch nicht einmal wissen, dass sie eine solche Bestrebung fördert.[89] Es werden also eine Vielzahl neutraler Verhaltensweisen verfasst, die Aussicht der betroffenen Person in keinerlei Zusammenhang zu einer solchen Streuung oder Tätigkeit stehen. Treffend hat hierzu der Sachverständige Prof. Dr. *Zöller* ausgeführt:

> „Damit kann faktisch jeder Mann ohne jeden Anlass in den Fokus der Verfassungsschutzbehörde geraten, beispielsweise Vermieter von Wohnraum oder Kraftfahrzeugen, Verkäufer von Waren, Anbieter von Dienstleistungen oder Informationen im Internet, Trainer in Sportvereinen oder Sprachlehrer.“[90]

Der Kreis der Personen ließe sich noch weiter illustrieren. Aus Sicht der betroffenen Personen ist es nicht voraussehbar,[91] ja zufällig, ob sie zu einer Kontaktperson wird oder nicht.

cc) Keine Subsidiarität

118 Verfassungsrechtlich wäre es geboten, dass im Normtext sichergestellt ist, dass primärer Adressat nachrichtendienstlicher Mittel die Zielperson nach § 11 Abs. 2 S. 1 Nr. 1 VSG NRW ist. Dies ist nicht gewährleistet, wenn sich die Subsidiaritätsklausel gleichermaßen auf die Zielperson wie die Kontaktperson bezieht und damit faktisch leerläuft. So ist es im

---

[88] *Zöller*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2838, S. 9; *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 13.
[89] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 148.
[90] *Zöller*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2838, S. 9.
[91] Zum Kriterium der Voraussehbarkeit von Überwachungsmaßnahmen beispielhaft BVerfGE 125, 260 Rn. 266; BVerfGE 155, 119 Rn. 131 – Bestandsdatenauskunft II; EGMR, Urteil vom 4. 12. 2008, Beschwerden 30562/04 u. 30566/04, Rn. 95, 99. – S. u. Marper/Vereinigtes Königreich.

Regierungsentwurf, der in diesem Punkt nicht verändert wurde, vorgesehen[92] und auch in der vom Landtag beschlossenen Fassung[93] sowie in der im Internet abrufbaren.[94] Gleichwohl bezieht sich die Subsidiaritätsklausel in der verkündeten Fassung nur auf § 11 Abs. 2 S. 1 Nr. 2 VSG NRW.[95] Dass eine Berichtung nach § 106 Abs. 2 Geschäftsordnung des Landtages von Nordrhein-Westfalen stattgefunden hätte, ergibt sich aus den öffentlich verfügbaren Gesetzgebungsmaterialien nicht; es wäre auch zweifelhaft, ob es sich hierbei um eine offensichtliche Berichtung handelt.

119 Damit besteht die Gefahr, dass der Verfassungsschutz zu leicht auf Kontaktpersonen zugreift. Diese werden nicht mit einer Überwachung rechnen und keine Gegenmaßnahmen ergreifen, sind also ein „leichtes Ziel". Erschwerend kommt hinzu, dass die weiteren Regelungen des VSG NRW, z.B. zur Weiterverarbeitung, Datenanalyse, Löschung, keine besonderen Regelungen für Kontaktpersonen vorsehen. Dies wird dem Grad ihrer persönlichen Verstrickung in eine beobachtungsbedürftige Bestrebung nicht gerecht.

III. § 20 VSG NRW (Zugriff auf Videoüberwachung des öffentlich zugänglichen Raumes)

120 § 20 VSG NRW verstößt gegen das allgemeine Persönlichkeitsrecht der Beschwerdeführenden, insbesondere in der Ausprägung als Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

1. Bedeutung der Regelung

121 Diese Regelung stellt einen **Paradigmenwechsel** dar. Sie erlaubt dem Verfassungsschutz unabhängig von einer konkreten Gefahrensituation die Nutzung aller öffentlichen und privaten Einrichtungen der Videoüberwachung, die den öffentlichen Raum beobachten. Voraussetzung ist lediglich, dass dies der Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebungen i.S.v. § 5 Abs. 2 VSG NRW dient. Eine weitere Eingrenzung durch spezifische Anforderungen an den Einsatz dieser Maßnahme findet nicht statt. Die Regelung erlaubt den Zugriff auf jede Einrichtung zur Videoüberwachung, wenn sie den öffentlichen Raum abdeckt. Auch dies ist denkbar weit. Ausgeklammert wird lediglich die Videoüberwachung privater Räume, die unter die sehr eng auszulegende Haushaltsausnahme nach Art. 2 Abs. 2 lit. c DSGVO fallen, sowie Räume, die

---

[92] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 21.
[93] Landtag von Nordrhein-Westfalen, Vorabdruck 18/108, S. 16.
[94] Vgl. https://recht.nrw.de/lrgv/gesetz/01042026-verfassungsschutzgesetz-nordrhein-westfalen-vsg-nrw/
[95] GV.NRW 2025 Nr. 46 S.994.

allgemein nicht zugänglich sind, also z.B. nicht dem Publikumsverkehr offenstehen.[96] Öffentliche Räume umfassen daher nahezu jeden Platz außerhalb der Wohnung, z.B. in Geschäften, Kaufhäusern, Einkaufszentren, Behörden, im ÖPNV, auf öffentlichen Straßen, in Treppenhäusern, Passagen, Parks, Veranstaltungsorten, Schulen und Universitäten sowie ggf. am Arbeitsplatz.[97]

122 Die potenzielle Reichweite der Regelung zeigt sich, wenn man sich vor Augen führt, wie viele Einrichtungen zur Videoüberwachung im Einsatz sind. Der Anwendungsbereich reicht dabei weit über die stationären Videokameras hinaus, die man zunächst denkt. Die Regelung knüpft – wie die Gesetzesbegründung und die komplementäre Änderung von § 20 LDSG NRW zeigen – an § 4 BDSG und § 20 LDSG NRW an.[98] Beide Regelungen definieren Videoüberwachung als „**optisch-elektronische Einrichtungen**" (§ 4 Abs. 1 S. 1 BDSG, § 20 Abs. 1 LDSG NRW). Erfasst werden damit alle Geräte, die Licht in elektronische Signale umwandeln, unabhängig davon, ob sie stationär, mobil oder auch temporär sind.[99] Die Regelung erfasst damit beispielsweise auch Dashcams,[100] Kameras in Drohnen und in der Sensorik von Autos sowie Webcams, Smartglasses und handelsübliche Smartphones, die Videos aufzeichnen können.[101] Aus dem Begriff der „Einrichtung" lässt sich nach bisherigem Verständnis daher keine Eingrenzung ableiten. Werden dabei Tonaufnahmen aufgezeichnet, bezieht sich die Verpflichtung nach § 20 Abs. 2 S. 1 VSG NRW auch auf diese; dies ergibt sich aus § 20 Abs. 2 S. 3 VSG NRW („angeforderte Bild- und Tonaufzeichnungen").

123 Mangels Eingrenzungen erlaubt die Regelung daher eine nahezu flächendeckende Überwachung im öffentlichen Raum, die in einem hohen Maße dritte Personen betrifft. Denkbar wäre es zum Beispiel einer Person, durch Nutzung privater oder öffentlicher Videoüberwachungsanlagen in einer Stadt über weite Strecken zu verfolgen oder zu suchen. Wie so etwas praktisch

---

[96] BVerwGE 165, 111 Rn. 14 zur Vorgängerregelung § 6b Abs. 1 BDSG a.F.; ausführlich *Scholz/Schindler* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, § 4 BDSG Rn. 52 ff.; *Reuter/Grabenschröer* in Taeger/Gabel, 5. Aufl. 2026, DSGVO – BDSG – TDDDG, § 4 Rn. 35 ff.

[97] Siehe auch die Aufzählung bei *Schindler/Scholz* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, § 4 BDSG Rn. 54 ff.

[98] Landtag Nordrhein-Westfalen, Drucksache 18/14557, S. 171.

[99] *Schwartmann/Jacquemais* in Schwartmann/Pabst, Landesdatenschutzgesetz NRW, 2020, § 20 Rn. 12; *Schindler/Scholz* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, § 4 BDSG Rn. 49.

[100] Deutlich in diese Richtung tendierend bereits zur Vorgängernorm § 6b BDSG a.F. BGHZ 218, 348 Rn. 21 – Dashcams.

[101] Siehe auch die Beispiele bei *Schwartmann/Jacquemais* in Schwartmann/Pabst, Landesdatenschutzgesetz NRW, 2020, § 20 Rn. 12; *Scholz/Schindler* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, Anhang 1 zu Art. 6 DSGVO Rn. 6; *Reuter/Grabenschröer* in Taeger/Gabel, 5. Aufl. 2026, DSGVO – BDSG – TDDDG, § 4 Rn. 34.

aussehen kann, lässt sich im Film *Staatsfeind Nr. 1*[102] aus dem Jahr 1998 erahnen. Wenn daher ein Sachverständiger von der „Möglichkeit der Schaffung eines totalen Überwachungsstaates“ spricht,[103] mag das zugespitzt sein, unterstreicht aber die grundrechtliche Sensibilität der Maßnahme.

124 In seiner Entscheidung zum Bayerischen Verfassungsschutzgesetz hat das Gericht bereits über eine Norm entschieden, die eine ähnliche Befugnis enthielt (Art. 19a Abs. 1 S. 2 BayVerfSchG). Diese Norm war jedoch aus anderen Gründen verfassungswidrig, so dass das Gericht diesem Aspekt keine Aufmerksamkeit schenken musste.[104]

2. Regelungsinhalt und -systematik

125 § 20 VSG NRW erlaubt zwei verschiedene Maßnahmen:

- Erstens die Mitnutzung der Videoüberwachung durch den Verfassungsschutz nach § 20 Abs. 1 VSG NRW: Der Betreiber hat dazu dem Verfassungsschutz Zutritt zu gewähren und die Mitbenutzung seiner Anlage zu dulden. Der Verfassungsschutz „übernimmt“ hier die Videoüberwachungseinrichtung. Der Gesetzgeber sieht hierin einen Unterfall technischer Observation.[105]
- Zweitens kann der Verfassungsschutz die Ausleitung und die Übermittlung von Aufzeichnungen verlangen. Dies ist dem Verfassungsschutz sowohl für „Live-Aufnahmen“ in Echtzeit gestattet wie auch für gespeicherte Aufnahmen – bis hin zu einem Jahr zurück (§ 20 Abs. 2 VSG NRW).

126 Nach § 20 Abs. 3 VSG NRW ist für den zweiten Fall immer eine richterliche Genehmigung erforderlich, für den ersten Fall des § 20 Abs. 1 VSG NRW nur, wenn die Grenzen des § 19 Abs. 2 Nr. 2 lit. b und c VSG NRW (punktuell an 21 Tagen in drei Monaten; punktuell, aber über drei Monate hinaus) überschritten werden. In den Fällen des § 20 Abs. 1 VSG NRW – gemeint sind wohl die übrigen Fälle – entscheidet die Leitung der Verfassungsschutzabteilung. Diese kann auch sonst die Anordnung bei Gefahr in Verzug anordnen (§ 13 Abs. 5 VSG NRW). Unklar ist allerdings, ob sich die richterliche Anordnung auf bestimmte Videoüberwachungseinrichtungen beziehen muss und wie konkret die Situationen der Überwachung und die Betroffenheit Dritter dem Gericht dargelegt werden müssen; § 13 Abs. 3 S.2

---

[102] *Enemy of the State*, 1998, Regie: Tony Scott, Hauptrollen: Will Smith und Gene Hackmann.
[103] *Zöller*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2838, S. 9.
[104] BVerfGE 162, 1 Rn. 358 ff. – Bayerisches Verfassungsschutzgesetz.
[105] Landtag Nordrhein-Westfalen, Drucksache 18/14557, S. 172.

VSG NRW nennt diese Punkt in seiner nicht abschließenden Aufzählung nicht.

127 Tatbestandlich reicht es aus, dass die Maßnahme zur Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebung erfolgt (§ 20 Abs. 1 und 2 VSG NRW). Es handelt sich um ein nachrichtendienstliches Mittel (§ 10 Abs. 1 Nr. 3 VSG NRW), so dass die weiteren Voraussetzungen des § 11 VSG NRW einzuhalten sind. Als Zielpersonen kommen daher auch Kontaktpersonen nach § 11 Abs. 2 S. 1 Nr. 2 VSG NRW in Betracht (zur Verfassungswidrigkeit dieser Regelung, → Rn. 104 ff.); die Regelung sieht eine allgemeine Subsidiarität nachrichtendienstlicher Mittel vor, nicht aber von Kontaktpersonen gegenüber primären Zielpersonen.

3. Grundrechtseingriff

128 Die Befugnisse nach §20 VSG NRW greifen in den Schutzbereich des allgemeinen Persönlichkeitsrechts in seiner Ausprägung als Recht auf informationelle Selbstbestimmung ein (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und andere Grundrechte, z.B. die Versammlungsfreiheit (Art. 8 Abs. 1 GG).

a) Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)

aa) Mitnutzung von Videoüberwachungseinrichtungen nach § 20 Abs. 1 VSG NRW

129 Die Mitnutzung von Videoüberwachungseinrichtungen durch den Verfassungsschutz nach § 20 Abs. 1 VSG NRW greift unmittelbar in das Recht das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in dessen Ausprägung als Recht auf informationelle Selbstbestimmung der beobachteten Personen ein. Dabei kommt es nicht darauf an, ob es sich um Zielpersonen nach § 11 Abs. 2 S. 1 VSG NRW handelt oder um Dritte, die zufällig miterfasst werden. Auch diese Dritten sind durch die Maßnahme betroffen.[106]

130 Nach der ständigen Rechtsprechung des Gerichts gewährleistet das Recht auf informationelle Selbstbestimmung

[106] Hiervon geht auch die Gesetzesbegründung aus: Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 148.

„die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Sachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen."[107]

Dahinter steht der Gedanke des vorgelagerten Schutzes der Verhaltensfreiheit, denn,

„wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."[108]

Diese Freiheit ist vor allem bedroht unter den Bedingungen moderner Datenverarbeitung.[109] Zu diesen gehört auch der weitverbreitete Einsatz von Videoüberwachungseinrichtungen.

131 Denn diese Systeme erlauben nicht nur die Beobachtung in Echtzeit, sondern auch die technische Speicherung, Auswertung, Analyse und Verknüpfung mit anderen Daten, um weitergehende Schlüsse über eine Person zu ziehen.[110] Dies gilt in jedem Fall dann, wenn die Aufzeichnungen gespeichert werden.[111] Ebenso gilt dies aber im Falle eines Kamera-Monitor-Systems, d.h. einer Echtzeitbeobachtung über einen Monitor ohne Speicherung der Bilder.[112] Auch bei diesem System werden optische Signale elektronisch verarbeitet, sobald eine digitale Kamera verwendet wird, weshalb sie auch unter § 4 Abs. 1 BDSG, § 20 Abs. 1 LDSG NRW fallen.[113] Dem liegt der Gedanke zugrunde, dass auch ohne eine Aufzeichnung, allein durch die Tatsache der Beobachtung, eine verhaltenslenkende Wirkung eintritt und die Verhaltensfreiheit der beobachteten Personen beeinträchtigt wird (sog. panoptischer Effekt).[114] Daher ist auch dann ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung gegeben, wenn ein Mitarbeiter des Verfassungsschutzes eine Videoüberwachungseinrichtung nur temporär nutzt,

---

[107] BVerfGE 65, 1 (42 f.) – Volkszählung; BVerfGE 152, 152 Rn. 84 – Recht auf Vergessen I; BVerfGK 10, 330 = NVwZ 2007, 688 (690) – Videoüberwachung öffentlicher Plätze.
[108] BVerfGE 65, 1 (45) – Volkszählung; BVerfGE 152, 152 Rn. 84 – Recht auf Vergessen I.
[109] BVerfGE 150, 244 Rn. 37 f. – Kfz-Kennzeichenüberwachung II; grundlegend BVerfGE 65, 1 (41 ff.) – Volkszählung.
[110] BVerfGK 10, 330 = NVwZ 2007, 688 (690) – Videoüberwachung öffentlicher Plätze.
[111] BVerwGE 141, 329 Rn. 23 f. – Videoüberwachung Reeperbahn („einhellige Meinung").
[112] So die Gesetzesbegründung zu § 6b BDSG a.F. Bundestags-Drucksache 14/4329, S. 38.
[113] BVerwGE 165, 111 Rn. 15 – Videoüberwachung in Arztpraxis.
[114] BVerwGE 165, 111 Rn. 17 – Videoüberwachung in Arztpraxis; noch offen gelassen in BVerwGE 141, 329 Rn. 24, 26 – Videoüberwachung Reeperbahn, ob ein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt; zum panoptischen Effekt durch Überwachung BVerfGE 65, 1 (43) – Volkszählung; BVerfGE 152, 152 Rn. 84 – Recht auf Vergessen I; BVerfGK 10, 330 = NVwZ 2007, 688 (690) – Videoüberwachung öffentlicher Plätze; BVerfGE 122, 342 Rn. 129 ff. – Bayerisches Versammlungsgesetz (zu einem Grundrechtseingriff durch Übersichtsaunahmen eines Kamera-Monitor-Systems).

indem er sich auf den Stuhl des Wachmannes setzt und an seiner Stelle das Geschehen „live“ aus der Distanz beobachtet.

132 Ein Eingriff liegt damit vor, sobald eine Person auf einem Bild identifizierbar ist. Dies ist der Fall, wenn ihr Gesicht zu erkennen ist.[115] Eine Identifikation ist aber auch anhand anderer biometrischer Merkmale oder Verhaltensweisen (z.B. Gang) möglich. Es ist davon auszugehen, dass der Verfassungsschutz über entsprechende Möglichkeiten zur Identifikation für eine Vielzahl von Personen verfügt. Es ist darauf hinzuweisen, dass die Restriktionen der KI-VO für eine Echtzeit-Fernidentifikation (Art. 5 Abs. 2 bis 7 KI-VO) für den Verfassungsschutz nicht gelten (Art. 2 Abs. 3 UAbs. 2 KI-VO).

133 Dabei ist es unerheblich, ob die Videoaufnahmen Informationen enthalten, die nur den öffentlichen Raum betreffen.[116] Das Recht auf informationelle Selbstbestimmung zeichnet sich gerade dadurch aus, dass es nicht nur sensible Informationen schützt und sein Schutzbereich nicht nach Intim-, Privat- und Intimsphäre differenziert ist.[117] Auch der Gedanke eines stillschweigenden Einverständnisses scheidet vorliegend von vornherein aus,[118] weil die betroffenen Personen nicht wissen, dass die Videoüberwachung sie auch nachrichtendienstlichen Zwecken dient. Im Gegenteil: Sie müssen davon ausgehen, dass die Videoüberwachung allein den eigentlichen Zwecken dient, über die sie gemäß Art. 13 Abs. 1 lit. c DSGVO informiert werden.[119] Es ist ebenfalls unerheblich, dass die Überwachung Dritte nur zwangsläufig miterfasst. Diese werden nicht nur technisch ungewollt miterfasst und dann wieder gelöscht.[120] Sie bleiben Teil der Bildaufnahmen.

bb) Verpflichtung zur Ausleitung von Bild- und Tonaufnahmen in Echtzeit und zur Herausgabe von Aufzeichnungen (§ 20 Abs. 2 VSG NRW)

134 Auch in der Verpflichtung des Betreibers einer Videoüberwachungsanlage, Bild- und Tonaufnahmen in Echtzeit auszuleiten oder Aufzeichnungen

---

[115] BVerwGE 165, 111 Rn. 15 – Videoüberwachung in Arztpraxis; EuGH, Urt. v. 11. 12.2014, C-212/13, ECLI:EU:C:2014:2428, Rn. 22 – Ryneš.

[116] BVerfGK 10, 330 = NVwZ 2007, 688 (690) – Videoüberwachung öffentlicher Plätze; BVerfGE 150, 244 Rn. 39 – Kfz-Kennzeichenüberwachung II; BVerwGE 141, 329 Rn. 25 – Videoüberwachung Reeperbahn.

[117] BVerfGE 65, 1 (45) – Volkszählung; BVerfGK 10, 330 = NVwZ 2007, 688 (690) – Videoüberwachung öffentlicher Plätze; BVerwGE 141, 329 Rn. 25 – Videoüberwachung Reeperbahn.

[118] BVerwGE 141, 329 Rn. 25 – Videoüberwachung Reeperbahn.

[119] Zur Anwendung des Art. 13 DSGVO im Kontext von Bodycams: EuGH, Urteil v. 18.12.2025, C-422/24, ECLI:EU:C:2025:980, Rn. 27 ff. – Storstockholms Lokaltrafik.

[120] Zu dieser Rechtsprechungslinie BVerfGE 150, 244 Rn. 43 m.w.N. – Kfz-Kennzeichenüberwachung II.

herauszugeben (§ 20 Abs. 2 VSG NRW) liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

135 Anders als im Fall des § 20 Abs. 1 VSG werden die Daten nicht unmittelbar vom Verfassungsschutz erhoben, sondern zunächst durch den Betreiber der Videoüberwachungsanlage. Der Wortlaut enthält keinen Anhaltspunkt, dass die Aufnahmen erst auf Wunsch des Verfassungsschutzes erstellt werden. Es liegt mithin eine Übermittlung und eine Zweckänderung durch die Herausgabe der Ausnahmen und Aufzeichnungen an den Verfassungsschutz vor.[121] Diese stellen einen eigenständigen Grundrechtseingriff dar. Gleiches gilt für die weitere Speicherung und Verwendung durch den Verfassungsschutz.

b) Weitere Grundrechte

136 Neben dem allgemeinen Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung kann die Befugnis auch in den Schutzbereich weiterer Grundrechte der beobachteten Personen eingreifen. So können die Aufnahmen etwa Versammlungen erfassen. Hierin liegt nicht nur ein Eingriff in das Recht auf informationelle Selbstbestimmung, weil sich Personen davon abgeschreckt fühlen könnten, wenn ihre Teilnahme potenziell auch von Verfassungsschutz registriert wird.[122] In der Anfertigung von Videoaufnahmen von Versammlungen liegt auch ein Eingriff in Art. 8 Abs. 1 GG.[123]

4. Rechtfertigung

137 Der Eingriff in das Recht auf informationelle Selbstbestimmung durch § 20 VSG NRW ist nicht gerechtfertigt. Die Regelung entspricht weder dem verfassungsrechtlichen Gebot der Normenklarheit und Bestimmtheit, insbesondere dem sog. Doppeltürenmodell, (a) noch ist sie aufgrund der geringeren Eingriffsvoraussetzungen verhältnismäßig im engeren Sinne (b).

---

[121] Vgl. BVerfGE 155, 119 Rn. 93 ff. – Bestandsdatenauskunft II; BVerfGE 130, 151 Rn. 124 – Bestandsdatenauskunft I.
[122] Vgl. zu diesem Beispiel bereits BVerfGE 65, 1 (43) – Volkszählungsurteil.
[123] BVerfGE 122, 342 Rn. 131 – Bayerisches Versammlungsgesetz; OVG NRW ZD 2020, 481 Rn. 6 ff.; VerfGH Berlin ZD 2015, 474 Rn. 48.

a) Verstoß gegen das Gebot der Normenklarheit und Bestimmtheit

aa) Funktionsweise des Doppeltürenmodells

138 Das Gericht hat für Übermittlungsregelungen das sog. Doppeltürenmodell[124] entwickelt. Das Gericht beschreibt die Funktionsweise wie folgt:

> „Bei der Regelung eines Datenaustauschs zur staatlichen Aufgabenwahrnehmung ist darüber hinaus aber auch zwischen der Datenübermittlung seitens der auskunftserteilenden Stelle und dem Datenabruf seitens der auskunftssuchenden Stelle zu unterscheiden. Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten. Dies schließt – nach Maßgabe der Kompetenzordnung und den Anforderungen der Normenklarheit – nicht aus, dass beide Rechtsgrundlagen auch in einer Norm zusammengefasst werden können.“[125]

139 Danach ist sind eine Übermittlungsbefugnis und eine Abrufbefugnis erforderlich. Diese erste Tür, die Befugnis der auskunftspflichtigen Stelle zur Übermittlung, sieht der Gesetzgeber in § 4 Abs. 3 S. 3 BDSG sowie § 20 Abs. 3 LDSG NRW.[126] Die Abrufbefugnis (= zweite Tür) ist § 20 VSG NRW. Es handelt sich aber nicht nur bei § 20 Abs. 2 VSG NRW um eine Übermittlungsregelung im Sinne des Doppeltürenmodells, sondern auch bei der Befugnis zur Mitbenutzung der Videoüberwachungseinrichtung nach § 20 Abs. 1 VSG NRW. Auch hier erfolgt ein staatlicher Zugriff auf eine laufende Datenverarbeitung – die Videoüberwachung; die Datenverarbeitung erfolgt auf einer rechtlichen Grundlage (§ 4 Abs. 1 BDSG, Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO) in der Verantwortung des Betreibers der Videoüberwachungseinrichtung. Es liegt also genau die identische Situation von Zugriffsgewährung und Zugriffsbefugnis vor wie bei einem Zugriff auf gespeicherte Datenbestände und den anderen Fällen, in denen das Gericht das Doppeltürenmodell bisher angewendet hat. Vorliegend erfolgt der Zugriff nur bereits eng verzahnt mit der Erhebung. Im Rahmen der Erhebung wird zudem die Datenverarbeitung bereits mit der Umwandlung von optischen in elektronische Signale beginnen. Die Erhebung ist also bereits erfolgt, wenn der Verfassungsschutz die Informationen im Rahmen der Mitnutzung zur Kenntnis nimmt.

140 Damit wird bereits deutlich, dass das Doppeltürenmodell nicht nur der Normenklarheit dient, indem es die Normbefehle von den – häufig privaten –

---

[124] BVerfGE 155, 119 Rn. 93, 95, 201 – Bestandsdatenauskunft II m.w.N.
[125] BVerfGE 130, 151 Rn. 123 – Bestandsdatenauskunft I; BVerfGE 155, 119 Rn. 93, 95, 130 ff., 201 f. – Bestandsdatenauskunft II m.w.N.
[126] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 171.

Adressaten des Abrufs einerseits und den Zugriff durch die staatliche Stelle andererseits trennt.[127] Das Doppeltürenmodell hat zudem vor allem dann Bedeutung, wenn für die beiden Regelungen – wie hier in Bezug auf private Videoüberwachung – unterschiedliche Gesetzgeber zuständig sind.[128] Beide Regelungen müssen daher

> „aufeinander abgestimmt sein und eine klare und konsistente Gesamtregelung treffen, auch wenn die Abrufregelung und die Übermittlungsregelung zu unterschiedlichen Gesetzgebungskompetenzen gehören."[129]

bb) Keine Übermittlungsbefugnis für nachrichtendienstliche Zwecke

141 § 20 VSG NRW verstößt bereits gegen den Grundsatz der Normenklarheit, weil die Übermittlungsbefugnisse in § 20 Abs. 3 LDSG NRW und § 4 Abs. 3 S. 3 BDSG eine solche Verwendung nicht erlauben. Dieser Mangel wirkt sich auch auf § 20 VSG NRW aus, denn eine Abrufbefugnis – die zweite Tür – darf aber nicht weiter geöffnet sein als die erste Tür.[130] Beide Regelungen erlauben eine Verwendung von personenbezogenen Daten, die durch eine Videoüberwachung gewonnen nur „zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit".

(1) § 4 Abs. 3 S. 3 BDSG

142 § 4 Abs. 3 S. 3 BDSG umfasst daher nicht die Verwendung für nachrichtendienstliche Zwecke. Denn Aufgabe des Verfassungsschutzes ist gerade nicht die Gefahrenabwehr, sondern das Sammeln und Auswerten von Informationen im Vorfeld (§ 3 Abs. 1 VSG NRW). Die Gesetzbegründung rekurriert auf eine Passage in den Ausschussdokumenten zu § 6b BDSG a.F., der Vorgängerreglung zu § 4 BDSG, worin die Notwendigkeit einer „Gefahrenvorfeldüberwachung" erwähnt werde.[131] Wenn man die Passage insgesamt liest, wird jedoch deutlich, dass sie auf Kriminalitätsbekämpfung und nicht auf die Aufgaben des Verfassungsschutzes zielt:

> „Dabei kommt es insbesondere darauf an, dass die Videoüberwachung öffentlich zugänglicher Räume in einem hohen Maße auch zur vorbeugenden Bekämpfung von kriminogenen Gefahren erfolgt, und zwar auch dann, wenn noch keine konkreten Hinweise für einen bestimmten Raum oder bestimmte Täter oder Taten vorliegen; d.

---

[127] Eingehend BVerfGE 155, 119 Rn. 201 f. – Bestandsdatenauskunft II.
[128] Dazu BVerfGE 125, 260 Rn. 264 – Vorratsdatenspeicherung; BayVGH ZD 2019, 515 Rn. 41f. (unter Verweis auf Art. 31 GG).
[129] *Basar/Heinelt* in Taeger/Pohle ComputerR-HdB, 40. EL März 2025, Teil 10. 100. Rn. 578.
[130] BVerfGE 155, 119 Rn. 130, 201 – Bestandsdatenauskunft II.
[131] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 171.

h.dass zur Legitimation notwendiger „Gefahrenvorfeldüberwachung“ auch Vorfelderermittlungen rechtlich möglich sein müssen.“[132]

Im weiteren Verlauf erwähnt der Ausschuss auch nur noch die Abwehr von Gefahren. Der nordrhein-westfälische Gesetzgeber unterstellt dem Bundesgesetzgeber also eine Intention, die dieser nicht hatte.[133] Auch die Verwendung von Begriffen wie „Gefahrenvorfeldüberwachung“ oder „Vorfeldermittlung“ in der oben zitierten Passage dürfte eher in Abgrenzung zur konkreten Gefahr gemeint sein, die im Polizeirecht zur damaligen Zeit noch die dominierende Eingriffsschwelle war. Andeutungen, dass damit auch Nachrichtendienste erfasst sein könnten, gibt es keine.

143 Dies wird auch deutlich an der Interpretation der Regelung durch die Literatur. Soweit ersichtlich wird eine Verwendung für nachrichtendienstliche Zwecke nicht angenommen. Der vergleichsweise ungewöhnliche Begriff der „staatlichen Sicherheit“ wird so ausgelegt, dass damit der „Bestand, Einrichtungen und Veranstaltungen des Staates“ gemeint seien.[134] Im Übrigen werden darunter Gefahrenabwehr und Strafverfolgung verstanden.[135] Sollte der Gesetzgeber damit nachrichtendienstliche Zwecke gemeint haben, wäre die Zweckbestimmung unter Berücksichtigung der erheblichen Eingriffstiefe nicht hinreichend präzise und für die betroffenen Personen kaum hinreichend voraussehbar.[136] Sie würden wohl kaum damit rechnen, dass eine Kamera nicht nur zur Verfolgung von Straftaten oder zur Abwehr konkreter Gefahren eingesetzt werden dürfte, sondern auch zu nachrichtendienstlichen Zwecken durch den Verfassungsschutz.[137]

(2) § 20 Abs. 3 LDSG NRW

144 Im Falle von § 20 Abs. 3 LDSG NRW soll die Ergänzung der „staatlichen Sicherheit“ gerade den Zugriff auf die Nachrichtendienste erlauben, der parallel mit der Änderung eingeführt worden ist.[138] Andererseits knüpft die

---

[132] Bundestagsdrucksache 14/5793, S. 59.
[133] Im Ergebnis ebenso *Deutscher Anwaltverein*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2844, S. 10 f.
[134] *Frenzel* in Paal/Pauly, DSGVO/BDSG, 4. Aufl. 2026, § 4 BDSG Rn. 31.
[135] Vgl. etwa *Marsch* in Sydow/Marsch, DSGVO/BDSG, 3. Aufl. 2002, § 4 BDSG Rn. 40; *Starnecker* in Gola/Heckmann, DSGVO/BDSG, 3. Aufl. 2022, § 4 BDSG Rn. 63; *Reuter/Grabenschröer* in Taeger/Gabel, 5. Aufl. 2026, DSGVO – BDSG – TDDDG, § 4 Rn. 95; *Buchner* in Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, § 4 BDSG Rn. 17; *Schindler/Scholz* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, § 4 BDSG Rn. 113.
[136] Zu dieser Anforderung beispielhaft BVerfGE 125, 260 Rn. 266; BVerfGE 155, 119 Rn. 131 – Bestandsdatenauskunft II; EGMR, Urteil vom 4. 12. 2008, Beschwerden 30562/04 u. 30566/04, Rn. 95, 99. – S. u. Marper/Vereinigtes Königreich.
[137] Vgl. zum Abruf von Telekommunikationsdaten durch Verfassungsschutzbehörden BVerfGE 162, 1 Rn. 335 – Bayerisches VSG.
[138] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 253.

Ergänzung ausdrücklich an § 4 Abs. 3 S. 3 BDSG an,[139] der – wie gezeigt (→ Rn. 142 f.) – gerade nicht die Verwendung zu nachrichtendienstlichen Zwecken umfasst. Damit ist sie zumindest nicht ausreichend präzise, um normenklar und damit voraussehbar eine solche Verwendung zu legitimieren.

cc) Unzureichende Bestimmtheit der Übermittlungsbefugnis

145 Selbst wenn man zu dem Ergebnis käme, dass § 4 Abs. 3 S. 3 BDSG und § 20 Abs. 3 LDSG NRW eine Übermittlung zu nachrichtendienstlichen Zwecken erlauben würden, wäre die Regelung nicht ausreichend bestimmt. Nach den Anforderungen des Gerichts muss auch der für die „erste Tür" zuständige Gesetzgeber die wesentlichen Regelungen festlegen und die

> „Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden, so dass insgesamt die verfassungsrechtlichen Anforderungen gewahrt werden."[140]

Daran fehlt es vorliegend. Allein die höchst allgemeine Zweckbestimmung („zur Abwehr von Gefahren für die öffentliche und staatliche Sicherheit") reicht nicht aus. Verstünde man diese als tatbestandlichen Eingriffsschelle und verlangt das Vorliegen einer konkreten Gefahr, würde § 20 VSG NRW weit darüber hinaus gehen, also die zweite Türe erheblich weiter öffnen als die erste, weil § 20 VSG NRW nicht an die Gefahrenschwelle anknüpft, sondern an die nachrichtendienstlichen Eingriffsschwellen, die bewusst sehr viel früher ansetzen.

146 Zudem enthalten § 4 Abs. 3 S. 3 BDSG und § 20 Abs. 3 LDSG NRW keine Ermächtigung zur Weitergabe für die weitgehende Art des Zugriffs. Sie regeln allein die Weiterverarbeitung, aber nicht die Duldung der Mitbenutzung der Videoüberwachungsanlage durch den Verfassungsschutz und auch nicht die Verpflichtung zur Ausleitung von Aufnahmen in Echtzeit mit den damit verbundenen Herausforderungen (→ Rn. 175 f.). Hierbei handelt es sich auch nicht um bloße Modalitäten. Die Möglichkeit des Echtzeitzugriffs auf Distanz erleichtert den Grundrechtseingriff erheblich und verändert damit die Dimension der Grundrechtsbeeinträchtigung im Vergleich zur Intention des Gesetzgebers bei Erlass des § 4 Abs. 3 S. 3 BDSG.

dd) Auswirkungen auf § 20 VSG NRW

147 Diese Mängel der „ersten Tür" schlagen auch auf die „zweite Tür", § 20 VSG NRW, durch und führen zu einem Verstoß gegen das Gebot der Normenklarheit. Die zweite Tür darf nicht weiter geöffnet werden als die erste

---

[139] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 253.
[140] BVerfGE 155, 119 Rn. 130 – Bestandsdatenauskunft II.

Tür. Der für die Abrufbefugnis zuständige Gesetzgeber darf lediglich höhere Anforderungen stellen, aber keine niedrigeren.[141] Dazu führt das Gericht aus:

> „Aus **Gründen der Normenklarheit** darf er aber selbst dann, wenn er – wie vorliegend – zugleich Gesetzgeber der Abrufregelungen ist, **nicht die in der Übermittlungsregelung begrenzten Verwendungszwecke unterlaufen und die Behörden zum Abruf zu anderen, weitergehenden Zwecken ermächtigen**, niedrigere Eingriffsschwellen oder einen weniger gewichtigen Rechtsgüterschutz vorsehen. Abrufregelungen mit solchermaßen abgesenkten Verwendungsregeln könnten zwar die Behörden – im Rahmen des verfassungsrechtlich Zulässigen – zum Datenabruf ermächtigen; die Diensteanbieter wären jedoch zur Auskunft weder berechtigt noch verpflichtet (vgl. § 113 II 1 TKG). **Derartige Abrufregelungen enthielten von daher einen mit der Übermittlungsregelung von vornherein unvereinbaren Normbefehl**. Die Verwendungszwecke der auszutauschenden Daten müssen aber gerade **durch das Zusammenwirken der Übermittlungs- und Abrufregelung normenklar begrenzt** sein. Es darf nicht der Anschein erweckt werden, dass eine Behörde losgelöst von den in der Übermittlungsregelung getroffenen Verwendungsregeln auf Daten zugreifen dürfte. **Dadurch würden Zugriffsmöglichkeiten eröffnet, die missbräuchlich und unvorhersehbar genutzt werden könnten**.“[142] (Hervorhebungen hinzugefügt)

148 Genau diese Problematik liegt im Verhältnis von § 4 Abs. 3 S. 3 BDSG und § 20 VSG NRW vor. Der Landesgesetzgeber ermächtigt den Verfassungsschutz zum Zugriff auf Videoüberwachungsanlagen, obwohl der Bundesgesetzgeber dies nicht oder nicht ausreichend präzise erlaubt hat. Dies stellt die Betreiber von Videoüberwachungsanlagen vor die Frage, ob sie ihre Aufzeichnungen an den Verfassungsschutz nach § 20 Abs. 2 VSG NRW ausleiten dürfen oder sie die Erfüllung dieser Verpflichtung mit Verweis auf den engeren § 4 Abs. 3 S. 3 BDSG verweigern dürfen. Die Problematik widersprüchlicher Normbefehle stellt sich aber auch dann, wenn – wie im Falle des § 20 Abs. 3 LDSG NRW – derselbe Gesetzgeber für beide „Türen“ zuständig ist.[143]

149 Dieser Normkonflikt kann auch nicht aufgelöst werden, indem man die Abrufregelung des § 20 VSG NRW ganz oder teilweise leerlaufen lässt[144] oder im Lichte der Übermittlungsermächtigung auslegt. Eine einschränkende Auslegung hat das Gericht abgelehnt:

> „Ein Widerspruch zwischen Übermittlungsregelung und einer weniger begrenzten Abrufregelung könnte auch **nicht dahin aufgelöst werden, dass ein Datenaustausch nur unter den engeren Voraussetzungen der Übermittlungsregelung erfolgen dürfte**. Die Einhaltung dieser engeren Voraussetzungen können und dürfen die Diensteanbieter in materieller Hinsicht nicht überprüfen. Sie liegt vielmehr allein in der Verantwortung der abfrageberechtigten Stellen (vgl. § 113 II 4 TKG) und kann auch nur dort zuverlässig beurteilt werden. Sie würden aber durch die fachrechtlichen Abrufregelungen zu einem

[141] BVerfGE 155, 119 Rn. 130, 201 – Bestandsdatenauskunft II.
[142] BVerfGE 155, 119 Rn. 201 – Bestandsdatenauskunft II.
[143] BVerfGE 155, 119 Rn. 201 – Bestandsdatenauskunft II.
[144] BVerfGE 162, 1 Rn. 335 – Bayerisches Verfassungsschutzgesetz.

weitergehenden Datenabruf ermächtigt, ohne dass eine behördeninterne Kontrolle am Maßstab der Übermittlungsregelung gewährleistet wäre. Auch insoweit würden Zugriffsmöglichkeiten eröffnet, die **rechtsstaatlich nicht mehr eingehegt und vorhersehbar** wären (dazu Dieterle ZD 2016, 517 [521]).“[145] (Hervorhebungen hinzugefügt)

Diese Erwägungen gelten auch im vorliegenden Fall. Betreiber von Videoüberwachungsanlagen wären gar nicht in der Lage, das Vorliegen der Anforderungen des § 20 VSG NRW zu prüfen. Denn der Verfassungsschutz muss gegenüber ihnen den Zugriff auf die Aufnahmen weder begründen noch dessen Voraussetzungen darlegen (§ 20 Abs. 5 i.V.m. § 8 Abs. 7 S. 1 und 2 VSG NRW).

b) Unverhältnismäßigkeit der Regelung im engeren Sinne

150 § 20 VSG NRW ist in seiner konkreten Ausgestaltung unverhältnismäßig. Der mit der Regelung verbundene Eingriff steht – auch unter Berücksichtigung des gewichtigen Ziels – außer Verhältnis zur Schwere des Eingriffs.

aa) Streubreite und Tiefe des Eingriffs

151 Nach der Rechtsprechung des Gerichts ist die Videoüberwachung des öffentlichen Raumes – selbst, wenn sie offen und punktuell erfolgt – bereits ein Eingriff in das Recht auf informationelle Selbstbestimmung von erheblichem Gewicht.[146] Nicht nur in die Grundrechte der weit definierten potenziellen Zielpersonen (§ 11 Abs. 2 S. 1 Nr. 2 VSG NRW) wird durch die Regelung eingegriffen, sondern auch in großem Umfang in die Grundrechte unbeteiligter Dritter (vgl. zur Definition § 5 Abs. 6 VSG NRW), die in keinem Zusammenhang mit einer beobachteten Bestrebung, einer geplanten Straftat oder einer Gefahr für die öffentliche Sicherheit stehen. Sie haben für die Überwachung keinen Anlass gegeben. Ihnen ist kein Fehlverhalten vorzuwerfen. Bereits aus diesem Grund handelt es sich um einen Eingriff von hoher Intensität.[147] Hinzu kommt, dass es den meisten Personen nicht möglich ist, einer potenziellen Überwachung auszuweichen, weil sie sich im öffentlichen Raum bewegen müssen, z.B. auf dem Weg zur Arbeit, Ausbildung oder Schule oder aus privaten Gründen. Dies wiegt bereits bei einer stationären offenen Videoüberwachung schwer.[148]

---

[145] BVerfGE 155, 119 Rn. 202 – Bestandsdatenauskunft II.
[146] BVerfGK 10, 330 = NVwZ 2007, 688 (691) – Videoüberwachung öffentlicher Plätze; ebenso BVerwGE 141, 329 Rn. 41 – Videoüberwachung Reeperbahn.
[147] BVerfGK 10, 330 = NVwZ 2007, 688 (691) – Videoüberwachung öffentlicher Plätze
[148] BVerwGE 141, 329 Rn. 41 – Videoüberwachung Reeperbahn.

152 Die vorliegende Regelung geht im Vergleich zu einer stationären Videoüberwachung noch erheblich weiter: Sie bezieht sich potenziell auf alle Videoüberwachungsanlagen – private wie staatliche – im öffentlichen Raum. Das Maß der potenziellen Überwachung ist daher mit einer punktuellen stationären Videoüberwachung nicht zu vergleichen, da die Anzahl der Videoüberwachungseinrichtungen erheblich zugenommen hat und Videokameras in einer Vielzahl von Situationen zum Einsatz kommen (ausführlich bereits →Rn. 121 ff.).

153 Hiergegen lässt sich auch nicht einwenden, dass nur Videoaufnahmen genutzt werden, die ohne angefertigt werden, und die Videoüberwachung schon aufgrund der Informationspflichten (vgl. Art. 13 DSGVO, § 4 Abs. 2 BDSG) hinreichend transparent ist. Transparent sind dabei aber nur die eigentlichen Zwecke der Videoüberwachung. Die Zweckänderung, die Nutzung zu nachrichtendienstlichen Zwecken, findet heimlich, im Verborgenen statt. Es stellt aber aus Sicht einer Bürgerin oder eines Bürgers und auch verfassungsrechtlich einen erheblichen Unterschied dar, ob eine Videoüberwachung durch ein Kaufhaus oder durch die örtlichen Verkehrsbetriebe erfolgt oder durch den Staat, insbesondere durch eine Sicherheitsbehörde wie einem Nachrichtendienst. Hieran können sich für eine Person typischerweise viel tiefgreifendere Folgen knüpfen.

154 Daran ändert es auch nichts, dass der Verfassungsschutz nicht jede Videoüberkamera in Nordrhein-Westfalen rund um die Uhr zu einem flächendeckenden Überwachungsnetz ausbaut. Das behauptet niemand und wird auch hoffentlich nie passieren. Grundrechtlich reicht bereits die Möglichkeit aus, dass der Verfassungsschutz Zugriff auf die Aufnahmen jeder Videokamera im öffentlichen Raum nehmen kann. Die Bürgerinnen und Bürger müssen mit dieser Möglichkeit rechnen (z.B. könnte ihr Nachbar im Bus oder die Person neben ihr im Fußballstation oder auf dem Weg zu einer Versammlung vom Verfassungsschutz auf diese Weise beobachtet werden). Da Zweckänderungen nach § 20 VSG NRW im Verborgenen erfolgen, kann er nie sicher wissen, ob der Verfassungsschutz diese Befugnis gerade einsetzt. Dieser panoptische Effekt verstärkt die verhaltenslenkende Wirkung, der von einer Videoüberwachung ausgeht, und damit die Auswirkungen auf die Verhaltensfreiheit durch Einschüchterung (*chilling effect*).[149] Diesen *chilling effect* hat das Gericht in seiner Rechtsprechung immer wieder herausgestellt:

> „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“[150]

[149] Dazu *Büscher/Hornung/Schindler et al.*, DuD 2023, 503 ff.
[150] BVerfGE 65, 1 (43) – Volkszählung.

155 In Kombination mit der räumlichen Verbreitung der Videoüberwachung kann so das „Gefühl eines ständigen Überwachtseins“ im öffentlichen Raum entstehen. Dieses Gefühl ist nach der Rechtsprechung des Gerichts mit einem freiheitlichen Gemeinwesen nicht vereinbar.[151]

bb) Auswirkung auf die Ausübung weiterer Grundrechte

(1) Meinungs- und Versammlungsfreiheit

156 Erschwerend ist zudem zu berücksichtigen, dass eine Videoüberwachung etwa im Kontext von Versammlungen erhebliche einschüchternde Wirkung auf die Ausübung weiterer Grundrechte haben kann. Dies sind insbesondere Art. 5 Abs. 1 und Art. 8 Abs. 1 GG, die im Zusammenhang mit politischer Betätigung stehen und damit von großer Bedeutung für das Funktionieren der Demokratie sind. Dies hat das Gericht bereits in seinem Volkszählungsurteil betont:

> „Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[152]

157 Die vorliegende Regelung enthält keine Einschränkungen in Bezug auf Versammlungen, so dass dieser Gesichtspunkt ungemindert zum Tragen kommt.

(2) Grundrechte der Betreiber der Videoüberwachungseinrichtung

158 Erschwerend zu berücksichtigen sind auch die Eingriffe in die Grundrechte der Betreiber von Videoüberwachungseinrichtungen. In Betracht kommen hier zum einen die allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) und die im Falle von Unternehmen die Berufsfreiheit (Art. 12 Abs. 1 GG). Sie werden durch die Maßnahme zur Erfüllung öffentlicher Aufgaben herangezogen.[153] Die Verpflichtung, in Echtzeit Übertragungen auszuleiten oder Aufzeichnungen zur Verfügung zu stellen, verursacht Aufwand, Kosten und bindet Ressourcen. Wie dabei die Ausleitung in Echtzeit erfolgen soll, regelt

---

[151] BVerfGE 150, 244 Rn. 51 – Kfz-Kennzeichenüberwachung II; BVerfGE 125, 260 Rn. 241 – Vorratsdatenspeicherung; BVerfGE 122, 343 Rn. 132 – Bayerisches Versammlungsgesetz (zu Videoaufnahmen) m.w.N.

[152] BVerfGE 65, 1 (43) – Volkszählung; BVerfGE 122, 343 Rn. 131 – Bayerisches Versammlungsgesetz.

[153] Zum Grundrechtseingriff durch solche Mitwirkungspflichten BVerfG BeckRS 2025, 14176 Rn. 67, 124 – Strompreisbremse.

die Norm nicht, sondern überlässt dies der Behörde. Es ist daher unklar, welche technischen Anpassungen seitens des Betreibers erforderlich sind, wenn er selbst etwa keinen Echtzeitzugriff auf Distanz vorgesehen hatte, sondern nur eine – vergleichsweise sichere und kostengünstige – lokale Aufzeichnung. Eine Kompensation erfolgt nicht. Die Erfüllung der Verpflichtungen erfolgt unentgeltlich. § 20 Abs. 5 VSG NRW verweist gerade nicht auf § 8 Abs. 7 S. 3 VSG NRW, der für Auskunftsverpflichtete eine Entschädigung vorsieht.

159 Nach § 20 Abs. 1 S. 2 VSG NRW muss der Betreiber dem Verfassungsschutz zudem Zugang zu seinen Räumlichkeiten gewähren. Diese Räumlichkeiten können Betriebsräume sein, die zumeist schon aus Gründen der Datensicherheit nicht für den öffentlichen Verkehr bestimmt sind, aber auch Wohnungen. Diese Verpflichtung kann daher in Art. 13 Abs. 1 GG eingreifen, ohne entsprechende Begrenzungen vorzusehen.

cc) Vertiefung des Eingriffs im Vergleich zur Observation

160 Nach Ansicht des Gesetzgebers handelt es sich zumindest im Falle des § 20 Abs. 1 VSG NRW um einen Unterfall der technischen Observation.[154] Eine solche Wertung durch den Gesetzgeber zeigt sich auch im Richtervorbehalt des § 20 Abs. 3 VSG NRW. Auch in der Diskussion im Landtag ist von einer Abgeordneten ausgeführt worden:

> „Mitarbeitende dürfen künftig also hinter diesen Bildschirmen sitzen, anstatt hinter der nächsten Straßenecke rumzulungern.“[155]

161 Diese Sichtweise spiegelt nicht annähernd die gerade dargestellte grundrechtliche Relevanz der Befugnis nach § 20 VSG NRW wider. Der technische Zugriff – insbesondere in Echtzeit auf Distanz sowie auf zusätzliche Aufzeichnungen – stellt einen erheblich tiefgreifenderen Grundrechtseingriff dar. Eine Observation ist personell und technisch sehr aufwändig. Die staatlichen Ressourcen begrenzen so den Grundrechtseingriff. Durch den Zugriff auf bestehende Videoüberwachungsanlagen und ihre Verbreitung wird es erheblich einfacher, Zielpersonen zu observieren und Aufzeichnungen zu erhalten, die von bestehenden Videoüberwachungsanlagen gespeichert werden, die daher weniger Verdacht erregen und schwerer zu vermeiden sind als Aufnahmen, die der Verfassungsschutz selbst anfertigt. Die Möglichkeit, auf private und staatliche Überwachungsanlagen zurückzugreifen, erlaubt daher in einem sehr größeren Umfang im Rahmen einer Observation nach § 19 VSG NRW Bildaufnahmen

[154] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 172.
[155] So die Abgeordnete *Dr. Julia Höller*, MdL, Landtag von Nordrhein-Westfalen, Plenarprotokoll 18/105 vom 5.12.2025, S. 50.

zu erstellen und die Zielperson genauer und damit grundrechtsinvasiver zu beobachten.[156]

dd) Keine ausreichenden Eingriffsschwellen und Eingrenzungen

162 § 20 VSG NRW enthält keine ausreichend hohen und bestimmten Eingriffsschwellen, die der Schwere des Eingriffs ausreichend Rechnung tragen. Dies betrifft insbesondere Personen, die selbst nicht Teil einer erheblich beobachtungsbedürftigen Bestrebung sind.

(1) Eingriffsschwelle

163 § 20 VSG NRW sieht als Eingriffsschwelle nur vor, dass die Maßnahme zur Aufklärung einer mindestens erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit erfolgt. Dies erfüllt nicht die verfassungsrechtlichen Anforderungen.

164 Das Gericht hat bereits für den verdeckten Einsatz der technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen im Rahmen einer Observationen einen **„gesteigerten Beobachtungsbedarf“**[157] verlangt. Aufgrund des Gewichts des Eingriffs ergibt sich, dass das Gericht damit eine sehr hohe Eingriffsschwelle für erforderlich hält. Das Eingriffsgewicht der Maßnahme nach § 20 VSG NRW ist vergleichbar, wenn nicht aufgrund der Streubreite und der Zweckentfremdung privater Einrichtungen noch höher.

165 Was das Gericht unter einem gesteigerten Beobachtungsbedarf versteht, hat es in den Entscheidungen zum Bayerischen und zum Hessischen Verfassungsschutzgesetz definiert:

> „Die Beobachtungsbedürftigkeit steigt, je deutlicher tatsächliche Anhaltspunkte es möglich erscheinen lassen, dass die Schutzgüter des Verfassungsschutzes **konkret bedroht sind und** dass das gegen sie gerichtete **Handeln erfolgreich sein kann**.“[158] (Hervorhebungen hinzugefügt)

Das Gericht geht für besonders schwere Eingriffe daher von zwei Voraussetzungen voraus: der Potentialität der Bestrebung und einer konkreten Bedrohung. Letztere kann sich z.B. in der Begehung von Straftaten niederschlagen, der Bestrebung oder Vorbereitung, Gewalt anzuwenden, oder in Volksverhetzung.[159] Daraus wird deutlich, dass allein die Potentialität einer Maßnahme nicht ausreicht. Dies gilt besonders im Bereich legalistischer

---

[156] Vgl. zum erhöhten Eingriffsgewicht durch die Kombination von Bildaufzeichnungen und Observation BVerfG NVwZ 2025, 495 Rn. 95 – PolG NRW – Observation.
[157] BVerfGE 162, 1 Rn. 359– Bayerisches Verfassungsschutzgesetz.
[158] BVerfGE 169, 130 Rn. 97, 149 – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 193 – Bayerisches Verfassungsschutzgesetz.
[159] BVerfGE 169, 130 Rn. 97 – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 194 – Bayerisches Verfassungsschutzgesetz.

Bestrebungen.[160] Das Gericht verweist vielmehr selbst auf das Kriterium des „Darauf Ausgehens“ im Sinne von Art. 21 Abs. 2 GG in Abgrenzung zu den geringeren Anforderungen des „Sich Richtens“ im Sinne einer „kämpferisch-aggressiven Grundhaltung“ im Sinne von Art. 9 Abs. 2 GG.[161] „Darauf Ausgehen“ versteht das Gericht als aktives Tun, das über die Potentialität hinausgeht und dieses Potential nutzt.

> „Ein Parteiverbot kommt vielmehr nur in Betracht, wenn eine Partei über hinreichende Wirkungsmöglichkeiten verfügt, die ein Erreichen der von ihr verfolgten verfassungsfeindlichen Ziele nicht völlig aussichtslos erscheinen lassen, und wenn sie von diesen Wirkungsmöglichkeiten auch **Gebrauch macht**. Ist dies nicht der Fall, fehlt es an einem „Darauf Ausgehen“ im Sinne von Art. 21 Abs. 2 GG.
>
> (…)
>
> Versucht eine Partei ihre verfassungswidrigen Ziele durch den Einsatz von Gewalt oder die Begehung von Straftaten durchzusetzen, ist die Anforderung des „Darauf Ausgehens“ regelmäßig erfüllt. (…) Gleiches gilt, wenn eine Partei unterhalb der Ebene strafrechtlich relevanten Verhaltens in einer die Freiheit des politischen Willensbildungsprozesses einschränkenden Weise **handelt**. Dies ist zum Beispiel der Fall, wenn eine Partei eine **„Atmosphäre der Angst“ oder der Bedrohung herbeiführt**, die geeignet ist, die freie und gleichberechtigte Beteiligung aller am Prozess der politischen Willensbildung nachhaltig zu beeinträchtigen. Ausreichend ist es dabei, wenn derartige Beeinträchtigungen in regional begrenzten Räumen **herbeigeführt werden**. Erforderlich ist allerdings, dass das Agieren der Partei objektiv geeignet ist, die Freiheit der politischen Willensbildung zu beschränken. Rein subjektive Bedrohungsempfindungen reichen insoweit nicht.“ [162] (Hervorhebungen hinzugefügt)

166 Legt man diesen Maßstab an die Beobachtungsstufen des VSG NRW an, ergibt sich, dass lediglich Bestrebungen, die gesteigert beobachtungsbedürftig nach § 5 Abs. 3 VSG NRW sind, uneingeschränkt diese Anforderungen erfüllen, nicht aber erheblich beobachtungsbedürftige nach § 5 Abs. 2 VSG NRW. Im Falle erheblich beobachtungsbedürftiger Bestrebungen fehlt es an der konkreten Gefährdung bzw. dem Handeln, das die Potentialität nutzt. Es reicht vielmehr die Eignung und damit die Potentialität aus, ein Verfassungsschutzgut erheblich zu beeinträchtigen (vgl. § 5 Abs. 2 S. 1 VSG NRW). Eine besondere Beobachtungsbedürftigkeit indiziert nach dem Gericht auch nicht die Begehung jeglicher Straftaten (so aber § 5 Abs. 2 S. 2 Nr. 2 VSG NRW), sondern nur besonders gewichtiger Straftaten, wie sie § 100b Abs. 2 StPO vorsieht.[163] Auch hinsichtlich der Potentialität verlangt das Gericht im Bereich legalistischen Handelns ein „hinreichendes Maß an

[160] Vgl. BVerfGE 162, 1 Rn. 360 – Bayerisches Verfassungsschutzgesetz.
[161] BVerfGE 169, 130 Rn. 97, 149 – Hessisches Verfassungsschutzgesetz; BVerfGE 162, 1 Rn. 193 – Bayerisches Verfassungsschutzgesetz.
[162] BVerfGE 142, 20 Rn. 586, 588 – NPD-Verbotsverfahren II.
[163] BVerfGE 162, 1 Rn. 197 – Bayerisches Verfassungsschutzgesetz.

konkreten und gewichtigen Anhaltspunkten“ für die Erfolgsaussichten der Bestrebung. Diese Anhaltspunkte verlangt § 5 Abs. 2 S. 2 Nr. 4 lit. a und b nicht. Die Regelung erfordert auch nicht, dass die Bestrebung ein Klima der Angst oder Bedrohung – zumindest lokal – herbeigeführt hat und nicht nur dazu in der Lage ist.[164]

(2) Weitere Anforderungen

167 Das Gericht verlangt zudem für die Rechtfertigung schwerwiegender Grundrechtseingriffe der Verfassungsschutzbehörden durch heimliche Überwachungsmaßnahmen:

> „(2) Die Überwachungsmaßnahme muss außerdem **im Einzelfall** zur Aufklärung der Bestrebung geboten sein (vgl. BVerfGE 130, 151 (206) = NJW 2012, 1419; BVerfGE 155, 119 (189) = NJW 2020, 2699 Rn. 151; BVerfGE 156, 11 (56) = NVwZ 2021, 226 Rn. 119). Für die Verhältnismäßigkeit der Überwachungsmaßnahme kommt es mithin auf die **konkrete Relevanz** der hierdurch zu gewinnenden Erkenntnisse für die weitere Aufklärung verfassungsfeindlicher Bestrebungen an. Eine Maßnahme, die ins Blaue hinein erfolgte, ohne dass benannt und anhand **tatsächlicher Anhaltspunkte** begründet werden könnte, dass und wie sie zur Aufklärung beitragen soll, wäre danach unzulässig. Ist die Maßnahme **gezielt** gegen bestimmte Personen gerichtet, muss insbesondere die **Überwachung gerade dieser Personen** zur Aufklärung beitragen.“[165] (Hervorhebungen hinzugefügt)

168 Diese Anforderungen erfüllt § 20 VSG NRW nicht. Auch die allgemeinen Anforderungen, an nachrichtendienstliche Mittel nach § 10 Abs. 1 Nr. 3 i.V.m. § 11 VSG NRW heilen diesen Mangel nicht. Zwar verlangt § 11 Abs. 1 VSG NRW tatsächliche Anhaltspunkte. Diese beziehen sich aber auf eine beobachtungsbedürftige Bestrebung nach § 3 Abs. 1 VSG NRW (§ 11 Abs. 1 Nr. 1 VSG NRW), nicht aber auf eine erheblich beobachtungsbedürftige Bestrebung nach § 5 Abs. 2 VSG NRW; deren Aufklärung dient aber § 20 VSG NRW. Eine Lösung dieses Problems durch Auslegung scheidet vorliegend aufgrund der hohen Bestimmtheitsanforderungen im Bereich heimlicher Überwachungsmaßnahmen aus. Auch das Gericht ist bisher kritisch, diese Anforderungen durch Auslegung zu ermitteln.[166] Das Erfordernis tatsächlicher Anhaltspunkte kann daher nicht in § 20 VSG NRW einfach vorausgesetzt werden.[167] Nicht hinreichend klar geregelt ist auch, ob die Maßnahme nach § 20 VSG auch für die Eigensicherung und zur

---

[164] BVerfGE 144, 20 Rn. 588 – NPD-Verbotsverfahren II; BVerfGE 162, 1 Rn. 197 – Bayerisches Verfassungsschutzgesetz.
[165] BVerfGE 162, 1 Rn. 206 – Bayerisches Verfassungsschutzgesetz; siehe auch BVerfGE 169, 130 Rn. 98 – Hessisches Verfassungsschutzgesetz.
[166] Vgl. BVerfGE 169, 130 Rn. 139 – Hessisches Verfassungsschutzgesetz.
[167] Vgl. zu einer ähnlichen Konstellation BVerfGE 169, 130 Rn. 139 – Hessisches Verfassungsschutzgesetz; BVerfGE 155, 119 Rn. 155 – Bestandsauskunft II.

Überprüfung der Nachrichtenehrlichkeit und Eignung von Vertrauenspersonen zulässig ist (§ 11 Abs. 1 S. 2 und 3 VSG NRW).

169 Eine wirksame Eingrenzung der Befugnis nach § 20 Abs. 1 S. 1 VSG NRW zur Mitbenutzung einer Videoüberwachungsanlage liegt nicht darin, dass diese Mitbenutzung nur „punktuell" erfolgen darf. Diese Anforderung ist nicht ausreichend bestimmt. Sie ist mehrdeutig und bisher nicht durch die Rechtsprechung ausreichend konkretisiert. Sie kann z.B. zeitlich („nur für einen kurzen Zeitraum"), aber auch räumlich („nur an bestimmten Punkten", d.h. nicht zahlreiche, sondern nur einzelne Videoüberwachungsanlagen) verstanden werden.

170 Eine wirksame Begrenzung ergibt sich auch nicht daraus, dass der Verfassungsschutz die angeforderten Aufnahmen und Ausleitungen nach „Datum, Ort und Zeit" eingrenzen muss (§ 20 Abs. 2 S. 3 VSG NRW). Dies ist keine zwingende Vorgabe, sondern sie steht unter dem Vorbehalt des Möglichen und spiegelt damit nur die Selbstverständlichkeit wider, dass personenbezogene Daten nur insoweit verarbeitet werden dürfen, wie dies erforderlich sind.

ee) Zu weiter Adressatenkreis

171 Nicht verhältnismäßig ist die Maßnahme auch, indem sie unmittelbar gegen Kontaktpersonen angewendet werden kann. Deren Definition wahrt generell schon nicht die verfassungsrechtlichen Grenzen (→ Rn. 104 ff.).

ff) Keine ausreichende Kompensation durch gerichtliche Vorabkontrolle

172 § 20 Abs. 3 S. 1 VSG NRW etabliert eine gerichtliche Vorabkontrolle und greift damit die Vorgaben des Gerichts für heimliche Überwachungsmaßnahmen von erheblichem Gewicht auf. Allerdings genügt die gerichtliche Vorabkontrolle in ihrer konkreten Ausgestaltung nicht den verfassungsrechtlichen Anforderungen.

173 Erstens bezieht sich die gerichtliche Vorabkontrolle nicht auf alle Maßnahmen nach § 20 Abs. 1 VSG NRW. So wird § 19 Abs. 2 Nr. 2 lit. a nicht in Bezug genommen und auch nicht § 19 Abs. 2 Nr. 1 VSG NRW, obwohl der Gesetzgeber gerade eine Situation in der Begründung beschreibt, in der ein Zugriff auf eine Videoüberwachungseinrichtung erfolgt, weil sich während einer Observation Mitarbeiterinnen und Mitarbeiter des Verfassungsschutzes der Zielperson nicht unbemerkt nähern können.[168] Kein Richtervorbehalt ist schließlich in den Situationen vorgesehen, in denen der Verfassungsschutz

[168] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 172.

Videoüberwachungsanlagen außerhalb von langfristigen Observationen nutzt. Dies erscheint etwa denkbar im Kontext einer Demonstration oder Veranstaltung einer beobachteten Bestrebung. Gerade hier kann eine Videoüberwachung eine erhebliche Breitenwirkung aufweisen und – durch Einsatz einer Gesichtserkennungssoftware – die Identifikation der Teilnehmer einer Versammlung ermöglichen.

174 Zweitens ist unklar, welchen Inhalt die Anordnung des Gerichts hat. Dies lässt sich aus § 13 VSG NRW nicht eindeutig ableiten. Ordnet das Gericht die Nutzung der Befugnis für einen bestimmten Zweck an? Bezieht sich die Anordnung auf bestimmte Videoüberwachungsanlagen? Bezieht sie sich nur auf bestimmte Situationen oder generell auf die Aufnahmen und Ausleitungen einer oder mehrerer Anlagen oder generell bestimmter Videoüberwachungsanlagen, soweit sie einem bestimmten Zweck dienen? § 13 Abs. 2 S. 1 VSG NRW verweist unspezifisch auf das FamFG; den allgemeinen Regelungen zum Inhalt von Beschlüssen (§ 38 Abs. 2 Nr. 3 FamFG) lassen sich auch keine näheren Einzelheiten entnehmen. Derartige Regelungen sind aber möglich – gerade in Bezug auf heimliche Überwachungsmaßnahmen (vgl. § 101a StPO).

gg) Zugriff in Echtzeit und Ermöglichung der Mitnutzung

175 Die Regelung ist auch unverhältnismäßig, weil sie nicht ausreichend die Belastungen berücksichtigt, die für die Betreiber von Videoüberwachungsanlagen aus der Duldungspflicht nach § 20 Abs. 1 VSG NRW bzw. der Verpflichtung zur Ausleitung nach § 20 Abs. 2 VSG NRW ergeben. Die Regelung würde es ihrem Wortlaut nach ermöglichen, von einem Autobesitzer die Herausgabe der Aufnahmen einer Dashcam zu verlangen, oder von einem Besitzer eines Smartphones die Übermittlung seiner Videos, auf denen im Hintergrund die Zielperson zu sehen ist. Engere Regelungen sind hier denkbar. So begrenzt § 28 Abs. 3 des Gesetzes zur Novellierung des Verfassungsschutzgesetzes Berlin – bei aller ansonsten berechtigter Kritik an der Regelung – die Inpflichtnahme auf Betreiber von Anlagen zur Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlich Schienen-, Schiffs- und Busverkehrs. Der Berliner Landesgesetzgeber lehnt sich hier an § 4 Abs. 1 S. 2 BDSG an.[169] Auch der Aufwand für die Betreiber wird weder berücksichtigt, noch ausgeglichen (vgl. § 20 Abs. 5, der nicht auf § 8 Abs. 7 S. 3 VSG NRW verweist, →Rn. 158 f.).

[169] Abgeordnetenhaus von Berlin, Drucksache 19/2466, S. 28.

176 Darüber hinaus wirft die Regelung neue Probleme der **Datensicherheit** auf. Sie trifft aber keine Regelungen, die diese Risiken adressieren, um die Datensicherheit zu gewährleisten.[170] Die Verpflichtung zu einem Echtzeitzugriff eröffnet neue Angriffsvektoren für Cyberangriffe und anderen Formen des unberechtigten Zugriffs, insbesondere wenn die Einrichtung bisher die Aufnahmen ohne Anbindung an das Internet lokal gespeichert hat. Es ist daher nicht ausgeschlossen, dass in der Praxis spontane Lösungen gesucht werden, welche die IT-sicherheitsrechtlichen Anforderungen nicht erfüllen. Auch steht der Betreiber vor dem Problem, dass er einerseits die Datensicherheit der Ausnahmen sicherstellen muss (vgl. § 32 DSGVO), andererseits aber den Zugang in Echtzeit auf Distanz. Der Gesetzgeber lässt die Betreiber daher mit einem Normkonflikt zurück, ohne seiner verfassungsrechtlichen Gewährleistungsverantwortung nachzukommen. Diese umfasst auch die Pflicht, die auf seine Veranlassung hin verarbeiteten Daten, nicht einem größeren Risiko auszusetzen als erforderlich.

hh) Speicherdauer

177 § 20 VSG NRW ist auch unverhältnismäßig, weil die erhobenen Daten über Dritte sehr lange gespeichert werden. § 6 Abs. 7 VSG NRW führt Maßnahmen ein, um die Verarbeitung von Daten über Dritte zu vermeiden. Diese Regelung ist auch im Rahmen des § 20 VSG NRW zu berücksichtigen. § 6 Abs. 7 S. 2 VSG NRW sieht jedoch eine Ausnahme von den Anforderungen des § 6 Abs. 7 S. 1 VSG NRW vor, wenn die personenbezogenen Daten über Dritte untrennbar mit den Informationen, auf die der Verfassungsschutz zielt, verbunden sind. Dies dürfte nahezu immer bei Videoaufnahmen der Fall sein, weil diese nicht nur die Zielpersonen erfassen, sondern zugleich auch unbeteiligte Dritte, die sich wie die Zielpersonen im öffentlichen Raum bewegen. Ebenso dürften unbeteiligte Dritte aus diesem Grund i.S.v. § 11 Abs. 2 S. 3 VSG NRW unvermeidbar betroffen sein.[171] Dem steht nicht § 20 Abs. 4 VSG NRW entgegen, denn die Regelung betrifft nur die Primärdaten, die der Betreiber zur Verfügung stellen musste, nicht die weitere Verarbeitung.

ii) Intransparenz mangels Benachrichtigung und Auskunftsanspruch

178 Zur Unverhältnismäßigkeit der Regelung trägt zudem bei, dass sie aus Sicht betroffener Dritter intransparent bleiben wird und sich damit einer gerichtlichen Kontrolle weitgehend entzieht. Typischerweise wird der Verfassungsschutz davon ausgehen, dass eine dritte Person kein Interesse an

[170] Vgl. zu dieser Anforderung BVerfGE 155, 119 Rn. 135, 188 – Bestandsdatenauskunft II.
[171] Zum unklaren Verhältnis von § 6 Abs. 7 und § 11 Abs. 2 S. 3 VSG NRW siehe *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 10.

einer Mitteilung hat und sie daher nicht benachrichtigen (§ 12 Abs. 2 S. 1 Nr. 1 VSG NRW). Zumeist werden die Daten auch nicht zur Person des Dritten gespeichert, so dass ein Auskunftsersuchen ebenfalls ins Leere geht (vgl. § 30 Abs. 1 VSG NRW). Er würde zudem nicht die Herkunft der Daten umfassen (§ 30 Abs. 3 VSG NRW) und damit kaum eine Kontrolle der Erhebung ermöglichen.

IV. Regelungen zur automatisierten Datenanalyse (§ 26, § 33 Abs. 3, § 36 und § 6 Abs. 4 S. 1 und 2 VSG NRW)

179 Die verschiedenen Regelungen zur automatisierten Datenanalyse sind mit dem Grundgesetz unvereinbar, weil sie gegen das allgemeine Persönlichkeitsrecht in seiner Ausprägung des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Dies betrifft sowohl die Regelungen zur umfassendsten Form der Datenanalyse nach § 26 Abs. 3 und 4 VSG NRW (1.), die der Gewinnung neuer Erkenntnisse dient, als auch für die mildere Form der Datenanalyse nach § 26 Abs. 2 VSG NRW zur Filterung, Sortierung und Priorisierung (2.). Verfassungswidrig sind aber auch auf die Regelungen zur Datenverarbeitung zum Zwecke des Trainings durch den Verfassungsschutz selbst (§ 26 Abs. 6 und 7 VSG NRW) oder Dritte (§ 36 VSG NRW) (3.) sowie die Übermittlungsregelung des § 33 Abs. 3 VSG NRW (4.). Ähnliche Bedenken wie gegen § 26 Abs. 2 VSG NRW begründen auch die Verfassungswidrigkeit der automatisierten Datenerhebung nach § 6 Abs. 4 S. 1 1. Alt. i.V.m. S. 2 VSG NRW (5.).

1. § 26 Abs. 3 VSG NRW

180 § 26 Abs. 3 und 4 VSG NRW greifen unverhältnismäßig in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Die Weiterverarbeitung von Daten, die für andere Zwecke gewonnen worden sind, ihre Zusammenführung und der Erlangung neuen grundrechtsrelevanten Wissens durch eine automatisierte Datenanalyse und Auswertung greifen in das Recht auf informationelle Selbstbestimmung aller Personen ein, deren Daten durch Verfassungsschutz auf diese Weise verarbeitet werden.[172] Der Eingriff ist nicht gerechtfertigt, weil er weder den Geboten der Bestimmtheit und Normenklarheit (a.), noch dem Gebot der Verhältnismäßigkeit im engeren Sinne genügt. Die Anforderungen aus diesem Gebot hängen nach der Rechtsprechung des Gerichts vor allem vom Eingriffsgewicht ab.[173] Nach den Kriterien, die das Gericht für die

[172] Vgl. BVerfGE 165, 363 Rn. 50 – automatisierte Datenanalyse; BVerfGE 156, 11 Rn. 73 f. – Antiterrordateigesetz II.
[173] Statt vieler BVerfGE 165, 363 Rn. 54 – automatisierte Datenanalyse; BVerfGE 155, 119 Rn. 128 – Bestandsdatenauskunft II.

automatisierte Datenanalyse entwickelt hat, handelt es sich um einen außergewöhnlich schweren Eingriff (b.). Die Eingriffsvoraussetzungen hierfür und die vorgesehenen kompensatorischen Maßnahmen reichen nicht aus, um einen so schwerwiegenden Eingriff zu rechtfertigen (c.).

a) Verstoß gegen die Gebote der Bestimmtheit und Normenklarheit

181 Der Gesetzgeber erlaubt ausdrücklich den Einsatz von maschinellem Lernen und Künstlicher Intelligenz. Diese versteht er als Formen mathematisch-statistischer Verfahren (§ 26 Abs. 3 S. 2 VSG NRW). Zugleich untersagt er den Einsatz „selbst weiter lernender Systeme“ (§ 26 Abs. 3 S. 3 VSG NRW. Diese Regelung ist widersprüchlich[174] und daher **zu unbestimmt**.

182 Ein solcher Widerspruch kann in einem so grundrechtsensiblen Normbereich mit entsprechend hohen Anforderungen an die Bestimmtheit nur zur Verfassungswidrigkeit der Regelung führen. Anderenfalls könnte die Verwaltung die grundrechtswesentlichen Weichen stellen (hier: Einsatz von KI – ja oder nein), da sie in der Praxis aufgrund des fehlenden Wechselspiels zwischen Verwaltung und gerichtlicher Kontrolle die Regelung weitgehend autonom und unkontrolliert auslegen kann.[175] Auch in einem technisch dynamischen Bereich wie Künstlicher Intelligenz muss der Gesetzgeber die grundlegenden Entscheidungen der Verarbeitungsmethode selbst normenklar und transparent treffen.[176]

183 Die Widersprüchlichkeit der Regelung besteht darauf, dass maschinelles Lernen und Künstliche Intelligenz – nach der Auffassung des Gerichts – sich gerade dadurch von deterministischen Algorithmen unterscheiden, dass sie sich weiterentwickeln.[177]

> „Deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster **automatisiert weiterentwickelt** oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines „predictive policing“ getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe **algorithmische Systeme könnten sich im Verlauf des maschinellen**

[174] Unklarheiten sieht auch *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 9 zu § 6 Abs. 4 VSG NRW.
[175] BVerfGE 165, 363 Rn. 113 – automatisierte Datenanalyse.
[176] BVerfGE 165, 363 Rn. 112, 114 – automatisierte Datenanalyse.
[177] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse; kritisch dazu *Kostov,* Der Staat 64 (2025) 537 (572 ff.); nach Art. 3 Nr. 1 KI-VO *kann* eine Anpassungsfähigkeit zum KI-System gehören, muss es aber nicht, dazu *Wendehorst/Nessler/Aufreiter/Aichinger*, MMR 2024, 605 (608).

> **Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen**, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein (vgl. EuGH, Urteil vom 21. Juni 2021, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, Rn. 195). Dann droht zugleich die staatliche Kontrolle über diese Anwendung verloren zu gehen."[178] (Hervorhebungen hinzugefügt)

Der Gesetzgeber wollte auf der einen Seite genau dies zwar verhindern[179] und unterscheidet daher zwischen dem Einsatz der Datenanalyse (§ 26 Abs. 3 VSG NRW) und dem Training (§ 26 Abs. 6 VSG NRW). Zugleich bleibt aber die Unterscheidung zwischen „maschinellem Lernen" nach § 26 Abs. 3 S. 2 und „weiterlernenden Systemen" nach § 26 Abs. 3 S. 3 VSG NRW unklar und damit zu unbestimmt.

184 Auf der anderen Seite zielt der Gesetzgeber gerade nach § 26 Abs. 4 VSG NRW auf Erkenntnisse, die nur durch „Data Mining" erreicht werden können. Dies hat das Gericht für die teilweise wortgleiche, aber weniger ambitionierte Regelung in § 49 Abs. 2 HmbPolDVG a.F. ausdrücklich festgestellt.[180]

b) Grundrechtseingriff von hohem Gewicht

185 Bei der Datenanalyse nach § 26 Abs. 3 S. 1 VSG NRW handelt es sich um einen Eingriff von erheblichem Gewicht. Sie erfüllt nahezu alle Kriterien, die das Gericht bisher entwickelt hat, um einen Eingriff von erheblichem Gewicht zu begründen.

aa) Ziel der Datenanalyse

186 Bereits aus der Zielrichtung der Datenanalyse nach § 26 Abs. 3 VSG NRW ergibt sich ein hohes Gewicht des Eingriffs. Die Verarbeitung von Daten im Rahmen einer Datenanalyse hat ein erhöhtes Eingriffsgewicht im Vergleich zur Erhebung der Daten, wenn sie darauf ausgerichtet ist, **neues Wissen zu generieren**,[181] das bei einer manuellen Auswertung nicht oder nur mit geringerer Wahrscheinlichkeit hätte erlangt werden können.[182] Genau dies ist vom Gesetzgeber durch eine Datenanalyse nach § 26 Abs. 3 VSG NRW beabsichtigt, wie sich aus § 26 Abs. 4 VSG NRW ergibt.[183] Dies kann, wie das Gericht feststellte,

---

[178] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse.
[179] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 192.
[180] BVerfGE 165, 363 Rn. 148 – automatisierte Datenanalyse.
[181] BVerfGE 165, 363 Rn. 67 – automatisierte Datenanalyse; BVerfGE 156, 11 Rn. 73, 109, 112 – Antiterrordateigesetz II; BVerfGE 115, 320 (350 f.) – Rasterfahndung.
[182] BVerfGE 165, 363 Rn. 68, 70 – automatisierte Datenanalyse.
[183] Vgl. BVerfGE 165, 363 Rn. 67 – automatisierte Datenanalyse zu den sehr ähnlichen Formulierungen in § 25a HSOG und § 49 Abs. 2 HmbPolDVG, die Gegenstand der Entscheidung waren.

„ein **Gefühl unkontrollierten Beobachtetwerdens** hervorgerufen und nachhaltige **Einschüchterungseffekte** auf die Freiheitswahrnehmung entfalten.“[184] (Hervorhebungen hinzugefügt)

Dies gilt erst recht, weil bei einer derartigen Analyse auch scheinbar „belanglose“ Daten auf einmal eine ungeahnte Bedeutung erhalten können und sich damit ein typisches Risiko manifestiert, vor dem das Recht auf informationelle Selbstbestimmung schützen soll.[185] Noch einmal stärker kommt dieser Effekt beim Einsatz von KI und maschinellem Lernen zum Tragen, weil die Gewichtung von Kriterien hier letztlich nicht mehr allein in menschlicher Hand liegt. Dies wird auch deutlich an der Definition von KI-Systemen nach Art. 3 Nr. 1 KI-VO; danach sind KI-Systeme gerade für den „autonomen Betrieb“ ausgelegt.

187 Durch die Kombination von großen Datenmengen über eine Person können dabei – auch durch statistische Korrelationen – nicht nur neue Erkenntnisse über diese Person gewonnen werden, sondern es kann eine Art „**Profiling**“ stattfinden. Diese Möglichkeit erhöht das Eingriffsgewicht noch einmal.[186] § 26 VSG NRW enthält keine Regelungen, welche die Breite und Tiefe der Erkenntnisse aus der Datenanalyse einschränken. § 26 Abs. 4 VSG NRW ist nur eine beispielhafte Aufzählung („insbesondere“). Die neuen Erkenntnisse (etwa Zusammenhänge zwischen einer Person und anderen Personen, Personengruppierungen, Organisationen oder Sachen) sind – zumindest in großen Teilen – personenbezogene Daten; dies entspricht der Tätigkeit des Verfassungsschutzes, der sich auf Organisationen und Personen konzentriert, während etwa die Identifikation von gefährlichen Orten oder Kriminalitätsschwerpunkten keine Bedeutung hat. Auch dieser Faktor erhöht das Gewicht der Datenanalyse.[187] Eine Einordnung einer Person als wahrscheinlich aktives Mitglied einer erheblich beobachtungsbedürftigen Bestrebung ist als Ergebnis einer solchen Analyse nicht ausgeschlossen und wäre **mit einer Gefährlichkeitsanalyse im Rahmen von „predictive policing“** vergleichbar.[188] Derartige personenbezogene Einschätzungen schließt das Gesetz nicht aus, obwohl dies nach der Rechtsprechung des Gerichts verfassungsrechtlich geboten wäre, wenn der Gesetzgeber das von einer Analyse mittels KI ausgehende Eingriffsgewicht mindern möchte.[189]

188 Die neuen Erkenntnisse können nach einer Freigabe durch einen Mitarbeiter oder eine Mitarbeiterin des Verfassungsschutzes (§ 26 Abs. 8 S. 2 VSG NRW)

---

[184] BVerfGE 156, 11 Rn. 112 – Antiterrordateigesetz II.
[185] Vgl. BVerfGE 65, 1 (45) – Volkszählung.
[186] BVerfGE 165, 363 Rn. 69 – automatisierte Datenanalyse.
[187] BVerfGE 165, 363 Rn. 96 ff., 121 – automatisierte Datenanalyse.
[188] Vgl. BVerfGE 165, 363 Rn. 96 ff., 121 – automatisierte Datenanalyse zum besonderen Eingriffsgewicht.
[189] Zu diesem Erfordernis BVerfGE 165, 363 Rn. 121 – automatisierte Datenanalyse.

unmittelbar verwendet werden, um **nachrichtendienstliche Mittel gegen eine Person einzusetzen**.[190] Auch eine **Übermittlung an andere Behörden** ist möglich und kann in Maßnahmen münden (vgl. § 33 Abs. 3 VSG NRW), welche – auch wenn es sich um keine operativen Anschlussbefugnisse im Sinne der Rechtsprechung des Gerichts handelt – die Grundrechte der betroffenen Personen intensiv beeinträchtigen können (z.B. im Bereich des Waffenrechts, Beamten- oder Dienstrechts oder zuletzt im Rahmen des „*Haber*-Verfahrens" beim Deutschen Buchhandelspreis). Eine eingriffsmindernde Verwendungsbeschränkung[191] sieht das VSG NRW trotz des erhöhten Eingriffsgewichts durch eine automatisierte Datenanalyse nicht vor.

bb) Mangelnde Nachvollziehbarkeit der Analyseergebnisse

189 § 26 Abs. 3 S. 2 VSG NRW erlaubt den Einsatz von „mathematisch-statistischen Verfahren, wie maschinelles Lernen und künstliche Intelligenz". Der Gesetzgeber hat eine Reihe von Regelungen zum Training getroffen (→ Rn. 243 ff.), aber keine Rahmenbedingungen, die eine Nachvollziehbarkeit der Ergebnisse gewährleisten. Dies ist aber verfassungsrechtlich geboten – nicht nur für selbstlernende Systeme, sondern auch deterministische Modelle.[192] In beiden Fällen droht ein **Blackbox-Effekt**.[193] Gerade in einem so grundrechtssensiblen Bereich mit einer Vielzahl von tiefgreifenden Anschlussbefugnissen nach dem VSG NRW, die auf einer solchen Analyse fußen können, führt dies zu einer Vertiefung des Grundrechtseingriffs. Der Gesetzgeber muss daher schützende Regelungen treffen.[194]

190 Zwar schließt § 26 Abs. 8 VSG NRW automatisierte Entscheidungen aus und legt die Letztbewertung und Veraktung in die Hände eines Menschen. Der Gesetzgeber erkennt selbst aber das Problem des „**automation bias**", wonach Menschen großes Vertrauen in die Vorschläge und Entscheidungen von Maschinen entwickeln.[195] Allein die Zwischenschaltung eines Menschen

---

[190] Zu diesem eingriffsvertiefenden Faktor BVerfGE 156, 11 Rn. 11 f. – Antiterrordateigesetz II.
[191] BVerfGE 165, 363 Rn. 99 – automatisierte Datenanalyse m.w.N.
[192] BVerfGE 165, 363 Rn. 90, 100 f. – automatisierte Datenanalyse; zum Erfordernis der Nachvollziehbarkeit BVerfGE 154, 152 Rn. 192 – nachrichtendienstliche Ausland-Ausland-Überwachung.
[193] *Ibold*, GSZ 2024, 10 (14 f.), die zwischen dem Blackbox-Effekt im engeren Sinne unterscheidet, der technisch bedingt ist, und dem Blackbox-Effekt im weiteren Sinne, der durch rechtliche Rahmenbedingungen wie Geschäftsgeheimnisschutz oder vertragliche Regelungen entsteht.
[194] BVerfGE 165, 363 Rn. 101 – automatisierte Datenanalyse
[195] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 192; *Ibold*, GSZ 2024, 10 (15); *Deutscher Ethikrat*, Mensch und Maschine – Herausforderungen druch künstliche Intelligenz (2023), S. 328 f.; zur Gefahr des „Abnickens" bereits *Golla,* NJW 2021, 667 (672).

reduziert daher nicht zwingend das Risiko, das von einer Verwendung von maschinellem Lernen oder KI ausgeht. Voraussetzung hierfür ist, dass er die Ergebnisse nachvollziehen und überprüfen kann (Stichwort: „explainable AI“).[196] Dies ist aber nur vom Gesetzgeber vorgesehen, „soweit dies technisch möglich ist“ (§ 26 Abs. 5 S. 2 VSG NRW). Dies kehrt aber das Verhältnis von Recht und Technik um: Die Technik (und deren Auswahl) muss den rechtlichen Vorgaben folgen – nicht umgekehrt. Wie die Nachvollziehbarkeit und Vermeidung des „automation bias“ im Rahmen des § 26 Abs. 8 VSG NRW und auch bei der späteren Verarbeitung der Analyseergebnisse gewährleistet werden soll (z.B. durch Prüfung, Begründungspflicht, Dokumentation, Protokollierung), ist ebenfalls nicht geregelt. Vorgesehen ist eine Prüfung der Nachvollziehbarkeit nur für die Nutzung als Trainingsdaten (§ 26 Abs. 1 S. 4 VSG NRW), nicht aber in § 26 Abs. 8 VSG NRW oder im Rahmen der weiteren Verarbeitung für andere Zwecke als zum Training.

191 Die Schwierigkeit der Nachvollziehbarkeit besteht bereits bei festgelegten, sog. deterministischen Algorithmen. Sie stellt sich aber, wie das Gericht hervorgehoben, in noch stärkerem Maße bei der „Verwendung lernfähiger Systeme, als Künstlicher Intelligenz (KI)“.

> „Deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster **automatisiert weiterentwickelt** oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines „predictive policing“ getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe **algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen**, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein (vgl. EuGH, Urteil vom 21. Juni 2021, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, Rn. 195). Dann droht zugleich die staatliche Kontrolle über diese Anwendung verloren zu gehen.“[197] (Hervorhebungen hinzugefügt)

Auch der EuGH hat im Kontext der Befugnisse staatlicher Sicherheitsbehörden (konkret der Auswertung von Fluggastdaten) davor gewarnt, dass die Ergebnisse durch den Einsatz Künstlicher Intelligenz kaum nachvollziehbar seien und dies auch die durch Art. 47 Grundrechte-Charta garantierte gerichtliche Überprüfung erschwere.[198] Auch das Gericht hat – im

---

[196] Vgl. etwa *Hacker/Cordes/Berz,* GRUR 2024, 1777 (1777, 1781) m.w.N.
[197] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse.
[198] EuGH, Urteil vom 21.06.2021, C-817/19, ECLI:EU:C:2022:491, Rn. 195 – Ligue des droits humains.

nachrichtendienstlichen Kontext – die Bedeutung der Nachvollziehbarkeit im Hinblick auf eine unabhängige Kontrolle betont, und zwar bereits im Kontext komplexer Algorithmen, ohne Einsatz von KI und maschinellem Lernen.[199]

cc) Einsatz von Künstlicher Intelligenz

192 Der Einsatz von KI vertieft den Eingriff nach der Rechtsprechung des Gerichts zusätzlich.[200] Denn mit dem Einsatz von KI geht ein Verlust an Kontrolle über den Vorgang der Datenverarbeitung und Analyse einher, der sich – wie gezeigt – bereits anhand des Problems offenbart, wie die Analyseergebnisse nachvollzogen werden können. Der Gesetzgeber hat hier den Einsatz von KI und maschinellem Lernen ausdrücklich zugelassen (§ 26 Abs. 3 S. 2 VSG NRW). Damit hat der den Einsatz von selbstlernenden Systemen gerade nicht oder zumindest nicht eindeutig (→Rn. 181 ff.) ausgeschlossen.[201]

dd) Keine Gewährleistung der Zuverlässigkeit und Qualität der verwendeten Software und ihres Anbieters

193 Erschwerend wirkt es sich zudem aus, dass der Gesetzgeber keine Regelungen vorgesehen hat, wie die Zuverlässigkeit und Qualität der verwendeten Software und ihres Anbieters sichergestellt werden können. Das Gericht hat auf die besondere Sensibilität hingewiesen, wenn Software verwendet wird, die keine Eigenprogrammierung ist:

> „Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte.“[202]

194 Die verwendete Software weist eine hohe Komplexität auf. Zugleich sind die verarbeiteten Daten von hoher Sensibilität – aufgrund ihrer Geheimhaltungsbedürftigkeit, aber auch ihrer grundrechtsintensiven Erhebung. Es muss daher sichergestellt sein, dass kein Dritter auf diese Daten Zugriff nehmen kann – auch nicht ein Vertragspartner, der dem Verfassungsschutz bereitstellt. Derartige Anforderungen sind Ausdruck einer **Folgenverantwortung des Staats**, wenn er sich entschließt, Bürgerinnen und Bürger zu überwachen, Daten über sie in großem Umfang zu speichern und mit einer naturbedingt intransparenten Software zu analysieren. Der Auswahl des Vertragspartners und der Kontrolle des Quellcodes der Software kommen daher größte Bedeutung zu. Dies gilt umso mehr, als nach einer Auswahl

---

[199] BVerfGE 154, 152 Rn. 192 – nachrichtendienstliche Ausland-Ausland-Überwachung.
[200] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse.
[201] Vgl. zu diesem Erfordernis BVerfGE 165, 363 Rn. 121 – automatisierte Datenanalyse.
[202] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse.

aufgrund der Investitionen und des Anpassungsaufwandes ein Wechsel schwierig ist. Zusätzlich ist zu berücksichtigen, dass Software regelmäßig Updates benötigt und KI-Analysen ein Training mit neuen Daten. Der Gesetzgeber ermöglicht hierzu sogar, dem Vertragspartner die Datenbestände des Verfassungsschutzes zur Verfügung zu stellen (§ 36 Abs. 1 VSG NRW).

195 Die Bedeutung dieses Aspekts ist nicht zu unterschätzen. Dem Gericht ist die Diskussion um das Softwareunternehmen ***Palantir*** bekannt. Diesem wird aufgrund seiner Nähe zur US-amerikanischen Regierung und den Äußerungen seiner Anteilseigner und Geschäftsführer großes Misstrauen entgegengebracht. Es wird die Frage aufgeworfen, ob sich deutsche Behörden in seinem so sicherheitssensiblen Bereich von ausländischen Anbietern abhängig machen oder vorranging Eigenentwicklungen einsetzen sollten.[203] Letztlich handelt es sich damit um eine Frage der **digitalen Souveränität**. Ferner wird der Abfluss von grundrechtlich sensiblen Daten befürchtet.[204] So können US-Unternehmen nach Sec. 702 Foreign Intelligence Surveillance Act zur Herausgabe der Daten verpflichtet sind oder einem Herausgabeverlangen nach dem sog. Cloud Act ausgesetzt sein.[205]

196 Das vorliegende Gesetz sieht nur gemäß § 26 Abs. 5 S. 1 VSG NRW vor, dass die IT-Produkte regelmäßig auf dem Stand der Technik zu halten sind. Regelungen zur Auswahl der Software und der Vertragspartner stellt das Gesetz nicht auf. Es sind auch keine Vorgaben enthalten, ob die Software auf den Servern des Verfassungsschutzes installiert sein muss oder eine Cloud-Lösung zulässig wäre und, wenn sie zulässig wäre, wo die Daten gespeichert werden dürften (in Deutschland? In der EU oder dem EWR? In einem Drittland?). Es sind keine Sicherungen vorgesehen, die einen Abfluss von Daten ausschließen, z.B. durch Kontrolle des Quellcodes, oder die Qualität der Software, z.B. durch Tests[206], gewährleisten.

ee) Keine ausreichende Gewährleistung der Qualität der Trainingsdaten und Maßnahmen gegen Diskriminierungen

197 Von zusätzlichen Eingriffsgewicht ist, dass der Gesetzgeber die statistische Auswertung der ihm vorliegenden Datenmengen erlaubt, ohne die Qualität der Trainingsdaten sicherzustellen und das Risiko von Diskriminierungen zu

---

[203] Hierfür *Kelber/Bortnikov*, NJW 2023, 2000 (2002); *S. D. Meyer*, GSZ 2025, 156 (160 f.); *Bäuerle*, ZD 2025, 128 (131).
[204] 31. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, S. 40 (zum parallelen Regelung im PolG NRW).
[205] Ausführlich *Anheier/Nau,* ZD 2025, 557 (auf Basis eines Gutachtens für das Bundesministeriums des Innern und für Heimat); *Schantz*, CR 2026, 91 Rn. 33 jeweils m.w.N.
[206] *S. D. Meyer*, GSZ 2025, 156 (161); zu diesem Erfordernis siehe auch Art. 16 Abs. 2 lit.g der KI-Konvention des Europarates.

verhindern. Dies ist jedoch bei der Anwendung statistischer Verfahren nach der Rechtsprechung des Gerichts und auch des EuGH erforderlich[207] und ist auch in vom Unionsgesetzgeber in EG 73 DSGVO und z.B. in Art. 10 Abs. 2 lit. f und g, Abs. 3 und 4 KI-VO adressiert worden. Das Gericht hat hierzu ausgeführt:

> „Eine spezifische Herausforderung besteht darüber hinaus darin, die Herausbildung und Verwendung diskriminierender Algorithmen zu verhindern. Daher dürften selbstlernende Systeme in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern."[208]

198 Als Trainingsdaten sollen neben den Datenbeständen des Verfassungsschutzes allgemein zugängliche Quellen genutzt werden. Kurzum: **Die KI kann mit dem Internet trainiert werden.**[209] Damit stellen sich Probleme der Datenrichtigkeit und Diskriminierung deutlich. Eine Quelle von Diskriminierungen sind Vorurteile, die sich aus den Trainingsdaten ergeben („bias in, bias out").[210] Diese Daten sollen daher so ausgewählt werden, dass „statistische Verzerrungen und diskriminierende Verarbeitungsprozesse möglichst vermieden" werden (§ 26 Abs. 6 S. 3 VSG NRW). Mit anderen Worten: Der Gesetzgeber erkennt das Problem, entscheidet sich aber sehenden Auges dafür, im Zweifel auf eine Lösung zu verzichten. Lässt sich eine diskriminierende Verarbeitung nicht ausschließen oder stehen nur mangelhafte Datenbestände zur Verfügung, soll der Verfassungsschutz diese trotzdem nutzen dürfen.

199 Es sind auch keine Verfahren vorgesehen, wie die Qualität der Datenquellen gewährleistet und die Gefahr von Diskriminierungen verhindert werden könnte. Das Gericht hat generell bei „komplexen Formen des automatisierten Abgleichs von Daten (…) Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit" verlangt, „was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann."[211] Dies erscheint auch notwendig, weil neben den Trainingsdaten auch der Algorithmus selbst Vorurteile beinhalten kann.[212] Regelungen, die diese Probleme adressieren, fehlen hier.

---

[207] BVerfGE 165, 363 Rn. 95, 77 – automatisierte Datenanalyse; zum Risiko von Diskriminierungen auch EuGH, Urteil vom 21.06.2021, C-817/19, ECLI:EU:C:2022:491, Rn. 195 – Ligue des droits humains.
[208] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse.
[209] So explizit die Gesetzesbegründung, siehe Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 193.
[210] *Ibold*, GSZ 2024, 10 (13).
[211] BVerfGE 165, 363 Rn. 109 – automatisierte Datenanalyse.
[212] Dazu *Lauscher/Legner*, ZfDR 2022, 368 (372 f.).

200 Diese Lücke füllt auch nicht § 54 Abs. 2 und 3 BDSG, der nach § 60 Abs.2 VSG NRW anwendbar ist. Nach § 54 Abs. 2 BDSG darf eine Entscheidung, die ausschließlich auf einer automatisierten Datenverarbeitung beruht und zu einer nachteiligen Entscheidung für die betroffene Person führt, nicht auf besonderen Kategorien von Daten (§ 46 Nr. 14 BDSG) beruhen, wenn keine Schutzmaßnahmen durch ein Gesetz vorgesehen sind. § 54 Abs. 3 BDSG verbietet ein Profiling auf der Grundlage dieser besonderen Kategorien von Daten. Eine personenbezogene Gefährlichkeitsprognose wäre als Profiling einzuordnen. Trotz der Entscheidung durch einen Menschen nach § 26 Abs. 8 VSG NRW ist es auch nicht ausgeschlossen, dass eine Entscheidung nach § 54 Abs. 1 und 2 BDSG vorliegt, die auf einer automatisierten Verarbeitung beruht; es ist durchaus möglich, dass aufgrund des automation bias die Datenanalyse nach § 26 Abs. 3 VSG NRW maßgeblich für die Entscheidung ist.[213] Durch ihre datenschutzrechtliche Anknüpfung an besondere Kategorien von Daten adressiert die Regelung die Diskriminierungsrisiken bestenfalls ausschnitthaft, denn Risiken einer Diskriminierung aufgrund anderer Kriterien bleiben außen vor.

ff) Unbeschränkte Datenmenge

201 Eingriffserhöhend wirkt sich zudem aus, dass die Datenmenge nicht eingeschränkt ist, sondern sich auf **sämtliche beim Verfassungsschutz vorhandenen Daten** bezieht. Denn die Eingriffsintensität ist umso höher, je größer und zahlreicher die verwendeten Datenbestände sind.[214] Damit werden alle Daten erfasst, welche der Verfassungsschutz nach § 24 VSG NRW verarbeitet (sowie zusätzlich weitere Daten nach § 26 Abs. 7 VSG NRW, die bereits gelöscht sein müssten, → Rn. 252 ff.). Es findet ein Einbeziehen von Datenbeständen ohne Relevanz zum Anlass und ohne Erforderlichkeit für das Erkenntnisziel statt.[215] § 26 Abs. 3 VSG NRW differenziert dabei nicht zwischen Daten über Personen, die einer erheblich beobachtungsbedürftigen Bestrebung angehören, Kontaktpersonen und unbeteiligten Dritten. Im Rahmen der Datenanalyse werden daher auch Daten über Personen verarbeitet, die durch ihr Handeln keine Verantwortung dafür tragen, dass Daten über sie vom Verfassungsschutz verarbeitet werden. Damit steigt aber für diese Unbeteiligten das Risiko, aufgrund von fehlerhaften Einschätzungen zum Adressat staatlicher Maßnahmen zu werden.[216] Zu denken ist hier an Personen, die sich in einer Funkzelle aufgehalten haben oder auf Videoaufzeichnungen zu erkennen sind (vgl. zu deren Weiterverarbeitung

---

[213] Vgl. EuGH v. 7.12.2023, C-324/21, ECLI:EU:C:2023:957, Rn. 50 – OQ ./. Hessen zur ähnlichen Auslegungsfrage im Rahmen von Art. 22 Abs. 1 DSGVO.
[214] Vgl. BVerfGE 165, 363 Rn. 78, 116 – automatisierte Datenanalyse.
[215] Vgl. BVerfGE 165, 363 Rn. 162 – automatisierte Datenanalyse.
[216] BVerfGE 165, 363 Rn. 77, 126 – automatisierte Datenanalyse.

§ 24 Abs. 3 S. 1, § 6 Abs. 7 S. 2 VSG NRW). § 26 Abs. 3 S. 1 a.E. VSG NRW sieht nur eine Einschränkung vor, wenn der Erhebungszweck der betroffenen Daten nicht außer Verhältnis steht; es kommt also nicht auf das Mittel der Erhebung und die betroffene Person an.

202 Es handelt sich dabei also um eine sehr große Datenmenge, die mit konventionellen Mitteln nicht mehr bewältigt werden könnte.[217] § 26 Abs. 4 VSG NRW verdeutlicht dies durch die Formulierung, dass die Analyse **„datei- und informationssystemübergreifend“** erfolgt. Die Beschränkung auf die „bei ihr vorhandenen Daten“ schließt zwar einen direkten Zugriff auf Datenbanken anderer Behörden, z.B. der Polizei aus (so auch ausdrücklich § 26 Abs. 3 S. 6 VSG NRW), erlaubt aber nach der Gesetzesbegründung die Auswertung übermittelter Informationen.[218] Diese können von der Polizei aber auch von anderen in- und ausländischen Nachrichtendiensten stammen oder von einer anderen staatlichen Behörden in einem anderen Kontext gewonnen worden sein.[219] Eine Eingrenzung, die hier eingriffsmindernd wirken könnte,[220] hat der Gesetzgeber nicht vorgesehen, auch keine Beschränkung der Datenarten oder -formate[221] oder eine Vorgabe zur händischen Auswahl des Datenbestandes.[222]

203 Auch die Einfügung im Gesetzgebungsverfahren, dass eine **Verknüpfung des Internets** mit dem Analysesystem ausgeschlossen ist (§ 26 Abs. 3 S. 4 VSG NRW), mindert das Eingriffsgewicht in dieser Hinsicht kaum. Zwar scheidet ein Abgleich mit dem Internet in Echtzeit aus. Die Regelung ist aber im Zusammenhang mit § 6 Abs. 4 S. 1 1. Alt. i.V.m. S. 2 VSG NRW zu sehen. Danach sind das Durchsuchen, Filtern, Sortieren und eine Priorisierung des Inhaltes des Internets mittels maschinellen Lernens und künstlicher Intelligenz zulässig. Der Gesetzgeber hatte hierbei offenbar vor Augen, dass dazu das gesamte Internet mittels Webcrawling durchsucht wird.[223] Dabei sollen auch Daten über lediglich beobachtungsbedürftige Bestrebungen erhoben werden dürfen; die Eingriffsschwelle ist damit sehr gering.[224] Auch diese Daten liegen dem Verfassungsschutz i.S.v. § 26 Abs. 3 S. 1 VSG NRW vor. Es wäre daher ohne weiteres möglich, das entsprechende Analyseprogramm mit dem Ergebnis des KI-basierten Webcrawlings „zu

---

[217] Hierzu BVerfGE 165, 363 Rn. 78, 70 – automatisierte Datenanalyse; BVerfGE 156, 63 Rn. 198 – Antiterrordateigesetz II.
[218] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 192.
[219] Vgl. BVerfGE 165, 363 Rn. 127 – automatisierte Datenanalyse.
[220] BVerfGE 165, 363 Rn. 79, 82 f. – automatisierte Datenanalyse.
[221] BVerfGE 165, 363 Rn. 87 – automatisierte Datenanalyse.
[222] BVerfGE 165, 363 Rn. 88 – automatisierte Datenanalyse.
[223] Landtag von Nordrhein-Westfalen, Drucksache 18/14457, S. 117.
[224] Ob hier noch ein Grundrechtseingriff abgelehnt werden kann angesichts des Gewichts der automatisierten Erhebung, erscheint fraglich, weil der Staat hier nicht wie eine beliebige Person durch das Internet surft, vgl. *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 8 m.w.N.

füttern“. Auf diese Weise können auch große Datenmengen aus dem Internet in die Analyse einbezogen werden, was zusätzlich den Eingriff vertieft.[225]

gg) Kein Ausschluss einer dauerhaften Zusammenführung

204 § 26 Abs. 3 S. 1 VSG NRW erlaubt potenziell die **Zusammenführung** dieser umfangreichen Daten mittels einer automatisierten Anwendung. Die Zusammenführung ist dabei – ausweislich des Wortlauts der Regelung – ein von der Analyse getrennter selbständiger Arbeitsschritt. Es ist vom Gesetz nicht ausgeschlossen, dass diese Zusammenführung nicht nur anlassbezogen, sondern dauerhaft erfolgt. § 26 Abs. 3 S. 1 VSG NRW formuliert den Zweck der Zusammenführung höchst allgemein. Sie muss „zur Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebungen und Tätigkeiten“ erfolgen, d.h. weder aufgrund eines bestimmten Anlasses noch zielgerichtet mit Blick auf eine bestimmte Bestrebung oder Tätigkeit. Die Spielräume dieser Regelungen zeigen sich auch im Vergleich mit § 26 Abs. 2 S. 1 VSG NRW, der an „bestimmte“ Bestrebungen und Tätigkeit „im Einzelfall“ anknüpft. Die Auslegung dieser Frage hat auch Auswirkungen auf die Wirksamkeit des Abteilungsleitervorbehalts in § 26 Abs. 9 S. 1 VSG NRW; dessen Entscheidung müsste dann nur die einmalige Zusammenführung erlauben.

205 Letztlich ist so nicht ausgeschlossen, dass das **funktionale Äquivalent einer von einer KI erschlossenen Datenbank** aufgebaut werden kann, die sämtliche Daten der Verfassungsschutzbehörde beinhaltet.[226] Dies wäre eine erhebliche Abkehr von der bisherigen Art des Umgangs mit Daten in einer Behörde. Deutlich wird dies im Vergleich zum Umgang mit Akten außerhalb der automatisierten Datenanalyse. Nach § 24 Abs. 6 S. 2 VSG NRW darf ein automatisierter Abgleich nur „beschränkt auf Akten eng umgrenzter Anwendungsgebiete“ erfolgen.

hh) Ungenügende Regelung der Zugriffsmöglichkeiten und Zugriffsberechtigungen

206 Das Gericht hat eine technisch und organisatorisch gesicherte Beschränkung des Zugriffs durch eine beschränkte Zahl von Personen als ein Instrument angesehen, das die Intensität des Eingriffs abschwächen kann.[227] § 26 Abs. 10 S. 1 VSG NRW verlangt jedoch nur – sehr unbestimmt – die Einführung eines Rechte- und Rollenkonzepts, das Nutzung und Zugang regelt.

---

[225] BVerfGE 165, 363 Rn. 88 – automatisierte Datenanalyse zur Verknüpfung mit dem Internet.
[226] Vgl. die Einschätzung zum ähnlich formulierten § 16a BKAG-E aus der letzten Legislaturperiode *BfDI*, Deutscher Bundestag, Stellungnahme 20 (4) 493 H, S. 6.
[227] BVerfGE 165, 363 Rn. 89 – automatisierte Datenanalyse.

207 Der Personenkreis ist dabei „angemessen“ zu begrenzen (§ 26 Abs. 10 S. 3 VSG NRW). Dies ist zu weitgehend. Verfassungsrechtlich muss der Kreis auf die Personen begrenzt sein, deren Zugriff für das jeweilige Analyseziel erforderlich ist. Eine solche Regelung ist auch nicht unüblich (z.B. § 6a Abs. 6 S. 1 ATDG: „Die Zugriffsberechtigung ist (…) auf die Personen zu beschränken, die unmittelbar mit Arbeiten auf diesem Anwendungsgebiet betraut sind.“). Dies entspricht auch dem im Geheimschutz üblichen Standard des „need-to-Prinzips“. Es darf immer nur die Person von einer sensiblen Information Kenntnis erlangen, die nicht nur dazu abstrakt berechtigt ist, sondern sie auch konkret benötigt. Eine nähere Ausgestaltung des Rechte- und Rollenkonzeptes, wie es das Gericht verlangt,[228] ist im Gesetz nicht vorgesehen.

208 Vorgaben zur technischen und organisatorischen Beschränkung des Zugriffs und der Nutzung sind nicht vorgesehen, obwohl sie nach der Rechtsprechung des Gerichts notwendig sind.[229] Sie sind auch nicht Gegenstand der Dienstanweisung nach § 26 Abs. 11 VSG NRW.

ii) Einbeziehung von Daten aus eingriffsintensiven Überwachungsmaßnahmen

209 Erschwerend zu berücksichtigen ist ferner, dass in die Analyse auch Daten aus eingriffsintensiven Überwachungsmaßnahmen einfließen.[230] Ausgeschlossen sind nur Daten, die durch eine akustische oder optische Wohnraumüberwachung gewonnen worden sind (§ 26 Abs. 3 S. 6 i.V.m. § 10 Abs. 1 Nr. 15 VSG NRW). Nach der Rechtsprechung des Gerichts kann es das Eingriffsgewicht vermindern, wenn in die Analyse keine Daten einfließen, die durch einen Eingriff in das Telekommunikationsgeheimnis (Art. 10 Abs.1 GG), das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) oder das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) gewonnen worden sind.[231]

210 In die Analyse nach § 26 Abs. 3 fließen Daten ein, die mit nachrichtendienstlichen Mitteln gewonnen worden sind. Diese greifen teilweise in Art. 10 Abs. 1 GG ein (§ 10 Abs. 1 Nr. 9 bis 14 VSG NRW), teilweise auch in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (insbesondere durch eine

---

[228] BVerfGE 165, 363 Rn. 140 – automatisierte Datenanalyse.
[229] Vgl. zu dieser Vorgabe BVerfGE 165, 363 Rn. 117 – automatisierte Datenanalyse.
[230] BVerfGE 165, 363 Rn. 118 – automatisierte Datenanalyse; *LfDI NRW,* Landtag von Nordrhein-Westfalen, Stellungnahme 18/2863, S. 24.
[231] BVerfGE 156, 11 Rn. 113 – Antiterrordateigesetz II; vgl. auch BVerfGE 165, 363 Rn. 118 – automatisierte Datenanalyse.

Quellen-TKÜ nach § 10 Abs. 1 Nr. 10 VSG sowie die Auswertung von Speichermedien nach § 6 Abs. 4 S. 1 VSG NRW→ Rn. 222 ff.).

211 Zusätzlich zu berücksichtigen ist, dass sogar Daten aus Eingriffen in die Analyse einfließen, die nur unter höheren Anforderungen gewonnen werden konnten als sie § 26 Abs. 3 S. 1 VSG NRW voraussetzt. Dies sind Daten, die durch Instrumente gewonnen werden, die nur gegen gesteigert beobachtungsbedürftige Bestrebungen und Tätigkeiten nach § 5 Abs. 3 VSG NRW eingesetzt werden durften. Hierunter fallen Daten, die durch den Einsatz von verdeckten Ermittlern, virtuellen Agenten oder V-Personen erlangt worden sind, deren Durchführung den persönlichen Lebensbereich in besonderem Maße betrifft (§ 15 Abs. 1 S. 2 i.V.m. §§ 16 Abs. 1, 17 Abs. 1 VSG NRW). Zwar ist es nicht ausgeschlossen die Verwendung dieser Daten für die Datenanalyse zum Erhebungszweck außer Verhältnis steht (vgl. § 26 Abs. 3 S. 1 a.E. VSG NRW); wie dies in der Praxis ausgelegt werden wird, ist jedoch höchst unsicher.

jj) Keine Begrenzung der Suchanfragen und Suchanlässe

212 Schließlich wirkt erschwerend, dass der Gesetzgeber die Suchanfragen weder auf bestimmte Anlässe noch auf eine bestimmte Art von Suchanfragen beschränkt.[232] Keine Begrenzung der Suchanfragen auf bestimmte Anlässe oder Ansätze. Zum besonderen Eingriffsgewicht einer unregulierten Suche führte das Gericht aus:

> „Das Eingriffsgewicht ist dagegen umso höher, je offener die Methode des Suchvorgangs gestaltet ist und je weniger die automatisierte Datenanalyse oder -auswertung durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster gesteuert wird. Denn je offener ein automatisierter Suchvorgang zur vorbeugenden Bekämpfung von Straftaten im Vorfeld konkreter Gefahren ausgestaltet ist, je weniger Sachverhaltsbezug die Suche also hat, umso eher werden durch die Suche überhaupt erst Anhaltspunkte für eine Gefahr generiert.“[233]

213 Wenn – wie im vorliegenden Fall – die zugrundeliegende Datenmenge sehr groß ist und hat der Gesetzgeber die Methode der Analyse nicht genau festgelegt, hielt das Gericht eine offene Suche für unzulässig:

> „Eine weder im Einzelfall durch einen konkreten Anlass getragene noch durch Vorgaben zur Verarbeitungsmethode inhaltlich eingeschränkte automatisierte Durchsuchung großer Bestände personenbezogener Daten auf bislang unbekannte Gesetzmäßigkeiten und gefahrenabwehrrechtlich bedeutende Zusammenhänge hin ist verfassungsrechtlich unzulässig.“[234]

---

[232] Dazu BVerfGE 165, 363 Rn. 93 ff. – automatisierte Datenanalyse.
[233] BVerfGE 165, 363 Rn. 93 – automatisierte Datenanalyse.
[234] BVerfGE 165, 363 Rn. 95 – automatisierte Datenanalyse.

c) Mangelnde Rechtfertigung des Eingriffs

214 Die vorgesehenen Voraussetzungen und Eingriffsschwellen sind nicht geeignet, diesen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen (aa). Es sind auch keine ausreichenden kompensatorischen Sicherungen durch eine aufsichtliche Kontrolle und eine externe Vorabkontrolle vorgesehen (bb). Schließlich ist die Einbeziehung von Daten, die aus Eingriffen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme stammen bereits für sich genommen unzulässig (cc).

aa) Keine ausreichend hohe Eingriffsschwelle

215 Die vorgesehene Eingriffsschwelle ist nicht ausreichend, um einen Eingriff von so erheblichem Gewicht zu rechtfertigen.[235] Das Gericht hat im Bereich der Gefahrenabwehr eine zumindest konkretisierte Gefahr gefordert. Im Bereich der Nachrichtendienste hat es bisher über eine Eingriffsschwelle nicht abschließend entschieden. Im Fall von § 6a ATDG hielt das Gericht es für ausreichend, wenn der Eingriff für die Aufklärung einer bestimmten beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten ist:

> „Diese verfassungsrechtlichen Anforderungen gelten grundsätzlich für alle Eingriffsermächtigungen mit präventiver Zielrichtung, also auch für die Verwendung dieser Daten durch Nachrichtendienste. Auch für ihre Tätigkeiten sind insoweit **tatsächliche Anhaltspunkte erforderlich** (zu den Besonderheiten der nachrichtendienstlichen Ausland-Ausland-Fernmeldeaufklärung vgl. jedoch BVerfG, Urteil des Ersten Senats vom 19. Mai 2020 - 1 BvR 2835/17 -, Rn. 155 ff.). Bei nicht tief in die Privatsphäre eingreifenden und insgesamt weniger gewichtigen Eingriffen kann es jedoch genügen, dass eine Auskunft zur Aufklärung einer **bestimmten**, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung **im Einzelfall geboten** ist, denn damit **wird ein wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt** (vgl. BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020 - 1 BvR 1873/13 und 1 BvR 2618/13 -, Rn. 151 m.w.N. – Bestandsdatenauskunft II). Diese zur Bestandsdatenauskunft formulierten Maßstäbe gelten auch für die erweiterte Nutzung der Antiterrordatei durch Nachrichtendienste. Zum einen haben diese von vornherein die Aufgabe, besonders gewichtige Rechtsgüter zu schützen (vgl. BVerfGE 141, 220 <339 f. Rn. 320>; vgl. auch BVerfGE 133, 277 <326 Rn. 118>). Zum anderen handelt es sich zwar hier nicht um „nicht tief in die Privatsphäre eingreifende und insgesamt weniger gewichtige“ Eingriffe (zum Eingriffsgewicht der erweiterten Nutzung oben Rn. 109 ff.). Maßgeblich ist hier indessen, dass bei deren ersten Erhebung durch die Polizeibehörden bereits die Eingriffsschwelle für die operativen Tätigkeiten der Polizei überschritten werden musste und diese nicht auch für die weitere Nutzung der erhobenen Daten gilt (vgl. insoweit BVerfGE 141, 220 <328 f. Rn. 289>).“[236] (Hervorhebungen hinzugefügt)

---

[235] *LfDI NRW*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2863, S. 22 f.; DAV, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2844), S. 14.
[236] BVerfGE 156, 11 Rn. 119 – Antiterrordateigesetz II.

216 Dieser Maßstab sollte aber nur gelten, wenn es sich „nicht um tief in die Privatsphäre reichenden Eingriffe oder insgesamt gewichtige Eingriffe“ handle. Bereits im Fall von § 25a HSOG und § 49 HmbPolDVG sah das Gericht einen gewichtigen Eingriff als gegeben an und wandte diesen milderen Maßstab nicht an.[237] Dies gilt ebenso für § 26 Abs. 3 VSG NRW, dessen Eingriffsgewicht sogar noch höher ist, denn – anders als im Fall des § 6a ATDG – ist das Eingriffsgewicht auch nicht gemindert, weil auf keine Daten zurückgegriffen wird, die durch besonders schwerwiegende Eingriffe in Art. 10, Art. 13 GG oder das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erhoben worden sind.[238] Auch ist die Datenmenge – alle vorhandenen Informationen des Verfassungsschutzes – sehr viel umfangreicher als in einer Verbunddatei. Darüber hinaus erlaubt die Regelung den Einsatz von KI und schließt personenbezogene Gefahrenprognosen nicht aus.

217 Infolgedessen ist ein höherer Maßstab an eine Datenanalyse nach § 26 Abs. 3 VSG NRW anzulegen. Die vorliegende Regelung lässt die undefinierte und den wenig zielgerichteten Zweck „zur Aufklärung mindestens erheblich beobachtungsbedürftiger Bestrebungen und Tätigkeiten“ ausreichen. Dies entspricht aber nicht den verfassungsrechtlichen Maßstäben, die sich der zitierten Rechtsprechung des Gerichts entnehmen lassen. Grundsätzlich sind danach – wie oben wiedergegeben – dieselben Maßstäbe an die nachrichtendienstliche Tätigkeit anzulegen wie im Bereich der Gefahrenabwehr. Die sind so das Gericht „tatsächliche Anhaltspunkte“.[239] Diese müssen sich grundsätzlich auf die Entstehung einer konkreten Gefahr beziehen.[240] Diese Anforderungen erfüllt § 26 Abs. 3 VSG NRW nicht.

218 Selbst wenn man den milderen Maßstab anwenden würde, würde ihn § 26 Abs. 3 VSG NRW nicht einhalten. Anders als im Fall des weniger eingriffsintensiven § 26 Abs. 2 VSG NRW setzt die Regelung nicht voraus, dass sich die Analyse auf eine bestimmte Bestrebung beziehen muss und im Einzelfall geboten sein muss.[241] Diese Anforderungen machen auch in der Praxis einen erheblichen Unterschied. So steht der Bezug zur Aufklärung einer bestimmten Bestrebung oder Tätigkeit – wie ihn § 26 Abs. 2 VSG NRW verlangt – einer dauerhaften und weitgehenden Zusammenführung aller Datenbestände entgegen, denn dieser Bezugspunkt erlaubt und erfordert eine Eingrenzung auf Datenbestände mit Relevanz für das konkrete Beobachtungsobjekt. Es verhindert auch, dass die Datenanalyse zu einem Standardinstrument wird, gewissermaßen einem „**ChatGPT für den**

[237] BVerfGE 165, 363 Rn. 167 f. – automatisierte Datenanalyse.
[238] BVerfGE 156, 11 Rn. 113, 119 – Antiterrordateigesetz II.
[239] BVerfGE 156, 11 Rn. 119 – Antiterrordateigesetz II.
[240] BVerfGE 156, 11 Rn. 118 – Antiterrordateigesetz II.
[241] Vgl. BVerfGE 156, 11 Rn. 119 – Antiterrordateigesetz II.

Verfassungsschutz NRW“. Die Aufklärung besonders beobachtungsbedürftiger Bestrebungen und Tätigkeiten ist ein Dauerzustand und würde den Einsatz einer Datenanalyse nach dem Wortlaut des § 26 Abs. 3 VSG NRW immer erlauben, während im Bereich der Polizei dies nur punktuell im Einfallfall zulässig wäre, wenn eine konkrete oder konkretisierte Gefahr vorliegt. Schließlich würden dann auch die Mängel der zu weiten Definition einer erheblichen Beobachtungsbedürftigkeit (→Rn. 163 ff.) hier zum Tragen kommen.

bb) Vorabkontrolle und aufsichtliche Kontrolle

219 In seinem Urteil zu § 6a ATDG hat das Gericht sich mit den verfassungsrechtlichen Anforderungen an den individuellen Rechtsschutz und die aufsichtliche Kontrolle auseinandergesetzt. Beides hielt das Gericht im Falle des § 6a ATDG in seiner Kombination für ausreichend.[242] Im Vergleich dazu bleiben die Sicherungen des § 26 Abs. 3 VSG NRW erheblich zurück.

(1) Fehlende Vorabkontrolle

220 Es fehlt an einer umfassenden vorherigen Rechtskontrolle.[243] Diese gewährleistete im Falle der Antiterror-Datei die G-10-Kommission (§ 6 Abs. 8 ATDG). Eine Befassung der G-10-Kommission ist nach dem VSG NRW demgegenüber nur vorgesehen, wenn mit nachrichtendienstlichen Mitteln erhobene Daten, deren Erhebung die G-10-Kommision vorab kontrolliert hat, zum Training der IT-Systeme genutzt werden (§ 21 Abs. 3 S. 2 i.V.m. § 26 Abs. 6 VSG NRW) sowie vor der Weiterverarbeitung von Daten aus einer Funkzellenabfrage (§ 21 Abs. 4 S. 4 VSG NRW). In den Fällen einer Datenanalyse nach § 26 Abs. 2 und 3 VSG NRW ist weder eine vorherige Kontrolle durch die G-10-Kommission gemäß § 14 VSG NRW vorgesehen, noch durch das Verwaltungsgericht nach § 13 VSG NRW. Es lässt sich auch nicht argumentieren, dass eine Vorabkontrolle bereits durch die Vorabkontrolle der Erhebung bei eingriffsintensiven Maßnahmen ausreichend sei. Dies spiegelt nicht das erhöhte Eingriffsgewicht durch eine Datenanalyse (→ Rn. 186 ff.) wider, die den Eingriff durch die Erhebung auch noch einmal vertiefen kann. Es ist daher ein Wertungswiderspruch, wenn der Gesetzgeber eine Befassung der G-10-Kommission anordnet, wenn die Daten für das Training genutzt werden, also ohne eine direkte Relevanz für den oder die Betroffene, nicht aber im Falle einer Datenanalyse, die über eine konkrete Person neues Wissen hervorbringen kann.

---

[242] BVerfGE 156, 11 Rn. 135 – Antiterrordateigesetz II.
[243] So auch *LfDI NRW*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2863, S. 23.

(2) Unzureichende aufsichtliche Kontrolle

221 Es bleibt nur eine aufsichtliche Kontrolle durch die Anordnungsbefugnis der Abteilungsleitung (§ 26 Abs. 9 VSG NRW). Diese ist im Vergleich zu § 6a Abs. 7 S. 5 bis 10 ATDG nur rudimentär ausgestaltet. Die Anordnungsbefugnis nach dem VSG NRW greift nur, wenn Daten verarbeitet worden sind, die mit nachrichtendienstlichen Mitteln erhoben worden sind (§ 26 Abs. 9 S. 1 VSG NRW). Diese Entscheidung ist zwar zu dokumentieren (§ 26 Abs. 9 S. 3 VSG NRW); dabei sind aber nur das Ziel der Datenauswertung und die einzubeziehenden Daten darzustellen. Es muss also nach dem Wortlaut der Regelung keine Begründung gegeben werden, sondern es reicht eine „Darstellung". Es muss auch nicht begründet werden, warum die Voraussetzungen vorliegen, eine Datenanalyse nach § 26 Abs. 2 und Abs. 3 VSG NRW durchzuführen. Mit anderen Worten: Es muss z.B. keine Begründung dafür geben, warum eine Datenanalyse überhaupt durchgeführt wird und im Einzelfall erforderlich ist, welche Daten einbezogen werden, warum der mit der Analyse verfolgte Zweck und der Erhebungszweck der einbezogenen Daten nicht außer Verhältnis stehen (vgl. § 26 Abs. 3 S. 1 VSG NRW). Dies erschwert eine spätere Kontrolle durch die Datenschutzaufsicht oder Gerichte erheblich.

cc) Einbeziehung von Daten, die durch das IT-System-Grundrecht geschützt werden

222 Die Weiterverarbeitung von Daten, die durch einen Eingriff in das IT-System-Grundrecht gewonnen worden sind, im Rahmen einer Datenanalyse nach § 26 Abs. 3 VSG NRW ist verfassungsrechtlich unzulässig. Nach der Rechtsprechung des Gerichts ist eine zweckändernde Weiterverarbeitung von Daten, die durch eine „Online-Durchsuchung"[244] bzw. einen „Zugriff auf informationstechnisches System"[245] gewonnen wurden, nur zulässig, wenn die Anforderungen einer hypothetischen Datenneuerhebung erfüllt wären. Voraussetzung wäre danach das Vorliegen einer konkreten oder konkretisierten Gefahr.

(1) Quellen-TKÜ

223 Nach der neueren Rechtsprechung des Gerichts müssen diese Anforderungen auch für die Quellen-TKÜ gelten, denn sie stellt nicht nur einen Eingriff in Art. 10 Abs. 1 GG dar, sondern auch in das IT-System-Grundrecht.[246] Das

[244] BVerfGE 141, 220 Rn. 283 – BKA-Gesetz; BVerfGE 165, 363 Rn. 59, 81 – automatisierte Datenanalyse.
[245] BVerfGE 141, 220 Rn. 291 – BKA-Gesetz; BVerfGE 165, 363 Rn. 64 – automatisierte Datenanalyse.
[246] BVerfG MMR 2026, 44 Rn. 102 ff. – Trojaner I.

Gericht hat daher auch für eine Quellen-TKÜ das Vorliegen einer konkreten oder zumindest konkretisierten Gefahr verlangt.[247] Eine Einbeziehung von Daten aus einer Quellen-TKÜ (§ 10 Abs. 1 Nr. 10 VSG NRW) ist daher nicht zulässig.

224 Während sich die Quellen-TKÜ auf laufende Kommunikation bezieht, zielte eine „Quellen-TKÜ plus“ auf Daten, die während der Übermittlung hätten überwacht werden können und jetzt auf einem informationstechnischen System gespeichert sind. Eine solche Befugnis sieht § 21 Abs. 5 S. 3 VSG NRW vor. Das Gericht hat jüngst klargestellt, dass darin ein Eingriff in das IT-System-Grundrecht liegt[248] und dessen Rechtfertigung ähnlich hohe Hürden wie eine Online-Durchsuchung überwinden muss.[249] Die Einbeziehung von Daten aus dieser Maßnahme ist daher erst recht nur unter der Voraussetzung einer zumindest konkretisierten Gefahr zulässig.

(2) Zugriff auf zugangsgesicherte Informations- und Kommunikationsinhalte im Internet

225 Auch der Zugriff auf zugangsgesicherte Informations- und Kommunikationsinhalte gemäß § 10 Abs. 1 Nr. 11 VSG NRW kann einen Eingriff in das IT-System-Grundrecht darstellen und eine Einbeziehung daher unzulässig sein. Zu einem informationstechnischen System gehört nicht nur das Gerät selbst (z.B. Rechner oder Smartphone), sondern es umfasst auch damit verbundene Systeme, z.B. Cloudspeicher,[250] und Online-Services.[251] Mit einem solchen Zugriff kann eine Behörde daher einen sehr weitgehenden Zugang zu sehr aussagekräftigen Datenbeständen erhalten.

226 Das IT-System-Grundrecht schützt dabei nicht nur gegen Online-Durchsuchungen, d.h. der Infiltration mit einer Überwachungssoftware,[252] die explizit ausgeschlossen sind, sondern bietet einen umfassenden Schutz einer besonders geschützten Zone der Privatheit.[253] Für das Eingriffsgewicht und damit die Verhältnismäßigkeit kommt es, so das Gericht, auch darauf an, welche Daten letztlich im Rahmen des Zugriffs genutzt werden.[254]

227 § 10 Abs. 1 Nr. 12 VSG NRW ermächtigt daher zu so schwerwiegenden Eingriffen, dass eine Nutzung der erhobenen Daten unter den Voraussetzungen des § 26 Abs. 3 VSG NRW unzulässig wäre.

---

[247] BVerfG MMR 2026, 44 Rn. 126 – Trojaner I
[248] BVerfG MMR 2026, 44 Rn. 228 ff. – Trojaner II.
[249] BVerfG MMR 2026, 44 Rn. 238 – Trojaner II.
[250] BVerfGE 141, 220 Rn. 209 f. – BKA-Gesetz.
[251] BVerfG MMR 2026, 44 Rn. 113 – Trojaner I
[252] BVerfG MMR 2026, 44 Rn. 117– Trojaner I
[253] Vgl. BVerfG MMR 2026, 44 Rn. 115 – Trojaner I
[254] BVerfG MMR 2026, 44 Rn. 124 – Trojaner I

Beispiel: Der Verfassungsschutz erhält Zugriff auf das Passwort einer Zielperson für dessen iCloud-Konto. Dieses Passwort erlaubt dann den Zugriff auf dort gespeicherte Fotos, Dokumente, Backups von Mails, Messenger-Nachrichten und ggf. sogar von ganzen Geräten.

(3) Auslesen von Speichermedien

228 § 6 Abs. 4 S. 1 2. Alt. VSG NRW erlaubt eine Durchsicht elektronischer Speichermedien. Wie diese Medien erlangt worden sind, lässt der Gesetzestext offen. Die Gesetzesbegründung verweist auf Handys oder USB-Sticks von Zielpersonen, die unmittelbar oder durch die Polizei in den Besitz des Verfassungsschutzes gelangen.[255] Wer diese Zielpersonen sein können, lässt das Gesetz ebenfalls offen. Es handelt sich bei der Maßnahme um kein nachrichtendienstliches Mittel nach § 10 VSG NRW, sodass § 11 Abs. 2 VSG NRW keine Anwendung findet. § 6 Abs. 4 S. 3 VSG NRW schließt eine Online-Durchsuchung ausdrücklich aus und lässt die Instrumente und Wege des Zugriffs im Übrigen offen.

229 Auch diese Maßnahme kann einen Eingriff in der IT-System-Grundrecht darstellen – auch ohne eine Online-Durchsuchung. Wie ausgeführt ist nach der Rechtsprechung des Gerichts der Schutz dieses Grundrechts vom System her zu denken.[256] Dieses ist aber auch bei einer Durchsicht von Speichermedien betroffen.[257] Dies mag bei einem USB-Stick wegen der eingeschränkten Datenmenge und fehlenden Vernetzung noch zu bezweifeln sein. Schon bei einem Smartphone wird es aber deutlich: Dieses ist ein geschütztes informationstechnisches System – gewissermaßen das „ausgelagerte Gehirn eines Menschen“ (Burkhard Hirsch). Der Speicher ist das „Gedächtnis“ dieses IT-Systems, das den Großteil der personenbezogenen Daten enthält. Der Zugriff auf diesen Speicher ist zugleich ein Zugriff auf das informationstechnische System. Er kann einen ungenau definierten Personenkreis betreffen, der möglicherweise nicht in Gefährdung der Rechtsgüter verfangen ist,[258] und es muss keine konkretisierte Gefahr als Anlass vorliegen. Eine zumindest konkretisierte Gefahr müsste jedoch bei der Erhebung vorliegen und nach der Rechtsprechung auch bei der zweckändernden Weiterverarbeitung dieser Daten, weil es sich um einen Eingriff in das IT-System-Grundrecht handelt.

---

[255] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 117.
[256] BVerfG MMR 2026, 44 Rn. 100 – Trojaner I
[257] *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 8.
[258] Vgl. zu diesem Erfordernis BVerfG MMR 2026, 44 Rn. 125 – Trojaner I; BVerfGE 141, 220 Rn. 108 f. – BKA-Gesetz.

2. § 26 Abs. 2 VSG NRW

230 § 26 Abs. 2 VSG NRW verstößt gegen das Allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) in seinen Ausprägungen als Recht auf informationelle Selbstbestimmung sowie als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

a) Mangelnde Bestimmtheit und Normenklarheit

231 Wie bereits § 26 Abs. 3 VSG NRW verstößt § 26 Abs. 2 VSG NRW gegen das Gebot der Bestimmtheit sowie das Gebot der Normenklarheit. Die Regelung legt die Instrumente der Datenanalyse nicht hinreichend bestimmt und normenklar fest. Auch hier besteht der Widerspruch zwischen dem Einsatz von KI und maschinellem Lernen einerseits (§ 26 Abs. 2 S. 1 VSG NRW) und dem Ausschluss selbst weiter lernender Systeme andererseits (§ 26 Abs. 2 S. 2 VSG NRW). Zur Unklarheit trägt zusätzlich bei, dass für das Ziel der „Filterung, Sortierung und Priorisierung“ KI und maschinelles Lernen nicht zwingend benötigt werden und § 26 Abs. 4 VSG NRW nicht in Bezug genommen wird, der typische Ziele des Einsatzes von KI und maschinellem Lernen nennt.

b) Verstoß gegen das Grundrecht auf informationelle Selbstbestimmung

232 § 26 Abs. 2 VSG NRW ist nicht verhältnismäßig im engeren Sinne. Die gesetzlich vorgesehenen Eingriffsvoraussetzungen reichen nicht aus, um den Eingriff von einem solchen Gewicht wie durch § 26 Abs. 2 VSG NRW in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen.

aa) Schwere des Eingriffs

233 Anders als § 26 Abs. 3 VSG NRW zielt § 26 Abs. 2 VSG NRW nicht primär auf die Gewinnung neuer Erkenntnisse durch die Datenanalyse. Ziel ist die Filterung, Sortierung und Priorisierung der gesamten dem Verfassungsschutz vorliegenden Daten. Hierdurch werden große Datenmengen sehr viel leichter und schneller erschlossen, als dies händisch möglich wäre. Insoweit ist der Eingriff weniger tief als im Rahmen der Datenanalyse nach § 26 Abs. 3 VSG NRW. Auch im Rahmen der Datenanalyse nach § 26 Abs. 2 VSG NRW gibt es eine Reihe von Faktoren, welche die Eingriffsintensität erhöhen, so dass auch hier ein Eingriff von erheblichem Gewicht anzunehmen ist.

(1) Große Datenmenge

234 Wie auch schon im Rahmen des § 26 Abs. 3 VSG NRW wirkt sich die große Datenmenge erschwerend aus.[259] Es werden sämtliche Daten, die dem Verfassungsschutz vorliegen einbezogen. Eine Eingrenzung findet nicht statt.

(2) Einbeziehung von Daten, die durch nachrichtendienstliche Mittel erhoben worden sind.

235 Im Rahmen dieser Datenmenge werden zudem Daten analysiert, die mit nachrichtendienstlichen Mitteln erhoben worden sind, teilweise durch Eingriffe in Art. 10 Abs. 1 und das IT-System-Grundrecht (zu § 26 Abs. 3 VSG NRW bereits → Rn. 222 ff.). Eine Ausnahme besteht nur für Daten, die durch eine Wohnraumüberwachung gewonnen wurden (§ 26 Abs. 2 S. 4 VSG NRW). Anders als nach § 26 Abs. 3 S. 5 VSG NRW ist im Rahmen von § 26 Abs. 2 VSG NRW nicht durch eine entsprechende Regelung gewährleistet, dass die Kennzeichnung dieser Daten erhalten bleibt.[260]

236 Auch eine Einschränkung danach, ob der Erhebungskontext eine Verarbeitung ermöglicht, findet – anders als nach § 26 Abs. 3 VSG NRW – nicht statt. Dies wäre im Fall des § 26 Abs. 2 VSG NRW allerdings besonders notwendig. Die Regelung erlaubt die Analyse bereits zur Aufklärung bestimmter beobachtungsbedürftiger Bestrebungen und Tätigkeiten – legt also die geringstmöglichen Anforderungen fest. Für die Aufklärung lediglich beobachtungsbedürftiger Bestrebungen dürften die nachrichtendienstlichen Mittel, mit denen die Daten erhoben worden sind, nicht genutzt werden. Es droht daher das **Risiko der Umgehung der Eingriffsvoraussetzungen** für nachrichtendienstliche Mittel.

(3) Fehlende Festlegung der Methoden, Ergebnisse und Suchanfragen

237 § 26 Abs. 2 VSG NRW trifft keine Festlegungen, wie die Suchanfragen aussehen müssen oder welche Methoden und Ergebnisse. Diese Entscheidung liegt vollkommen in den Händen des Verfassungsschutzes. Soweit auf die „Filterung, Sortierung und Priorisierung“ als Ergebnis der Analyse abgestellt wird, ist auch dies vieldeutig. Auf den ersten Blick klingt dies wie eine Suchmaschine, gewissermaßen ein „**Google für den Verfassungsschutz“**. Dies wäre jedoch eine Untertreibung. Bereits die Verwendung der Begriffe „Filterung, Sortierung und Priorisierung“ zeigt, dass es nicht um einen einfachen Abgleich geht, sondern Informationen mit diesem Ziel aufbereitet werden. Dies setzt jedoch bereits wertende Elemente voraus. Zum Vergleich: Auch bei Google oder Facebook sortiert ein Algorithmus die Ergebnisse und

[259] BVerfGE 165, 363 Rn. 109 – automatisierte Datenanalyse.
[260] Zur fehlenden Kennzeichnung BVerfGE 165, 363 Rn. 144 – automatisierte Datenanalyse.

steuert so die Aufmerksamkeit der Nutzerinnen und Nutzer. Selbst bei einer Sortierung und Priorisierung würde daher die Datenanalyse die Aufmerksamkeit des Anfragenden auf bestimmte Sachverhalte lenken, anderen weniger Gewicht beimessen oder sie gar aussondern. Dies kann eine grundrechtsrelevante Frage sein, weil eine unbescholtene Person so in den Fokus des Staates rücken kann (mit den entsprechenden Folgen →Rn. 188). Diese Problematik stellt sich verstärkt, wenn maschinelles Lernen und KI eingesetzt werden, denn deren Ergebnisse sind schwerer nachvollziehbar und *per definitionem* zu einem gewissen Grade autonom zustande gekommen (vgl. die Definition in Art. 3 Nr. 1 KI-VO).

(4) Keine Eingrenzung der Suchaufträge

238 § 26 Abs. 2 S. 1 VSG NRW sieht eine freie Suche innerhalb dieses größtmöglichen Datenpools, der dem Verfassungsschutz zur Verfügung steht, vor.[261] Dies vertieft den Eingriff. Denkbar sind auch Suchaufträge, die Auswirkungen einzelne Personen haben, z.B. „Ordne die Hinweise zu den einzelnen Mitgliedern einer Gruppe nach ihrer Gefährlichkeit".[262] Eine solche „Sortierung" oder „Priorisierung" wäre nicht ausgeschlossen.

(5) Einsatz von KI und maschinellem Lernen

239 Der Eingriff wird vertieft durch die Möglichkeit KI und maschinelles Lernen einzusetzen (§ 26 Abs. 2 S. 1 VSG NRW).[263] Hieran ändert auch das Verbot selbst weiterlernender Systeme nach § 26 Abs. 2 S. 2 VSG NRW nichts, denn dieses Verbot ist widersprüchlich und unbestimmt (→ Rn. 181 ff.). Wie soeben dargelegt sind auch die Ziele des § 26 Abs. 2 VSG NRW keine rein deterministische Aufgabe. Es ist daher auch hier nicht ausgeschlossen, dass die KI sich den Anfragen auch ohne weitere Trainingsdaten anpasst. Damit stellt sich auch hier – wie bei § 26 Abs. 3 VSG – das Problem der Nachvollziehbarkeit (→ Rn. 189 ff.), da diese unter dem Vorbehalt des technisch Möglichen steht.

(6) Keine Maßnahmen zur Gewährleistung der Qualität und der Vermeidung von Diskriminierungen

240 § 26 Abs. 2 VSG NRW leidet unter den gleichen Mängeln wie § 26 Abs. 3 VSG NRW im Hinblick auf die Gewährleistung der Qualität der Trainingsdaten, der Verhinderung von Diskriminierungen und der

[261] BVerfGE 165, 363 Rn. 93 ff. – automatisierte Datenanalyse
[262] Vgl. zu solchen Gefährlichkeitsprognosen BVerfGE 165, 363 Rn. 96 ff. 121 – automatisierte Datenanalyse.
[263] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse.

Sicherstellung der Zuverlässigkeit und Qualität der verwendeten Software und ihres Anbieters (siehe oben → Rn. 193 ff. und 197 ff.).

bb) Keine Rechtfertigung des Eingriffs

241 Die vorgesehenen Eingriffsschwellen sind nicht ausreichend, um einen Grundrechtseingriff von so erheblicher Tiefe zu rechtfertigen. Der Gesetzgeber hat sich die geringstmögliche Eingriffsschwelle gewählt. Es reicht das Vorliegen einer beobachtungsbedürften Bestrebung oder Tätigkeit aus. Eine Eingrenzung erfolgt nach § 26 Abs. 2 S. 1 VSG NRW nur dadurch, dass es sich um eine bestimmte Bestrebung handeln muss und die Maßnahme im Einzelfall erforderlich sein muss. Das Gericht hat diese Schwelle aber nur für nicht tief in die Privatsphäre eingreifende und insgesamt weniger gewichtige Eingriffe im nachrichtendienstlichen Bereich für ausreichend gehalten.[264] Wie dargelegt ist die Verarbeitung nach § 26 Abs.2 VSG NRW in mehrfacher Hinsicht ein gewichtiger Eingriff. Zwar zielt die Verarbeitung nicht auf die Gewinnung neuer Erkenntnisse, sie beruht aber auf einer sehr großen Datenmenge, dem Einsatz von KI und maschinellem Lernen lässt die Suchbegriffe und Erkenntnisziele weitgehend offen, trifft keine ausreichende Sicherungen, um auf die Herausforderungen durch KI und maschinelles Lernen zu reagieren (etwa Nachvollziehbarkeit, Diskriminierungsschutz, Datenqualität, Zuverlässigkeit der Software und ihres Anbieters), und erlaubt die Verarbeitung von Daten, die mit nachrichtendienstlichen Mitteln unter erheblich höheren Eingriffsschwellen gewonnen wurden, als sie § 26 Abs. 2 VSG NRW vorsieht und, ohne dass die Kennzeichnung der Erhebung sicher gewährleistet bleibt.

c) Verstoß gegen das IT-System-Grundrecht

242 Die Verarbeitung von Daten im Rahmen des § 26 Abs. 2 VSG NRW, die durch Eingriffe in das IT-System-Grundrecht – hier die Quellen-TKÜ nach § 10 Abs. 1 Nr. 10, den Zugriff auf im Internet gespeicherte Daten nach § 10 Abs. 1 Nr. 11 und den Zugriff auf Speichermedien nach § 6 Abs. 4 S. 1 2. Alt. VSG NRW – gewonnen worden sind, verstößt gegen das IT-System-Grundrecht. Wie schon im Rahmen des § 26 Abs. 3 (→ Rn. 222 ff.) wäre die Verarbeitung dieser Daten nur bei Vorliegen einer konkretisierten Gefahr auf Basis einer hinreichend bestimmten Regelung denkbar. Diese Eingriffsschwelle ist hier weit unterschritten.

---

[264] BVerfGE 156, 11 Rn. 119 – Antiterrordateigesetz II; vgl. auch BVerfGE 165, 363 Rn. 163 – automatisierte Datenanalyse.

3. Weiterverarbeitung von Daten zum Training

243 Die Regelungen zum Trainieren von IT-Produkten nach § 26 Abs. 6 und 7 sowie § 36 VSG NRW verstoßen gegen das allgemeine Persönlichkeitsrecht in seiner Ausprägung des Rechts auf informationelle Selbstbestimmung sowie des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), weil sie nicht verhältnismäßig im engeren Sinne sind. Es ist zwischen allgemein zugänglichen Daten aus dem Internet und Echtdaten bzw. Originaldaten des Verfassungsschutzes, d.h. des Aktenbestandes der Behörde, zu unterscheiden.

a) § 26 Abs. 6 VSG NRW

244 § 26 Abs. 6 S. 1 VSG NRW erlaubt die Nutzung von allgemein zugänglichen Daten und beim Verfassungsschutz vorhandenen Daten zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten. Hierbei handelt es sich nach dem Wortlaut um eine Weiterverarbeitung bereits vorliegender Daten.

aa) Erhebung allgemein zugänglicher Daten aus dem Internet

245 Die Gesetzesbegründung geht davon aus, dass die Erhebung allgemein zugänglicher Informationen aus dem Internet kein Grundrechtseingriff ist.[265] Dies ist nicht zutreffend. Der Gesetzgeber bezieht sich hier auf eine Aussage des Gerichts im Urteil zur Online-Durchsuchung:

> „Eine Kenntnisnahme öffentlich zugänglicher Informationen ist dem Staat grundsätzlich nicht verwehrt. Dies gilt auch dann, wenn auf diese Weise im Einzelfall personenbezogene Informationen erhoben werden können (vgl. etwa Böckenförde, Die Ermittlung im Netz, 2003, S. 196f.; Zöller, GA 2000, 563 [569]). Daher liegt kein Eingriff in das allgemeine Persönlichkeitsrecht vor, wenn eine staatliche Stelle im Internet verfügbare Kommunikationsinhalte erhebt, die sich an jedermann oder zumindest an einen nicht weiter abgegrenzten Personenkreis richten. So liegt es etwa, wenn die Behörde eine allgemein zugängliche Webseite im World Wide Web aufruft, eine jedem Interessierten offenstehende Mailingliste abonniert oder einen offenen Chat beobachtet.
>
> Ein Eingriff in das Recht auf informationelle Selbstbestimmung kann allerdings gegeben sein, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt. Hierfür bedarf es einer Ermächtigungsgrundlage.“[266]

[265] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 193.
[266] BVerfGE 120, 274 Rn. 308 f. – Online-Durchsuchung.

246 Das Gericht hatte damals den Aufruf einzelner Websites vor Augen. Gewissermaßen geht der Staat hier im Netz Streife. Für die Entwicklung, das Training, die Änderung und Überprüfung von IT-System werden aber nicht nur einzelne Daten erhoben werden. Typischerweise werden hierzu automatisiert große Datenmengen aus dem Internet im Wege des Webcrawlings oder Webscrapings aus dem Netz zusammengetragen,[267] um sie in der Folge im Rahmen des Trainings zum Erkennen von Mustern zu verarbeiten. Diese Praxis wird bereits in Bezug auf private KI-Unternehmen kritisch diskutiert. Es bedarf daher für eine staatliche Stelle erst recht einer hinreichend bestimmten Rechtsgrundlage für die automatisierte Datenerhebung aus dem Internet.[268] § 6 Abs. 4 S. 1 1. Alt. VSG NRW kann hierzu nicht herangezogen werden, weil die Regelung keine Erhebung für diese spezifischen Zwecke[269] erlaubt; es wäre für die betroffenen Personen aufgrund des Normtextes kaum voraussehbar, dass ein Nachrichtendienst potenziell das gesamte Internet zu dem Training eines eigenen KI-Modells nutzen könnte. Eine entsprechende Regelung müsste auch risikoverringernde Maßnahmen vorsehen, wie sie etwa der Europäische Datenschutzausschuss empfiehlt.[270] Darüber hinaus würde es sich bei einer solchen weitgehend ungeregelten Erhebung um eine Maßnahme von großer Streubreite handeln.

bb) Weiterverarbeitung von Echtdaten

247 Die Weiterverarbeitung von Echtdaten oder Originaldaten, die nur subsidiär zu anonymisierten und pseudonymisierten Datenbeständen erfolgt, wenn unveränderte Daten benötigt werden, stellt eine Zweckänderung dar. Die Nutzung von Daten für einen neuen Zweck stellt einen eigenständigen rechtfertigungsbedürftigen Grundrechtseingriff dar.[271] Hierfür gilt das Kriterium der **hypothetischen Datenneuerhebung**.[272]

(1) Durch Eingriffe in das IT-System-Grundrecht gewonnene Daten

248 Danach scheidet eine Verwendung von Daten im Rahmen des § 26 Abs. 6 VSG NRW aus, wenn diese durch einen **Zugriff auf ein**

---

[267] *EDSA*, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen v. 2.12.2024, Rn. 13; *Dieker* ZD 2024, 132 (132).
[268] *Hornung*, AöR 147 (2022) 1 (26 f.) (auch mit Blick auf Art. 8 EMRK); *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 8.
[269] Zur Anforderung an spezifische Zwecke BVerfGE 155, 119 Rn. 123 – Bestandsdatenauskunft II; BVerfGE 156, 11 Rn. 83 – Antiterrordateigesetz II.
[270] *EDSA*, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen v. 2.12.2024, Rn. 105 ff.; zur Schwere des Eingriffs durch Webscraping auch OLG Köln, NJW 2025, 3156 Rn. 59.
[271] BVerfGE 141, 220 Rn. 285 – BKA-Gesetz m.w.N.
[272] BVerfGE 141, 220 Rn. 287 – BKA-Gesetz; BVerfGE 165, 363 Rn. 61 – automatisierte Datenanalyse; BVerfGE 162, 1 Rn. 232. – Bayerisches Verfassungsschutzgesetz.

informationstechnisches System und damit durch einen Eingriff in das IT-System-Grundrecht gewonnen worden sind (hierzu bereits →Rn. 222 ff.). Hierfür wäre zumindest eine konkretisierte Gefahr erforderlich.[273]

(2) Durch nachrichtendienstliche Mittel erhobene Daten

249 Unverhältnismäßig ist zudem eine Weiterverarbeitung von Daten, die durch **nachrichtendienstliche Mittel** erhoben worden sind. Diese setzten regelmäßig eine höhere Eingriffsschwelle voraus. Das Gericht verlangt insoweit nicht, dass die Eingriffsschwelle auch bei der Weiterverarbeitung vorliegen muss, wohl aber – im Bereich der Gefahrenabwehr – ein konkreter Ermittlungsansatz.[274] Vorliegend geht es jedoch um eine Nutzung, die losgelöst von einem bestimmten Beobachtungsvorgang erfolgt, sondern nur der Verbesserung der Fähigkeiten der Behörde als Ganzes dient.[275] Selbst wenn man dies für ausreichend halten sollte, wären noch immer Regelungen notwendig, um die besondere Sensibilität dieser Daten zu berücksichtigen. Durch das Training werden die verwendeten Daten Teil der abstrakten Wissensgrundlage des KI-Modells.[276] Die Umstände ihrer Erhebung lassen sich üblicherweise nur durch eine Kennzeichnung der Daten erreichen.[277] Eine solche Kennzeichnung ist nach § 26 Abs. 3 S. 5 VSG NRW für die Datenanalyse vorgesehen und generell für die Weiterverarbeitung nach § 24 Abs. 5 VSG NRW, aber nicht im Rahmen der Weiterverarbeitung für die Zwecke des § 26 Abs. 6 VSG NRW.

(3) Allgemein zugängliche Daten Dritter

250 Keine ausreichende Eingriffsgrundlage besteht für die Nutzung von **öffentlich zugänglichen Daten**. Diese Daten sollen sogar vorrangig für das Training genutzt werden (§ 26 Abs. 6 S. 2 VSG NRW) Auch wenn Daten öffentlich zugänglich sind und damit ihre Vertraulichkeitserwartungen herabgesetzt sind, stellt ihre Weiterverarbeitung einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.[278] Dies gilt besonders, wenn – wie hier – auch Daten von Personen verarbeitet werden können, die in keinem Zusammenhang zu einer beobachtungsbedürftigen Bestrebung oder Tätigkeit stehen, also überhaupt keinen Anlass haben, damit zu rechnen Gegenstand

---

[273] BVerfGE 165, 363 Rn. 64 – automatisierte Datenanalyse; BVerfGE 162, 1 Rn. 271. – Bayerisches Verfassungsschutzgesetz.
[274] BVerfGE 165, 363 Rn. 62 – automatisierte Datenanalyse; BVerfGE 162, 1 Rn. 270. – Bayerisches Verfassungsschutzgesetz.
[275] Ähnliche Einordnung für den Bereich der Gefahrenabwehr *Kühne/Golla/Schäfer,* GSZ 2025, 272 (276).
[276] *Kostov*, Der Staat 64 (2025) 537 (564).
[277] Angedeutet, aber offengelassen in BVerfGE 165, 363 Rn. 65 – automatisierte Datenanalyse.
[278] *Hornung*, AöR 147 (2022) 1 (25 ff.).

einer Verarbeitung durch den Verfassungsschutz zu werden. Eine Eingrenzung nimmt das Gesetz nicht vor; es kommt nicht auf die Relevanz der Daten für die Arbeit des Verfassungsschutzes an, sondern nur auf die Vermeidung von statistischen Verzerrungen und diskriminierenden Verarbeitungsprozessen (§ 26 Abs. 6 S. 3 VSG NRW). Auch § 26 Abs. 7 VSG NRW bietet keinen Schutz, weil er erst nach der Weiterverarbeitung eine Löschung von Daten Dritter vorsieht, nicht aber für das Training, die Entwicklung, Änderung und Überprüfung von IT-Produkten – und auch nicht für die Verarbeitung als Teil des trainierten Modells selbst.

251 Keinen Niederschlag in der Regelung findet der Faktor, dass die personenbezogenen Daten unbescholtener Dritter damit **Teil des abstrakten Wissens der entwickelten oder trainierten Software werden**, da sie zum abstrakten Wissen dieser Software gehören.[279] Sie verbleiben damit im KI-Modell.[280] Hiervon geht auch die Gesetzesbegründung zu § 26 Abs. 7 VSG NRW aus.[281] Auch der Europäische Datenschutzausschuss kam zu dem Ergebnis, dass eine KI-Modell nicht ohne Weiteres als anonym gelten kann[282] und das Risiko des Zugriffs auf die Daten durch Extraktion oder des „Erinnerns“ besteht.[283] Es besteht damit die Möglichkeit, dass bei der folgenden Datenanalyse Personen, mit deren allgemein zugänglichen Daten das Modell trainiert worden ist, in den Fokus des Verfassungsschutzes geraten; hieran können sich weitere Grundrechtseingriffe anschließen.[284]

b) § 26 Abs. 7 VSG NRW

252 § 26 Abs. 7 VSG NRW verstößt gegen das Recht auf informationelle Selbstbestimmung, weil er die Verarbeitung personenbezogener Daten erlaubt, die eigentlich hätten gelöscht werden müssen, weil sie für die Aufgabenerfüllung des Verfassungsschutzes nicht mehr erforderlich sind.[285] Es handelt sich hierbei um eine Spezialregelung zu § 27 VSG NRW.[286] Die Gesetzesbegründung führt hierzu aus:

> „Diese Daten sind der allgemeinen Tätigkeit der Verfassungsschutzbehörde entzogen, da ggf. Daten enthalten sein können, die zur konkreten Aufgabenerfüllung nicht mehr zur Verfügung stehen dürfen zum Beispiel, weil sich eine Person vom Extremismus

[279] *Kostov*, Der Staat 64 (2025) 537 (564).
[280] So *LfDI NRW*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2863, S. 23.
[281] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 193.
[282] *EDSA*, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen v. 2.12.2024, Rn. 31 ff. und Rn. 35 ff.
[283] Dazu *Pesch/Böhme*, MMR 2023, 917 (920 f.); OLG Köln NJW 2025, 3156 Rn. 34 m.w.N.
[284] Vgl. BVerfGE 165, 363 Rn. 77 – automatisierte Datenanalyse zum Eingriffsvertiefung hierdurch.
[285] *LfDI NRW*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2863, S. 23.
[286] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 193.

abgewandt hat und die letzte relevante Erkenntnis zu ihr mehr als fünf Jahre zurückliegt. Sind solche Daten einmal rechtmäßig für die Zwecke gemäß der Absätze 5 und 6 genutzt worden und bestehen die IT-Produkte fort, werden die Daten weiterhin benötigt. Sie sind durch die separate Vorhaltung aber verarbeitungsbeschränkt."[287]

253 Die weitere Verarbeitung dieser Daten ist zwar beschränkt, nicht aber die Weiterverarbeitung im Rahmen des IT-Produkts – hier: des verwendeten KI-Modells. Der Gesetzgeber steht hier vor der Schwierigkeit, wie die Betroffenenrechte auch im Rahmen von KI-Modellen gewährleistet werden können.[288] Es werden aber keine Maßnahmen getroffen, welche den Ausschluss der Löschung versuchen zu kompensieren. So werden diese Informationen nicht generell mit einem „Verfallsdatum" versehen. Denkbar wäre auch eine Beschränkung auf Ebene des KI-Systems, das z.B. direkte Fragen in Bezug auf Personen, die sich vom Extremismus abgewandt haben, ausschließt.

254 Nach dem vorliegenden Regelungskonzept wären Informationen, die eigentlich gelöscht werden müssten, immer noch im abstrakten Modellwissen des KI-Modells enthalten. Es bestände die Gefahr, dass sich KI-Modelle erinnern, speziell bei gezielten Anfragen zu Personen.[289] Dies könnte eine ähnliche Wirkung haben wie eine „ewige Datenbank".[290] Dies stände jedoch im Widerspruch zum Allgemeinen Persönlichkeitsrecht, das es dem Einzelnen ermöglichen muss, im Leben neue Wege einzuschlagen.[291] In den Worten des Gerichts:

„Die Möglichkeit des Vergessens gehört zur Zeitlichkeit der Freiheit."[292]

Das Gericht hat dies auf die Wiedereingliederung von Straftätern bezogen. Dies muss aber auch für den Bereich des Verfassungsschutzes gelten. Man denke nur an die Folgen einer Ablehnung einer Sicherheitsüberprüfung.

c) § 36 VSG NRW

255 § 36 VSG NRW ist mit dem Recht auf informationelle Selbstbestimmung unvereinbar, weil die Regelung eine Übermittlung an öffentliche und nichtöffentliche Stellen zum Training von IT-Produkten erlaubt, ohne ausreichende Gewährleistungen zur Sicherung der übermittelten Daten vorzusehen. Die Übermittlung stellt einen eigenständigen

[287] Landtag von Nordrhein-Westfalen, Drucksache 18/14557, S. 193.
[288] *LfDI NRW*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2863, S. 23.
[289] *Pesch/Böhme*, MMR 2023, 917 (920 f.).
[290] Zum Spannungswirkung zum „Recht auf Vergessen" *Pesch/Böhme*, MMR 2023, 917 (920 f.).
[291] BVerfGE 152, 152 Rn. 104 ff. – Recht auf Vergessen I.
[292] BVerfGE 152, 152 Rn. 105 – Recht auf Vergessen I.

Grundrechtseingriff dar.[293] Im Rahmen der Verhältnismäßigkeit kommt es nicht nur auf den Zweck der Datenverarbeitung an, sondern auch auf die weiteren Risiken, die für die betroffenen Personen damit verbunden sind. Hierzu gehören etwa auch Regelungen zur Datensicherheit.[294] Diese hat das Gericht vor allem für die Speicherung und Übermittlung von Daten durch Private an staatliche Stellen vorgesehen. Diese Anforderungen müssen aber erst recht gelten, wenn der Staat Daten an Private übermittelt und sie damit seine unmittelbare Einflusssphäre verlassen. Den Gesetzgeber trifft in diesem Fall eine besondere **Folgenverantwortung** für die mit staatlichen Befugnissen erhobenen Daten.

aa) Regelungsinhalt

256 § 36 Abs.1 VSG NRW erlaubt die Übermittlung von Daten des Verfassungsschutzes zu den Zwecken nach § 26 Abs. 6 VSG NRW an private und öffentliche Stellen. Personenbezogene Daten sind dabei – wie schon nach § 26 Abs. 6 S. 1 VSG NRW – nur subsidiär zu verwenden. Mit nachrichtendienstlichen Mitteln erhobene Daten sind ausgeschlossen (§ 36 Abs. 3 VSG NRW). Zur Sicherung ist vorgesehen, dass nur Personen von den übermittelten Daten Kenntnis erhalten, die zur Verschwiegenheit verpflichtet worden sind und gegen unbefugte Kenntnisnahme Maßnahmen ergriffen worden sind.

bb) Problemaufriss

257 Die Regelung ist grundrechtlich und auch politisch mit Blick auf die Akzeptanz der Nutzung von KI und maschinellem Lernen durch Sicherheitsbehörden von größter Brisanz: Sie erlaubt, dass private Stellen von Informationen Kenntnis erhalten, die in höchsten Maße geheimhaltungsbedürftig sind – und zwar nicht nur von einzelnen Informationen, sondern potenziell von allen dem Verfassungsschutz vorliegenden Informationen, die nicht mit nachrichtendienstlichen Mitteln erhoben worden sind. Es handelt sich auch dann um höchst sensible Daten, z.B. eigene Ausarbeitungen des Verfassungsschutzes, Auskünfte nach §§ 7, 8 VSG NRW, Inhalte von ausgewerteten Speichermedien nach § 6 Abs. 4 S.1 2. Alt., Ergebnisse von Datenanalysen (vgl. § 26 Abs. 6 S. 4 VSG NRW) oder auch aus Sicherheits- und Zuverlässigkeitsüberprüfungen (§ 3 Abs. 4 VSG NRW).

---

[293] BVerfGE 162, 1 Rn. 230 – Bayerisches Verfassungsschutzgesetz m.w.N.
[294] Vgl. BVerfGE 155, 119 Rn. 128, 135, 188 – Bestandsdatenauskunft II zur verfassungsrechtlich gebotenen Datensicherheit.

258 Praktisch könnte diese Regelung bedeuten: Große Teile des Informationsbestandes des Verfassungsschutzes werden an *Palantir* übermittelt, um ein KI-Modell zu trainieren. Dabei ist nicht klar geregelt, nach welchen Kriterien die Anbieter ausgewählt werden. Mit Blick auf kritische Infrastruktur (Stichwort: Huawei) stellt sich hier etwa die Frage, ob Unternehmen ausgeschlossen werden können, die unter ausländischem Einfluss stehen oder die Daten eventuell außerhalb der EU bzw. des EWR verarbeiten und dort verpflichtet werden könnten, die übermittelten Daten an eine fremde Macht herauszugeben. Es ist auch nicht eindeutig geregelt, ob mit diesen Daten nur ein Modell trainiert werden soll, das exklusiv dem Verfassungsschutz zur Verfügung steht oder ob die Ergebnisse dieses Trainings auch Dritten zur Verfügung stehen könnten (z.B. anderen Regierungen).

cc) Verfassungsrechtliche Bewertung

259 § 36 VSG NRW ist unverhältnismäßig, weil die Regelung keine ausreichenden Sicherungen für die übermittelten Daten vorsieht. Hierbei kann es offenbleiben, ob es einen „Vorrang der Eigenentwicklung“ oder ein Verfassungsgebot der „digitalen Souveränität“ gibt.[295] Auch das Gericht hat in der Kooperation mit anderen Staaten und dem IT-Outsourcing eine Herausforderung gesehen:

> „Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte.“[296]

260 Es fehlt bereits an Regelungen, welche die Auswahl des Empfängers, d.h. des KI-Anbieters, adressieren und Kriterien festlegen, z.B. ob es sich um einen inländischen Anbieter handeln muss, wie ein Einfluss oder Zugriff fremder Mächte verhindert werden kann, wie eine lückenlose Datenschutzaufsicht sichergestellt sein kann und wie das Datenschutzniveau im Zielland ist. Bereits ein Vergleich mit einem „normalen“ Auftragsverarbeitungsverhältnis nach Art. 28 DSGVO bzw. § 62 BDSG zeigt, wie rudimentär § 36 VSG NRW ausgestaltet ist. Selbst wenn man in hier ein Auftragsdatenverhältnis nach § 60 Abs. 2 VSG NRW i.V.m. § 62 BDSG annehmen würde, wären diese Fragen nur unzureichend adressiert. Würde es sich allerdings um eine Auftragsdatenverarbeitung handeln, wäre eine Übermittlungsregelung unnötig.

---

[295] Dafür *Kelber/Bortnikov*, NJW 2023, 2000 (2002); S. *D. Meyer*, GSZ 2025, 156 (160 f.); *Bäuerle*, ZD 2025, 128 (131); für eine stärkere Eigenverantwortung des Staates auch *Kühne/Golla/Schäfer,* GSZ 2025, 272 (272).
[296] BVerfGE 165, 363 Rn. 100 – automatisierte Datenanalyse.

261 Geregelt ist auch nicht, welches Modell trainiert wird. Da die Daten Teil des Modells werden, muss – eigentlich selbstverständlich – klargestellt sein, dass auf dieses Modell niemand sonst Zugriff hat und nicht nur die übermittelten Daten, sondern auch das Modell beim Anbieter nach dem Training gelöscht wird.

4. Übermittlung nach § 33 Abs. 3 VSG NRW

262 Die Übermittlungsregelung des § 33 Abs. 3 VSG NRW verstößt gegen das Recht auf informationelle Selbstbestimmung, weil sie nicht verhältnismäßig im engeren Sinne ist. Sie stellt für die Übermittlung von Analyseergebnisse nach § 26 Abs. 1 bis 4 VSG NRW allein auf das Eingriffsgewicht bei der Erhebung ab. Dabei bleibt das besondere Eingriffsgewicht der Datenanalyse[297] nach § 26 Abs. 2 und vor allem § 26 Abs. 3 VSG NRW unberücksichtigt.[298]

263 Eine andere Behörde als ein Nachrichtendienst dürfte für Zwecke der Gefahrenabwehr diese Maßnahmen nur bei Vorliegen einer zumindest konkretisierten Gefahr anwenden. Nach dem Grundsatz der hypothetischen Datenneuerhebung[299] dürfen die Erkenntnisse aus einer automatisierten Datenanalyse von hohem Eingriffsgewicht daher nur unter diesen Voraussetzungen an eine andere Behörde übermittelt werden. Anderenfalls könnten die hohen Anforderungen für den Einsatz automatisierter Datenanalyse außerhalb der Nachrichtendienste umgangen werden.[300] Denn zwingend vorgesehen ist eine zumindest konkretisierte Gefahr nur für die Übermittlung an Gefahrenabwehrbehörden, wenn der Verfassungsschutz zur Erhebung nachrichtendienstliche Mittel eingesetzt hat. Eine Übermittlung an eine Behörde ohne Zwangsbefugnisse wäre daher auch zulässig, wenn keine konkretisierte Gefahr vorliegt. Dies entspricht aber nicht den Anforderungen des Gerichts.

264 Zudem können die ohne nachrichtendienstliche Mittel vom Verfassungsschutz mit weniger invasiven Mitteln zusammengetragenen und analysierten Informationen ein besonderes Gewicht haben, weil die Eingriffsschwellen des Verfassungsschutzes sehr niedrig sind und er verdeckt agiert. Dies hat das Gericht deutlich hervorgehoben[301] – obwohl hierbei noch

---

[297] BVerfGE 165, 363 Rn. 72 – automatisierte Datenanalyse.
[298] *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 27; hierzu auch *Till* in: Lukosek/Schlüter, Linien der Rechtsprechung des Bundesverfassungsgerichts, Band 7 (2024), S. 361 (386).
[299] BVerfGE 169, 130 Rn. 105, 111 – Hessisches Verfassungsschutzgesetz m.w.N.
[300] Zur Gefahr der Umgehung BVerfGE 162, 1 Rn. 171 – Bayerisches Verfassungsschutzgesetz.
[301] BVerfGE 162, 1 Rn. 238 ff. – Bayerisches Verfassungsschutzgesetz

nicht einmal die eingriffsvertiefenden Mittel einer automatisierten Datenanalyse im Raum standen.

5. Automatisierte Datenerhebung nach § 6 Abs. 4 S. 1 1. Alt. und S. 2 VSG NRW

265 Die Befugnis zur automatisierten Datenerhebung nach § 6 Abs. 4 S. 1 1. Alt. und S. 2 VSG NRW verstößt gegen das Recht auf informationelle Selbstbestimmung, weil sie nicht verhältnismäßig im engeren Sinne ist. Die vorgesehene Eingriffsschwelle ist unter Berücksichtigung der fehlenden weiteren Eingrenzungen nicht geeignet, einen potentiell so schwerwiegenden Eingriff zu rechtfertigen.

266 Zur Schwere des Eingriffs kann auf die Auswirkungen zu § 26 Abs. 2 VSG NRW verwiesen werden (→Rn. 230 ff.). Erschwerend kommt hier jedoch zum Tragen, dass die Regelung nicht nur zu einer besseren Erschließung der bereits erhobenen Daten ermächtigt, sondern zur automatisierten Erhebung.[302] § 6 Abs. 4 S. 1 1. Alt. VSG NRW erlaubt die automatisierte Erhebung von Daten. Die Quelle der Daten bleibt offen, ebenso das genaue Erkenntnisinteresse oder die Art der Erhebung. In der Begründung wird die Erhebung der allgemein zugänglichen Daten im Internet beispielhaft genannt. Die massenhafte Erhebung solcher Daten erhöht das Eingriffsgewicht noch einmal. Potentiell könnte die Verfassungsschutzbehörde damit mittels Webcrawling im gesamten Internet eine „Online-Rasterfahndung" durchführen. Ähnlich wie bei einer Rasterfahndung ist die Streubreite der Maßnahme sehr groß.[303]

267 Demgegenüber hat der Gesetzgeber die geringstmögliche Eingriffsschwelle gewählt. Diese erscheint wie schon im Rahmen des § 26 Abs. 2 VSG NRW zu niedrig, um einen Eingriff von dieser Intensität zu rechtfertigen.

[302] *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 8.
[303] *Löffelmann*, Landtag von Nordrhein-Westfalen, Stellungnahme 18/2751, S. 8.

E. Festlegung eines Gegenstandswertes

268 Die Beschwerdeführenden bitten das Gericht, einen angemessenen Gegenstandswert nach eigenem Ermessen festzulegen und verzichten hierzu auf weiteren Vortrag.

Sollte das Gericht zu einem oder mehreren Punkten zusätzliche Informationen benötigen, bitte ich **um einen entsprechenden Hinweis**.

Dr. Peter Schantz
Rechtsanwalt