Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Alt-Moabit 59-61, 10555 Berlin

Abgeordnetenhaus von Berlin
Ausschuss für Verfassungsschutz
Der Vorsitzende
Herrn Kurt Wansner

Nur per E-Mail:
VerfSch@parlament-berlin.de

Geschäftszeichen:	BlnBDI-262-3-41/2025-2
Telefon:	030 13889-0
Durchwahl-Nr.:	317
Datum:	12. September 2025

Stellungnahme zum Gesetz zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts (Abghs. Drucksache 19/2466 vom 26. Mai 2025)

Sehr geehrter Herr Wansner,
sehr geehrte Damen und Herren,

vielen Dank für die Einladung zur Anhörung im Rahmen der Sitzung des Ausschusses für Verfassungsschutz am 15. September 2025. Gemäß § 11 Abs. 1 Nr. 3, Abs. 2 Berliner Datenschutzgesetz (BlnDSG) nehme ich nachfolgend schriftlich Stellung zum Gesetz zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzrechts (Abghs. Drucksache 19/2466 vom 26. Mai 2025) und bitte Sie um Übermittlung der Stellungnahme an die Mitglieder des Ausschusses für Verfassungsschutz.

Die durch den Senat erarbeitete und ins Abgeordnetenhaus eingebrachte Vorlage zur Beschlussfassung sieht eine konstitutive Neufassung des Berliner Verfassungsschutzgesetzes vor. Der Gesetzentwurf beinhaltet dabei sowohl eine neue Normierung bereits bestehender Befugnisse der Verfassungsschutzbehörde als auch die Etablierung neuer nachrichtendienstlicher Maßnahmen, die zum Teil mit tiefen Eingriffen in das Recht auf informationelle Selbstbestimmung der Betroffenen verbunden sind.

Die BlnBDI ist anders als dies in der Vergangenheit bisher geübte Praxis war nicht vorab in den Änderungsprozess eingebunden worden. Vor dem Hintergrund der umfassenden Neuregelung mit erheblichen datenschutzrechtlichen Bezügen wäre eine frühzeitige Einbindung der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) angemessen gewesen.

Nach § 38 Satz 1 Verfassungsschutzgesetz Berlin (VSG Bln) i. V. m. § 11 Abs. 2 Satz 2 BlnDSG besteht eine gesetzliche Pflicht zur Anhörung der BlnBDI vor dem Erlass von Gesetzen, Rechtsverordnungen oder Verwaltungsvorschriften, wenn sie die Verarbeitung personenbezogener Daten betreffen. Sinn und Zweck dieser Vorschrift ist es, die Expertise der BlnBDI und die Institution als Kontrollbehörde zu einem Zeitpunkt einzubeziehen, zu dem realistisch auch noch umfangreiche Änderungen an dem Gesetzentwurf möglich sind. Solche Möglichkeiten ergeben sich auch noch im parlamentarischen Verfahren; gleichwohl müssen insbesondere auch die zeitlichen Rahmenbedingungen einen fundierten Abgleich mit dem Verfassungsrecht und der verfassungsgerichtlichen Rechtsprechung gerade bei so umfangreichen Änderungen ermöglichen. Dies sehe ich nicht gewährleistet, wenn eine Beteiligung zu umfangreichen Gesetzesänderungen erst zu einem späten Zeitpunkt erfolgt und die Anhörungsrechte der BlnBDI damit ausgehöhlt werden.

Angesichts des bereits eingeleiteten parlamentarischen Verfahrens und der insoweit gebotenen Eile für die Abgabe meiner Stellungnahme war eine umfassende Prüfung des vorliegenden Gesetzentwurfs nicht möglich. Nachfolgend beschränke ich mich insoweit auf einige wesentliche Änderungen bzw. die neu geregelten Befugnisse des Verfassungsschutzes. Weitere Stellungnahmen behalte ich mir ausdrücklich vor.

A. Grundsätzliche Anmerkungen

Mit dem hiesigen Entwurf (VSG Bln-E) soll ausweislich der Gesetzesbegründung einerseits die überfällige Umsetzung der Vorgaben des Bundesverfassungsgerichts zu den modifizierten Eingriffsschwellen für Überwachungsmaßnahmen und Datenübermittlungen aus den Entscheidungen des Bundesverfassungsgerichts zum Bayrischen Verfassungsschutzgesetz und zum Bundesverfassungsschutzgesetz aus dem Jahr 2022 erfolgen. Andererseits sieht der Entwurf aber auch eine massive Ausweitung von teils höchst eingriffsintensiven neuen Überwachungsbefugnissen für den Verfassungsschutz vor. So sollen u. a. Befugnisse der Verfassungsschutzbehörde zum Zugriff auf Videoüberwachungen des öffentlich zugänglichen Raums (§ 28 Abs. 3 VSG

Bln-E), zur Wohnraumüberwachung – auch bei Dritten (§ 49 VSG Bln-E) – sowie zur Online-Durchsuchung (§ 50 VSG Bln-E) geschaffen werden.

Das Bundesverfassungsgericht hat in verschiedenen Zusammenhängen, insbesondere aber in Bezug auf die Sicherheitsgesetzgebung, festgestellt, dass der Gesetzgeber jedenfalls verpflichtet ist, die Folgen seines Handelns und die Wirkungen der verabschiedeten Gesetze nach ihrem Inkrafttreten zu beobachten und im Hinblick auf notwendige Korrekturen oder Nachbesserungen zu überprüfen (BVerfG, Urteil v. 3.3.2004 - 1 BvR 2378/98 u. a., Rn. 213; BVerfG, Urteil v. 12.4.2005 - 2 BvR 581/01, Rn. 64). Die evidenzbasierte Gesetzgebung stellt ein wesentliches Qualitätsmerkmal moderner Rechtsetzung dar – insbesondere bei Eingriffen in Grundrechte. Evaluationsklauseln sind eine wichtige rechtsstaatliche Maßnahme, die eine wissenschaftlich fundierte, unabhängige Überprüfung der eingreifenden Befugnisse sicherstellt. Eine solche Evaluation dient nicht nur der Nachbesserung bestehender Normen, sondern auch der Legitimation grundrechtsintensiver Eingriffe. Evaluationsklauseln sieht der Gesetzentwurf bislang zu keiner Vorschrift vor. Jedenfalls zu den eingriffsintensiven neuen Befugnissen sollte eine Pflicht zur Evaluation gesetzlich festgelegt werden. Die zu evaluierenden Normen sollten gleichzeitig zeitlich befristet und im Rahmen der Evaluierung sollte durch den Gesetzgeber über ihre Weiterbefristung oder Entfristung entschieden werden.

Angesichts des grundsätzlichen Gewichts von heimlichen Grundrechtseingriffen durch die Nachrichtendienste sowie die Polizei einschließlich der Speicherung und Nutzung der dadurch gewonnenen Daten hat das Bundesverfassungsgericht aus den betroffenen Grundrechten und dem Verhältnismäßigkeitsgrundsatz das Erfordernis einer Kompensation für die mangelnde Transparenz gegenüber den Betroffenen und den damit verbundenen Einschränkungen des individuellen Rechtsschutzes abgeleitet (BVerfG, Urteil v. 24.4.2013 – 1 BvR 1215/07 – Rn. 204 ff.). Als Instrumente zur Herstellung einer (nachträglichen) Transparenz der Datenverarbeitung kommen Auskunftsrechte, Benachrichtigungspflichten sowie eine effektive Aufsicht und Kontrolle durch die Datenschutzbehörden in Betracht. Darüber hinaus sind parlamentarische Berichtspflichten Voraussetzung für die gesetzgeberisch zu gewährleistende Transparenz und demokratische Kontrolle bei tief in die Privatsphäre eingreifenden Ermittlungs- und Überwachungsbefugnissen mit spezifisch breitenwirksamem Grundrechtsgefährdungspotential (vgl. BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 u. a., Rn. 143).

Das Auskunftsrecht betroffener Personen soll durch die hier vorgeschlagene Regelung (§ 53 VSG Bln-E) künftig deutlich eingeschränkt werden (s. hierzu ausführlich unter B.). Zu den Berichtspflichten der Verfassungsschutzbehörde sieht der Gesetzentwurf mit § 60 VSG Bln-E zwar eine Regelung vor. Jedoch beinhaltet diese eine Unterrichtung des Abgeordnetenhauses bzw. seines Ausschusses für Verfassungsschutz nur in Bezug auf Auskunftsersuchen der Verfassungsschutzbehörde zu Verkehrs-, Nutzungs- und weiteren Daten nach §§ 20, 21 VSG Bln-E. Die parlamentarischen Berichtspflichten sollten insoweit dringend in Bezug auf weitere grundrechtsintensive Maßnahmen des Verfassungsschutzes erweitert werden. Dies gilt insbesondere für die Wohnraumüberwachung, die Online-Durchsuchung, die Ausleitung von Videoüberwachung und langfristige Observationen sowie den verdeckten Einsatz von Dienstkräften und Vertrauensleuten. Die Benachrichtigung der von einer nachrichtendienstlichen Maßnahme betroffenen Personen bestimmt der Gesetzentwurf gemäß § 52 Abs. 2 VSG Bln-E nur für einzelne Maßnahmen – die Wohnraumüberwachung und Online-Durchsuchung – ausdrücklich. Als kompensatorische Maßnahme sollte jedoch auch für andere besonders eingriffsintensive Überwachungsbefugnisse die Benachrichtigungspflicht gesetzlich normiert werden, wie z. B. für die Bestandsdatenauskunft, den verdeckten Einsatz von Dienstkräften und Vertrauensleuten sowie langfristige Observationen (s. hierzu im Einzelnen unter B.) Das Bundesverfassungsgericht leitet aus dem betroffenen Grundrecht i. V. m. Art. 19 Abs. 4 GG die grundsätzliche Verpflichtung ab, nach Beendigung einer verdeckt durchgeführten Überwachungsmaßnahme die Betroffenen zu benachrichtigen (vgl. u. a. BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 u. a., Rn. 134 ff.). Für die Nachrichtendienste gelten zwar Besonderheiten, aber keine generelle Ausnahme (BVerfG, Urteil v. 19.5.2020 - 1 BvR 2835/17, Rn. 267). Demnach gehört zu den Anforderungen an die verhältnismäßige Ausgestaltung der jeweiligen Überwachungsmaßnahmen stets auch die gesetzliche Anordnung von Benachrichtigungspflichten. Das Bundesverfassungsgericht verbindet hierbei den in Art. 19 Abs. 4 GG unmittelbar gründenden subjektiven Zweck der Ermöglichung eines nachträglichen Rechtsschutzes mit den objektiven Zwecken, durch Transparenz Vertrauen in der Öffentlichkeit zu schaffen und einen demokratischen Diskurs über die Maßnahmen zu ermöglichen (stRspr, vgl. BVerfGE, Urteil v. 19.5.2020 - 1 BvR 2835/17, Rn. 269 m.w.N.). Ausnahmen kann der Gesetzgeber in Abwägung mit verfassungsrechtlich geschützten Rechtsgütern Dritter vorsehen, die jedoch auf das unbedingt Erforderliche zu beschränken sind (BVerfG, Beschl. v. 12.10.2011, - 2 BvR 236/08 u. a., Rn. 227). Denkbar sind Ausnahmen von den Benachrichtigungspflichten etwa, wenn die Kenntnis von der Maßnahme dazu führen würde, dass diese ihren Zweck verfehlt, wenn die Benachrichtigung nicht ohne Gefährdung von Leib und Leben einer Person geschehen kann, oder wenn ihr

überwiegende Belange einer betroffenen Person entgegenstehen, z. B. weil durch die Benachrichtigung von einer Maßnahme, die keine weiteren Folgen gehabt hat, der Grundrechtseingriff noch vertieft würde (vgl. u. a. BVerfG, Urteil v. 20.4.2016 - 1 BvR 966/09 u. a., Rn. 136). Es sollte eine zentrale Norm zur Benachrichtigung der Betroffenen in das VSG Bln aufgenommen werden (vgl. BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 134).

Je nach Eingriffsintensität der Maßnahmen kann sich aus dem Verhältnismäßigkeitsgrundsatz außerdem die Notwendigkeit ergeben, die Maßnahme vor ihrer Durchführung einer Kontrolle zu unterziehen (BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 181 und 213). Für die Wohnraumüberwachung ergibt sich dies schon aus Art. 13 Abs. 4 GG. Daneben gilt dies aber auch für andere eingriffsintensive Überwachungsmaßnahmen, bei denen damit zu rechnen ist, dass sie auch höchstprivate Informationen erfassen, und die gegenüber den Betroffenen heimlich durchgeführt werden. Auch die Dauer der Maßnahme ist zu berücksichtigen (BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 220). Die Kontrolle muss durch eine unabhängige Stelle erfolgen, beispielsweise in Form einer richterlichen Anordnung (BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 214). Der Gesetzgeber hat die Kontrollen in spezifischer und normenklarer Form zu regeln. Regelmäßig erforderlich ist eine Kontrolle bei längerfristigen Observationen (insbes. mit Bildaufzeichnungen), der Erfassung nichtöffentlicher Gespräche und dem Einsatz von Vertrauenspersonen (BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 219). Das Erfordernis einer (richterlichen) Kontrolle wurde im VSG Bln-E nur teilweise umgesetzt (s. hierzu im Einzelnen unter B.).

Ein weiterer Aspekt der Verhältnismäßigkeit bei der Sicherheitsgesetzgebung ist die gesetzliche Formulierung von Eingriffsschwellen und Anforderungen an den Rechtsgüterschutz abhängig vom Eingriffsgewicht und dem jeweils betroffenen Grundrecht. Das Bundesverfassungsgericht misst der verhältnismäßigen Ausgestaltung der Eingriffsschwellen große Bedeutung zu, geht jedoch auch davon aus, dass das Eingriffsgewicht der Überwachungsmaßnahme einer Verfassungsschutzbehörde im Vergleich zu Polizeibehörden grundsätzlich geringer ist, weil dieser operative Anschlussbefugnisse fehlen, die mit Zwang durchgesetzt werden könnten (vgl. u. a. BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17 sowie Beschl. v. 9.12.2022 – 1 BvR 1345/21). Aus der spezifischen Funktionalität der Nachrichtendienste als „Frühwarnsystem“ und dem Ausschluss (polizeilicher) Zwangsbefugnisse folgt, dass die Nachrichtendienste zur Erfüllung ihres Beobachtungsauftrags grundsätzlich nicht an Eingriffsschwellen wie die konkrete Gefahr oder den Anfangsverdacht gebunden sind. Sie können und sollen Aufklärung schon im Vorfeld von Gefährdungslagen betreiben, um die politischen Entscheidungsträger

frühzeitig und angemessen zu informieren, sodass grundsätzlich eine „den Beobachtungsbedarf auslösende Bedrohungslage“ bzw. eine „beobachtungsbedürftige Bedrohungslage von Verfassungsschutzgrundsätzen genügt (BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 163.) Dem für polizeiliche Maßnahmen geltenden Erfordernis einer konkretisierten Gefahr entspricht daher als verfassungsschutzspezifische Eingriffsschwelle die konkretisierte Beobachtungsbedürftigkeit, die „hinreichende tatsächliche Anhaltspunkte“ dafür voraussetzt, dass die jeweilige Überwachungsmaßnahme „zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung im Einzelfall geboten“ ist („Erfordernis eines verfassungsschutzspezifischen Aufklärungsbedarfs“ – BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17). Für nachrichtendienstliche Befugnisse von erheblicher Eingriffsintensität sind jedoch höhere Anforderungen vorzusehen. Der Gesetzgeber muss daher Befugnisnormen, die Grundrechtseingriffe von erheblichem Gewicht erlauben, an eine qualifizierte Eingriffsschwelle knüpfen, die eine Schutzgutsgefährdung von vergleichbarem Gewicht voraussetzt, d.h. eine hinreichend erhebliche Beobachtungsbedürftigkeit (oder auch „gesteigerte Beobachtungsbedürftigkeit“ – vgl. BVerfG, Beschl. v. 17.7.2024 – 1 BvR 2133/22, Rn. 97, 136, 143, 149 u. 188; BVerG, Beschl. v. 28.9.2022 - 1 BvR 2354/13, Rn. 119; BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 193 f., 197, 213, 222, 328 u. 359 f.). Zu den eingriffsintensiven Maßnahmen gehören demnach etwa langfristige Observationen, die Erfassung nichtöffentlicher Gespräche, der Einsatz von Vertrauenspersonen und verdeckt agierenden Mitarbeiter:innen des Verfassungsschutzes sowie die Online-Durchsuchung. Nicht bei allen hiesigen Regelungen werden die Eingriffsschwellen ausreichend spezifisch geregelt (vgl. unter B. 10. zu § 28 Abs. 3 VSG Bln-E).

Modifizierte Anforderungen der Eingriffsschwellen für weitreichende heimliche Überwachungsmaßnahmen einer Verfassungsschutzbehörde, können verfassungsrechtlich jedoch nur gerechtfertigt werden, wenn die aus der jeweiligen Überwachung gewonnenen Informationen nicht ohne Weiteres an andere Behörden mit operativen Anschlussbefugnissen übermittelt werden dürfen (Zum „informationellen Trennungsprinzip“ vgl. BVerfG, Urteil vom 24.4.2013 – 1 BvR 1215/07, Rn. 123). Ansonsten böte der Umstand, dass die Verfassungsschutzbehörde selbst nicht über operative Anschlussbefugnisse verfügt, den überwachten Personen am Ende doch kaum Schutz (BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 171): Die der Verfassungsschutzbehörde verschlossenen eingriffsintensiven Folgemaßnahmen könnten dann von operativ ausgestatteten Behörden durchgeführt werden, die dabei die durch die Verfassungsschutzbehörde erlangten Informationen weiternutzten, ohne dass die für sie selbst als operative Behörden geltenden Datenerhebungsvoraussetzungen erfüllt sein müssten.

Somit sind modifizierte Anforderungen an heimliche Überwachungsmaßnahmen einer Verfassungsschutzbehörde nur dann verfassungsgemäß, wenn Übermittlungen der aus nachrichtendienstlichen Maßnahmen erlangten Informationen an andere Stellen an Bedingungen gebunden sind, die den Anforderungen genügen, die von Verfassungs wegen an entsprechende eigene Grundrechtseingriffe der empfangenden Stellen zu richten sind („Kriterium der hypothetischen Datenneuerhebung“ – vgl. BVerfG, Urteil v. 20.04.2016 - 1 BvR 966/09 u. a., Rn. 287 ff.).

Danach unterliegt eine weitere Verwendung der von Nachrichtendiensten gesammelten Daten durch Gefahrenabwehrbehörden Anforderungen an das damit zu schützende Rechtsgut und an die sogenannte Übermittlungsschwelle, die mit den Anforderungen vergleichbar sind, die an eine erneute Erhebung der übermittelten Daten durch die empfangende Behörde zu stellen wären. Schutzgut- und Schwellenerfordernis zusammen bewahren die Betroffenen so vor einer Umgehung grundrechtsschützender Eingriffsvoraussetzungen (BVerfG Urteil vom 26.4.2022 – 1 BvR 1619/17, Rn. 173). In den im Unterabschnitt 6 des Entwurfs geregelten Vorschriften zu den Datenübermittlungen wurden die verfassungsrechtlichen Vorgaben nur bedingt eingehalten (s. hierzu unter B. 13.).

B. Datenschutzrechtliche Anmerkungen zu einzelnen Vorschiften

1. Definition der Aufgaben des Verfassungsschutzes- §§ 5, 9, 12 VSG Bln-E und Begriffsbestimmungen – § 6 VSG Bln-E

Die Aufgaben der Verfassungsschutzbehörde waren bisher im Wesentlichen in einer Vorschrift zusammengefasst (§ 5 VSG Bln). Nunmehr sollen die Aufgaben zum einen auf mehrere Normen verteilt werden (§§ 5, 9 und 12 VSG Bln-E). Zum anderen wird hinsichtlich zentraler Begrifflichkeiten bei der Aufgabenbeschreibung lediglich auf die Bezeichnung im Bundesverfassungsschutzgesetz (BVerfSchG) verwiesen, statt diese im Gesetzentwurf konkret auszuführen. Beispielsweise werden die „Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben“, auf die sich die Befugnis der Informationssammlung und -auswertung bezieht, nicht mehr ausdrücklich im VSG Bln-E benannt, sondern es erfolgt ein Verweis auf § 3 Abs. 1 Nr.1 BVerfSchG. Dies führt dazu, dass an einigen Stellen im Gesetzentwurf Doppelverweisungen enthalten sind (bspw. in § 13 Abs. 1 Satz 1

VSG Bln-E, worin auf Tätigkeiten nach § 5 Abs. 2 Nr. 2 VSG Bln-E Bezug genommen wird, während hierin wiederum auf § 3 Abs. 1 Nr. 2 BVerfSchG verwiesen wird). Ähnlich ist dies bei den näheren Begriffsbestimmungen in § 6 Abs. 1 VSG Bln-E. Hier verweist der Gesetzentwurf pauschal auf die Bestimmung in § 4 Abs. 1 Satz 1 bis 4 und Abs. 2 BVerfSchG. Darüber hinaus erklärt § 6 Abs. 2 VSG Bln-E die Anwendbarkeit der Begriffsbestimmungen des BVerfSchG auf die übrigen Vorschriften, es sei denn, dass im VSG Bln-E eine abweichende Begriffsbestimmung vorsieht.

Diese Regelungstechnik vergleichsweise schwer auffindbarer Verweisungen in andere Gesetze ist unter dem Gesichtspunkt der Normenklarheit bedenklich und erschwert die Verständlichkeit der Vorschriften im gesamten Gesetzentwurf erheblich. Durch die Verweisungen auf bundesgesetzliche Regelungen würde der Berliner Gesetzgeber zudem die Definitionshoheit für die Bestimmung maßgeblicher Aufgaben des Verfassungsschutzes aus der Hand geben, auch wenn § 6 Abs. 2 Satz 2 VSG Bln-E eine abweichende Begriffsbestimmung zulässt. In jedem Fall birgt dies die Gefahr einer unklaren Rechtslage durch potentiell auseinanderfallende Begriffsbestimmungen. Es wird daher empfohlen, die Definitionen wieder unmittelbar in das VSG Bln aufzunehmen und von Verweisungen auf das BVerfSchG abzusehen. Dies dient auch dazu, dass die Einhaltung des Gesetzes in der Praxis unterstützt wird.

2. Nutzung personenbezogener Daten für andere Zwecke – § 11 Abs. 3 VSG Bln-E

Der Wortlaut der Regelung erlaubt die zweckändernde Nutzung personenbezogener Daten („für einen anderen in Absatz 1 genannten Zweck“). So steht es auch im ersten Satz der Gesetzesbegründung. Allerdings ist im Folgenden in der Gesetzesbegründung lediglich von einer „Weiternutzung“ die Rede. Die Nutzungsformen einer zweckkonformen Weiternutzung und einer zweckändernden Nutzung personenbezogener Daten werden in der Begründung nicht sauber getrennt. Dies ist insofern problematisch, da das Bundesverfassungsgerichts jeweils unterschiedliche Anforderungen für entsprechende Rechtsgrundlagen formuliert hat, die es zu beachten gilt (vgl. BVerfG, Urteil v. 20.4.2016 – 1 BvR 966/09 u. a., Rn. 275 ff.).

In der Gesetzesbegründung ist insoweit klarzustellen, welche Nutzungsform hier tatsächlich geregelt werden soll.

3. Auskunftsersuchen zu Bestands- und gleichstehenden Daten – § 19 VSG Bln-E

Während die (bundesgesetzlichen) Schwellen für die Übermittlung von Bestandsdaten an Sicherheitsbehörden (erste Tür) im Telekommunikationsgesetz (TKG) geregelt sind, soll durch

§ 19 VSG Bln-E die Datenabrufbefugnis durch die Verfassungsschutzbehörde (zweite Tür) geregelt werden. Ich begrüße insoweit, dass mit der Vorschrift die Vorgaben des Bundesverfassungsgerichts zum sog. Doppeltürmodell umgesetzt werden sollen. Allerdings entspricht die Vorschrift nicht den materiellrechtlichen Vorgaben des Bundesverfassungsgerichts und ist damit unverhältnismäßig. Zwar kann es bei der Verwendung der Daten durch Nachrichtendienste bereits genügen, dass eine Auskunft zur Aufklärung einer bestimmten, nachrichtendienstlich beobachtungsbedürftigen Aktion oder Gruppierung geboten ist, da hiermit ein wenigstens der Art nach konkretisiertes und absehbares Geschehen vorausgesetzt wird. Allerdings ist grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr erforderlich (BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13).

Die Vorschrift des § 19 Abs. 1 Satz 1 VSG Bln-E ermächtigt hingegen die Verfassungsschutzbehörde allgemein, Auskünfte bei Anbietern der Telekommunikation zum Zweck der Aufklärung einer Bestrebung oder Tätigkeit nach § 5 Abs. 2 VSG Bln-E einzuholen. Es fehlt an einer Beschränkung auf den Einzelfall, mithin die Maßgabe, dass das Auskunftsverlangen nur erfolgen darf, wenn die Daten zur Aufklärung tatsächlich erforderlich sind. Nicht ausreichend ist, dass dies in der Gesetzesbegründung (Abghs. Drucksache 19/2466, Seite 53) am Rande erwähnt wird. Eine entsprechende Formulierung zur Erforderlichkeit im Einzelfall ist daher direkt in den Gesetzestext aufzunehmen (z. B. „Soweit dies zur Aufklärung einer Bestrebung oder Tätigkeit nach § 5 Absatz 2 im Einzelfall erforderlich ist, darf die Verfassungsschutzbehörde […]“). Gleiches gilt für die Bestandsdatenabfrage gegenüber den Anbietern von Telediensten nach § 19 Abs. 2 VSG Bln-E.

Nach § 19 Abs. 1 Satz 1 Nr. 3 VSG Bln-E darf der Verfassungsschutz auch besonders qualifizierte Bestandsdaten erheben. Dies sind solche der Zugriffssicherung (Zugangsdaten), die dazu dienen, den Zugriff Fremder auf das Endgerät oder den Speicher zu verhindern. Hierunter fallen zum Beispiel Passwörter, PIN und PUK, Fingerabdruck-Daten und jede andere Art von Zugriffscodes. Die Erhebung solcher Zugangsdaten darf gemäß der Rechtsprechung des Bundesverfassungsgerichts nur dann erfolgen, wenn auch die Voraussetzungen für die Nutzung dieser Daten gegeben sind (BVerfG, Beschl. v. 24.1.2012 – 1 BvR 1299/05, Rn 185). Der Akzessorietät zur Nutzungsbefugnis wird durch § 19 Abs. 1 Satz 2 VSG Bln-E Rechnung getragen.

Allerdings ist zu beanstanden, dass weder für die Abfrage von Zugangsdaten noch für die Erhebung der übrigen Bestandsdaten nach § 19 Abs. 1 und Abs. 2 VSG Bln-E eine vorherige Anordnung durch die Leitung des Verfassungsschutzbehörde festgelegt ist. Dieses Erfordernis ist nach der besonderen Verfahrensvorschrift des § 22 Abs. 1 VSG Bln-E nur für die Auskünfte nach §§ 20 und 21 VSG Bln-E vorgesehen, wobei es sich hier um ein redaktionelles Versehen handeln könnte, da sowohl in der Überschrift zu § 22 VSG Bln-E als auch in der Gesetzesbegründung hierzu auch auf § 19 VSG Bln-E Bezug genommen wird. In jedem Fall sollte dringend eine Änderung erfolgen.

Zusätzlich empfehle ich entsprechend § 10 Abs. 4 BKAG aufgrund des erhöhten Eingriffsgewichts den Abruf der Zugangsdaten auch unter den Vorbehalt einer richterlichen Anordnung zu stellen. Hierdurch wird dem Rechtsschutzbedürfnis der Betroffenen Rechnung getragen, indem sichergestellt wird, dass kein heimlicher Zugriff ohne richterliche Zustimmung erfolgt.

Darüber hinaus wird, auch gerade angesichts des bislang fehlenden Vorbehalts einer gerichtlichen Prüfung sehr kritisch gesehen, dass als Kompensation für die heimlichen Überwachungsbefugnisse nach § 19 VSG Bln-E auch keine nachträgliche Benachrichtigungspflicht an die betroffene Person gesetzlich statuiert wird. Diese Pflicht sollte ebenfalls ergänzt werden (vgl. insoweit § 8d Abs. 4 BVerfSchG und Art. 17 Abs. 3 Satz 3 BayVSG sowie § 10 Abs. 5 BKAG).

4. Auskunft zu Verkehrs- und Nutzungsdaten – § 20 VSG Bln-E

Die Regelung sieht die Abfrage von sog. Verkehrs- und Nutzungsdaten vor und gestattet dem Verfassungsschutz damit, unter bestimmten Voraussetzungen auch in den Bereich des durch Art. 10 GG besonders geschützten Brief-, Post- und Fernmeldegeheimnisses eingreifen zu dürfen.

a) <u>Bestandsdatenauskunft mittels dynamischer IP-Adressen</u>

Die Befugnis nach § 20 Abs. 1 VSG Bln-E steht im engen Zusammenhang mit § 19 Abs. 1 VSG Bln-E. Gemeint ist hier eine Bestandsdatenauskunft auf Basis einer automatisierten Verkehrsdatenauswertung in Form der Auswertung dynamischer IP-Adressen (Internet-Protocol-Adress). Die Bestandsdatenabfrage anhand einer dynamischen IP-Adresse hat ein gegenüber der allgemeinen Bestandsdatenauskunft erhöhtes Eingriffsgewicht (BVerfG, Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. a., Rn. 165 ff.), da es sich hierbei um ein zu einer spezifischen

Kommunikation in Verbindung stehendes Datum handelt, welches unter den Schutz des Telekommunikationsgeheimnisses zu stellen ist (BVerfG, Beschl. v. 12.1.2012 – 1 BvR 1299/05, Rn. 116 ff.; zuletzt auch BVerfG Beschl. v. 27.5.2020 – 1 BvR 1873/13 u. a., Rn. 165 ff.). Eine Auskunft an den Verfassungsschutz beinhaltet demnach stets eine personenbezogene Information in Bezug auf einen bestimmten Telekommunikationsvorgang bzw. auf ein bestimmtes Nutzungsverhalten dieser Person zu einem bestimmten Zeitpunkt. Zudem setzt die Zuordnung dynamischer IP-Adressen zu bestimmten Anschlüssen eine Verarbeitung von Verkehrsdaten seitens der Auskunft gebenden Stelle voraus.

Durch den Verweis in § 20 Abs. 1 VSG Bln-E auf § 19 VSG Bln-E sind in Bezug auf die Bestandsdatenabfrage anhand dynamischer IP-Adressen die dort genannten Voraussetzungen zugrunde zu legen, sodass auf die vorzunehmenden ergänzenden Anforderungen unter 3. verwiesen wird. Wie bei den Auskünften nach § 19 VSG Bln-E sollte auch hier insbesondere eine nachträgliche Benachrichtigungspflicht an die betroffene Person gesetzlich festgelegt werden (vgl. insoweit § 8d Abs. 4 BVerfSchG und Art. 17 Abs. 3 Satz 3 BayVSG).

b) Verkehrs- und Nutzungsdatenauskünfte

§ 20 Abs. 2 VSG Bln-E gestattet die Abfrage von Verkehrs- und Nutzungsdaten bei Post-, Telekommunikations- und Telemediendienstleistern zur Aufklärung einer „Bestrebung von erhöhter Beobachtungsbedürftigkeit“. Ebenso wie bei § 19 Abs. 1 Satz 1 VSG Bln-E fehlt es an einer Festlegung der Erforderlichkeit (s. bereits unter 3.). Die Einholung der Auskunft muss im Einzelfall zur Aufklärung erforderlich sein. Eine entsprechende Formulierung (z. B. „soweit dies zur Aufklärung einer [...] im Einzelfall erforderlich ist“) ist daher in das Gesetz aufzunehmen. Ferner wird ebenfalls die Regelung einer Pflicht zur Benachrichtigung empfohlen (s. ebenfalls bereits unter 3.; vgl. insoweit auch Art. 17 Abs. 3 Satz 3 BayVSG).

5. Weitere Auskunftsersuchen – § 21 VSG-Bln-E

Die Vorschrift regelt zum einen Auskunftsersuchen gegenüber Luftfahrtunternehmen und Finanz- sowie Kreditinstituten (§ 21 Abs. 1 VSG Bln-E) und zum anderen Auskunftsersuchen gegenüber dem Bundeszentralamt für Steuern, das bei den Kreditinstituten eine Abfrage in dem gemäß § 93b Abs. 1 Abgabenordnung zu führenden Dateisystem vornehmen kann (§ 21 Abs. 2 VSG Bln-E). Wie bei § 19 und § 20 VSG Bln-E fehlt es zwar nach dem Wortlaut an einer Eingrenzung auf die Erforderlichkeit im Einzelfall (s. bereits unter 3. und 4.). Allerdings enthält § 21 Abs. 1 Satz 2 VSG Bln-E erfreulicherweise eine Einschränkung, wonach die Befugnis zur Einholung der Auskünfte nur besteht, wenn tatsächliche Anhaltpunkte vorliegen, die es möglich

erscheinen lassen, dass die Schutzgüter des Verfassungsschutzes konkret bedroht sind und dass das gegen sie gerichtete Handeln erfolgreich sein kann (vgl. BVerfG, Beschl. v. 17.7.2024 – 1 BvR 2133/22). Hierdurch wird eine nach der Rechtsprechung des Bundesverfassungsgerichts hinreichende Eingriffsschwelle vorgesehen. Es sollte in Bezug auf die Auskünfte nach § 21 VSG Bln-E eine Regelung zur Benachrichtigung der Betroffenen vorgesehen werden (s. bereits unter 3. und 4.; vgl. insoweit auch Art. 17 Abs. 3 Satz 3 BayVSG).

6. Verfahren zu den besonderen Auskünften – § 22 VSG Bln-E

Die Vorschrift beinhaltet besondere Verfahrensvorschriften für die §§ 19 bis 21 VSG Bln-E, insoweit wird auf die Ausführungen zu diesen Normen verwiesen (s. hierzu bereits unter 3. bis 5.). Da § 174 Abs. 2 Satz 1 TKG die Auskunftserteilung durch den Telekommunikationsdiensteanbieter unter die Maßgabe stellt, dass die Auskunft ersuchende Stelle den Antrag schriftlich oder elektronisch unter Angabe einer Rechtsgrundlage für die Datenerhebung stellt, sollte in § 22 VSG Bln-E zudem eine insoweit klarstellende Regelung für das entsprechende Vorgehen durch den Verfassungsschutz aufgenommen werden.

7. Verdeckt eingesetzte Dienstkräfte - § 26 VSG Bln-E

§ 26 Abs. 1 Satz 7 VSG Bln-E regelt zwar, dass bundesverfassungsgerichtlich geforderte Verbot, intime oder vergleichbar engste persönliche Beziehungen zu Zielpersonen einzugehen. Darüber hinaus fehlt aber eine Regelung dazu, dass der Einsatz eines verdeckten Mitarbeiters oder einer verdeckten Mitarbeiterin abzubrechen ist, wenn intime Beziehungen oder vergleichbar engste persönliche Bindungen begründet werden. Zudem ist gemäß dem Bundesverfassungsgericht auch vorzusehen, dass der Einsatz (komplett oder temporär) abzubrechen ist, wenn erkennbar wird, dass in den Kernbereich privater Lebensgestaltung eingedrungen wird. Dabei kann es unter Umständen ausreichen, dass lediglich die kernbereichsrelevante Kommunikation oder Interaktion abgebrochen wird (vgl. BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 113). Eine Ausnahme kann für Fälle vorgesehen werden, wenn durch einen Abbruch Leib oder Leben der verdeckt Ermittelnden in Gefahr geriete (vgl. BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 115). Sofern festgestellt wird, dass der Kernbereich privater Lebensgestaltung berührt ist und die Daten daher zu löschen sind, ist danach zu prüfen, ob der Einsatz weiter fortgeführt werden kann (vgl. BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 119). Auch wenn sich das hier zitierte Urteil des Bundesverfassungsgerichts (BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21) auf ein Gesetz über die öffentliche Sicherheit und Ordnung (in Mecklenburg-Vorpommern) bezieht, sind die Erwägungen auf den Bereich des Verfassungsschutzes übertragbar, da es sich um Maßnahmen der höchsten Eingriffsstufe

handelt (Eingriff in den Kernbereich privater Lebensgestaltung), für die keine andere Bewertung verfassungsrechtlich angezeigt ist (Vgl. BVerfG, Beschl. v. 9.12.2022 – 1 BvR 1345/21, Rn. 175). Die Vorschrift des § 26 VSG Bln-E ist somit entsprechend zu ergänzen. Die Regelung des § 15 VSG Bln-E wird insoweit nicht als ausreichend spezifisch erachtet, zumal hier lediglich von einer Unterbrechung der Maßnahme die Rede ist.

§ 26 Abs. 5 Satz 1 VSG Bln-E sieht eine Anordnungspflicht durch die Leitung der Abteilung für Verfassungsschutz in Fällen des § 26 Abs. 1 Satz 1 und Satz 2 Nr. 1 und 2 VSG Bln-E vor. Grund und Umfang des Einsatzes sind bei der Anordnung zu dokumentieren und die Anordnung ist zu befristen, wobei das Höchstmaß der Frist zwölf Monate beträgt (§ 26 Abs. 5 Satz 2 und 3 VSG Bln-E). Allerdings darf der Anordnung gemäß § 26 Abs. 5 Satz 4 VSG Bln-E eine „Vorbereitungs- und Einführungszeit“ von zwölf Monaten vorausgehen, worüber die Leitung der Abteilung für Verfassungsschutz entscheiden kann. Dabei ist unklar, welche Aktivitäten und Handlungen die „Vorbereitungs- und Einführungszeit“ umfasst und welche Voraussetzungen hierfür vorliegen müssen. Es ist insoweit zu befürchten, dass hierdurch die Möglichkeit des voraussetzungslosen Einsatzes verdeckter Dienstkräfte geschaffen wird, ähnlich einer „Testphase“, in der jedoch bereits verdeckte Ermittlungen i. S. v. § 26 Abs. 1 VSG Bln-E stattfinden. Das Bundesverfassungsgericht hat in Bezug auf den Einsatz von Vertrauenspersonen (s. hierzu ebenfalls unter 8.) ausdrücklich klargestellt, dass bereits in einer vorgelagerten Anwerbungszeit ein hinreichender verfassungsschutzspezifischer Aufklärungsbedarf bestehen muss (vgl. BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 353). Dies ist auf die hier vorgesehene Vorbereitungs- und Einführungszeit übertragbar. Bereits während dieser Phase müssen daher tatsächliche Anhaltspunkte dafür vorliegen, dass es eine (mindestens) beobachtungsbedürftige Bestrebung gibt. Anderenfalls könnte die Regelung des § 26 Abs. 1 VSG Bln-E in den ersten zwölf Monaten einer Maßnahme umgangen und der auf maximal zwölf Monate befristete Einsatz von verdeckten Dienstkräften ggf. auf den doppelten Zeitraum ausgeweitet werden. Die Regelung in § 26 Abs. 5 Satz 4 und 5 VSG Bln-E sollte daher gestrichen oder eine entsprechende gesetzliche Klarstellung getroffen werden.

Zur Wahrung der Verhältnismäßigkeit der Überwachungsmaßnahme sind beim Einsatz verdeckter Dienstkräfte in bestimmten Fällen Benachrichtigungspflichten als kompensatorischer Ausgleich gegenüber den Betroffenen vorzusehen. Aufgrund ihrer erhöhten Eingriffsintensität sind zumindest Maßnahmen der gezielten Überwachung einer Person nach § 26 Abs. 1 Satz 2 Nr. 2 VSG Bln-E bzw. des gezielten Einsatzes in zu privaten Wohnzwecken genutzten Räum-

lichkeiten nach § 26 Abs. 1 Satz 2 Nr. 4 VSG Bln-E der Zielperson bzw. dem Wohnungsinhaber grundsätzlich nach Beendigung der Maßnahme mitzuteilen. Hiervon können Ausnahmen vorgesehen werden, z. B. die Mitteilung zu einer Gefährdung der eingesetzten menschlichen Quelle führen würde (s. bereits unter A.). Eine entsprechende gesetzliche Benachrichtigungspflicht betroffener Personen ist auch in Bezug auf den Einsatz von verdeckt eingesetzten Dienstkräften zu ergänzen (vgl. Art. 18 Abs. 3 Satz 3 BayVSG).

8. Einsatz von Vertrauensleuten - § 27 VSG Bln-E

Laut § 27 Abs. 1 Satz 2, Halbsatz 1 VSG Bln-E soll der Anordnung des Einsatzes von Vertrauensleuten eine Anwerbungs- und Erprobungszeit von zwölf Monaten vorausgehen dürfen. Das Bundesverfassungsgericht hat zwar grundsätzlich anerkannt, dass eine solche Anwerbungszeit sinnvoll sein kann, um sich zu vergewissern, dass die entsprechenden Personen tatsächlich den erwartbaren Erkenntnisgewinn liefern können. Dennoch hat das Gericht auch für die Anwerbungszeit festgelegt, dass von Anfang an ein hinreichender verfassungsschutzspezifischer Aufklärungsbedarf bestehen muss (Vgl. BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 353). Bereits während der Anwerbungsphase müssen daher schon tatsächliche Anhaltspunkte dafür vorliegen, dass es überhaupt eine (mindestens) beobachtungsbedürftige Bestrebung gibt, die den Einsatz der entsprechenden Vertrauensleute rechtfertigt (vgl. auch die Ausführung unter 7. zu § 26 Abs. 5 Satz 4 VSG Bln-E). Eine solche Voraussetzung enthält § 27 Abs. 1 Satz 2 VSG Bln bislang nicht und ist daher entsprechend zu ergänzen.

Darüber hinaus hat das Bundesverfassungsgericht vorgegeben, dass die Anwerbungsphase nur von begrenzter Dauer sein darf und über die Verpflichtung einer Vertrauensperson in angemessener Zeit entschieden wird (Vgl. BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 353). Aus der Gesetzesbegründung ist nicht ersichtlich, inwiefern der hier festgelegte Zeitraum von zwölf Monaten tatsächlich in jedem Fall notwendig ist. Ein solcher Zeitraum dürfte ohne nähere Bedingungen unter Verhältnismäßigkeitsgesichtspunkten zu lang sein. Dies gilt vor allem vor dem Hintergrund der im Entwurf vorgesehenen Verlängerungsmöglichkeit um weitere sechs Monate (vgl. § 27 Abs. 1 Satz 2, Halbsatz 2 VSG Bln-E). Es empfiehlt sich zumindest eine Ergänzung des § 27 Abs. 1 Satz 2 VSG-Bln-E wie folgt: „Für den Einsatz ist § 26 mit der Maßgabe entsprechend anzuwenden, dass der Anordnung eine Anwerbungs- und Erprobungszeit von *bis zu* zwölf Monaten vorausgehen darf […].“

In Bezug auf den Einsatz von Vertrauensleuten sollte aus Gründen der Verhältnismäßigkeit eine Benachrichtigungspflicht geprüft und ggf. in bestimmten Fällen geregelt werden (s. bereits unter 7. sowie unter A.).

9. Observation - § 28 Abs. 1 und 2 VSG Bln-E

§ 28 Abs. 1 und 2 VSG Bln-E trifft Regelungen zu der Durchführung von Observationen und bestimmt – je nach Eingriffsgewicht – unterschiedliche Eingriffsvoraussetzungen (vgl. hierzu BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 357).

In Absatz 1 soll ausweislich der Gesetzesbegründung „die Anwendung weniger eingriffsintensiver Observationen zum Zwecke der Aufklärung von Bestrebungen oder Tätigkeiten nach § 5 Absatz 2“ geregelt werden. In der Vorschrift selbst heißt es jedoch, dass die „Observation zu Zwecken des § 11 Abs. 1 Nummer 1“ erfolgt. Hier besteht entsprechender Klarstellungsbedarf.

In Absatz 2 werden die Voraussetzungen für eingriffsintensivere langfristige Observationen festgelegt. Trotz des in der Begründung hierzu hervorgehobenen erhöhten Eingriffsgewichts sieht die Vorschrift keine Benachrichtigungspflicht an die Betroffenen vor. Dies ist mit den vom Bundesverfassungsgericht festgestellten Verhältnismäßigkeitsanforderungen nicht vereinbar. Aus Art. 19 Abs. 4 GG ergibt sich, dass Betroffene das Recht auf gerichtlichen Rechtsschutz haben müssen, dessen Ausübung bei heimlichen Maßnahmen nur möglich ist, wenn sie davon auch Kenntnis erlangen. Ausnahmen hiervon sind auf das unbedingt erforderliche Maß zu beschränken (vgl. BVerfG, Urteil v. 20.4.2016 – 1 BvR 966/09 u. a., Rn. 136). Daher sind Betroffene grundsätzlich bei eingriffsintensiven Observationen zu benachrichtigen, es sei denn, dass im Einzelfall die gesondert geregelten Ausnahmevorschriften greifen, wonach beispielsweise davon Abstand genommen werden kann, wenn und solange dies die Aufklärung erschweren würde. Es ist insofern eine Regelung zur Benachrichtigung in Fällen der langfristigen Observation vorzusehen (vgl. insoweit Art. 19a Abs. 2 Satz 4 BayVSG).

10. Zugriff auf Videoüberwachungen des öffentlich zugänglichen Raums – § 28 Abs. 3 VSG Bln-E

In der Vorschrift zur Durchführung von Observationen (§ 28 VSG Bln-E) findet sich auch – in Absatz 3 Satz 1 – die Regelung einer gänzlich neuen Befugnis für die Verfassungsschutzbehörde: das Recht, zur Durchführung der Observation private und öffentliche Betreiberinnen

und Betreiber von bestimmten Videoüberwachungen zu verpflichten, „die Überwachung auszuleiten und Aufzeichnungen zu übermitteln." Soweit aus der Verankerung bei der (allgemeinen) Observationsbefugnis deutlich werden soll, dass die Ausleitung von Videoüberwachung und die Übermittlung von Videoüberwachungsaufzeichnungen „nur" eine Form der Observation ist, ist dies nicht nur aus gesetzessystematischer Sicht zweifelhaft. Die Ausleitung und die Übermittlung sind als gesonderte Datenverarbeitungen anzusehen, wobei jedenfalls die Aufzeichnungsübermittlung keine „Observation" i. S. v. § 23 Abs. 1 Nr. 1 VSG Bln-E darstellt. Darüber hinaus handelt es sich um gegenüber der einfachen Observation deutlich eingriffsintensivere Maßnahmen, für die strengere Maßstäbe und gesetzliche Erfordernisse gelten (s. hierzu unten). Schließlich ist die Verortung dieser neuen Maßnahmen in § 28 VSG Bln-E aber insbesondere auch aus Gründen der Transparenz und Normenklarheit problematisch, da die Maßnahme an sich und ihre gesetzlichen Voraussetzungen nicht hinreichend deutlich werden.

Die Befugnis erlaubt sowohl den Zugriff auf bestimmte Videoüberwachungsanlagen des öffentlichen Raums in Echtzeit als auch auf die mittels der Videoüberwachungsanlagen angefertigten Aufzeichnungen. Der öffentlich zugängliche Raum (vgl. § 4 Abs. 1 BDSG) beinhaltet eine große Anzahl von Flächen. Darunter fallen öffentliche Straßen, Wege oder Plätze, aber bspw. auch Verkaufsbereiche von Geschäften, Kaufhäusern und Tankstellen, Einkaufspassagen, Restaurants und Cafés sowie Schalterhallen von Banken. Sogar der Besucherbereich einer Arztpraxis oder eines Krankenhauses während der Öffnungs- bzw. Besuchszeiten, Flughäfen, Bahnhofshallen und Bahnsteige sowie Kinos, Museen, Theater, Fußballstadien und die Fahrgastbereiche einschließlich der Haltestellen öffentlicher Verkehrsmittel fallen darunter. Nicht zuletzt sind frei zugängliche Gärten, Parks und Spielplätze sowie Waldgebiete unter den Begriff des öffentlich zugänglichen Raums zu fassen (vgl. hierzu ausführlich: Schindler/Scholz in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Auflage 2025, § 4 BDSG Rn. 54 ff.). Viele dieser Bereiche werden heute tatsächlich auch durch Einrichtungen der Videoüberwachung beobachtet, sei es durch öffentliche Stellen oder private Betreiberinnen und Betreiber. Durch den Zugriff auf deren Anlagen wäre es insoweit möglich, die Bewegungen einer (nachrichtendienstlich überwachten) Person nachzuvollziehen, im innerstädtischen Bereich sogar im Zweifel nahezu lückenlos. Daneben würden so auch die Daten zahlreicher weiterer betroffener Personen, die ebenfalls von der Videoüberwachung erfasst wurden, durch den Verfassungsschutz verarbeitet.

Auch wenn § 28 Abs. 3 VSG Bln-E lediglich den Zugriff auf die „Videoüberwachung von öffentlich zugänglichen großflächigen Anlagen“ sowie von „Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs“ (vgl. § 4 Abs. 1 Satz 2 BDSG) regelt, so ändert dies nichts an der Einschätzung, dass hierdurch die Möglichkeit einer nahezu flächendeckenden Überwachung geschaffen wird. Angesichts der in Großstädten wie Berlin engen räumlichen Situation dürfte selbst mittels der hier vorgesehenen Zugriffsbefugnisse auf diese Orte einer Videoüberwachung die Erstellung von Bewegungs- und Persönlichkeitsprofilen ohne Weiteres Realität werden. Gerade auch im Hinblick auf den zukünftig denkbaren Einsatz von automatisierten Datenanalysesystemen birgt dies die Möglichkeit der Erstellung von umfassenden Bewegungs- und Persönlichkeitsprofilen inklusive der Verarbeitung biometrischer Daten.

Zudem ist die zeitliche Dauer des Zugriffs auf die Videoüberwachung nicht eindeutig geregelt. Aus dem Wortlaut wird nicht ersichtlich, ob dieser sich aus § 28 Abs. 1 und 2 VSG Bln-E ergeben soll. Die zulässige Dauer der Mitnutzung bzw. Ausleitung bleibt damit im Unklaren. Es besteht daher die Gefahr, dass eine „punktuelle“ Mitnutzung ohne gesetzliche Eingrenzung und ohne gerichtliche Vorabkontrolle über einen längeren Zeitraum durchgeführt wird.

Die Norm ist im Ergebnis unverhältnismäßig, da sie insbesondere keine spezifische Eingriffsschwelle vorsieht. Das potentielle Eingriffsgewicht dürfte in Einzelfällen so hoch sein, dass zur Wahrung der Verhältnismäßigkeit als Eingriffsschwelle zumindest eine gesteigerte Beobachtungsbedürftigkeit vorzusehen ist. Dies folgt aus den Grundsätzen der Rechtsprechung des Bundesverfassungsgerichts, das eine abgestufte Regelung der Eingriffsvoraussetzungen differenziert nach dem Eingriffsgewicht verlangt (vgl. BVerfG, Urt. v. 26.04.2022 – 1 BvR 1619/17, Rn. 357). Die Ausleitung von Videoüberwachung und die Übermittlung von Aufzeichnungen greift tiefer als die verdeckte Beobachtung einer Person i. S. v. § 23 Abs. 1 Nr. 1 VSG Bln-E in die Grundrechte Betroffener ein. Nicht zuletzt auch, weil auf den Videoüberwachungen ein größerer Kreis von Personen erfasst wird. Neben einer mindestens erhöhten Beobachtungsbedürftigkeit als Eingriffsvoraussetzung sollte daher auch ein genereller Richtervorbehalt gesetzlich vorgesehen werden. Darüber hinaus ist eine spezielle Regelung für die Löschung der erhaltenen Daten aufzunehmen. Ferner bedarf es einer gesetzlichen Klarstellung, dass nur die Nutzung gesetzeskonformer Videoüberwachungsanlagen zulässig ist. Die BlnBDI stellt im Rahmen ihrer aufsichtsbehördlichen Tätigkeit sowohl eine Ausweitung der Überwachung mittels Videotechnik als auch eine Zunahme der Verstöße wegen unzulässiger Videoüberwachung

fest. Die Nutzung unzulässiger Videoüberwachungsanlagen wäre in jedem Fall unverhältnismäßig.

11. Befugnis zur Datenverarbeitung – § 34 VSG Bln-E

Die Vorschrift enthält zum einen eine allgemeine Datenverarbeitungsbefugnis für die Verfassungsschutzbehörde (§ 34 Abs. 1 VGS Bln-E) und zum anderen ein Verbot der Weiterverarbeitung unzulässig erhobener Daten (§ 34 Abs. 2 Satz 1 VSG Bln-E) sowie Regelungen zur Löschung (§ 34 Abs. 3 Satz 1 und 2 VSG Bln-E) und zur Verwendungsbeschränkung (§ 34 Abs. 3 Satz 4 VSG Bln-E). Sie führt damit verschiedene Regelungen aus aktuellen Vorschriften (u. a. §§ 11 Abs. 1, 14 und 15 VSG Bln) zusammen, was zu einer insgesamt unübersichtlichen Struktur führt. Dies auch, weil bspw. die Löschung nicht ausdrücklich in der Überschrift genannt, jedoch Gegenstand der Vorschrift ist. Aus Gründen der Transparenz und Rechtssicherheit sollten hier genaue Bezeichnungen und klare Regelungen zur Datenlöschung getroffen werden.

Zudem wird die Pflicht zur Löschung gelockert. Während nach derzeitiger Rechtslage eine Löschung stets zu erfolgen hat, wenn eine Datenspeicherung irrtümlich erfolgte, unzulässig war oder die Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist und schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden (vgl. § 14 Abs. 2 VSG Bln), sieht § 34 Abs. 2 Satz 1 VSG Bln-E lediglich ein Weiterverarbeitungsverbot für unzulässig erhobene Daten vor. Erst im zweiten Schritt – im Falle einer erfolgten Weiterverarbeitung unzulässig erhobener Daten – wird eine „Vernichtung“ unzulässig erhobener Daten angeordnet (§ 34 Abs. 3 VSG Bln-E), wobei zugleich eine Ausnahme vorgesehen wird. Wenn sich die Umstände im Nachhinein dergestalt geändert haben, dass die betroffenen Daten nunmehr rechtmäßig erhoben werden könnten, soll die Vernichtung unterbleiben. Hierdurch wird es dem Verfassungsschutz erlaubt, unzulässig erhobene Daten weiter zu verarbeiten. Damit wird das Wesen der finalen Schutzmaßnahme „Löschung“ ausgehöhlt, da die Daten auf Vorrat für eine mögliche spätere ggf. durch gesetzliche Änderung erreichte rechtmäßige Weiterverarbeitung aufbewahrt werden, obwohl zum aktuellen Zeitpunkt kein Rechtsgrund dafür gegeben ist.

Nicht geregelt wird zudem, ob es sich bei der Weiterverarbeitung um den gleichen Zweck handeln muss. Auch im Hinblick auf den Grundsatz der hypothetischen Datenneuerhebung ist die Regelung zu streichen oder zu ergänzen. Letztlich müssen Daten aber bereits gelöscht werden, wenn sie unzulässig erhoben wurden und nicht erst im Falle der Weiterverarbeitung.

Zusätzlich lässt der Wortlaut des § 34 Abs. 2 Satz 2 VSG Bln-E den irrtümlichen Schluss zu, dass unzulässig erhobene Daten allein solche sind, die aufgrund einer gerichtlich nicht bestätigten Dringlichkeitsanordnung nach § 33 VSG Bln-E verarbeitet werden. Aus der Gesetzesbegründung ergibt sich zwar, dass es dabei nur um einen möglichen Fall der unzulässigen Datenerhebung handelt. Gleichwohl muss dies auch im Normtext selbst klargestellt werden.

Schließlich ist auch darauf hinzuweisen, dass die bisherige Regelung in § 12 VSG Bln ein Verbot der Speicherung von Daten Minderjähriger, die das 14. Lebensjahr nicht vollendet haben, vorsah und diese Regelung ohne nähere Begründung nunmehr weggefallen ist. Angesichts der besonderen Schutzwürdigkeit von Kindern und Jugendlichen ist nicht nachvollziehbar, aus welchen Gründen bei der Speicherung ihrer Daten keine Restriktionen vorgesehen werden. Das Speicherungsverbot im Hinblick auf Daten unter 14-jähriger Personen ist dringend wieder aufzunehmen. Darüber hinaus wird angeregt, dezidierte Vorgaben für die Verarbeitung von Daten sonstiger Minderjähriger in Form einer Sonderregelung vorzusehen (vgl. § 11 BVerfSchG).

12. Dauer der Speicherung sowie Beseitigung von Unrichtigkeiten und Widerspruch betroffener Personen – § 35 VSG Bln-E und § 36 VSG Bln-E

Die Normen §§ 35, 36 VSG Bln-E führen ebenfalls verschiedene Regelungen aus dem derzeitigen VSG Bln zusammen (insbesondere §§ 13, 14 VSG Bln), ohne dass die Gesetzessystematik hierdurch verbessert würde (s. bereits unter 11.). Kritikwürdig ist aus Transparenzgründen insbesondere, dass § 35 VSG Bln-E eine weitere Regelung zur Löschung enthält. Die einzelnen Tatbestände der Löschung sollten in einer zentralen Norm zusammengeführt und eine Regelung zu den regelmäßigen Prüffristen sollte hiervon gesondert getroffen werden.

Nach der Gesetzesbegründung zu § 35 Abs. 3 VSG Bln-E soll die Norm bei Daten minderjähriger Personen eine „Höchstspeicherfrist“ von zwei Jahre vorsehen. Der Wortlaut der Vorschrift selbst verweist aber lediglich auf die Prüffrist nach § 35 Abs. 2 VSG Bln-E, die bei Minderjährigen zwei Jahre beträgt. Diese verkürzte Prüffrist soll jedoch dann nicht gelten, wenn die betroffene Person zum Zeitpunkt der letztmaligen Speicherung die Volljährigkeit erlangt hat. Es werden hier demnach die (Höchst-) Speicherdauer mit den Prüffristen der Behörde vermischt. Gerade in Bezug auf Minderjährige ist eine klare Regelung zu treffen, wann die Daten zu löschen sind und wann ggf. eine Prüfung zur Erforderlichkeit der weiteren Speicherung stattfindet (vgl. insoweit § 11 Abs. 2 BVerfSchG).

Aus Klarstellungsgründen sollte schließlich auch in der Überschrift von § 36 VSG Bln-E der gängige datenschutzrechtliche Begriff „Berichtigung“ beibehalten werden, damit dies mit dem Wortlaut der Regelung und der Gesetzesbegründung konform ist. Die Regelung zur Information von Empfängern unrichtiger Daten ist zudem zu unbestimmt. Hier sollte eine klare Festlegung erfolgen, dass eine unverzügliche Unterrichtung der empfangenden Stelle zu erfolgen hat, wenn sich personenbezogene Daten nach ihrer Übermittlung als unvollständig oder unrichtig herausstellen. Wann hiervon ausnahmsweise abgesehen kann, muss ebenfalls eindeutig normiert werden. Aus der Gesetzesbegründung ergeben sich jedenfalls keine Anhaltspunkte, wann eine „nicht nur unerhebliche Beeinträchtigung des Informationswerts“ gegeben sein soll, was die praktische Anwendung der Norm erheblich erschweren würde.

13. Informationsübermittlung – §§ 38 ff VSG Bln-E

In diesem Abschnitt des Gesetzentwurfs sollen ausweislich der Begründung die in den letzten Jahren ergangenen umfangreichen Vorgaben des Bundesverfassungsgerichts zu Datenübermittlungen der Verfassungsschutzbehörden umgesetzt werden (s. hierzu bereits unter A.). Es wird bei den Vorschriften zur Informationsübermittlung an Strafverfolgungs- und Gefahrenabwehrbehörden allerdings danach unterschieden, ob Daten mit oder ohne nachrichtendienstliche Mittel erhoben wurden (vgl. §§ 40 Abs. 1 und 2, 41 Abs. 1 und 2 VSG Bln-E). Das widerspricht den unter A. zusammengefassten Feststellungen des Bundesverfassungsgerichts im Hinblick auf Übermittlungsvorschriften. Dieses hat ausgeführt: „*Eine Differenzierung nach dem Eingriffsgewicht der jeweiligen Einzelmaßnahme kommt insoweit nach dem Kriterium der hypothetischen Datenneuerhebung wegen der Besonderheiten nachrichtendienstlicher Aufgabenwahrnehmung nicht in Betracht. […] Denn durch die Betrachtung eines einzelnen, für sich genommen weniger eingriffsintensiven Datenerhebungsvorgangs würde die Grundrechtsbelastung, die von der breit angelegten, teils niederschwelligen Beobachtungstätigkeit nachrichtendienstlicher Behörden ausgeht, nicht in Gänze erfasst. Nachrichtendienstliche Behörden schöpfen ihre Erkenntnisse aus einer Fülle von Daten, die sie weit im Vorfeld konkreter Gefahren und operativer Tätigkeit erheben, miteinander und mit Erkenntnissen anderer Stellen verknüpfen und filtern, um daraus relevante Informationen zu gewinnen und auch weiterzugeben; dies ist eine Besonderheit ihrer Aufgabe*“ (BVerfG Urteil vom 26.4.2022 – 1 BvR 1619/17, Rn. 238).

Den Verfassungsschutzbehörden ist es immanent, dass sie ggf. bereits mit niedrigeren Eingriffsschwellen weit im Vorfeld personenbezogene Daten erheben dürfen, so wie es den anderen Sicherheitsbehörden überhaupt nicht möglich wäre. Dies ist im Rahmen der Übermittlung

zu beachten und daher sind strenge Anforderungen auch schon an die Übermittlung nicht mit nachrichtendienstlichen Mitteln erhobener personenbezogener Daten zu knüpfen (BVerfG Urteil vom 26.4.2022 - 1 BvR 1619/17, Rn. 242). Die Regelungen sollten dementsprechend überarbeitet werden. Dabei ist auch zu berücksichtigen, dass die in § 48 VSG Bln-E genannten Verhältnismäßigkeitsmaßstäbe bereits in den jeweiligen Übermittlungsnormen zu verorten sind.

In § 40 Abs. 3 VSG Bln-E sollten zudem die in Betracht kommenden Straftaten konkret benannt werden. Die Norm gibt zwar die Rechtsprechung des Bundesverfassungsgerichts zur Definition der besonders schweren Straftat anknüpfend an das Höchststrafmaß wieder, legt jedoch nicht konkret fest, welche Straftatbestände als besonders schwer gelten sollen (vgl. jedoch BVerfG, Beschl. v. 17.7.2024 - 1 BvR 2133/22, Rn. 206 ff.).

14. Wohnraumüberwachung - § 49 VSG-Bln-E

Grundsätzlich ist zu begrüßen, dass bei der Regelung dieser Maßnahme die Vorgaben des Bundesverfassungsgerichts weitestgehend berücksichtigt werden. Dennoch möchte ich hierzu einige Anmerkungen insbesondere zum Wortlaut und zur Gesetzessystematik, aber auch zur Verfassungskonformität der Regelungen zum Kernbereichsschutz machen.

In § 49 Abs. 1 VSG Bln-E ist die grundsätzliche Befugnis normiert, das in einer Wohnung nichtöffentlich gesprochene Wort mit technischen Mitteln mitzuhören oder aufzuzeichnen. Angesichts des grundgesetzlich gewährleisteten Schutzes der Unverletzlichkeit der Wohnung (Art. 13 GG) und der insoweit besonders hohen Eingriffsintensität dieser Maßnahme, sollte im Gesetzeswortlaut klargestellt werden, dass dies nur im Einzelfall erlaubt ist.

§ 49 Abs. 2 Nr. 1 VSG Bln-E soll den Schutz des Kernbereichs privater Lebensgestaltung gewährleisten, indem eine Wohnungsüberwachung nur dann zulässig sein soll, „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass den im Schutzbereich von Artikel 13 des Grundgesetzes geführten Gesprächen der betroffenen Person mit Personen ihres besonderen persönlichen Vertrauens der höchstvertrauliche Charakter fehlen wird [...]“. Die Formulierung legt allerdings den Schluss nahe, dass Gespräche nur dann dem Kernbereichsschutz unterfallen, wenn sie mit einer (in der Wohnung anwesenden) Vertrauensperson geführt werden. Indessen sind auch Selbstgespräche oder Telefonate mit Vertrauenspersonen hiervon umfasst. Nach der Definition des Bundesverfassungsgerichts gehört die Möglichkeit, innere Vorgänge

wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen – sei es in einem Gespräch mit engen Vertrauten, in Selbstgesprächen oder in Form von Tagebucheinträgen – ohne Angst, dass staatliche Stellen dies überwachen, zum Kernbereich privater Lebensgestaltung. Umfasst sind davon auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität. Ausschlaggebend ist daher nicht der Gesprächspartner, sondern der Gesprächsinhalt (vgl. Heusch/Ullrich/Posser VerfassungsR-HdB/Braun § 7 Rn. 89-91 m.w.N.). Es sollte deshalb eine entsprechende Formulierung erfolgen.

Der für die Wohnraumüberwachung nach der höchstrichterlichen Rechtsprechung vorzusehende Richtervorbehalt findet sich nicht unmittelbar in der Vorschrift des § 49 VSG Bln-E, sondern in § 51 VSG Bln-E. Vorzugswürdig wäre aus Gründen der Normenbestimmtheit und Normenklarheit eine entsprechende Formulierung in einem gesonderten Absatz des § 49 VSG Bln-E, damit die Bedingung für Anwender:innen und Betroffene ohne Weiteres nachvollziehbar ist. Denn neben den aus § 51 VSG Bln-E zu entnehmenden Maßgaben gelten für das Verfahren auch die §§ 30 ff. VSG Bln-E, auf die in § 51 Abs. 2 VSG Bln-E verwiesen wird. Zudem legt § 51 Abs. 2 Satz 2 VSG Bln-E fest, dass für eine Dringlichkeitsanordnung nach § 33 VSG Bln-E nicht die Leitung der Verfassungsschutzbehörde, sondern die Leitung der für Inneres zuständigen Senatsverwaltung zuständig ist. Insgesamt wird die Regelung der Vorabkontrolle damit unübersichtlich. Um zu vermeiden, dass die Maßnahme ohne eine richterliche Anordnung erfolgt, sollte in § 49 VSG Bln-E zumindest ein Verweis auf den Richtervorbehalt nach § 51 VSG Bln-E aufgenommen werden. Aufgrund der gesonderten Regelung des Richtervorbehalts in § 51 VSG Bln-E steht auch § 49 Abs. 6 VSG Bln-E ohne Zusammenhang mit der richterlichen Anordnung. Es wird insofern nicht klar, welchem Gericht die erhobenen Daten unverzüglich vorzulegen sind. Hier muss zwingend eine Klarstellung erfolgen.

Nach § 49 Abs. 6 Satz 3 und 4 VSG Bln-E können die erhobenen Daten bei Gefahr im Verzug unter Aufsicht einer Dienstkraft des Verfassungsschutzes mit Befähigung zum Richteramt gesichtet werden und diese Dienstkraft kann im Benehmen mit der Datenschutzbeauftragten oder dem Datenschutzbeauftragten der Abteilung für Verfassungsschutz über eine vorläufige Verwertung der Erkenntnisse entscheiden. Diese Vorgaben sind nicht verfassungskonform. Das Bundesverfassungsgericht hat im Zusammenhang mit seiner Entscheidung zum Bayerischen Verfassungsschutzgesetz entschieden, dass es bei einer dem Kernbereichsschutz dienenden Sichtung auf Auswertungsebene nicht zu einer (weiteren) Kenntnisnahme durch die Behörde

selbst kommen darf, auch wenn bei der Ausgestaltung der im Grundsatz umfassenden Kontrollbefugnis für Ausnahmefälle bei Gefahr im Verzug besondere Regelungen vorgesehen werden können (vgl. BVerfG, Urteil v. 26.4.2022 – 1 BvR 1619/17, Rn. 282/283). Die verfassungsrechtlich gebotene Sichtung durch eine unabhängige Stelle dient neben der Rechtmäßigkeitskontrolle maßgeblich dem Ziel, kernbereichsrelevante Daten so frühzeitig herauszufiltern, dass sie den Sicherheitsbehörden nach Möglichkeit nicht offenbar werden. Die Kontrolle muss von externen, nicht mit Sicherheitsaufgaben betrauten Personen wahrgenommen werden, wobei die Hinzuziehung einer Dienstkraft der Verfassungsschutzbehörde nicht ausgeschlossen ist. Die tatsächliche Durchführung und Entscheidungsverantwortung muss jedoch maßgeblich in den Händen von unabhängigen Personen liegen (BVerfG, Urteil vom 20.4.2016 – 1 BvR 966/09 u. a., Rn. 204 und 224.). Dies ist durch die vorliegende Regelung nicht gewährleistet. § 49 Abs. 6 Satz 3 bis 5 VSG Bln-E ist zu streichen.

15. Online-Durchsuchung – § 50 VSG Bln-E

§ 50 VSG Bln-E sieht eine weitere neue Befugnis für den Verfassungsschutz vor: den verdeckten Zugriff auf informationstechnische Systeme und die Erhebung von Daten aus diesen – die sog. verdeckte oder heimliche Online-Durchsuchung. Unabhängig von datenschutzpolitischen Bedenken gegen Eingriffe in informationstechnische Systeme ist zunächst anzuerkennen, dass die bundesverfassungsgerichtliche Rechtsprechung weitestgehend Berücksichtigung gefunden hat.

Der heimliche Zugriff auf informationstechnische Systeme ohne Wissen der Betroffenen greift in das aus dem allgemeinen Persönlichkeitsrecht abgeleitete Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ein. Der Eingriff wiegt dabei besonders schwer, da die betroffenen Personen die informationstechnischen Systeme gerade in der berechtigten Erwartung von Vertraulichkeit als eigene nutzen und davon ausgehen, dass diese ihrer alleinigen, selbstbestimmten Verfügung unterliegen. Darüber hinaus haben informationstechnische Systeme eine hohe Aussagekraft über die Lebensgestaltung und -wirklichkeit von Personen, da ein großer Teil davon inzwischen virtuell stattfindet. Das Bundesverfassungsgericht stellt daher besondere Anforderungen u. a. an die Eingriffsschwelle und Verhältnismäßigkeit der Online-Durchsuchung (BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17). Unter einem heimlichen Zugriff auf ein informationstechnisches System ist eine technische Infiltration zu verstehen, die etwa Sicherheitslücken des Zielsystems ausnutzt oder über die Installation eines Spähprogramms erfolgt (Lisken/Denninger PolR-HdB/Graulich E. Rn. 797). Die Infiltra-

tion ermöglicht es, die Nutzung des betreffenden Systems zu überwachen oder gar fernzusteuern sowie die Speichermedien durchzusehen. Durch das Einschleusen von Spionagesoftware in ein informationstechnisches System (z. B. PC, Smartphone, Festplatte usw.) wird jedenfalls einmal, typischerweise aber längerfristig dessen Inhalt ausgeforscht und ggf. an den Verfassungsschutz übermittelt (sog. Leseangriff).

Neben der Heimlichkeit der Maßnahme wirken sich demnach auch die infolge des Zugriffs entstehenden Gefahren für die Integrität des Zugriffsrechners sowie für Rechtsgüter des Betroffenen oder auch Dritter auf das Eingriffsgewicht der Online-Durchsuchung aus (vgl. BVerfG, Urteil v. 27.2.2008 – 1 BvR 370/07 u. a., Rn. 238 ff.). Bereits die Existenz der Befugnis zur Online-Durchsuchung schafft für die Verfassungsschutzbehörde einen Anreiz, ihr bekannt werdende Sicherheitslücken offenzuhalten, um sie zur Infiltration nutzen zu können (BVerfG, Urteil v. 26.4.2022 - 1 BvR 1619/17, Rn. 316). Zudem wird die bisher nur der Polizei im Falle einer konkreten Gefahr und den Strafverfolgungsbehörden bei der Verfolgung besonders schwerer Straftaten vorbehaltene Maßnahme, auf das riesige Vorfeld der nachrichtendienstlichen Beobachtung ausgeweitet, das zeitlich wesentlich früher beginnt und insofern einen weiteren Schritt hin zu einer Rundum-Überwachung darstellt.

Diese grundsätzlichen Anmerkungen vorangestellt, verwundert es angesichts der Einführung einer äußerst eingriffsintensiven Maßnahme sehr, dass die Gesetzesbegründung zu § 50 VSG Bln-E mit gerade einmal drei kurzen Absätzen äußerst knapp gehalten ist und auf die hier dargestellte grundrechtliche Relevanz und Problematik nicht eingeht.

Kritisch ist dies insbesondere im Hinblick auf den weiten Wortlaut der Regelung des § 50 Abs. 1 Satz 1 VSG Bln-E zu sehen, wonach aus dem von dem Betroffenen genutzten informationstechnischen System „Daten erhoben werden“ dürfen. Es erfolgt weder in der Vorschrift selbst noch in der Begründung eine Einschränkung. Hier sollte in der Vorschrift selbst jedenfalls konkretisiert werden, welche Daten erhoben werden dürfen (vgl. Art. 10 Abs. 1 Satz 1 BayVSG). Ferner ist hierzu anzumerken, dass zwar begrifflich die Erhebung aller auf dem System gespeicherten Daten zugelassen sein mag, jedoch darf dies im Einzelfall nicht unverhältnismäßig sein oder einen unzulässigen Eingriff in den Kernbereich der Lebensgestaltung darstellen (vgl. § 50 Abs. 2 VSG Bln-E). Aus dem Verhältnismäßigkeitsgrundsatz folgt, dass sich die Maßnahme auf Datenbestände beschränken muss, die zur Abwehr der jeweils konkretisierten Gefahr relevant sind.

Im Übrigen wird auf die vorangehenden Ausführungen (unter 14.) zur Normierung des Richtervorbehalts verwiesen. Dieser sollte unmittelbar in § 50 VSG Bln-E aufgenommen werden. Da aufgrund des Verweises in § 50 Abs. 4 VSG Bln-E die Regelungen zur Sichtung der Erkenntnisse bei Gefahr im Verzug in § 49 Abs. 6 Satz 3 ff. VSG Bln-E entsprechend für die Online-Durchsuchung gelten, wird diesbezüglich ebenfalls auf die obigen Ausführungen verwiesen. Die Vorschrift ist im Hinblick auf den auch auf der Verwertungsebene zu wahrenden Kernbereichsschutz nicht verfassungskonform (vgl. unter 14.) und damit zu streichen.

16. Auskunftsanspruch betroffener Personen – § 53 VSG Bln-E

Der Auskunftsanspruch gegenüber der Verfassungsschutzbehörde wird durch § 53 Abs. 1 VSG Bln-E an eine Mitwirkungspflicht der antragstellenden Person geknüpft. Diese muss auf einen konkreten Sachverhalt hinweisen und ein berechtigtes Interesse darlegen. Hierdurch wird der Auskunftsanspruch unverhältnismäßig eingeschränkt. Die Maßnahmen des Verfassungsschutzes erfolgen regelmäßig verdeckt und ohne Kenntnis der betroffenen Personen. Im Nachhinein besteht kaum eine Möglichkeit, diese Heimlichkeit aufzuheben und ggf. Rechtsschutz zu erlangen. Der Umstand, dass die Betroffenen nach § 53 Abs. 1 VSG Bln-E künftig auf einen konkreten Sachverhalt hinweisen sollen, kann zum weitgehenden Ausschluss des Auskunftsrechts und damit einer nachträglichen Kenntnis führen. Dies kann insbesondere der Fall sein, wenn Betroffene keine Ahnung haben, in welchem Zusammenhang sie Gegenstand einer nachrichtendienstlichen Erfassung sein könnten. Wer beispielsweise erfasst ist, weil ein Informant ihn mit einer anderen Person verwechselt hat, wird bei Beantragung einer Auskunft zum konkreten Sachverhalt naturgemäß keine Angaben machen können. Das könnte im Ergebnis dazu führen, dass Daten zur Person unrichtig gespeichert sind und diese dennoch darüber keine Auskunft erhält. Ihr wird damit die Möglichkeit genommen, fehlerhafte Speicherungen zu unterbinden. Deshalb darf der Antrag nicht von vornherein abgelehnt werden, wenn betroffene Personen keine Angaben zu einem konkreten Sachverhalt machen (ebenso zu § 15 BVerfSchG – Bergemann in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Kap. H Rn. 181).

Dasselbe gilt in Bezug auf die Darlegung eines berechtigten Interesses durch die betroffene Person. Zweck dieser Regelung ist ausweislich der Gesetzesbegründung, dass „konzertierte Anfragen (etwa von Mitgliedern einer verfassungsfeindlichen Organisation), die zum Ziel haben, eine Vielzahl von Auskünften zu erlangen, aus deren Gesamtschau Rückschlüsse auf den Erkenntnisstand der Verfassungsschutzbehörde zu erlangen wären," erschwert werden. Es soll

folglich einer Ausforschungsgefahr begegnet werden, was grundsätzlich ein legitimes Ziel darstellt. Hierzu ist allerdings anzumerken, dass eine Ausforschungsgefahr dogmatisch eher als Ablehnungsgrund im Sinne des § 53 Abs. 3 Nr. 2 VSG Bln-E zu subsumieren sein dürfte. Der Verfassungsschutz kann demnach eine Auskunft ohnehin verweigern, wenn ein Geheimhaltungsinteresse gegenüber dem Auskunftsinteresse der betroffenen Person überwiegt. Es ist insoweit bereits fraglich, ob es einer Eingrenzung des Auskunftsrechts durch das Erfordernis eines dargelegten berechtigten Interesses überhaupt bedarf. Jedenfalls ist dabei zu beachten, dass ein Auskunftsantrag durch den Verfassungsschutz nicht allein deshalb abgelehnt werden dürfte, weil eine betroffene Person kein berechtigtes Interesse dargelegt hat. Nach dem einfachgesetzlichen Regelungsgehalt, der unter Beachtung der Grundrechtsvorgaben auszulegen und anzuwenden ist, entfällt in einem solchen Fall lediglich die Auskunftspflicht. Nach höchstrichterlicher Rechtsprechung ergibt sich jedoch aus dem Grundrecht auf informationelle Selbstbestimmung zumindest ein Anspruch auf eine Ermessensentscheidung, die die grundrechtlichen Belange des Betroffenen insbesondere mit einer entgegenstehenden Ausforschungsgefahr abwägt (vgl. zu § 15 BVerfSchG – BVerfG, Beschl. v. 10.10.2000 – 1 BvR 586/90 u. a.).

In Absatz 2 wird des Weiteren eine Pflicht des Verfassungsschutzes normiert, sich zu vergewissern, „dass der Antrag von der antragstellenden Person selbst oder einer zur Wahrnehmung ihrer Rechte berechtigten Person gestellt wurde." Hierzu darf die Verfassungsschutzbehörde „die Vorlage geeigneter Mittel der Glaubhaftmachung verlangen." Wir haben uns im vergangenen Jahr mit dem Verfassungsschutz intensiv über die Frage der Identitätsprüfung der antragstellenden Person ausgetauscht, da wir die bisher geübte Praxis, wonach stets die Kopie eines amtlichen Ausweises vor Bearbeitung eines Auskunftsantrags vorgelegt werden musste, für unzulässig halten. Der Verfassungsschutz hat uns hierzu erst zu Jahresbeginn mitgeteilt, dass von der generellen Anforderung einer Ausweiskopie künftig abgesehen werde. Dies begrüßen wir ausdrücklich. Vor diesem Hintergrund und zur Vermeidung von Rechtsunsicherheiten ist es wünschenswert, wenn in der Gesetzesbegründung näher ausgeführt wird, welche „geeigneten Mittel der Glaubhaftmachung" in Betracht kommen und nach welchem Maßstab die Anforderung dieser erfolgen darf.

Zu der nunmehr vorgelegten Regelung des § 53 Abs. 2 VSG Bln-E ist daher vorsorglich anzumerken, dass hieraus keinesfalls eine generelle Notwendigkeit zur Vorlage eines Identitätsnachweises abgeleitet werden darf. Das Recht auf Auskunft setzt zwar voraus, dass die um

Auskunft ersuchende Person identisch mit der betroffenen Person ist. Die Anforderung von zusätzlichen, zur Bestätigung der Identität der betroffenen Person erforderlichen Informationen ist allerdings nur dann zulässig, wenn die Verfassungsschutzbehörde begründete Zweifel an der Identität der antragstellenden Person hat (für den Anwendungsbereich der DSGVO bzw. der JI-Richtlinie geht dies aus Art. 12 Abs. 6 DSGVO, Art. 12 Abs. 5 JI-Richtlinie und § 59 Abs. 4 BDSG hervor). Ohne besonderen Anlass darf die auskunftspflichtige Behörde damit keinen Identitätsnachweis von einem Antragsteller bzw. einer Antragstellerin verlangen (so für eine Auskunftserteilung gemäß § 59 BDSG auch: VG Berlin, Urteil vom 31. August 2020 – VG 1 K 90.10). Dies gebietet zudem der datenschutzrechtliche Erforderlichkeitsgrundsatz. Bei der Beurteilung der Frage, ob die Anforderung weiterer Angaben oder gar die Vorlage eines Identitätsnachweises notwendig sind, sind folglich die Umstände des Einzelfalls zu berücksichtigen. Um zu verhindern, dass die Auskunft an Unbefugte übermittelt und so personenbezogene Daten offengelegt werden, kann eine Zustellung mittels persönlicher Übergabe, z. B. per Einschreiben, erfolgen, ohne dass die Vorlage eines Identitätsnachweises erforderlich wäre.

17. Anwendung des Berliner Informationsfreiheitsgesetzes – § 54 Abs. 3 VSG Bln-E

Obwohl es der bisherigen Rechtslage entspricht, ist nicht nachvollziehbar, aus welchem Grund die Akten des Verfassungsschutzes weiterhin in Gänze nicht dem Berliner Informationsfreiheitsgesetz (IFG) unterliegen sollen. Ungeachtet des Umstandes, dass diese Bereichsausnahme ohnehin gesetzessystematisch richtiger im IFG selbst zu verorten wäre, könnte der Verfassungsschutz allgemeine Informationen über seine Aufgaben und Befugnisse, Arbeitsfelder und Vorgehensweisen interessierten Bürger:innen auf Antrag zugänglich machen. Im Übrigen sollten – wie in anderen Bereichen der inneren Sicherheit auch – die im IFG vorgesehenen Ausnahmetatbestände (z. B. § 11) genügen, um den schutzbedürftigen Informationen des Verfassungsschutzes Rechnung zu tragen.

Ich bitte um Berücksichtigung meiner Stellungnahme im weiteren Gesetzgebungsverfahren.

Für Rückfragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen

Meike Kamp