20. Wahlperiode

Drucksache **20/11235**

HESSISCHER LANDTAG

20. 06. 2023

Plenum

Änderungsantrag

Fraktion der CDU,
Fraktion BÜNDNIS 90/DIE GRÜNEN,

zu Gesetzentwurf
Fraktion der CDU,

Fraktion BÜNDNIS 90/DIE GRÜNEN

Gesetz zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei

in der Fassung der Beschlussempfehlung und des Berichts des Innenausschusses Drucksache 20/11194 zu 20/8129

Der Landtag wolle beschließen:

Der Gesetzentwurf wird wie folgt geändert:

Der Gesetzentwurf in der Fassung der Beschlussempfehlung und des Berichts des Innenausschusses wird wie folgt geändert:

I. Art. 1 Nr. 21 wird wie folgt geändert:

§ 20a Satz 2 wird wie folgt gefasst:

„Besonders schwere Straftaten sind solche, die mit einer Höchststrafe bedroht sind von mindestens

a) zehn Jahren Freiheitsstrafe oder

b) fünf Jahren Freiheitsstrafe, wenn sie im Zusammenhang mit der Beteiligung an einer beobachtungsbedürftigen Bestrebung i. S. d. § 2 Abs. 2 Nr. 1, 3, 4 oder 5 oder in Ausübung einer beobachtungsbedürftigen Tätigkeit i. S. d. § 2 Abs. 2 Nr. 2 begangen werden.“

II. Art. 2 wird wie folgt geändert:

1. Das einleitende Vollzitat des Gesetzes wird wie folgt gefasst:

„Das Hessische Gesetz über die öffentliche Sicherheit und Ordnung in der Fassung der Bekanntmachung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Gesetz vom 22. März 2023 (GVBl. S. 150), wird wie folgt geändert:“

2. Nr. 5 wird wie folgt gefasst:

„5. § 13a wird wie folgt geändert:

a) In Abs. 1 Satz 1 werden die Wörter „Hessische Sicherheitsüberprüfungsgesetz“ durch die Wörter „Hessische Sicherheitsüberprüfungs- und Verschlusssachengesetz“ ersetzt.

b) In Abs. 2 wird Satz 3 durch folgende Sätze ersetzt:

„Im Fall des Abs. 1 Satz 1 Nr. 1 Buchst. a ist eine Überprüfung der betroffenen Personen anhand von Datenbeständen des Landesamts für Verfassungsschutz regelmäßig erforderlich. Für die Einwilligung gilt § 46 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes.““

3. Nr. 6 wird wie folgt geändert:
Folgender Satz wird angefügt:
„Abs. 1 Satz 2 und 3 und Abs. 3 Satz 2 und 3 gilt entsprechend.“

4. Nr. 9 Buchst. b) wird wie folgt geändert:
Die Angabe „und 2“ wird gestrichen.

5. Der Änderungsbefehl Nr. 16 Buchst. b wird wie folgt gefasst:
„b) Satz 2 wird durch folgenden Satz ersetzt:“

6. Nr. 18 wird wie folgt geändert:
„18. § 25a wird wie folgt gefasst:

„§ 25a
Automatisierte Anwendung zur Datenanalyse

(1) Die Polizeibehörden dürfen rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen. Sie dürfen nach Maßgabe der Sätze 3 bis 6 und der Abs. 2 bis 5 diese zusammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden (automatisierte Anwendung zur Datenanalyse). Die automatisierte Anwendung zur Datenanalyse ist ein technisches Hilfsmittel, das es den Polizeibehörden bei der Erfüllung ihrer Aufgaben nach Maßgabe der folgenden Absätze ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen. Sie erfolgt immer anhand anlassbezogener und zielgerichteter Suchkriterien. Sie wird manuell ausgelöst und läuft regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ab. Eine direkte Anbindung an Internetdienste ist ausgeschlossen.

(2) Die Polizeibehörden können gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten,

1. wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, erforderlich ist (Abwehr konkreter Gefahren),
2. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten mit erheblicher Bedeutung begangen werden und dies zur Verhinderung dieser Straftaten erforderlich ist (Abwehr konkretisierter Gefahren),
3. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass schwere oder besonders schwere Straftaten begangen werden sollen, und die Weiterverarbeitung erforderlich ist, um diese Straftaten zu verhüten (Vorbeugende Bekämpfung von Straftaten).

Zum Zweck der automatisierten Anwendung zur Datenanalyse können Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen können ergänzend einbezogen werden. Bei einer Maßnahme nach Satz 1 Nr. 3 dürfen Verkehrsdaten nicht in die Analyse einbezogen werden.

(3) Bei der Anwendung zur automatisierten Datenanalyse gilt § 20 Abs. 1 und 2. Dies wird durch eine Verwaltungsvorschrift sichergestellt, die zu veröffentlichen ist. Sie beinhaltet ein Rollen- und Rechtekonzept und ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten. Unter Berücksichtigung der in Abs. 2 Satz 1 nach Schutzgütern und Eingriffsschwellen unterschiedenen Lagebilder orientieren sich diese Konzepte an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter (funktionale Reduzierung der Eingriffsintensität).

1. Das Rollen- und Rechtekonzept regelt die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen. Maßstab für dieses Konzept sind das Gewicht der zu schützenden Rechtsgüter und der Grad der Dringlichkeit des polizeilichen Einschreitens. Es ist nach dem Prinzip auszugestalten, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform zusammengeführten Daten haben dürfen. Es müssen darin mindestens die einzelnen Phänomenbereiche, ihre Gewichtung und ihr Verhältnis zueinander umschrieben und die dienstrechtliche Stellung der Berechtigten, ihre Funktion und ihre spezifische Qualifizierung bezogen auf den Umfang der jeweiligen Berechtigung festgelegt werden.
2. Das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten regelt anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen.
   a) Maßstab für dieses Konzept ist zum einen der sachliche Bezug der von der Analyse betroffenen Personen zum jeweiligen Phänomenbereich (Veranlassungszusammenhang). Es folgt dem Prinzip, wonach eine automatisierte Datenanalyse umso komplexer sein darf, je gewichtiger der Veranlassungszusammenhang ist, und dass sie umso einfacher sein muss, je weniger gewichtig der Veranlassungszusammenhang ist. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen. Zum Schutz Unbeteiligter werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Das Nähere regelt eine Verwaltungsvorschrift, die insbesondere für Verkehrsdaten eine Speicherfrist von regelmäßig zwei Jahren in der Analyseplattform vorsieht.
   b) Maßstab für dieses Konzept ist zum anderen die Kategorisierung personenbezogener Daten nach der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung bei ihrer Erhebung (Grundrechtsrelevanz). Es müssen abstrakte Regelungen getroffen werden, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen, und es muss durch technisch-organisatorische Vorkehrungen sichergestellt werden, dass diese Regelungen praktisch wirksam werden. In die automatisierte Anwendung zur Datenanalyse werden keine personenbezogenen Daten einbezogen, die aus Wohnraumüberwachung und Online-Durchsuchung gewonnen wurden.

(4) Der Zugang zur automatisierten Anwendung zur Datenanalyse ist reglementiert (Zugriffskontrolle). Die Zugriffe unterliegen hierbei der ständigen Protokollierung. Jeder Fall der automatisierten Anwendung zur Datenanalyse ist von der Anwenderin oder dem Anwender zu begründen. Die Begründung dient der Selbstvergewisserung und der nachträglichen Kontrolle. Die Einzelheiten der Zugriffskontrolle und des notwendigen Inhalts der Begründung werden in einer Verwaltungsvorschrift geregelt. Die oder der behördliche Datenschutzbeauftragte ist zur Durchführung stichprobenartiger Kontrollen berechtigt.

(5) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. Die oder der Hessische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder einer wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen. Im Übrigen bleiben die Aufgaben und Befugnisse der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit unberührt.““

III. Art. 3 wird wie folgt geändert:

In § 3 wird die Angabe „1. Januar 2023“ durch die Angabe *„… [einsetzen: Datum des ersten Tages des vierten auf die Verkündung folgenden Kalendermonats]* ersetzt.

IV. Art. 5 wird wie folgt geändert:

Die Angabe „vom 14. Dezember 2021 (GVBl. 931, 987)“ wird durch die Angabe „vom 28. März 2023 (GVBl. S. 183)“ ersetzt.

V. Art. 6 wird wie folgt gefasst:

„Artikel 6
Änderung des Hessischen Personalvertretungsgesetzes

Das Hessische Personalvertretungsgesetz vom 28. März 2023 (GVBl. S. 183) wird wie folgt geändert:

In § 82 Abs. 1 Nr. 2 werden die Wörter „Hessischen Bereitschaftspolizeipräsidium“ durch „Hessischen Polizeipräsidium Einsatz“ ersetzt.“

VI. Art. 7 wird wie folgt geändert:

Hinter die Angabe „(GVBl. 2021 S. 931)“ wird die Angabe „zuletzt geändert durch Gesetz vom 28. März 2023 (GVBl. S. 183),“ eingefügt.

VII. Art. 8 wird wie folgt gefasst:

„Artikel 8
Einschränkung von Grundrechten

„Das Grundrecht auf das Brief-, Post- und Fernmeldegeheimnis (Art. 10 Abs. 1 des Grundgesetzes, Art. 12 der Verfassung des Landes Hessen) wird durch Art. 1 dieses Gesetzes eingeschränkt. Die Grundrechte auf die Freiheit der Person (Art. 2 Abs. 2 Satz 2 des Grundgesetzes, Art. 5 der Verfassung des Landes Hessen), auf die Versammlungsfreiheit (Art. 8 Abs. 1 des Grundgesetzes, Art. 14 Abs. 1 der Verfassung des Landes Hessen), auf das Brief-, Post- und Fernmeldegeheimnis (Art. 10 Abs. 1 des Grundgesetzes, Art. 12 der Verfassung des Landes Hessen), auf die Freizügigkeit (Art. 11 Abs. 1 des Grundgesetzes, Art. 6 der Verfassung des Landes Hessen) sowie auf die Unverletzlichkeit der Wohnung (Art. 13 des Grundgesetzes, Art. 8 der Verfassung des Landes Hessen) werden durch Art. 2 dieses Gesetzes eingeschränkt.“

Begründung:

I. Allgemeines

Hessen war im Jahr 2018 das erste Bundesland, das mit der Bestimmung des § 25a eine spezielle Rechtsgrundlage dafür geschaffen hat, bisher unverbundene Dateien und Datenquellen in einer Analyseplattform zu vernetzen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen. Vergleichbare Rechtsgrundlagen wurden später in die Polizeigesetze Hamburgs und Nordrhein-Westfalens aufgenommen. Die überwiegende Mehrheit der anderen Bundesländer bereitet derzeit unter der Leitung des Bayerischen Landeskriminalamts ihre Einführung unter dem Arbeitsnamen VeRA (Verfahrensübergreifende Recherche- und Analyseplattform) vor. In Hessen trägt die Analyseplattform die Bezeichnung HessenData.

In allen Fällen wird, weil sie vergleichbaren Produkten anderer Hersteller überlegen ist, derzeit bzw. künftig die Software der Firma Palantir Technologies Inc. verwendet. Ihre besondere Eignung war auch im sogenannten Palantir-Untersuchungsausschuss des Hessischen Landtags von Anfang an unumstritten (vgl. Abweichender Bericht Teil B der Mitglieder der Fraktion der SPD zu dem Zwischenbericht des Untersuchungsausschusses 19/3, Seite 11): „Auch aus Sicht der SPD-Fraktion war die Anschaffung der Analysesoftware unstreitig notwendig".

Eine Prüfung des Quellcodes dieser Software durch das Fraunhofer Institut hat zuletzt ergeben, dass ihr Einsatz ohne durchgreifende Sicherheitsbedenken möglich ist. Eine sogenannte Backdoor, die einen unzulässigen Abfluss von Daten unter Umgehung von Zugriffsbeschränkungen oder einen nicht gewollten Zugriff auf das System von außen zuließe, wurde nicht gefunden.

Nachdem das Bundesverfassungsgericht mit Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – die Bestimmung des § 25a Abs. 1 teilweise für verfassungswidrig erklärt hat, besteht die Notwendigkeit einer Neuregelung. Dies gilt insbesondere für eine Datenanalyse bereits im Gefahrenvorfeld (BVerfG, a. a. O., Rn. 153 ff.). Abhängig vom Eingriffsgewicht dieser Maßnahme (BVerfG, a. a. O., Rn. 75 ff.) können sich je unterschiedliche Anforderungen sowohl an ihren Anlass als auch ihr Ziel ergeben (BVerfG, a. a. O, Rn. 103 ff.), sofern eine Maßnahme nicht bereits durch die Grundsätze der Zweckbindung und Zweckänderung gerechtfertigt ist (BVerfG, a. a. O., Rn. 55 ff.).

II. Im Einzelnen

Zu I. (Art. 1 – Hessisches Verfassungsschutzgesetz)

Aus dem Kreis der im Innenausschuss zum Änderungsantrag angehörten wissenschaftlichen Sachverständigen war an dem Entwurf der Vorschrift betreffend die Übermittlung an Strafverfolgungsbehörden Kritik geäußert worden. Es wurde darauf hingewiesen, dass der Entwurf des § 20a HVSG hinsichtlich der Auswahl der Straftatbestände, die zu einer Übermittlung mit nachrichtendienstlichen Mitteln ersterhobener personenbezogener Daten an Strafverfolgungsbehörden berechtigen, zu stark beschränkt sei. Dies sei verfassungsrechtlich nicht erforderlich, da der Gesetzgeber durch das BVerfG berufen sei, einen im Verfassungsschutzkontext eigenständigen Begriff der besonders schweren Straftat zu definieren, der nicht zwingend mit den Katalogen der StPO übereinstimmen müsse. Die Ausgestaltung der Entwurfsnorm mit einer strikten Beschränkung auf Straftaten mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe erfasse wesentliche, relevante Straftaten nicht. In der mündlichen Sachverständigenanhörung wurden als Beispiele genannt die heimliche Fortführung einer verbotenen extremistischen Vereinigung (§ 85 StGB) oder die Spionage- und Sabotagetätigkeit ausländischer Geheimdienste (sofern es sich nicht um einen „besonders schweren Fall" handele, § 99 Abs. 1 StGB), die beide dem Landesamt für Verfassungsschutz nicht mehr die rechtliche Möglichkeit gäben, vorliegende Erkenntnisse dazu an die zuständigen Strafverfolgungsbehörden weiterzuleiten.

Diese Kritik der Sachverständigen aufgreifend wird daher die Vorschrift des § 20a HVSG geändert, um einen spezifisch dem Auftrag und den Schutzgütern des Verfassungsschutzes entsprechenden Begriff der besonders schweren Straftat zu definieren. Neben den Straftaten mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe wird eine Erweiterung um Straftaten mit einer Höchststrafe von mindestens fünf Jahren aufgenommen, wenn diese Straftaten im Zusammenhang mit der Beteiligung an einer beobachtungsbedürftigen Bestrebung oder einer beobachtungsbedürftigen Tätigkeit im Sinne des Verfassungsschutzgesetzes (§ 2 Abs. 2 HVSG) begangen werden. Daneben wird aus Gründen der Übersichtlichkeit der Norm der bisherige Katalog des § 20a Satz 2 ersetzt durch die Formulierung „Straftaten, die mit einer Höchststrafe bedroht sind von mindestens zehn Jahren Freiheitsstrafe". Bei gesteigerter Lesbarkeit und Zugänglichkeit der Norm ist damit kein Verlust an Normklarheit und Bestimmtheit verbunden, da sich durch die Benennung des Strafrahmens die zur Übermittlung berechtigenden Straftatbestände eindeutig identifizieren lassen.

Zu II. (Art. 2 – Hessisches Gesetz über die öffentliche Sicherheit und Ordnung)

Zu Nr. 1 (Art . 2)

Aufgrund von anderen zwischenzeitlich vorgenommenen Gesetzesänderungen war das Vollzitat zu aktualisieren.

Zu Nr. 2 (Art. 2 Nr. 5 – § 13a HSOG)

Aufgrund weiterer Änderungen in § 13a war Art. 2 Nr. 5 neu zu fassen.

Buchst. a – § 13a Abs. 1 Satz 1
Es handelt sich um eine redaktionelle Änderung. Das Hessische Sicherheitsüberprüfungsgesetz wurde mit Gesetz vom 11. Dezember 2019 umbenannt (GVBl. S. 406). Die Überschrift des Gesetzes lautet „Hessisches Sicherheitsüberprüfungs- und Verschlusssachengesetz“.

Buchst. b – § 13a Abs. 2 Satz 3 und 4 neu

Es handelt sich bei Satz 3 inhaltlich um die ursprüngliche Formulierung aus Art. 2 Nr. 5 des Gesetzentwurfs.

Durch die Umformulierung des Änderungsbefehls wird der bisherige Satz 3 zu Satz 4. Zudem erfolgt die Streichung des zwingenden Schriftformerfordernisses für die dort geregelte Einwilligungserklärung. Hierbei kommt der Gesetzgeber einem Bedarf der Praxis nach. Das Schriftformerfordernis stellt die Behörden insbesondere bei Großereignissen vor große Herausforderungen. Sobald eine Vielzahl an Zuverlässigkeitsüberprüfungen in kurzer Zeit durchgeführt werden muss, geht mit dem zwingenden Schriftformerfordernis ein sehr hoher Verwaltungsaufwand einher. Ein Verfahren mit einer qualifizierten elektronischen Signatur, welche ebenfalls die Anforderungen an die gesetzliche Schriftform erfüllen würde, ist derzeit nicht praxistauglich.

Auch weiterhin kann eine Zuverlässigkeitsüberprüfung nur durchgeführt werden, wenn eine freiwillige Einwilligung der betroffenen Person vorliegt. Die Vorgaben des § 46 Hessisches Datenschutz- und Informationsfreiheitsgesetz, auf welche zur Klarstellung in Satz 4 ausdrücklich verwiesen wird, gelten unmittelbar. Die Form der Einwilligungserklärung kann danach frei gewählt werden, wobei der Verantwortliche auch weiterhin die Einwilligung der betroffenen Person nachweisen können muss. Die Gesetzesänderung stellt eine Weiterentwicklung und nachhaltige Modernisierung des Verfahrens der Zuverlässigkeitsüberprüfung dar, da z. B. die Möglichkeit einer einfachen elektronischen Einwilligungserklärung im Rahmen von Großveranstaltungen mit mehreren zehntausenden zu überprüfenden Personen papierlos und mit weniger Aufwand gestaltet werden kann. Insofern ist der Wegfall des zwingenden Schriftformerfordernisses auch zeitgemäß und entspricht den Regelungen in vielen anderen Ländern.

Der betroffenen Person wird im Rahmen der freiwilligen Einwilligung auch weiterhin mitgeteilt, wo sie weitere Auskünfte zu dem Verfahren erhalten kann und dass sie sich an den Hessischen Datenschutzbeauftragten wenden kann (§ 13a Abs. 2 Satz 4 HSOG). Auch das jederzeitige Recht, die Einwilligung zu widerrufen, bleibt bestehen (§ 46 Abs. 3 HDSIG).

Zu Nr. 3 (Art. 2 Nr. 6 – § 14 Abs. 3a HSOG)

Dem durch Art. 2 Nr. 6 eingefügten Abs. 3a wird ein weiterer Satz angefügt. Hierdurch wird klargestellt, dass für Videoüberwachungsanlagen nach Abs. 3a die gleichen Vorgaben wie für Videoüberwachungsanlagen nach Abs. 3 gelten.

Dies betrifft die Vorgaben hinsichtlich Vernichtung und weitere Verwendung der personenbezogenen Daten in Abs. 1 Satz 2 und 3 sowie die Hinweispflicht und die zweijährige Überprüfungspflicht für fest installierte Anlagen in Abs. 3 Satz 2 und 3.

Zu Nr. 4 (Art. 2 Nr. 9 Buchst. b – § 15a Abs. 2 Satz 1 HSOG)

Redaktionelle Änderung. Es handelt sich um die Behebung eines redaktionellen Versehens, nach welchem auch auf § 9 Abs. 1 Satz 2 des Telekommunikation-Telemedien-Datenschutz-Gesetzes verwiesen wurde.

Zu Nr. 5 (Art. 2 Nr. 16 Buchst. b – § 20 Abs. 6 Satz 2 HSOG)

Redaktionelle Änderung. Der durch Art. 2 Nr. 16 Buchst. b eingefügte neue Satz 2 entspricht im zweiten Satzteil dem bisherigen Satz 2. Daher ist der bisherige Satz 2 zu streichen.

Zu Nr. 6 (Art. 2 Nr. 18 – § 25a HSOG)

Das Bundesverfassungsgericht hat in seinem Urteil bestätigt, dass die Bestimmung des § 25a dem legitimen Zweck dient, vor dem Hintergrund informationstechnischer Entwicklungen die Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten zu steigern, indem Anhaltspunkte für bevorstehende schwere Straftaten gewonnen werden, die im Datenbestand der Polizei ansonsten unerkannt blieben. Auch sei die Regelung des § 25a zur Steigerung der Wirksamkeit der vorbeugenden Straftatenbekämpfung geeignet und erforderlich. Denn durch eine automatisierte Datenanalyse könnten für die Verhütung von Straftaten relevante Erkenntnisse erschlossen werden, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 52 f.). Allerdings ist die Regelung des § 25a derzeit nicht präzise genug gefasst, um die Verhältnismäßigkeit einer Datenanalyse in jedem Einzelfall sicherstellen zu können (BVerfG, a. a. O., Rn. 123 ff., 152 ff.). Dieser Fehler soll mit der Neuregelung behoben werden.

Zu Abs. 1

Sätze 1 und 2 beschreiben im Sinne einer Legaldefinition das technische Verfahren einer automatisierten Datenanalyse. Es besteht aus zwei logisch aufeinander aufbauenden, aber praktisch zeitgleich stattfindenden Schritten, nämlich dem Zusammenführen unterschiedlicher „Datentöpfe“ auf der Analyseplattform und der sich daran anschließenden Recherche innerhalb des so zusammengeführten Datenbestands. Der erste Schritt überwindet das strukturelle Problem, dass in den Beständen der Polizei Daten in unterschiedlichen Formaten und disparaten Dateien gespeichert und damit nicht im selben Bearbeitungskontext gleichzeitig verfügbar sind, der zweite führt zu der verfassungsrechtlich relevanten Frage, was genau die Polizei mit den so zusammengeführten Daten machen darf und was nicht.

Satz 3 enthält mit seiner deskriptiv-programmatischen Aussage bereits eine erste rechtsverbindliche Antwort auf diese Frage. Mit Blick auf die vom Bundesverfassungsgericht geäußerte Besorgnis, dass eine Analysesoftware die polizeiliche Arbeit möglicherweise so verändern könnte, dass der Faktor Mensch in den Hintergrund tritt („maschinelle Gefährlichkeitsaussagen“, BVerfGE, a. a. O., Rn. 121), dass diese Software von Menschen getroffene Entscheidungen sogar ersetzen könnte („predictive policing“, BVerfG, a. a. O., Rn. 100), stellt diese Bestimmung klar, dass immer – und natürlich immer auch in all seiner Fehlerhaftigkeit – der Mensch am Anfang und am Ende des Entscheidungsprozesses steht. Die Analyseplattform darf die Arbeitsweise der Polizei also nicht „entscheidend verändern“ (BVerfG, a. a. O., Rn. 70), sondern sie soll helfen, ihre bewährte Arbeitsweise zu verbessern, nämlich Informationen aus verschiedenen Quellen zusammenzustellen und sie zu bewerten. Dass etwa eine polizeiliche Sachbearbeiterin bei Dienstbeginn das Analysetool gleichsam befragt, was heute denn zu tun sei, wird durch diesen Satz ausgeschlossen, und dieses Verbot ist durch Zugriffskontrollen und Begründungspflichten gemäß Abs. 5 organisatorisch und verfahrensrechtlich zudem streng abgesichert (vgl. zum Sachverhaltsbezug BVerfG, a. a. O., Rn. 93). Bereits die Kriterien der Anlass-, Fall- und Zielbezogenheit als Voraussetzung für die Nutzung dieses Instruments stellen damit sicher, dass eine Analysesoftware nicht etwa ein wie immer geartetes Eigenleben oder gar eigene Gesetzmäßigkeiten entwickelt, sondern dass sie bleibt, was sie derzeit schon ist, nämlich ein bloßes Hilfsinstrument.

Die Eigenschaft des Analysetools als ein vom Menschen hergestelltes und von ihm kontrolliertes Hilfsinstrument wird auch durch die Vorgabe des Satzes 4 abgesichert, wonach die automatisierte Datenanalyse manuell ausgelöst wird und weitere Verarbeitungsschritten von Menschen veranlasst werden oder von ihnen vorher festgelegt worden sind. Der Analysevorgang selbst besteht aus einer Reihe simultan ausgelöster und miteinander in Verbindung gesetzter, auf Wenn-Dann-Operatoren beruhender Suchaktionen über den zuvor zusammengeführten Datenbestand. Als regelbasierte oder, gleichbedeutend, deterministische (vgl. BVerfG, a. a. O., Rn. 101) Datenanalyse folgt sie einem klar definierten, unveränderlichen Ablauf und erzeugt deshalb auch konsistente und reproduzierbare Ergebnisse, die einer Gegenkontrolle leichter zugänglich sind als die Datenanalyse unter Einbeziehung selbstlernender Systeme.

Satz 5 enthält ein ausdrückliches und striktes Verbot der Anbindung des Analysetools an das Internet, weil damit die automatisierte Verarbeitung einer unüberschaubar großen Zahl personenbezogener Daten Unbeteiligter verbunden wäre (vgl. BVerfG, a. a. O., Rn. 88). Auch dieses Verbot hat insofern programmatischen Charakter, als es sichtbar machen will, dass eine Analyseplattform die Nutzbarmachung lediglich der von der Polizei zulässigerweise gespeicherten Daten verbessern will. Erforderlichenfalls können aber die bei der Bearbeitung eines konkreten Fallkomplexes gezielt ermittelten und zuvor von den Polizeibehörden gespeicherten Daten, die bei einer Internetrecherche angefallen sind, in die automatisierte Datenanalyse einbezogen werden (dazu unten).

Zu Abs. 2

Abs. 2 überträgt das in Abs. 1 Satz 2 normierte Prinzip der Anlass-, Fall- und Zielbezogenheit der automatisierten Datenanalyse in die Polizeirechtsdogmatik. Mit Blick auf die verfassungsrechtlich hier vorgegebenen Parameter (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 51 ff., insb. Rn. 107 ff.) umschreibt er drei Tatbestandsvarianten, nach denen eine automatisierte Datenanalyse erlaubt ist. Die praktisch bedeutsameren Varianten Nr. 2 und Nr. 3 stehen dabei in einem reziproken Verhältnis zueinander. Erstere erlaubt den Einsatz bereits zum Schutz von Rechtsgütern mittleren Gewichts und verlangt dafür das Vorliegen einer wenigstens konkretisierten Gefahr, letztere verlangt den Schutz von Rechtsgütern hohen Gewichts und erlaubt ihren Einsatz deshalb schon im Gefahrenvorfeld. Ihnen vorgeschaltet ist die Tatbestandsalternative Nr. 1. Sie stellt hier die strengsten Anforderungen sowohl an die zeitliche Nähe des befürchteten Schadens als auch an den Rang der zu schützenden Rechtsgüter. Diese Variante ist im Verfahren 1 BvR 1547/19 vom Bundesverfassungsgericht nicht beanstandet worden, weil insoweit die Beschwerdeführer eine Grundrechtsverletzung nicht hinreichend substantiiert darlegen konnten (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rd. 71 ff., Rn. 47 f.). Die in der Entscheidung angeschnittenen, aber notwendigerweise offengelassenen verfassungsrechtlichen Erfordernisse auch für diese Variante (a. a. O., Rn. 48) werden in der Neuregelung aufgegriffen und berücksichtigt.

Alle drei Varianten sind in Beziehung zu setzen zum je spezifischen Eingriffsgewicht der automatisierten Datenanalyse, dessen Austarierung wiederum Voraussetzung dafür ist, dass die Verhältnismäßigkeit dieser Maßnahme im Einzelfall gewahrt bleibt (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 71 ff., 110 ff.). Die Notwendigkeit einer sorgfältigen Austarierung des Eingriffsgewichts kommt vor allem, wenn auch nicht nur (BVerfG, a. a. O., Rn. 111), beim Einsatz dieses Instruments im Gefahrenvorfeld zum Tragen (BVerfG, a. a. O., Rn. 112 ff.). Das heißt, dass im Fall einer Datenanalyse nach Variante Nr. 1 – Anhaltspunkte für einen drohenden terroristischen Anschlag auf ein Einkaufszentrum, Hinweise auf bevorstehende Sabotageakte gegen eine Energieversorgungsanlage, Spuren zum Aufenthaltsort eines entführten Kindes – das Eingriffsgewicht einer Datenanalyse im Einzelfall vergleichsweise hoch sein darf, und dass im Fall einer Datenanalyse nach Variante Nr. 3 – Aufdeckung von Absatzwegen, Nachzeichnung von Geldflüssen oder Identifizierung von Hintermännern bei der vorbeugenden Bekämpfung des Rauschgifthandels, der Geldwäsche oder der Waffenschieberei – das Eingriffsgewicht der Datenanalyse im Vergleich dazu „erheblich gesenkt“ (BVerfG, a. a. O., Rn. 110) sein muss. Die Variante Nr. 2 bewegt sich zwischen diesen beiden Varianten.

Das verfassungsrechtliche Erfordernis einer gleichsam auf dem Hintergrund unterschiedlicher Ebenen, Sektoren und Skalen auszudifferenzierenden Rechtsgrundlage für ein und dasselbe Instrument wirft gesetzestechnisch nicht leicht zu bewältigende Regelungs- und Anwendungsprobleme auf. Wegen der dem Gefahrenbegriff eigentümlichen Wechselwirkung zwischen Schadenshöhe und Eintrittswahrscheinlichkeit beschreibt jede der drei Varianten einen Korridor, dessen Grenzen schon für sich beweglich sind. Hier müssen, will man die Möglichkeiten eines solchen Instruments gleichzeitig nutzbringend und verfassungskonform einsetzen, mehrere bewegliche Korridore, die zudem nicht trennscharf nebeneinander verlaufen, sondern ineinander übergehen und sich sogar überlappen können, zwecks Bemessung des je zulässigen Eingriffsgewichts zueinander in Beziehung gesetzt werden. Und es müssen mit einer solchen Regelung alltagspraktische Situationen normativ bewältigt werden können, in denen derselbe Sachkomplex, weil im Laufe der Fallbearbeitung angefallene Erkenntnisse zu einer oder mehreren kategorialen Neubewertungen führen, nacheinander in den Anwendungsbereich unterschiedlicher Korridore fällt. Quer zu dieser Differenzierung verläuft das aus dem Grundsätzen der Zweckbindung und Zweckänderung abgeleitete Gebot, an die Weiterverarbeitung besonders grundrechtssensibler Daten besondere Anforderungen zu stellen, sowie das übergeordnete, aus dem Rechtsstaatsprinzip abgeleitete Ziel, dass in jedem Stadium des Verfahrens die Rechte Unbeteiligter maximal zu schonen sind, ihre Daten also schon zu Beginn des Verarbeitungsprozesses unsichtbar gemacht oder jedenfalls nicht automatisiert weiterverarbeitet werden, um zu vermeiden, dass am Ende, gewissermaßen ungewollt-systembedingt, Polizeieinsätze gegen Personen stattfinden, die mit der Sache nichts zu tun haben (zu dieser Befürchtung BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 77, 84, 126), woran nicht zuletzt die Polizei selbst das größte Interesse hat.

Das Gesetz will dieser Aufgabe – Effektuierung der Möglichkeiten einer automatisierten Datenanalyse bei bestmöglichem Grundrechtsschutz – durch eine Verschränkung zweier Prinzipien gerecht werden, nämlich der gegenständlichen Reduzierung der Eingriffsintensität bereits durch Gesetz sowie ihrer funktionalen Reduzierung durch Verwaltungsvorschriften. Der gegenständlichen Reduzierung der Eingriffsintensität geht eine Identifizierung und Bewertung besonders grundrechtssensibler Teilmaterien voraus, deren verschiedene Aspekte in eine Interessenabwägung einfließen und dort nach Möglichkeit schon auf der Ebene der Gesetzgebung zu einem Ausgleich gebracht werden. Ein Ergebnis dieses Prozesses ist beispielsweise die Entscheidung, dass Verkehrsdaten, weil sie viele personenbezogene Daten vieler Unbeteiligter enthalten, nur bei mindestens konkretisierten Gefahren in die Analyseplattform überführt werden dürfen, nicht aber schon bei Maßnahmen im Gefahrenvorfeld, weil hier der Faktor Zeit im Verhältnis zur Grundrechtsrelevanz (Streubreite) tendenziell nachrangig ist und im Einzelfall entstehende Effektivitätseinbußen deshalb hinzunehmen sind. Ein anderes Beispiel ist die Entscheidung, dass personen-

bezogene Daten aus Wohnraumüberwachungen und Online-Durchsuchungen wegen der Schwere des Grundrechtseingriffs vollständig auszusondern sind, sodass sie in keinem der Anwendungsfälle automatisiert weiterverarbeitet werden können, obwohl es verfassungsrechtlich zulässig gewesen wäre, das Verbot auf den Anwendungsbereich der Variante Nr. 3 zu begrenzen (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 118). Auch diese Entscheidung mag im Einzelfall zu Effizienzverlusten führen. Sie ist aber geeignet, einer verfassungsrechtlich problematischen Erstellung umfassender Persönlichkeitsbilder vorzubeugen (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 70).

Ein weiteres Ergebnis dieses Abwägungsprozesses ist aber auch die Entscheidung dafür, die Anzahl der „Datentöpfe“, die in der Analyseplattform zusammengeführt werden dürfen, nicht noch weiter zu reduzieren. Dies gilt namentlich auch für die praktisch relevanten Daten aus strafprozessualen TKÜ-Maßnahmen. Denn gerade im (schnellen) Auffinden von Daten, die bei der Polizei in unterschiedlichen Beständen gespeichert sind, liegt die besondere Qualität der Analyseplattform, und auch daran besteht ein legitimes öffentliches Interesse (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 52, 70), welches in die Gesamtbetrachtung einzustellen ist. Die tatbestandlichen Voraussetzungen für ihre Verwendung als Spurenansatz im Rahmen der automatisierten Datenanalyse sind unter Berücksichtigung des Umstands, dass die Kommunikationsinhalte selbst nicht automatisiert weiterverarbeitet werden, deshalb so gefasst, dass die zweckändernde Weiterverwendung den verfassungsrechtlichen Anforderungen genügt. Sie dienen im Einzelfall nach jeder der drei Varianten des Abs. 2 als konkrete Ermittlungsansätze zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die, zu deren Schutz die Datenerhebung zulässig ist (vgl. BVerfG, a. a. O., Rn. 63; BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 290). Zum einen sind die Schutzgüter nach Variante Nr. 2 ihrem Gewicht nach (Verhütung von Straftaten von erheblicher Bedeutung gemäß § 13 Abs. 3) vergleichbar mit denen, zu denen die Datenerhebung erlaubt wird (Verfolgung schwerer Straftaten, vgl. unten). Zum anderen erlaubt auch die Verhütung von Straftaten nach Variante Nr. 3 keine Maßnahmen ins Blaue hinein, sondern nur solche auf mittlere Sicht.

Die gebotene Reduzierung der Datenmenge und damit die Verringerung der Eingriffsintensität erfolgt deshalb schwerpunktmäßig funktional, indem unter Berücksichtigung und Fortentwicklung bewährter arbeitsteiliger Organisations- und Rechtsformen (vgl. BVerfG, a. a. O., Rn. 12, 27) die Schaffung zeitgemäßer, an situativen Anforderungen ausgerichteter Rollen- und Rechtekonzepte durch die Verwaltung verbindlich vorgeschrieben wird mit der Folge, dass die im Einzelfall jeweils zu verarbeitende Datenmenge immer nur ein – mehr oder weniger großer – Ausschnitt des auf der Plattform zusammengeführten und damit potentiell verfügbaren Datenbestandes ist. Die Datentöpfe sind also zwar vorhanden. Ihr Inhalt darf aber jeweils nur in Teilen entnommen werden. Weil der Gesetzgeber in seinem an die Verwaltung adressierten Regelungsauftrag hierfür nur übergeordnete Ziele, abstrakte Maßstäbe und beispielhafte Kriterien vorgibt, ist es der Verwaltung nicht verwehrt, in Fällen dringender Gefahren für höchstrangige Rechtsgüter – drohender Terroranschlag – erforderlichenfalls auch das „volle Programm“ zuzulassen, also einzelnen Anwendern den Zugriff auf den vollständigen Inhalt aller Datentöpfe zu erlauben.

Zu Abs. 2 Satz 1

Abs. 2 Satz 1 verlangt in allen drei Tatbestandsvarianten eine von den Polizeibehörden anzustellende Prognose für ein künftiges Geschehen. Unabhängig von der je unterschiedlichen zeitlichen Komponente – konkrete Gefahr, konkretisierte Gefahr, Gefahrenvorfeld – muss eine solche Prognose immer von tatsächlichen Anhaltspunkten getragen werden. Dieses – auch der tradierten Variante Nr. 1 immanente – Tatbestandsmerkmal ist weit zu verstehen und umfasst alles, was Menschen von ihrer Außenwelt wahrnehmen können, mit anderen Worten die Gesamtheit dessen, was unter dem Begriff Wirklichkeit verstanden wird und als solche beobachtet werden kann. Es erfasst von vornherein nur äußere Tatsachen, nicht innere. So sind die verbrecherische Gesinnung, der Hang zu Straftaten oder Gewissenlosigkeit (innere) Tatsachen, die typischerweise in strafgerichtliche Urteile einfließen, aber auch der Polizei Anlass für die Einschätzung geben können, jemand werde künftig Straftaten begehen. Diese inneren Tatsachen müssen aber immer aus solchen Tatsachen erschlossen werden, die der äußeren Geschehenswelt angehören (vgl. Rachor in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Auflage, 2012, Kap. E Rn. 159). Im Polizeialltag sind das in erster Linie sämtliche Informationen, die der Polizei von Dritten, etwa von Anzeigeerstattern und Hinweisgebern zugetragen oder von anderen Behörden übermittelt werden, sowie solchen, welche die Polizei eigeninitiativ und zielgerichtet ermittelt, etwa durch Zeugenbefragungen, behördliche Auskunftsersuchen oder auch verdeckte Ermittlungen, einschließlich der bei diesen Maßnahmen typischerweise nebenbei anfallenden Erkenntnisse oder auch zufällig und völlig unerwartet sich ergebenden Beobachtungen, die für sich oder in Kombination mit anderen ein mehr oder weniger komplexes, nicht selten sich fortlaufend wandelndes – sich verdichtendes, sich abschwächendes – polizeiliches Lagebild ergeben. Jedes Detail, jede Facette und jede Randnotiz kann zu diesem Bild beitragen.

Wegen der Weite des Begriffs und der daraus resultierenden Schwierigkeit, ihn zu konturieren und damit positiv zu umschreiben, wird er meist negativ, von seinen Grenzen her gefasst. Danach sind tatsächliche Anhaltspunkte Tatsachen, die eine polizeiliche Prognose tragen können und die von reinen Spekulationen, hypothetischen Erwägungen, fallunabhängigen Vermutungen sowie allgemeinen Erfahrungssätze als Grundlage einer Prognose und von einem Handeln ins Blaue hinein abzugrenzen sind (vgl. nur BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 158, 161; BVerfG, Beschluss vom 10. November 2020 – 1 BvR 3214/15 –, BVerfGE 156, 11-63, Rn. 130; BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08 –, BVerfGE 125, 260-385, Rn. 231; BVerfG, Urteil vom 20. Februar 2001 – 2 BvR 1444/00 –, BVerfGE 103, 142-164, Rn. 46). Diese Abgrenzung „nach unten“ macht den Begriff für die alltägliche Rechtsanwendung praktisch handhabbar und ermöglicht gleichzeitig eine effektive nachträgliche Rechtskontrolle.

Der Begriff der tatsächlichen Anhaltspunkte bringt, anders als das Wort Tatsachen, bereits für sich das dem polizeilichen Kontext inhärente prognostische Element zum Ausdruck („Anhaltspunkte wofür?“, vgl. Rachor in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Auflage, 2012, Kap. E Rn. 158). Die aus einer unübersehbaren Anzahl von Tatsachen bestehende Lebenswirklichkeit ist für die polizeiliche Aufgabenstellung nur insoweit relevant, als sie Informationen darüber enthält, dass ein Schaden für polizeilich geschützte Rechtsgüter zu erwarten ist und wie der Eintritt eines Schadens verhindert werden kann. Tatsächliche Anhaltspunkte sind also Indiztatsachen (VGH Kassel, Urteil vom 23. Juni 2017 – 8 D 2714/16 – juris Rn. 18). Nur an Indiztatsachen hat die Polizei ein Interesse, und nur darauf ist die Analyseplattform deshalb ausgerichtet. Damit beschreibt der Begriff der tatsächlichen Anhaltspunkte in seinem zweiten Wortbestandteil das normative Erfordernis und die tatsächliche, idealerweise auf guter Ausbildung sowie kriminalistischer Erfahrung (vgl. VGH Kassel, Urteil vom 23. Juni 2017 – 8 D 2714/16 – juris Rn. 18; vgl. dazu auch Bäcker, in Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Kap. D Rn. 88) beruhende Fähigkeit der Polizeibeamtinnen und -beamten, Tatsachen als Indiztatsachen zu erkennen, einzuordnen und zu bewerten, um sie im Fall ihrer Brauchbarkeit als Spuren- oder Ermittlungsansätze, allein oder in Verknüpfung mit bereits vorliegenden Informationen, nach der Methode der abgestuften Erkenntnisverdichtung zum Ausgangspunkt weiterer Ermittlungen machen zu können (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 68 f.).

Das im Unterschied zur repressiven Ermittlungstätigkeit zusätzliche Erfordernis der Prognose eines (künftigen) Geschehensablaufs bei der Gefahrenabwehr – der schwierigste Teil des polizeilichen Entscheidungsfindungsprozesses – wird, abgestuft nach Wahrscheinlichkeitsgraden, in den drei Tatbestandsvarianten des Satzes 1 abgebildet. Der in Variante 1 verwendete traditionelle polizeirechtliche Begriff der konkreten Gefahr setzt eine Sachlage voraus, die bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens im Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einer Verletzung eines polizeilichen Schutzguts führt (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 – Rn. 111). Eine konkretisierte Gefahr im Sinne der Variante 2 liegt dann vor, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, aber bereits bestimmte Tatsachen darauf hinweisen, dass eine Straftat von mindestens erheblichem Gewicht begangen werden wird. Die Tatsachen müssen zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die automatisierte Datenanalyse gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (vgl. BVerfG, a. a. O., Rn. 112; BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 112). Das von der Variante 3 schließlich erfasste Vorfeld einer konkretisierten Gefahr (vgl. zur Zulässigkeit solcher Vorfeldmaßnahmen bei der automatisierten Datenanalyse BVerfG, Urteil vom 16. Februar 2023, a. a. O., Rn. 107, 112 ff.) ist durch eine höhere Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet, weil die Geschehnisse in harmlosen Zusammenhängen verbleiben, aber auch den Beginn eines Vorgangs bilden können, der in eine Gefahr mündet (vgl. BVerfG, Urteil vom 20. April 2016, a. a. O., Rn. 113). Indem diese Tatbestandsvariante ein größeres Maß an Ungewissheit darüber erlaubt, in welche Richtung ein Geschehen sich entwickeln wird, hat sie nach den Prinzipien der sogenannten Anscheinsgefahr – wie würde, rückblickend betrachtet, eine gewissenhafte, besonnene und sachkundige Beamtin gehandelt haben – auch eine größere Fehlertoleranz. Wie oben ausgeführt sind die Übergänge zwischen den jeweils „benachbarten“ Varianten fließend mit der Folge, dass die Anforderungen an die Vergewisserung bei der Nutzung der automatisierten Datenanalyse nach den unterschiedlichen Varianten eher gradueller denn kategorialer Natur sind.

Grenzt man also das der Polizei hier offenstehende Vorfeld der konkretisierten Gefahr von dem weiter reichenden, nur den Verfassungsschutzbehörden offenstehende Vorfeld, nämlich dem „Vorfeld von Gefährdungslagen“ (BVerfG, Urteil 26.04.2022 –1 BvR 1619/17 – Rn. 154) und der damit aufgabenspezifisch verbundenen langen Sicht ab, wird man den Unterschied annähernd mit dem Begriff der „auf mittlere Sicht drohenden Gefahren“ (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 63; BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/0 – Rn. 290) umschreiben können, einer Sachlage also, die im Vergleich zur konkretisierten Gefahr durch größere Ungewissheiten sowohl in Bezug auf die Tatsachengrundlage als auch den

möglichen Kausalverlauf geprägt ist (vgl. Bäcker, in Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Kap. D Rn. 235 ff., Rn. 259) und deshalb zwar keine operativen Maßnahmen, aber die weitere Aufklärung des Sachverhalts im Wege einer Auswertung der vorhandenen Datenbestände rechtfertigen kann.

Tragfähiger Anknüpfungspunkt einer Prognose ist in der polizeilichen Praxis typischerweise die bereits bekannte Verstrickung einer bestimmten Person in strafbare Handlungen. Tatsachen, die jemanden zum Tatverdächtigen oder Beschuldigten machen oder gar zu seiner strafgerichtlichen Verurteilung geführt haben, können, für sich oder in Kombination mit sonstigen Erkenntnissen – Art oder Ausführung der Tat (vgl. § 19 Abs. 2 Nr. 2), Häufigkeit früherer Ermittlungsverfahren, Verbindungen zu anderen Personen oder Gruppierungen –, die Einschätzung rechtfertigen, dass auch künftig mit (vergleichbaren) Straftaten zu rechnen ist. Auch die damit korrespondierende Neufassung des § 20 Abs. 6 stellt jetzt ausdrücklich klar, dass personenbezogene Daten von Tatverdächtigen auch nach Abschluss des Ermittlungsverfahrens zum Zweck der Verhinderung künftiger Straftaten nur dann gespeichert werden dürfen, wenn zuvor eine sogenannte Negativprognose erstellt worden ist (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 126). Praktisch relevant wird die automatisierte Datenanalyse für die Polizei deshalb vor allem dann, wenn es um die Verhinderung solcher Straftaten geht, die regelmäßig in Serie begangen werden (vgl. § 13 Abs. 3 Buchst. c). In der konkreten Fallbearbeitung wird auf der Grundlage kriminalistischer Erfahrungssätze bereits aus der Begehung einer solchen Straftat regelmäßig geschlossen werden können, dass künftig weitere Straftaten begangen werden (vgl. BVerfG, a. a. O., Rn. 160 f.).

Die Wertigkeit der Schutzgüter nach den Varianten Nr. 2 und Nr. 3 – beide Varianten erlauben von vornherein nur weniger gewichtige Eingriffe (BVerfG, a. a. O, Rn. 107) – korreliert jeweils mit dem Anlass, zu dem die automatisierte Datenanalyse stattfinden darf.

Weil eine Maßnahme reduzierten Eingriffsgewichts nach Variante Nr. 3 bereits im Gefahrenvorfeld zulässig ist, sind hohe Anforderungen an das Gewicht der zu schützenden Rechtsgüter zu stellen. Mit Blick darauf, dass in der Praxis der Anlass für eine automatisierte Datenanalyse zum Zweck der Gefahrenverhütung typischerweise ein strafrechtliches Ermittlungsverfahren ist, und weil sich insbesondere bei der Beobachtung der schweren und organisierten Kriminalität repressive und präventive Elemente häufig überschneiden, knüpft diese Variante aus Gründen der Kohärenz mit strafprozessualen Maßnahmen und in Anlehnung an die – verfassungsgerichtlich gebilligte (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 52) – Terminologie des § 1 Abs. 4 – vorbeugende Bekämpfung von Straftaten, Verhütung von Straftaten – nicht an eine abstrakte Umschreibung von hochrangigen Rechtsgütern an, die vor Schäden zu bewahren sind, sondern an schwere und besonders schwere Straftaten, deren Begehung verhindert werden soll. In Anlehnung an die vom Bundesverfassungsgericht in seinem Urteil zur akustischen Wohnraumüberwachung entwickelte (BVerfG, Urteil vom 3. März 2004 – 1 BvR 2378/98 – Rn. 248) und bis heute fortgeschriebene (vgl. BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 – Rn. 107; BVerfG, Urteil vom 16. April 2022, a. a. O, Rn. 251) und damit verfestigte Nomenklatur sind schwere Straftaten solche, die mit einer Höchststrafe von mindestens fünf Jahren Freiheitsstrafe und sind besonders schwere Straftaten solche, die mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe bedroht sind. Maßgeblicher Anknüpfungspunkt für die Einordnung ist der abstrakte Strafrahmen, wie er vom Gesetzgeber für eine bestimmte Straftat festgelegt wird (BVerfG, Urteil vom 3. März 2004, a. a. O., Rn. 247 f.), praktisch relevant sind vor allem die Straftatenkataloge der §§ 100a Abs. 2, 100b Abs. 2 StPO.

Weil eine Maßnahme reduzierten Eingriffsgewichts nach Variante Nr. 2 eine mindestens konkretisierte Gefahr voraussetzt, ist sie bereits dann zulässig, wenn sie der Verhütung von Straftaten von erheblicher Bedeutung dient (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 107). Das sind die in § 13 Abs. 3 teils konkret benannten, teils abstrakt umschriebenen Straftaten (vgl. zur Bestimmtheit dieses Begriffs nur BVerfG, Beschluss vom 3. März 2004 – 1 BvF 3/92 – Rn. 39). Praktisch bedeutsam sind hier nicht zuletzt die gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangenen Straftaten, die im Einzelfall nach Art und Schwere geeignet sind, den Rechtsfrieden besonders zu stören, weil bereits Art und Weise ihrer Begehung häufig ein tragfähiges Indiz dafür sein dürften, dass mit ihrer Begehung auch künftig zu rechnen ist. Wie im Übrigen die Aufzählungen in § 13 Abs. 3 Nr. 1 (Verbrechen), Nr. 2a (z. B. Straftaten gegen Leib, Leben oder Freiheit) und Nr. 2b (z. B. Staatsschutzstraftaten) zeigen, gibt es zwischen den Varianten Nr. 2 und Nr. 3 deutliche Überschneidungen.

Weil eine Maßnahme nach Variante Nr. 1 eine konkrete Gefahr voraussetzt und dem Schutz ausschließlich hochrangiger Rechtsgüter dient, lässt sie eine automatisierte Datenanalyse mit ohem Eingriffsgewicht zu (BVerfG, a. a. O., Rn. 107). Sie ist von allen drei Varianten diejenige, die am wenigstens strafrechtsinduziert ist, bei welcher also weder regelmäßig ein strafprozessualer Ausgangssachverhalt den Anlass für eine präventive Datenanalyse gibt noch ein Fallkomplex sich als mehr oder weniger unübersichtliche Gemengelage gleichzeitig präventiver und repressiver Aspekte, Erwägungen und Herangehensweisen darstellt. Die von Variante Nr. 1 erfassten Fälle der Verhinderung eines geplanten Anschlags, der raschen Beendigung eines Amoklaufs oder der Befreiung einer Geisel zeigen, dass hier die schnelle und effektive Gefahrenabwehr die alles über-

ragende Grundüberlegung bei der Erstellung des Lagebilds und der darauf aufbauenden Einsatztaktik ist, hinter welche strafprozessuale Erwägungen wie etwa die Beweissicherung mindestens zeitweise zurücktreten müssen. Aus diesem Grund werden die zu schützenden Rechtsgüter in dieser Variante nicht mit Hilfe von Straftatbeständen definiert, sondern durch ihre positive Benennung.

Zu Abs. 2 Satz 2

Abs. 2 Satz 2 bestimmt, welche Datenbestände auf der Analyseplattform zusammengeführt werden dürfen. Die positive Benennung hat den Charakter einer abschließenden Regelung und enthält damit gleichzeitig eine Begrenzung der Datenmenge (vgl. BVerfG, a. a. O., Rn. 78). Im Einzelfall, hier in Bezug auf die Verkehrsdaten, ist es aus Gründen der Verhältnismäßigkeit bereits gesetzlich ausgeschlossen, dass Daten auf die Plattform gezogen werden (dazu unten zu Satz 4). In ihrem Umfang begrenzte, zielgenau abgefragte Datensätze aus Datensätzen, die bei anderen Behörden gespeichert sind, dürfen erforderlichenfalls in eine automatisierte Datenanalyse ergänzend einbezogen werden (dazu unten zu Satz 3).

- Praktisch sehr bedeutsam sind die Daten aus der **Vorgangsverwaltung** gemäß § 20 Abs. 9 (Vorgangsdaten). Das von der hessischen Polizei aktuell verwendete Vorgangsverwaltungssystem heißt ComVor. Ziel der Vorgangsverwaltung ist es, die bei einer Dienststelle anfallenden Informationen in Form einer elektronischen Akte geordnet aufzubewahren und ein Wiederauffinden zu ermöglichen. Aufgenommen werden darin insbesondere Anzeigen, Ermittlungsberichte und Vermerke, enthalten sind nicht nur Daten von Verdächtigen oder Beschuldigten oder sonstigen Anlasspersonen, sondern auch Daten von Anzeigeerstattern und Zeugen. Ein Vorgang umfasst also sämtliche Unterlagen, die im Zusammenhang einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder einen sonstigen Gegenstand polizeilichen Handelns geführt werden (vgl. Müller/Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G, Rn. 832 m. w. N.); Arzt, in: Lisken/Denninger, a. a. O., Abschnitt G, Rn. 1184 m. w. N., zusammenfassend BVerfG, Urteil vom 20. Februar 2023, a. a.O., Rn. 134). Weil Daten im Vorgangsverwaltungssystem typischerweise auch viele Unbeteiligte betreffen, werden deren Daten, um die Eingriffsintensität zu verringern, bei der automatisierten Datenanalyse unsichtbar gemacht.
- In **Fallbearbeitungssystemen** enthaltene Falldaten dienen dazu, die polizeiliche Fallbearbeitung bei komplexen, fallübergreifenden Ermittlungen oder Strukturermittlungen zu unterstützen. Ein Fallbearbeitungssystem geht insoweit über die reine Verwaltung von Vorgangsdaten hinaus, als es dem Anwender ein benutzerfreundliches, speziell auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug zur Verfügung stellt, das weniger personenbezogen als vielmehr ereignisbezogen ausgerichtet ist und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen abbildet und sowohl zu präventiven als auch repressiven Zwecken eingesetzt werden kann (vgl. Arzt, in Lisken/Denninger, a. a. O., Rn. 1289 ff.). Vorgangsverwaltungssysteme enthalten ganz überwiegend Daten von Anlasspersonen und deren Kontaktpersonen aus strafrechtlichen Ermittlungsverfahren. Die hessische Polizei verwendet zur Fallbearbeitung aktuell eine Software namens CRIME-ST.
- **Polizeiliche Auskunftssysteme** enthalten personenbezogene Informationen, die überwiegend, wenn auch nicht ausschließlich, aus strafrechtlichen Ermittlungsverfahren stammen und dort sowohl zum Zweck der Gefahrenabwehr gemäß § 1 Abs. 1 bzw. zur vorbeugenden Straftatenbekämpfung gemäß § 1 Abs. 4 als auch zum Zweck der Strafverfolgung und -vollstreckung gespeichert werden. Das bei der hessischen Polizei verwendete Auskunftssystem heißt POLAS und besteht aus unterschiedlichen Datengruppen. Die derzeit relevantesten Datengruppen sind

  - Kriminalaktennachweise: Diese beinhalten Informationen über laufende und abgeschlossene Ermittlungsverfahren, insbesondere die Straftatbestände, wegen derer ermittelt wurde, Datum und Art der Einstellungsverfügung, deren Gründe, Angaben zur Anklageerhebung sowie zum Ausgang des Hauptverfahrens.
  - Personenfahndung: Diese listet in einem Katalog den Anlass und den Zweck der Ausschreibung einer Person zur Fahndung mit dem Ziel auf, fahndungsrelevante Erkenntnisse über Täter, Tathergang, Zeugen, Geschädigte etc. zu erlangen. Die Personenfahndung dient u. a. der Festnahme oder Aufenthaltsermittlung von Straftätern (Strafverfolgung) oder dem Schutz von vermissten Personen (Gefahrenabwehr).
  - Sachfahndung: Diese ähnelt dem Katalog der Fahndung nach Personen. Sie dient u. a. der Beweissicherung sowie der Eigentümer-/Besitzerermittlung von Sachen, die durch eine Straftat oder sonst abhandengekommen sind.
  - Haftdatei: Sie beinhaltet Daten von Personen, die wegen einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen.

- Erkennungsdienst und DNA-Analyse-Datei: Die Erfassung und Speicherung von biometrischen Merkmalen (insbesondere Fingerabdrücke, Lichtbilder und DNA-Identifizierungsmuster) bildet die Grundlage für die Ermittlung von Tätern in Strafverfahren, die Zuordnung von Tatortspuren, das Erkennen von Tatzusammenhängen, aber auch für die Identifizierung von hilflosen Personen oder unbekannten Toten. Die aus der DNA-Analyse nach § 81g StPO oder § 19 HSOG resultierenden Identifizierungsmuster werden in einer zentralen DNA-Analyse-Datei (DAD) gespeichert.

POLAS unterstützt somit im polizeilichen Alltag den zügigen Informationsaustausch über bereits einschlägig in Erscheinung getretene Straftäter und dient als Grundlage der Personenüberprüfung und Identifizierung im Rahmen der Aufklärung fahndungsrelevanter Sachverhalte wie Haftbefehle oder auch Vermisstenfahndungen. Durch die Bündelung der polizeilich relevanten Informationen, insbesondere zu bereits einschlägig in Erscheinung getretenen Straftätern, nimmt POLAS als eine an die Analyseplattform angebundene Quelle eine zentrale Rolle ein. Durch die Weiterverarbeitung und Analyse dieser Daten innerhalb der automatisierten Anwendung können beispielsweise sehr schnell Mittäter identifiziert, Verbindungen visualisiert sowie Falldaten miteinander abgeglichen oder Tatbeteiligungen anhand der Haftdaten auch ausgeschlossen werden.

- Die mit dem Begriff **Verkehrsdaten** erfassten polizeilichen Datenbestände enthalten personenbezogene Informationen, die auf strafprozessualer Grundlage (z. B. § 100g StPO) oder damit korrespondierender polizeirechtlicher Vorschriften (z. B. § 15 Abs. 2 HSOG) von Telekommunikationsanbietern auf Ersuchen der Polizeibehörden an diese übermittelt oder von diesen dort erhoben und anschließend gespeichert wurden. Zu den in § 3 Nr. 70 TKG gesetzlich definierten Verkehrsdaten – Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind – gehören insbesondere auch die für die Polizeiarbeit praktisch bedeutsamen Standortdaten (vgl. § 9 Abs. 1 Nr. 1 TTDSG), deren Erhebung durch Funkzellenabfragen gemäß § 100g Abs. 3 StPO erfolgt oder – gezielt und präziser – durch den Einsatz von IMSI-Catchern (vgl. zur Funktionsweise BVerfG, Nichtannahmebeschluss vom 22. August 2006 – 2 BvR 1345/03) auf der Grundlage des § 100i Abs. 1 Nr. 2 StPO ermöglicht wird. Im gefahrenabwehrrechtlichen Bereich kann nach § 15a Abs. 1 und 3 HSOG der Standort über die jeweilige Funkzelle ermittelt und durch den Einsatz von IMSI-Catchern präzisiert werden. Die Kenntnis darüber, welche Mobiltelefone zu einem bestimmten Zeitpunkt an einem bestimmten Ort angemeldet waren, kann im konkreten Fall ein wesentlicher Baustein erfolgreicher polizeilicher Ermittlungsarbeit sein, weil der Aufenthaltsort der Anschlussinhaber Rückschlüsse auf eine mögliche Tatbeteiligung zulässt oder Aussagen über Organisationsstrukturen einer Mehrheit von Tatverdächtigen ermöglicht. Wegen der großen Streubreite solcher Maßnahmen – es sind häufig eine Vielzahl unbeteiligter Personen betroffen – wird die Verwendung dieser Daten zum Zweck der vorbeugenden Straftatenbekämpfung gemäß Abs. 2 Satz 1 Nr. 1 von vornherein ausgeschlossen und wird für die übrigen Tatbestandsvarianten eine Speicherfrist von regelmäßig zwei Jahren festgelegt (vgl. hierzu BVerfG, Urteil vom 20. Februar 2023, a. a. O., Rn. 85, 142).

- Der Begriff **Telekommunikationsdaten** bezeichnet die bei der hessischen Polizei gesondert gespeicherten Datenbestände, in denen ausschließlich Daten aus polizeilichen Telefonüberwachungsmaßnahmen gemäß § 100a StPO und § 15a HSOG zusammengeführt werden. Weil diese Datenbestände nicht nur die bei dem jeweiligen Kommunikationsvorgang angefallenen Verkehrsdaten enthalten, sondern in gewissem Umfang auch die typischerweise besonders grundrechtssensiblen Kommunikationsinhalte selbst, werden diese Daten nicht zusammen mit den ebenfalls aus der Sphäre der Telekommunikation stammenden Verkehrsdaten, sondern von vornherein in einem eigenen, organisatorisch besonders gesicherten „Datentopf“ aufbewahrt. Die Kommunikationsinhalte selbst sind in einem Freitextfeld gespeichert, dessen Inhalt im Rahmen der automatisierten Datenanalyse per extra Mausklick zwar angezeigt wird, aber ohne vorherige gesonderte polizeiliche Bewertung und technische Aufbereitung nicht automatisiert weiterverarbeitet werden kann, was bedeutet, dass wegen der geringen Komplexität des Analysevorgangs die Eingriffsintensität insoweit vergleichsweise gering ist. Weil gemäß § 100d StPO und § 15a Abs. 1 Satz 4 i. V. m. § 15 Abs. 4 Satz 4 bis 6 und § 12a HSOG Daten aus dem Kernbereich der privaten Lebensgestaltung ohnehin nicht gespeichert werden, und weil aus Gründen sowohl der Erforderlichkeit als auch der Verfahrensökonomie die Verschriftlichung eines Gesprächsmitschnitts immer nur mit Blick auf die Relevanz für das jeweilige Ermittlungsverfahren erfolgt, der Freitext mit anderen Worten immer nur einen mehr oder weniger großen Ausschnitt eines in der Vergangenheit liegenden Kommunikationsvorgangs abbildet, erscheint die Einbeziehung der so definierten Telekommunikationsdaten in eine automatisierte Datenanalyse unter grundrechtlichen Gesichtspunkten vertretbar. Das verfassungsrechtliche Gebot, die Eingriffsintensität möglichst gering zu halten, wird durch den in Abs. 3 Nr. 2 Buchst. b an die Polizeibehörden adressierten Auftrag abgesichert, wonach der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen effektiv Rechnung zu tragen ist.

- **Asservate** im Sinne dieser Bestimmung sind amtlich in Verwahrung genommene und als Beweismittel in Frage kommende Gegenstände, soweit sie zur Aufbewahrung personenbezogener Daten dienen. Hierunter fallen beispielsweise Datenträger wie USB-Sticks, Festplatten, Smartphones und Laptops. Es kann sich dabei sowohl um von den Polizeibehörden förmlich beschlagnahmte oder sichergestellte Datenträger handeln als auch um solche, die ihnen von Hinweisgebern oder Zeugen auf deren Initiative hin überlassen werden. Auch die hieraus gewonnenen Daten werden, nicht zuletzt weil es sich um vergleichsweise unstrukturierte und heterogene Daten handelt, in einem gesonderten Datentopf zusammengeführt.
- Unter **Daten aus dem polizeilichen Informationsaustausch** ist das bundesweite webbasierte Fernschreibsystem EPOST 810 zu verstehen. Damit werden polizeiinterne Informationen zwischen den Länderpolizeien ausgetauscht, z. B. Informationen mit hoher Relevanz zu überregionalen Straftätern und serienmäßigen Straftaten. Sie sind in „Postkörbe“ unterteilt, die den jeweiligen Zuständigkeitsbereichen entsprechen (schwere Kriminalität, Organisierte Kriminalität usw.).

Zu Abs. 2 Satz 3

Abs. 2 Satz 3 regelt die der Einbeziehung von Daten aus staatlichen Registern in die automatisierte Datenanalyse. Daten aus staatlichen Registern sind beispielsweise Daten aus dem Melderegister, dem Zentralen Verkehrsinformationssystem (ZEVIS) oder dem Waffenregister, welche über die Analyseplattform auf direktem Weg abgefragt werden können, wenn dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Die Regelung dient der Klarstellung. Die Befugnis zur Abfrage als solcher ergibt sich bereits aus den speziellen Übermittlungsregelungen (z. B. § 34 Abs. 2 Nr. 1 BMG, § 35 StVG, §§ 13 ff. WaffRG). So können Abfragen in ZEVIS dazu dienen, sich über die Mobilität einer Anlassperson Klarheit zu verschaffen. Hat diese Person außerdem eine Waffenerlaubnis, kann darin ein gefahrerhöhendes Indiz gesehen werden. Die Funktionalität der Analyseplattform stellt sicher, dass solche Informationen schnell zusammengeführt und bewertet werden können.

Mit Blick auf die Regelung des Abs. 1 Satz 6, wonach eine Anbindung an das Internet ausgeschlossen ist, dient Abs. 2 Satz 3, wonach gesondert gespeicherte Datensätze aus Internetquellen in die automatisierte Datenanalyse einbezogen werden dürfen, ebenfalls der Klarstellung. Es handelt sich bei diesen Datensätzen vor allem um die Ergebnisse polizeilicher Recherchen in für jedermann offenen sozialen Netzwerken. Sie werden in einem gesonderten Format, meist als PDF, gespeichert und auf die Analyseplattform aufgespielt. Voraussetzung für eine solche Maßnahme ist, dass die Einbeziehung erforderlich ist, um einen gefahrengeneigten Sachverhalt weiter aufzuklären. Vorstellbar sind Fallkonstellationen, in denen auf sozialen Netzwerken ein Amoklauf angekündigt wird oder Verabredungen zu gemeinsamen Aktionen getroffen werden, die den Tatbestand des Landfriedensbruchs erfüllen würden.

Zu Abs. 2 Satz 4

Verkehrsdaten dürfen nicht zur vorbeugenden Straftatenbekämpfung gemäß Abs. 1 Satz 1 Nr. 3 im Wege der automatisierten Datenanalyse weiterverarbeitet werden, d. h. sie dürfen bei einer Recherche auf der Grundlage dieser Tatbestandsvariante nicht zusammen mit den anderen Datenbeständen auf der Analyseplattform zusammengeführt werden. Bei Maßnahmen nach dieser Variante fällt die zeitliche Komponente im Verhältnis zur Grundrechtsrelevanz weniger ins Gewicht, weshalb Effektivitätseinbußen aus Gründen des hier im Vordergrund stehenden Schutzes Unbeteiligter – Verkehrsdaten enthalten typischerweise eine Vielzahl personenbezogener Daten von Personen, die keinen objektiv zurechenbaren Anlass für polizeiliche Ermittlungen geben (vgl. BVerfG, a. a. O., Rn. 77; siehe auch oben zu Abs. 2 Satz 2 und unten zu Abs. 3 Nr. 2 Buchst. b) – hinzunehmen sind.

Zu Abs. 3

Abs. 3 erklärt, um Unklarheiten vorzubeugen (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Rn. 133), die Bestimmungen über die zweckwahrende und zweckändernde Weiternutzung personenbezogener Daten der Absätze 1 und 2 des § 20 ausdrücklich für anwendbar und verknüpft die Folgerungen aus dem verfassungsrechtlichen Zweckbindungsgrundsatz mit Regelungen über die bei einer automatisierten Datenanalyse verfassungsrechtlich darüber hinaus geforderten materiellen Rechtfertigungsanforderungen. Die Regelungsaufgabe wird auf zwei Schultern verteilt, die des Gesetzgebers und die der Verwaltung (vgl. zu dieser Aufgabenverteilung BVerfG, a. a. O., Rn. 112 ff.). Ihr regulatorischer Ansatz ist eine Kombination aus organisatorischen und materiellen Elementen, die hier als funktionale Reduzierung der Eingriffsintensität bezeichnet wird. Sie besteht zum einen Teil aus einer Verschränkung der aus dem verfassungsrechtlichen Zweckbindungsgrundsatz abgeleiteten Prinzipien der zweckwahrenden und der zweckändernden Weiternutzung von Daten (vgl. zum Verhältnis von Zweckbindung und Begrenzung des Datenumfangs BVerfG, a. a. O., Rn. 80) mit dem auf einem zeitgemäßen und flexiblen, die Funktionalität einer Analyseplattform unterstützenden, an vorhandene Organisationsstrukturen anschließbaren Rollen- und Rechtekonzept (Buchstabe a) und zum anderen Teil aus einer eingriffsreduzierenden Vorauswahl, nämlich der Kategorisierung und Kennzeichnung

personenbezogener Daten anhand der materiellen Kriterien des Veranlassungszusammenhangs und der Grundrechtsrelevanz (Buchstabe b), die dazu führt, dass bestimmte grundrechtssensible Daten von vornherein nur in begrenztem Umfang oder überhaupt nicht in die automatisierte Datenanalyse einbezogen werden dürfen.

Die an die Polizeibehörden adressierten, übergeordneten und deshalb vorrangig zu beachtenden verfassungsrechtlichen Maßstäbe und Zielvorgaben werden im Gesetz hervorgehoben und sind von ihnen bei der Ausarbeitung des Rollen- und Rechtekonzepts und des Konzepts der Kategorisierung und Kennzeichnung personenbezogener Daten zwecks Verringerung der Eingriffsintensität vorrangig umzusetzen. Sie lauten:

- Reduzierung des Datenvolumens
- Angemessenheit der Analysemethode
- Schutz Unbeteiligter

Die Reduzierung des Umfangs der Daten (vgl. BVerfG, a. a. O., Rn. 78 ff., 115 ff., 125 ff.) und die Angemessenheit der Analysemethode (vgl. BVerfG, a. a. O., Rn. 90 ff., 120 ff., 146 ff.) sind die Schaltstellen für die Austarierung des je zulässigen Eingriffsgewichts und damit der Zulässigkeit einer automatisierten Datenanalyse nach den in Abs. 2 Satz 1 normierten drei Tatbestandsvarianten. Der vom Bundesverfassungsgericht an vielen Stellen seines Urteils außerdem besonders hervorgehobene (BVerfG, a. a. O., Rn. 77, 84, 126) und nicht zuletzt aus polizeitaktischen Gründen bedeutsame Schutz Unbeteiligter knüpft an das ebenfalls systembildende Kriterium der „Art der Daten“ an (BVerfG, a. a. O., Rn. 80 ff., 117 ff., 126) und überführt es unter dem Gesichtspunkt des Veranlassungszusammenhangs in das von den Polizeibehörden im Detail auszuarbeitende Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten gemäß Nr. 2 (dazu unten).

Zu Abs. 3 Nr. 1

Das Rollen- und Rechtekonzept legt fest, welche Personen innerhalb der Polizeiorganisation Zugriff auf welche Daten haben können, und mit welchen Rechten und Pflichten der Zugriff für die jeweilige Person verbunden ist. Weil dieses Konzept die Zugriffsrechte an Rollen und nicht an Individuen anknüpft, ist es prinzipiell möglich, dass eine Person mehrere Rollen hat und deshalb, verglichen mit der Mehrzahl der meisten Personen der gleichen Organisationseinheit, über erweiterte Zugriffsrechte verfügt. Es gibt den Polizeibehörden die Möglichkeit, Personen mit höherer (z. B. Referats- oder Abteilungsleiter) oder herausgehobener Verantwortung (z. B. Behördenleiter) mehrere Rollen zu übertragen, damit sie ihrer Aufsichts- und Kontrollfunktion innerhalb der Behördenhierarchie gerecht werden können. Hier wird das gesetzlich normierte Prinzip wirksam, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform zusammengeführten Daten haben.

Gleichzeitig ist das Rollen- und Rechtekonzept schon in seiner Anlage ein der Zusammenführung verschiedener Datentöpfe und also der Anreicherung von Datenbeständen gegenläufiges Konzept, weil es dazu führt, dass im normalen Polizeialltag sozusagen niemand in alle der zusammengeführten Datentöpfe schauen kann, sondern immer nur einen Ausschnitt der zusammengeführten Daten sieht. Bildlich gesprochen formieren sich die auf der Analyseplattform zusammengeführten Datenbestände für den jeweiligen Anwender also zu voneinander abgeschotteten Kammern, je nachdem welche Phänomenbereiche ihm zwecks Bearbeitung zugewiesen sind. Das Rollen- und Rechtekonzept führt deshalb zu einer funktionsbedingten Reduzierung des Umfangs der jeweils zu verarbeitenden Daten und damit zu einer strategischen Verringerung der Eingriffsintensität, ohne dadurch die Arbeitsweise der Analyseplattform strukturell zu hemmen.

Die Ausgestaltung des Rollen- und Rechtekonzepts hat sich am Gewicht der zu schützenden Rechtsgüter und der Dringlichkeit der Sache auszurichten. Abstrakter Maßstab sind die drei Tatbestandsvarianten des Abs. 2 Satz 1, konkreter Anknüpfungspunkt sind die kriminologischen Phänomenbereiche, denen innerhalb einer Behörde die verschiedenen Sachbearbeiter zugeordnet sind. Es ist Aufgabe der Verwaltung, die Erfordernisse der Praxis und die verfassungsrechtlichen Vorgaben so zusammenzuführen, dass effiziente Polizeiarbeit nicht einseitig zu Lasten des Grundrechtsschutzes führt und umgekehrt. Das allgemeine Prinzip der praktischen Konkordanz verlangt, dass das Rollen- und Rechtekonzept einer laufenden Überprüfung durch die Verwaltung unterzogen und erforderlichenfalls angepasst wird, damit die unterschiedlichen Interessen und Rechtsgüter zu möglichst optimaler Wirksamkeit gelangen können. Dies kann beispielsweise bedeuten, dass nur wenige und besonders geschulte Berechtigte Zugriff auf Verkehrsdaten oder Daten aus Asservaten haben, weil es sich dabei um große Datenmengen handelt, die typischerweise viele personenbezogene Daten Unbeteiligter beinhalten und deshalb mit besonderer Sensibilität zu behandeln sind. Diese Feinjustierung ist Aufgabe der Polizeibehörden und in einer Verwaltungsvorschrift niederzulegen.

Ein zentraler Wirkungsfaktor eines Rollen- und Rechtekonzepts ist, dass die Berechtigung für einen Zugriff nur entsprechend qualifizierten Personen erteilt wird, was eine Schulung und deren erfolgreichen Abschluss voraussetzt. Die Einzelheiten sind in einer Verwaltungsvorschrift zu regeln. Der Prozess der Rechtevergabe ist klar zu definieren, zu dokumentieren und technisch abzusichern. Bestandteil des Rollen- und Rechtekonzepts ist auch die in Abs. 4 geregelte Zugriffskontrolle, die einem Missbrauch des Analysetools effektiv entgegenwirkt (dazu unten).

Zu Abs. 3 Nr. 2

Die Verringerung der Eingriffsintensität der automatisierten Datenanalyse erfolgt außerdem über eine Kategorisierung der in die Weiterverarbeitung einbezogenen Daten, indem anhand des Veranlassungszusammenhangs entschieden wird, ob und in welcher Weise personenbezogene Informationen verwendet werden (Buchst. a). Grundlegend ist hier die Unterscheidung zwischen einerseits unbeteiligten und andererseits verurteilten, beschuldigten und verdächtigen Personen sowie sonstigen Anlasspersonen und deren Kontaktpersonen (zu letzteren § 15 Abs. 2 Nr. 4). Diese von der Verwaltung erforderlichenfalls näher zu präzisierende bzw. konturierende Kategorisierung beruht im Wesentlichen auf einer eingeführten, im Bundeskriminalamtsgesetz (§ 18) und Zollfahndungsdienstgesetz (§ 11) sowie einigen neueren Länderpolizeigesetzen (§ 23 SOG LSA, § 40 ThürPAG) verwendeten Terminologie. Zentrales Element des Veranlassungszusammenhangs ist die tatsachengestützte Annahme, dass die betroffene Person künftig Straftaten begehen wird (Negativprognose, vgl. BVerfG, a. a. O., Rn. 126), was in der Polizeipraxis häufig bei Serienstraftätern der Fall ist (vgl. BVerfG, a. a. O., Rn. 160). Die Beziehung, in welcher eine von der automatisierten Datenverarbeitung betroffene Person zu einem polizeilichen Ermittlungskomplex steht, ist ein begrenzender Faktor der automatisierten Datenanalyse, der bei allen Arbeitsschritten zu beachten ist. Denn das Eingriffsgewicht dieser Maßnahme ist umso höher, je weniger die betroffene Person objektiv in Beziehung zu einem konkreten Fehlverhalten steht und deshalb durch ihr Fehlverhalten einen polizeilichen Eingriff zurechenbar veranlasst (BVerfG, a. a. O., Rn. 77).

Dies gilt vor allem für Unbeteiligte. Personen, die mit einem polizeilich relevanten Sachverhalt nur zufällig in Berührung stehen oder standen, sind besonders schutzwürdig. Ihre personenbezogenen Daten dürfen deshalb grundsätzlich nicht in eine automatisierte Datenanalyse einbezogen werden. Dies kann dadurch erreicht werden, dass ihre Daten für eine Recherche auf der Analyseplattform gewissermaßen unsichtbar gemacht werden, obwohl sie in den Quellsystemen, etwa einem Vorgangsbearbeitungssystem, noch auffindbar sind. Soweit in den Quellsystemen, etwa in Protokollen über Zeugenvernehmungen oder Abschlussberichten in Form von Freitext, personenbezogene Daten Unbeteiligter gespeichert werden, ist der Schutz dieser Personen dadurch gewährleistet, dass mangels spezifischer Erfassung dieser Daten im Quellsystem ihre elektronische Verknüpfung und somit auch ihre automatisierte Weiterverarbeitung nicht möglich ist. Der polizeiliche Sachbearbeiter kann also das entsprechende Dokument und darin enthaltene Namen zwar lesen. Er kann diese Namen aber nicht automatisch weiterverarbeiten, ohne zuvor eine überprüfbare Bewertung darüber abgegeben zu haben, dass die betreffende Person nunmehr als Anlassperson (oder als Begleitperson einer Anlassperson) einzustufen ist.

Unter diesen Maßgaben ist die Beeinträchtigung der Rechte Unbeteiligter, weil der Prozess der abgestuften Erkenntnisgewinnung tendenziell darauf ausgerichtet ist, ihre personenbezogenen Daten auszufiltern, bevor weitere Bearbeitungsschritte ergriffen werden, als gering einzustufen.

Bereits auf der Ebene der Gesetzgebung ist zu regeln, dass für Daten über Unbeteiligte eine Speicherfrist gilt (BVerfG, a. a. O., Rn. 85). Die jetzt gesetzlich festgeschriebene Zwei-Jahres-Frist ist bereits Praxis. Vergleichbar mit den Aussonderprüffristen gemäß § 27 Abs. 4 steht sie allerdings unter dem Vorbehalt, dass die Daten nach Ablauf der Frist nicht zu löschen sind, wenn sie für die Fallbearbeitung ausnahmsweise noch erforderlich sein sollten. Die Entscheidung, diese Daten nicht zu löschen, ist zu begründen.

Zur Verringerung der Eingriffsintensität der automatisierten Datenanalyse führt auch, dass die Weiterverarbeitung von personenbezogenen Daten, die aus schwerwiegenden Grundrechtseingriffen stammen, begrenzt oder ausgeschlossen wird (Buchst. b). Wegen der besonderen Intensität von Grundrechtseingriffen aus Wohnraumüberwachungen und Online-Durchsuchungen (BVerfG, a. a. O., Rn. 81) wird bereits auf der Ebene der Gesetzgebung die Entscheidung getroffen, dass die daraus gewonnenen personenbezogenen Daten von vornherein nicht in eine automatisierte Datenanalyse einbezogen werden dürfen. In Bezug auf Daten allerdings, die aus anderen schwerwiegenden Grundrechtseingriffen gewonnen wurden, also etwa aus Telefonüberwachungsmaßnahmen oder längerfristigen Observationen, trifft nicht schon der Gesetzgeber eine solche kategoriale Entscheidung. Weil solche Daten im Rahmen einer der vorbeugenden Bekämpfung von Straftaten dienenden Datenanalyse oder -auswertung schon nach dem Grundsatz der Zweckbindung zweckändernd (nur) dann einbezogen werden dürfen, wenn sich hieraus im Einzelfall konkrete Ermittlungsansätze zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren ergeben (BVerfGE a. a. O., Rn. 81), kommt es hier auf die konkreten Umstände des Einzelfalls an. Mit Blick darauf, dass die Eingriffsvoraussetzungen nach Maßgaben des Eingriffsanlasses und der Bedeutung der Schutzgüter streng konzipiert sind, und unter Berücksichtigung des Umstands, dass die in den Varianten Nr. 2 und Nr. 3 des Abs. 2 Satz 1 definierten Tatbestandsmerkmale

fließend ineinander übergehen (Anlass) oder sich überlappen (Schutzgüter), wird eine Weiterverwendung auch solcher Daten regelmäßig zulässig sein (siehe oben zu Abs. 2). Es ist Aufgabe der Verwaltung, Ausnahmekonstellationen zu identifizieren und sie gegebenenfalls normativ zu erschließen.

Zu Abs. 4

Abs. 4 enthält Regelungen zur Gewährleistung von Kontrolle, Transparenz, Richtigkeitsvergewisserung und Rechtsschutz (vgl. BVerfG, a.a.O., Rn. 109).

Ein zentrales Element des Rollen- und Rechtekonzepts ist die in Abs. 4 geregelte Zugriffskontrolle. Sie wird durch die Protokollierung der einzelnen Arbeitsschritte abgesichert und gewährleistet, dass nur berechtigte – und damit auch entsprechend qualifizierte – Personen eine automatisierte Datenanalyse vornehmen können. Sie effektuiert auf der praktischen Ebene das eingriffsmindernde Prinzip, wonach die auf der Analyseplattform zusammengeführten Daten jeweils nur ausschnittsweise in einer automatisierten Recherche verarbeitet werden können (dazu bereits oben zu Abs. 2 und Abs. 3 Nr. 1). Die technisch-organisatorischen Einzelheiten sind in einer Verwaltungsvorschrift zu regeln, die an sich verändernde Anforderungen anzupassen ist. Sie kann zum Beispiel vorsehen, dass der Zugriff durch nicht autorisierte Personen bereits auf der technischen Ebene gesperrt wird, wie es in der Polizeipraxis bereits der Fall ist. Die gesetzlich vorgeschriebene fortlaufende Protokollierung bei der Nutzung des Analysetools sichert die nachträgliche aufsichtliche Kontrolle gemäß Satz 5 und ist gleichzeitig Voraussetzung für die Gewährleistung effektiven Rechtsschutzes gemäß Art. 19 Abs. 4 GG.

Die in den Sätzen 3 und 4 geregelte Begründungspflicht ist für die Umsetzung der verfassungsrechtlichen Vorgaben und Einhaltung einfachgesetzlicher Normierungen ein ebenfalls bedeutsamer Faktor. Aus der Pflicht, jeden Einsatz dieses Instruments schriftlich zu begründen, folgt zwangsläufig, dass die Anwenderin oder der Anwender nicht anlasslos, sondern einzelfallbezogen und zielgerichtet vorgeht (dazu oben zu Abs. 1). Es müssen deshalb in jedem Einzelfall Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden (BVerfG, a. a. O., Rn. 109). Der Zweck der Begründungspflicht liegt zum einen in der Vergewisserung über die Rechtmäßigkeit des Handelns. Es ist eine Erfahrungstatsache, dass der Zwang zur schriftlichen Fixierung der Gründe für eine Entscheidung nicht nur mäßigend wirkt, sondern auch eine größere Richtigkeitsgewähr bietet als ein Entscheidungsprozess, der sich lediglich im Kopf abspielt (vgl. Rachor in: Lisken/Denninger, Handbuch des Polizeirechts, 5. Aufl. 2012, Kap. E Rn. 317). Ihr Zweck liegt zum anderen darin, eventuell anschließende aufsichtliche Kontrollen oder gerichtliche Überprüfungen überhaupt erst zu ermöglichen. Die Einzelheiten hierzu sind nach Satz 5 in Verwaltungsvorschriften zu regeln. Diese müssen in abstrakter Form festlegen, welchen Inhalt eine solche Begründung mindestens haben soll, und sie dürfen abstrakt festlegen, wie die Begründung formal zu strukturieren ist, wobei die Verwendung eines Freitextfeldes allerdings obligatorisch ist (vgl. BVerfG, a. a. O, Rn. 109 – „eigenständig ausformulierte Begründungen“). Die polizeiliche Praxis entspricht bereits diesen Voraussetzungen.

Satz 6 regelt die Befugnis des behördlichen Datenschutzbeauftragten, stichprobenartige Kontrollen durchzuführen. Im Zusammenspiel mit den in Abs. 5 geregelten (Satz 2) bzw. bekräftigten (Satz 3) Kontrollbefugnissen der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit gewährleistet diese Bestimmung eine effektive, zwischen behördlichem und unabhängigem Datenschutzbeauftragten aufgeteilte Kontrolle. Dass im Rahmen dieses abgestuften Kontrollkonzepts ein stichprobenartiges Vorgehen ausreichend ist, hat das Bundesverfassungsgericht ausdrücklich festgestellt (BVerfG, a. a. O., Rn. 109).

Zu Abs. 5

Der neue Abs. 5 entspricht Abs. 3 der bisherigen Regelung. Er wird ergänzt um die Klarstellung, dass die sonstigen Aufgaben und Befugnisse der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit unberührt bleiben. Dies entspricht dem vom Bundesverfassungsgericht geforderten Konzept einer abgestuften, arbeitsteiligen Vorgehensweise zwischen unabhängigen und behördlichen Datenschutzbeauftragten (BVerfG, a. a. O., Rn. 109).

Zu III. (Art. 3 – Gesetz zur Umorganisation der hessischen Bereitschaftspolizei)

Aufgrund des vorangeschritten Gesetzgebungsverfahrens ist die Regelung zum Inkrafttreten des § 3 überholt und wurde daher angepasst.

Zu IV. (Art. 5 – Hessisches Besoldungsgesetz)

Es handelt sich um die redaktionelle Anpassung des Vollzitats des Gesetzes, welches am 28. März zuletzt geändert wurde.

Zu V. (Art. 6 – Hessisches Personalvertretungsgesetz)

Aufgrund der umfassenden Änderung des Hessischen Personalvertretungsgesetzes mit Gesetz vom 28. März 2023 musste Art. 6 neu gefasst werden. Es handelt sich um eine redaktionelle Anpassung.

Zu VI. (Art. 7 – Hessischen Hochschulgesetzes)

Es handelt sich um die redaktionelle Anpassung des Vollzitats des Gesetzes, welches am 28. März 2023 zuletzt geändert wurde.

Zu VII. (Art. 8 – Zitiergebot)

Es handelt sich um eine Korrektur des Verweises in Art. 8 Satz 2 auf Art. 2 des Gesetzes. Im Gesetzentwurf wurde irrtümlich auf Art. 4 verwiesen.

Wiesbaden, 20. Juni 2023

Für die Fraktion
der CDU
Die Fraktionsvorsitzende:
Ines Claus

Für die Fraktion
BÜNDNIS 90/DIE GRÜNEN
Der Fraktionsvorsitzende:
Mathias Wagner (Taunus)