CHRISTIAN-ALBRECHTS-UNIVERSITÄT ZU KIEL

INSTITUT FÜR KRIMINALWISSENSCHAFTEN

ZENTRUM FÜR DIGITALISIERUNG UND RECHT IN FORSCHUNG UND LEHRE

Professur für Strafrecht, Strafprozessrecht, Wirtschaftsstrafrecht und Sanktionenrecht

RiOLG Prof. Dr. Janique Brüning

Schleswig-Holsteinischer Landtag
Umdruck 20/7148

**Gutachterliche Stellungnahme**

**zum Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen**

**für einen wirksamen Schutz der öffentlichen Sicherheit**

für den Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages

11. September 2026

Leibnizstraße 2 · D-24118 Kiel · ☏ 0431/880-3473
✉ jbruening@law.uni-kiel.de

## Inhaltsverzeichnis

## I. Gegenstand und Perspektive

Diese Stellungnahme beschränkt sich auf die automatisierte Datenanalyse nach §§ 188c und 188d LVwG-E. Im Mittelpunkt steht ihr Verhältnis zu den bundesrechtlichen Gesetzesentwürfen zur automatisierten Datenanalyse.

Den Ausgangspunkt bilden die parallel verfolgten Regelungsvorhaben des Bundes. Mit § 98e StPO-E sowie §§ 9b, 63c BKAG-E sind auch dort Vorschriften zur automatisierten Datenanalyse vorgesehen. Diese setzen ein polizeiliches Datei- und Informationssystem voraus, in dem rechtmäßig gespeicherte personenbezogene Daten für eine Analyseplattform zusammengeführt werden. Vorgesehen ist damit ein dauerhaft verfügbarer, behördenübergreifend nutzbarer Datenpool, eine Art „Superdatenbank". Um „Doppelstrukturen" zu vermeiden[1], soll diese Infrastruktur – so die Prämisse der Bundesgesetzentwürfe – auch Daten der Landespolizeien einbeziehen.

Vor diesem Hintergrund ist zu prüfen, wie sich die hier zu bewertenden landesrechtlichen Vorschriften zu den geplanten bundesrechtlichen Regelungen verhalten und ob sie die verfassungsrechtlichen Anforderungen an den vorgesehenen Datenaustausch erfüllen: Sind beide Regelungsebenen aufeinander abgestimmt? Ist eine solche Abstimmung überhaupt erstrebenswert und wie kann sie gegebenenfalls rechtlich hergestellt werden?

Maßgeblich ist dabei die Zugriffsarchitektur einer möglichen gemeinsamen Datenplattform. Zu klären ist, welche Schutzmechanismen erforderlich sind, sollten Behörden sowohl zu Zwecken der Gefahrenabwehr als auch der Strafverfolgung auf dieselbe technische Infrastruktur zugreifen und dort Daten auswerten können.

Dabei sind drei Ebenen zu unterscheiden: die einzelnen Ausgangsdaten, der aus ihnen zusammengeführte Analysebestand und die durch seine Auswertung neu gewonnenen Analyseergebnisse. Diese Unterscheidung bildet die Leitlinie der Untersuchung. Nach der Darstellung des technischen Ablaufs und der verfassungsrechtlichen Maßstäbe (II. und III.) werden zunächst die Regelungskonzepte für die Bildung und Nutzung der Analysebestände im Bund und im Land (IV.) und sodann die unterschiedliche Ausgestaltung der automatisierten Datenanalyse verglichen (V.). Darauf aufbauend sind die rechtlichen Voraussetzungen einer zweckändernden Datennutzung auf jeder der

[1] Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, 01.07.2026, BT-Drucks. 21/6806, S. 19.

drei Ebenen zu prüfen (VI.). Abschließend werden die Anforderungen an die Zugriffsarchitektur begründet (VII.), der daraus folgende Regelungsbedarf benannt (VIII.) und die Ergebnisse zusammengefasst (IX.).

Eine Gesamtwürdigung des Entwurfs und seine europarechtliche Einordnung bleiben außer Betracht.

Maßgeblich sind LT-Drs. 20/4284 und der Änderungsantrag Umdruck 20/6786.

## II. Die Datenanalyse – der technische Ablauf

Die rechtliche Bewertung automatisierter Datenanalyse setzt zunächst voraus, dass der technische Vorgang hinreichend geklärt ist. Denn die technische Ausgestaltung bestimmt, welche rechtlichen Folgefragen sich stellen.

Eine polizeiliche Analyseplattform erschöpft sich dabei nicht in einer bloßen Suchmaske, die mehrere vorhandene Dateien gleichzeitig durchsucht. Sie schafft vielmehr eine eigene Analyseumgebung, in der Daten aus unterschiedlichen Quellen zusammengeführt, in eine gemeinsame Struktur überführt, miteinander verknüpft und anschließend gezielt ausgewertet werden können. Dabei sind vier Aspekte zu unterscheiden.[2]

Erstens sind die Quelldaten, auch Ausgangsdaten genannt, in den Blick zu nehmen. Sie werden angebunden und für die Analyse verfügbar gemacht. Polizeiliche Informationen liegen typischerweise nicht in einem einheitlichen Bestand vor. Sie stammen etwa aus Vorgangs- und Fallbearbeitungssystemen, polizeilichen Auskunfts- und Informationssystemen, Dateien des Informationsaustauschs, Asservatenbeständen sowie gegebenenfalls aus besonderen Erhebungsmaßnahmen.

Bereits an dieser Stelle ist darauf hinzuweisen, dass die erwähnten Gesetzesentwürfe unterschiedliche Quelldaten in die automatisierte Datenanalyse einbeziehen wollen.

[2] Zum Ganzen etwa: *Andrew Iliadis & Amelia Acker* (2022) The seer and the seen: Surveying Palantir's surveillance platform, The Information Society, 38 (5), 334-363, DOI: 10.1080/01972243.2022.2100851; Katerina Hadjimatheou (2025), 'The dream to know everything about everyone': Affordances of commercial data systems and digital net-widening in policing, Theoretical Criminology 29 (3) 325-345, DOI: 10.1177/13624806251334954.

Die Quelldaten können technisch entweder nur im Einzelfall aus den jeweiligen Quellsystemen abgefragt oder ganz bzw. teilweise in einen eigens für die Analyse vorgehaltenen Datenbestand übernommen werden.
Praktisch wird häufig eine längerfristige technische Aufbereitung erforderlich, zumindest sinnvoll sein. Die Bundesregierung geht in der Begründung zu § 9b BKAG-E davon aus, dass ein Grunddatenbestand bereits zusammengeführt, fortlaufend aktualisiert und in einem einheitlichen Datenformat in der Analyseanwendung vorliegen müsse. Andernfalls müsste die technisch aufwendige Aufbereitung bei jeder einzelnen Analyse erneut erfolgen (dazu IV. 1.).

Zweitens werden die Daten für die gemeinsame Auswertung technisch erschlossen, vereinheitlicht und in ein gemeinsames Modell eingeordnet.
Dabei sind unterschiedliche technische Architekturen möglich. Bei einem föderierten Zugriff können die Daten grundsätzlich in ihren jeweiligen Quellsystemen verbleiben. In diesem Fall verteilt die Plattform die Abfragen auf die hierfür freigegebenen Bestände und führt die Ergebnisse zusammen.
Darüber hinaus kommt ein persistenter Analysebestand in Betracht, bei dem Daten – oder zumindest für die Analyse wesentliche Repräsentationen – dauerhaft in eine gemeinsame, einheitlich durchsuchbare Struktur überführt werden. Zwischen beiden Modellen sind Mischformen denkbar. Entscheidend ist daher weniger die physische Speicherung der Daten in einer einzigen Datenbank als vielmehr die Frage, welche systemübergreifenden Such- und Verknüpfungsmöglichkeiten die technische Architektur eröffnet.
Eine solche technische Aufbereitung bzw. Modellierung der Daten ist erforderlich, weil dieselbe Information in verschiedenen Systemen unterschiedlich gespeichert sein kann. Ein Name kann etwa einmal als „Nachname, Vorname“, ein anderes Mal nur als Kurzbezeichnung erfasst sein. Auch Telefonnummern, Anschriften, Fahrzeugkennzeichen, Vorgangsnummern oder Objektbezeichnungen können unterschiedlichen Formaten folgen. Damit die Plattform solche Informationen systemübergreifend auffinden, abgleichen und miteinander in Beziehung setzen kann, müssen sie vereinheitlicht, indexiert und gemeinsamen Kategorien zugeordnet werden.

Die Analyseplattform stellt damit nicht lediglich technischen Speicherplatz oder eine gemeinsame Suchoberfläche bereit. Sie legt zugleich fest, welche Arten von Objekten im System unterschieden werden – etwa Personen, Fahrzeuge, Adressen, Orte, Kommunikationsvorgänge, Gegenstände oder Ereignisse – und welche Beziehungen zwischen ihnen dargestellt werden können. Bei der derzeit in Polizeibehörden eingesetzten Software wird diese Struktur als herstellereigene „Ontologie“ bezeichnet. Vereinfacht ausgedrückt schafft sie eine gemeinsame Sprache für Daten, die ursprünglich aus unterschiedlichen Systemen stammen. Erst diese Modellierung ermöglicht es, Informationen über Datei-, Format- und Systemgrenzen hinweg automatisiert abzugleichen und zu verknüpfen und daraus etwa Personen-, Ereignis-, Kommunikations- oder Beziehungsnetze abzuleiten.

Rechtlich kommt es deshalb nicht entscheidend auf Bezeichnungen wie „Datenbank“, „Datenhaus“, „Plattform“ oder „technische Aufbereitung“ an. Maßgeblich ist vielmehr, ob und in welchem Umfang personenbezogene Daten aus bislang getrennten Kontexten in eine gemeinsame Such- und Verknüpfungsstruktur einbezogen werden und dadurch die Erkenntnismöglichkeiten erweitert werden.

Insbesondere die dauerhafte Zusammenführung personenbezogener Daten in einem neuen Analysebestand stellt bereits einen Eingriff in das Recht auf informationelle Selbstbestimmung dar (dazu III. 1. b.).

Drittens folgt die eigentliche Suche und Analyse, die anlassbezogen ausgelöst wird. Die Plattform sucht dann nicht lediglich nach einem zuvor bekannten Namen in mehreren Dateien. Sie kann Daten miteinander vergleichen, Beziehungen sichtbar machen und Zusammenhänge strukturieren, die bei isolierter Betrachtung der einzelnen Dateien nicht ohne Weiteres erkennbar wären.

§ 98e Abs. 4 StPO-E beschreibt die möglichen Funktionen anschaulich. Die Anwendung soll Beziehungen zwischen Verfahren, Personen, Organisationen, Orten und Objekten identifizieren, herstellen, klassifizieren, strukturell analysieren und visualisieren können. Sie darf Suchkriterien gewichten und Daten statistisch auswerten. Der qualitative Unterschied zu einem bloßen Datenabgleich liegt darin, dass die Anwendung nicht nur bereits bekannte Angaben auffindbar macht. Vielmehr soll sie neue Erkenntnisansätze und damit neues Wissen erzeugen.

Viertens entstehen Analyseergebnisse, in denen sich das neu erzeugte Wissen niederschlägt. Das können einzelne Treffer, grafisch dargestellte Beziehungsnetze, zeitliche Abläufe, Auffälligkeiten oder Hinweise auf bislang nicht erkannte Verbindungen sein. So kann die Plattform etwa aufzeigen, dass eine Person über mehrere polizeilich erfasste Sachverhalte, Telefonnummern und Fahrzeuge mit einem bestimmten Objekt oder Personenkreis verbunden ist. Dieser Zusammenhang muss in keiner Ausgangsdatei ausdrücklich enthalten gewesen sein. Er entsteht erst durch die Kombination und Auswertung der Daten.

Die Ergebnisse werden dokumentiert und anschließend durch die zuständigen Bediensteten bewertet. Sie können Anlass für weitere Ermittlungen oder gefahrenabwehrrechtliche Maßnahmen geben, einen vorhandenen Verdacht verdichten, bislang nicht beachtete Personen in den Blick rücken oder weitere Datenerhebungen veranlassen. Gerade diese Fähigkeit, aus einer Vielzahl getrennt gespeicherter Informationen neue, personenbezogene Erkenntnisse zu erzeugen, begründet nach Ansicht des BVerfG das besondere Eingriffsgewicht automatisierter Datenanalyse (dazu III. 1. a.).

## III. Verfassungsrechtlicher Rahmen

Für die Frage, welche Schutzmechanismen eine gemeinsame Zugriffsarchitektur für Gefahrenabwehr und Strafverfolgung erfordert, sind zunächst die verfassungsrechtlichen Anforderungen zu klären, die das BVerfG an automatisierte Datenanalysen stellt (1.).

Anschließend ist die Trennung von Gefahrenabwehr und Strafverfolgung näher zu betrachten. Sie gewinnt besondere Bedeutung, wenn beide Aufgaben künftig über dieselbe technische Plattform erfüllt werden sollten und die einbezogenen Daten Sachverhalte betreffen können, die zugleich präventiv- und repressiv-polizeilich relevant sind (2.).

Schließlich ist zu untersuchen, unter welchen Voraussetzungen Daten ganz grundsätzlich zwischen beiden Rechtsregimen ausgetauscht werden dürfen. Maßgeblich sind insoweit der Grundsatz der Zweckbindung und die Anforderungen an zulässige Zweckänderungen (3.).

## 1. Die Maßstäbe des BVerfG

### a) BVerfG-Urteil zu Palantir

Ausgangspunkt aller hier betrachteten Entwürfe ist das Urteil des BVerfG vom 16. Februar 2023[3], in dem das Gericht § 25a HSOG und § 49 HmbPolDVG für unvereinbar mit dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG erklärte. Beide Vorschriften erlaubten es der Polizei, vorhandene Datenbestände mit Hilfe einer Analyseplattform automatisiert zusammenzuführen, abzugleichen und auszuwerten.

Die weiteren Ausführungen knüpfen vor allem an vier zentrale Aussagen des Urteils an: Erstens stelle die automatisierte Datenauswertung, mithin die Datenanalyse, einen eigenständigen Eingriff dar.[4] Sie erschöpfe sich nicht in der Wiederholung der ursprünglichen Erhebung der Quelldaten, sondern realisiere zusätzliche Persönlichkeitsrisiken, weil sie aus vorhandenen Beständen neues Wissen erzeuge. Dieser Zweiteingriff habe ein Eigengewicht und bedürfe daher einer eigenständigen Rechtsgrundlage.

Zweitens bestimme sich das Gewicht des Zweiteingriffs nach zwei Kriterien. Maßgeblich sind danach zum einen das Eingriffsgewicht des Ersteingriffs, aus dem die Daten stammen[5], zum anderen das Eigengewicht der Analyse[6]. Letzteres ergebe sich aus Art und Umfang der einbezogenen Daten, aus ihrer Zusammenführung und aus der eingesetzten Methode. Je sensibler die Ausgangsdaten und je weitergehend ihre Verknüpfung, desto höher falle das Gewicht des Zweiteingriffs aus. Werden etwa durch eine Wohnraumüberwachung gewonnene Kommunikationsinhalte mit Bewegungs-, Kontakt- und Finanzdaten zusammengeführt und automatisiert auf bislang unbekannte Beziehungen und Verhaltensmuster ausgewertet, wiegt der Zweiteingriff besonders schwer.

[3] BVerfGE 165, 363.
[4] BVerfGE 165, 363, Rn. 54, 72.
[5] BVerfGE 165, 363, Rn. 78 ff.
[6] BVerfGE 165, 363, Rn. 90 ff.

Daraus sei drittens ein abgestuftes Verhältnis zwischen Eingriffsgewicht und Eingriffsschwelle abzuleiten.[7] Je umfangreicher die Datenbasis und je leistungsfähiger die Methode, desto höher müsse die Eingriffsschwelle liegen. Umgekehrt könne der Gesetzgeber das Eingriffsgewicht dadurch absenken, dass er Datenbasis und Methode begrenze.

Viertens müssten Zweckbindungen und Verwendungsbeschränkungen auch technisch und organisatorisch abgesichert werden.[8] Insbesondere seien Daten und Zugriffsrechte danach zu unterscheiden, ob sie der Gefahrenabwehr oder der Strafverfolgung dienen. Das BVerfG verlangt hierfür insbesondere getrennte bzw. gekennzeichnete Datenbestände und zweckabhängige Zugriffsrechte.

### b) BVerfG-Urteil BKAG II

Das BVerfG hat im BKAG-II-Urteil vom 1. Oktober 2024[9] ausdrücklich herausgearbeitet, was im Palantir-Urteil bereits angelegt war: Schon die weitere, zusammenführende Verwendung zuvor getrennt gespeicherter Daten könne einen eigenständigen Grundrechtseingriff darstellen.[10] Das gilt insbesondere dann, wenn Daten außerhalb ihres ursprünglichen Erhebungszwecks in einem neuen Bestand für spätere Nutzungen bereitgehalten würden. Eine solche vorsorgende Speicherung sei selbst eine Zweckänderung und bedürfe daher einer eigenen gesetzlichen Grundlage.

Davon zu trennen sei die spätere zweckfremde Nutzung der gespeicherten Daten. Sie bedürfe ihrerseits einer Rechtfertigung nach den Grundsätzen der Zweckänderung (dazu 3.).

## 2. Unterscheidung zwischen Strafverfolgung und Gefahrenabwehr

Die bereits mehrfach erwähnte Unterscheidung zwischen Strafverfolgung und Gefahrenabwehr ist in der Kompetenzordnung des Grundgesetzes angelegt. Art. 70 Abs. 1 GG weist die Gefahrenabwehr grundsätzlich den Ländern zu, während

[7] BVerfGE 165, 363, Rn. 103 ff.
[8] BVerfGE 165, 363, Rn. 139 ff.
[9] BVerfGE 169, 332.
[10] BVerfGE 169, 332, Rn. 99.

dem Bund nach Art. 74 Abs. 1 Nr. 1 GG die konkurrierende Gesetzgebung für das Strafverfahrensrecht zusteht.

Beide Rechtsgebiete verfolgen unterschiedliche Zwecke. Das Gefahrenabwehrrecht dient der Abwehr bestehender und der Verhütung künftiger Rechtsgutsverletzungen. Das Strafverfahren richtet sich demgegenüber auf die Aufklärung bereits begangener Straftaten auf Grundlage eines Anfangsverdachts und gegebenenfalls auf deren staatliche Sanktionierung. Aus diesen unterschiedlichen Zwecken folgen unterschiedliche Anforderungen an Eingriffsschwellen, Anordnungszuständigkeiten, Verfahrenssicherungen und Rechtsschutz. Dass beide Aufgaben häufig von denselben Polizeibehörden und sogar denselben Beschäftigten wahrgenommen werden, hebt diese rechtliche Trennung nicht auf. Dies gewinnt insbesondere für die noch zu erörternde Zweckbindung Bedeutung.

In der Praxis lässt sich die Grenze allerdings nicht immer ohne Weiteres ziehen. Derselbe Sachverhalt kann zugleich präventiv und repressiv von Bedeutung sein. Eine organisierte Deliktsserie kann etwa Anlass geben, bereits begangene Taten aufzuklären und zugleich weitere Taten zu verhindern. Entscheidend bleibt deshalb, zu welchem Zweck eine konkrete Datenverarbeitung erfolgt. Dies ist mit Blick auf die hier zu untersuchende Analyseplattform in den Fokus zu nehmen.

Die Notwendigkeit einer eindeutigen Zweckzuordnung besteht allerdings unabhängig davon, ob präventive und repressive Auswertungen technisch getrennt oder auf derselben Plattform stattfinden. Auch bei getrennten Systemen muss feststehen, welchem Aufgabenbereich ein Analysevorgang zuzurechnen ist und auf welcher Rechtsgrundlage er erfolgt. Die technische Trennung erleichtert diese Zuordnung lediglich, weil der jeweilige Zweck regelmäßig bereits durch das verwendete System sichtbar wird. Werden dagegen beide Aufgaben auf derselben Plattform wahrgenommen, entfällt diese technische Trennlinie. Insoweit muss für jeden Analysevorgang auf andere Weise eindeutig festgelegt und abgesichert werden, ob er der Gefahrenabwehr oder der Strafverfolgung dient. Die rechtliche Zuordnung folgt dann nicht mehr aus der technischen Systemgrenze, sondern muss innerhalb des Systems hergestellt werden (dazu VII. 2.).

### 3. Zweckbindung und Zweckänderung

Die Trennung von Gefahrenabwehr und Strafverfolgung wird durch den eben bereits angesprochenen Zweckbindungsgrundsatz abgesichert. Personenbezogene Daten dürfen danach grundsätzlich nur zu dem Zweck weiterverarbeitet werden, zu dem sie erhoben wurden.[11]

Eine Nutzung, die über diesen Zweckzusammenhang hinausgeht, ist zwar nicht ausgeschlossen. Als Zweckänderung bedarf sie jedoch einer gesetzlichen Grundlage, die bestimmt, unter welchen Voraussetzungen sie zulässig ist.

Für zweckändernde Datenübermittlungen zwischen verschiedenen Behörden ist das sog. Doppeltürmodell[12] entwickelt worden. Danach muss auf Seiten der datenübermittelnden Behörde die erste Tür geöffnet werden, d.h. eine gesetzliche Vorschrift muss die Übermittlung, Bereitstellung oder zweckändernde Nutzung erlauben. Auf Seiten der empfangenden Behörde muss die zweite Tür zur Datenabfrage geöffnet werden, d.h. es bedarf einer weiteren Rechtsgrundlage für den Abruf und die anschließende Verwendung.

Auch bei einem bloßen Funktionswechsel innerhalb derselben Polizeibehörde entfällt dieses Erfordernis nicht. Zwar fehlt es dann häufig an einer faktischen Übermittlung zwischen zwei Behörden. Materiell wird jedoch der präventive Verwendungszweck durch einen repressiven ersetzt. Auch dieser Zweckwechsel bedarf daher einer gesetzlichen Grundlage.

Damit ist allerdings lediglich das Erfordernis einer gesetzlichen Grundlage für die Zweckänderung geklärt. Offen bleibt, unter welchen Voraussetzungen die Daten für den neuen Zweck verwendet werden dürfen. Entscheidend ist insoweit der Grundsatz der hypothetischen Datenneuerhebung.[13] Danach dürfen Daten, die ursprünglich durch einen schwerwiegenden Grundrechtseingriff erlangt wurden, für einen anderen Zweck grundsätzlich nur genutzt werden, wenn sie für diesen neuen Zweck auch mit einer vergleichbar eingriffsintensiven Maßnahme neu erhoben werden dürften. Sollen etwa besonders sensibel erhobene Daten aus einer Telekommunikations- oder

[11] BVerfGE 165, 363, Rn. 55 ff. mit Verweis auf BVerfGE 65, 1, 46 ff.
[12] BVerfGE 130, 151, 184.
[13] BVerfGE 169, 332, Rn. 138.

Wohnraumüberwachung in eine automatisierte Analyse einbezogen werden, ist zu prüfen, ob diese Daten für den neuen Analysezweck hypothetisch auch neu hätten erhoben werden dürfen. Nur dann ist ihre zweckändernde Verwendung grundsätzlich zulässig.

## IV. Zusammengeführter Datenbestand – Zu den unterschiedlichen Regelungskonzeptionen von Bund und Land

Ausgangspunkt einer effektiven automatisierten Datenanalyse ist ein Datenbestand, in dem die für eine Auswertung in Betracht kommenden Quelldaten technisch erschlossen und in einer gemeinsamen Such- und Verknüpfungsstruktur verfügbar sind. Wie oben dargestellt, ist diese Zusammenführung von der eigentlichen Analyse zu unterscheiden. Zunächst werden die Daten für eine gemeinsame Verarbeitung verfügbar gemacht. Erst im Anschluss wird dieser Bestand anlassbezogen durchsucht und ausgewertet.

Gerade auf dieser vorgelagerten Ebene zeigt sich jedoch ein grundlegender Unterschied zwischen den Regelungskonzepten des Bundes und Schleswig-Holsteins. Unterschiedliche Ansätze verfolgen die Konzepte nicht nur bei der Frage, welche Quelldaten in eine Analyse einbezogen werden dürfen. Die Vorstellungen unterscheiden sich bereits darin, wann und zu welchem Zweck diese Daten zusammengeführt werden, wie lange der dadurch entstehende Bestand vorgehalten werden darf und ob derselbe Bestand sowohl für die Gefahrenabwehr als auch für die Strafverfolgung genutzt werden soll.

Von diesen Unterschieden hängt ab, ob die Regelungen in der Praxis ineinandergreifen können. Der folgende Vergleich untersucht deshalb zunächst, wie die Analysebestände nach den jeweiligen Entwürfen entstehen, wie lange sie vorgehalten werden dürfen und für welche Aufgaben sie zur Verfügung stehen sollen. Welche rechtlichen Folgen sich daraus für einen Wechsel zwischen Gefahrenabwehr und Strafverfolgung ergeben, ist anschließend gesondert zu prüfen (dazu unten VI.).

## 1. Das Regelungsmodell des Bundes

### a) § 9b BKAG-E: Superdatenbank

Besonders deutlich wird das bundesrechtliche Modell in § 9b BKAG-E.[14] Die Vorschrift ermächtigt das BKA, Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zusammenzuführen und anschließend zum Zwecke der Analyse weiterzuverarbeiten. Gesetzestext und Begründung unterscheiden damit ebenfalls zwischen der technischen Zusammenführung und der darauf aufbauenden Analyse.

Entscheidend ist jedoch, wann die Zusammenführung erfolgen soll. Die Bundesregierung geht davon aus, dass jedenfalls ein „Grunddatenbestand“ bereits zusammengeführt, fortlaufend aktualisiert und in einem einheitlichen Datenformat in der Anwendung vorhanden sein müsse.[15] Eine erst bei Eintritt eines konkreten Analyseanlasses vorgenommene Zusammenführung sei wegen der Masse der Daten technisch zu aufwendig und werde dem Ziel einer schnellen und effektiven Straftatenverhütung und -verfolgung nicht gerecht. Die technische Zusammenführung müsse deshalb vom Einzelfall und weiteren Eingriffsschwellen unabhängig erfolgen.

Der Entwurf setzt damit auf einen dauerhaft technisch vorbereiteten Analysebestand, der bereits vorhanden ist, bevor die Voraussetzungen einer konkreten Analyse eintreten. Die Eingriffsschwelle der jeweiligen Analyse entscheidet dann darüber, ob und in welchem Umfang dieser vorbereitete Bestand im Einzelfall ausgewertet werden darf. In diesem technisch vereinfachten Sinne lässt sich von einer Art „Superdatenbank“ sprechen. Damit ist nicht notwendig eine einzige physische Datenbank gemeint. Entscheidend ist, dass ein großer Datenbestand bereits vor dem konkreten Analyseanlass so zusammengeführt und modelliert ist, dass er unmittelbar automatisiert ausgewertet werden kann.

Ferner ist ein zweiter Gesichtspunkt zu berücksichtigen. Dieser Datenbestand soll nicht ausschließlich innerhalb eines einzigen Aufgabenregimes nutzbar sein. § 9b Abs. 1 S. 2

---

[14] Bundesregierung, Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, 26.05.2026, BT-Drucks. 21/6132.

[15] Bundesregierung, Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, 26.05.2026, BT-Drucks. 21/6132, S. 28.

BKAG-E bestimmt ausdrücklich, dass die nach S. 1 zusammengeführten Daten auch für Zwecke der Strafverfolgung nach Maßgabe von § 98e StPO-E weiterverarbeitet werden dürfen. Die Gesetzesbegründung bezeichnet § 98e StPO-E dementsprechend als Ermittlungsmaßnahme, die auf einer „bestehenden polizeilichen Analyseplattform“[16] aufsetzt.

### b) § 98e StPO-E: Strafverfolgung auf der bereits vorhandenen Plattform

Noch klarer tritt diese Konzeption in dem Regelungsentwurf zu § 98e StPO-E hervor. Die geplante Vorschrift knüpft nach dem Regierungsentwurf an personenbezogene Daten an, die in Datei- und Informationssystemen der Polizei rechtmäßig gespeichert und bereits für eine polizeiliche Analyseplattform zusammengeführt worden sind. § 98e StPO-E schafft damit in seiner gegenwärtigen Fassung gerade keine eigenständige Befugnis, zunächst für Zwecke der Strafverfolgung einen neuen verfahrensübergreifenden Analysebestand aufzubauen. Vielmehr setzt er diesen zusammengeführten Datenbestand voraus.

Die Strafverfolgungsbehörden sollen diejenigen Daten auswerten können, die die Polizeibehörden der Länder und des Bundes bereits für den Betrieb verfahrensübergreifender Recherche- und Analyseplattformen zur Gefahrenabwehr zusammengeführt haben. Zur „Vermeidung von Doppelstrukturen“[17] soll gerade keine separate verfahrensübergreifende Analyseplattform für die Strafverfolgung und keine nochmalige Zusammenführung derselben Daten erforderlich sein.

Die gesetzgeberische Konzeption ist damit eindeutig: Die Plattform der Strafverfolgung soll grundsätzlich dieselbe bereits vorhandene polizeiliche Analyseplattform des jeweiligen Bundeslands sein. Gefahrenabwehr und Strafverfolgung sollen technisch nicht voneinander getrennt werden, obgleich die rechtlichen Voraussetzungen, unter denen auf die gemeinsam vorbereiteten Daten zugegriffen dürfen, unterschiedlich sind.

---

[16] Bundesregierung, Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, 26.05.2026, BT-Drucks. 21/6132, S. 28.

[17] Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, 01.07.2026, BT-Drucks. 21/6806, S. 19.

Allerdings erkennt auch die Bundesregierung, dass § 98e StPO-E allein hierfür nicht genügt. Die für die Gefahrenabwehr zusammengeführten Daten unterliegen weiterhin dem für die speichernde Stelle geltenden Recht einschließlich seiner Übermittlungs- und Verwendungsregelungen. Deshalb führt die Gesetzesbegründung ausdrücklich aus, dass in den Landespolizeigesetzen „spiegelbildlich Regelungen geschaffen werden“[18] müssten, welche die Nutzung der für Zwecke der Gefahrenabwehr zusammengeführten Daten für eine Strafverfolgung nach § 98e StPO-E ermöglichen.
Damit ist das bundesrechtliche Konzept im Ausgangspunkt ein Doppeltürmodell: § 98e StPO-E soll die strafprozessuale Nutzung ermöglichen; das jeweilige Landesrecht muss seinerseits den präventiv gebildeten Bestand für diesen neuen Zweck öffnen.

Der Bundesrat hat im Gesetzgebungsverfahren erkannt, dass diese Konstruktion die Anwendung des § 98e StPO-E von einer vorgelagerten landesrechtlichen Datenzusammenführung abhängig macht. Er weist zutreffend darauf hin, dass der Regierungsentwurf ins Leere laufen kann, wenn ein Land entweder keine Rechtsgrundlage für eine gefahrenabwehrrechtliche Analyseplattform besitzt oder die Voraussetzungen einer solchen Zusammenführung im konkreten Fall nicht vorliegen. § 98e StPO-E enthalte selbst keine Befugnis zur eigenständigen Vorab-zusammenführung ausschließlich für Zwecke der Strafverfolgung.[19]
Der Bundesrat schlägt deshalb vor, diese Abhängigkeit zu beseitigen. Nach seiner Fassung sollen die in den Datei- und Informationssystemen der Polizei rechtmäßig gespeicherten Daten unmittelbar auf Grundlage des § 98e StPO-E zusammengeführt und darüber hinaus weiterverarbeitet werden dürfen. Die Voraussetzung, dass die Daten zuvor bereits für eine polizeiliche Analyseplattform zusammengeführt worden sein müssen, soll entfallen.
Damit stehen sich zwei Regelungsmodelle gegenüber: Der Regierungsentwurf setzt auf die weitere Nutzung eines bereits für die Gefahrenabwehr gebildeten Analysebestands. Der Vorschlag des Bundesrates ermöglicht dagegen eine eigenständige Zusammenführung der Quelldaten nur für Zwecke der Strafverfolgung.

---

[18] Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, 01.07.2026, BT-Drucks. 21/6806, S. 19.

[19] Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, 01.07.2026, BT-Drucks. 21/6806, Anlage 2, S. 26.

Die Bundesregierung hält hingegen an ihrer Ausgangskonzeption fest. In ihrer Gegenäußerung betont sie ausdrücklich, sie habe gerade dem Anliegen der Länder entsprochen, keine gesonderten Analyseplattformen für die Strafverfolgung zu schaffen. Die für die Analyse erforderliche Datenaufbereitung erfolge nach ihrer Vorstellung „dauerhaft und unabhängig von einer konkreten Gefahrenlage“[20]. Diese dauerhaft aufbereiteten Daten sollten anschließend auch für die Strafverfolgung ausgewertet werden können.

### 2. Die Regelungskonzeption des § 188c LVwG-E

§ 188c LVwG-E verfolgt eine andere Konzeption, ohne dabei die parallelen Gesetzgebungsverfahren zu erwähnen.

Der Entwurf erkennt zunächst ausdrücklich an, dass die Zusammenführung der Daten selbst ein rechtfertigungsbedürftiger Verarbeitungsvorgang ist. Die Begründung unterscheidet dementsprechend einen ersten Schritt, in dem die bislang getrennten Datenbestände zusammengeführt werden, von einem zweiten Schritt, in dem dieser Bestand mit konkreten Suchoperationen ausgewertet wird.[21]

Diese Zweistufigkeit schlägt sich unmittelbar im Gesetzestext nieder. Nach § 188c Abs. 2 S. 1 LVwG-E darf die Polizei die in polizeilichen Dateisystemen gespeicherten personenbezogenen Daten zu den in Absätzen 3 und 4 beschriebenen gefahrenabwehrrechtlichen Zwecken „anlassbezogen zusammenführen und anschließend“ zur Gewinnung neuer Erkenntnisse verarbeiten.

Dementsprechend wird auch kein dauerhaft zusammengeführter Grunddatenbestand geschaffen. § 188d Abs. 5 LVwG-E bestimmt vielmehr, dass die anlassbezogen zusammengeführten personenbezogenen Daten als Datenbestand nur so lange vorgehalten werden dürfen, wie dies für den gefahrenabwehrrechtlichen Zweck der in § 188c Abs. 3 und 4 LVwG-E normierten Datenanalyse erforderlich ist. Dauert die Zusammenführung länger als sechs Monate an, ist ihre weitere Erforderlichkeit regelmäßig zu überprüfen. Die Begründung stellt ausdrücklich fest, dass die

[20] Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, 01.07.2026, BT-Drucks. 21/6806, Anlage 3, S. 28.

[21] Schleswig-Holsteinische Landesregierung, LT-Drs. 20/4284, S. 50.

Zusammenführung nicht mehr gerechtfertigt ist, sobald der Zweck der Maßnahme erreicht ist oder nicht mehr erreicht werden kann.[22]

Der Landesgesetzgeber unterscheidet dabei ausdrücklich zwischen einem zusammengeführten Analysebestand und der bloßen Analysefähigkeit der Daten.[23] Letztere könne dadurch hergestellt werden, dass Daten bereits separat in einem Format vorgehalten werden, das ihre spätere Zusammenführung und Analyse erleichtert. Eine dauerhafte technische Vorbereitung der Quelldaten wird also nicht ausgeschlossen. Nicht vorgesehen ist dagegen, die Daten bereits unabhängig von einem konkreten Analyseanlass dauerhaft zu einem gemeinsamen personenbezogenen Analysebestand zusammenzuführen.

Darin liegt ein erster grundlegender Unterschied zum Bundesmodell. Die Bundesregierung geht für § 9b BKAG-E und in ihrer Gegenäußerung zu § 98e StPO-E – wie bereits erwähnt – davon aus, dass der für die Analyse erforderliche Grunddatenbestand vorab und unabhängig vom konkreten Analyseanlass zusammengeführt bzw. aufbereitet vorliegt. Schleswig-Holstein lässt demgegenüber zwar eine technische Vorstrukturierung der getrennten Quelldaten zu, erlaubt deren eigentliche Zusammenführung aber erst anlassbezogen und nur für die Dauer der konkreten gefahrenabwehrrechtlichen Analyse.

Ein zweiter und für das Verhältnis zu § 98e StPO-E noch wichtigerer Unterschied ergibt sich aus § 188c Abs. 2 S. 2 LVwG-E. Danach ist „eine Verarbeitung des zusammengeführten Datenbestandes zu anderen Zwecken […] ausgeschlossen“.

Der nach § 188c Abs. 2 LVwG-E gebildete Bestand ist damit sowohl an einen konkreten Anlass als auch an die gefahrenabwehrrechtlichen Analysezwecke des § 188c Abs. 3 und 4 LVwG-E gebunden. Anders als § 9b Abs. 1 S. 2 BKAG-E sieht der Landesentwurf keine ausdrückliche Öffnung für eine strafprozessuale Anschlussverwendung vor. Die Folgen dieser unterschiedlichen Zweckbestimmung für die Anwendung des § 98e StPO-E werden unter VI. 2. untersucht.

[22] Schleswig-Holsteinische Landesregierung, LT-Drs. 20/4284, S. 55.
[23] Schleswig-Holsteinische Landesregierung, LT-Drs. 20/4284, S. 55.

## V. Automatisierte Datenanalyse – unterschiedliche rechtliche Voraussetzungen

### 1. Das Grundproblem

Nach der Betrachtung der Konzepte zur Zusammenführung der Datenbestände ist nunmehr die eigentliche Datenauswertung zu untersuchen. Der folgende Vergleich soll zeigen, weshalb unterschiedliche Befugnisse bei technisch vergleichbaren Analysen besondere Anforderungen an die Zwecktrennung stellen. Gefahrenabwehr und Strafverfolgung unterliegen unterschiedlichen rechtlichen Eingriffsvoraussetzungen; ihre Analysen können jedoch technisch und/oder personell miteinander verbunden sein. Selbst bei getrennten Plattformen bleibt das Problem bestehen, wenn dieselben Bediensteten beide Systeme nutzen und dabei gewonnene Erkenntnisse in den jeweils anderen Aufgabenbereich übertragen.

Deutlich wird dies, wenn ein Sachverhalt zugleich einen strafprozessualen Verdacht und eine gefahrenabwehrrechtliche Gefahr begründet. Für technisch vergleichbare Analysen können dann unterschiedliche Rechtsgrundlagen mit unterschiedlichen Eingriffsschwellen, Datenumfängen und Anordnungsvorbehalten zur Verfügung stehen. Damit entsteht die Gefahr, auf die jeweils leichter zugängliche Befugnis auszuweichen und die so gewonnenen Erkenntnisse anschließend in den anderen Aufgabenbereich zu überführen. Zunächst sind deshalb die hierfür maßgeblichen Unterschiede der Befugnisse herauszuarbeiten (2.). Anschließend ist zu untersuchen, wie sie ein sog. „Befugnishopping“ und einen Zweckwechselkreislauf begünstigen können (3.).

### 2. Vergleich der Vorschriften von StPO und LVwG

§ 188c LVwG-E und § 98e StPO-E erlauben technisch vergleichbare Formen automatisierter Datenanalyse, ordnen sie aber unterschiedlichen Aufgaben zu: § 188c LVwG-E der Gefahrenabwehr, § 98e StPO-E der Strafverfolgung. Gemeinsam ist beiden Vorschriften die automatisierte Verknüpfung und Auswertung vorhandener personenbezogener Daten. Die Befugnis zu ihrer vorgelagerten Zusammenführung ist dagegen unterschiedlich geregelt (dazu IV. 1. b) und IV. 2.).

Für die hier zu untersuchende Zugriffsarchitektur kommt es deshalb weniger auf einen abstrakten Vergleich beider Vorschriften als auf die Unterschiede an, die bei einer gemeinsamen oder technisch verbundenen Nutzung praktisch relevant werden. Dies

betrifft vor allem die Eingriffsschwelle, den zulässigen Datenumfang, die Analysemethoden sowie die Anordnungs- und Kontrollmechanismen.

**a) Zweck und Eingriffsschwelle**

§ 188c LVwG-E folgt dem vom BVerfG vorgezeichneten Stufenmodell: Je umfangreicher die Datenbasis und je größer das Eingriffsgewicht der Analyse, desto höher sind die materiellen Voraussetzungen.
Die Analyse mit geringerem Eingriffsgewicht nach § 188c Abs. 3 LVwG-E setzt tatsächliche Anhaltspunkte für eine hinreichend konkretisierte Gefährdung bestimmter gewichtiger Rechtsgüter oder – unter vergleichbaren Voraussetzungen – die Gefahr weiterer gleichgelagerter Straftaten voraus. Für die weitergehende Analyse nach § 188c Abs. 4 LVwG-E verlangt das Gesetz demgegenüber eine Gefahr für Leben, Leib, Freiheit oder sexuelle Selbstbestimmung einer Person oder für Bestand oder Sicherheit des Bundes oder eines Landes. Sollen Daten aus dem Einsatz technischer Mittel in Wohnungen einbezogen werden, muss darüber hinaus eine dringende Gefahr vorliegen.

§ 98e StPO-E kennt eine solche Abstufung nicht. Die Analyse setzt einheitlich voraus, dass bestimmte Tatsachen den Verdacht einer auch im Einzelfall schwerwiegenden, in § 100a Abs. 2 StPO bezeichneten schweren Straftat begründen. Sie muss der Aufklärung dieser Straftat oder der Ermittlung des Aufenthalts einer Person, nach der für die Zwecke des Strafverfahrens gefahndet wird, dienen.

Damit unterscheiden sich bereits die Zugangsschwellen erheblich. Das Landesrecht staffelt sie nach dem Eingriffsgewicht der konkreten Analyse. Das Strafprozessrecht knüpft dagegen einheitlich an einen qualifizierten Straftatverdacht an. Bei einem Sachverhalt, der zugleich sowohl präventiv als auch repressiv von Bedeutung ist, kann daher dieselbe oder eine technisch sehr ähnliche Analyse also nach unterschiedlichen materiellen Voraussetzungen zulässig sein.

**b) Zulässige Datenbestände**

Noch deutlicher treten die Unterschiede bei den Daten hervor, die in die Analyse einbezogen werden dürfen.

§ 188c Abs. 3 LVwG-E beschränkt die Datenbasis auf die dort abschließend genannten Vorgangs-, Fallbearbeitungs-, Auskunfts-, Kommunikations-, Einsatzleit- und Einsatzdokumentationssysteme sowie auf Daten aus Asservaten und anderen Beweismitteln. Daten aus Wohnraumüberwachungen und Online-Durchsuchungen sind auf dieser Stufe ausgeschlossen.

Für die eingriffsintensivere Analyse nach § 188c Abs. 4 LVwG-E ist die Datenbasis dagegen erheblich umfangreicher. Grundsätzlich können personenbezogene Daten aus sämtlichen Dateisystemen der Polizei und automatisierten Verfahren einbezogen werden. Der Ausschluss besonders eingriffsintensiv erhobener Daten in § 188c Abs. 6 S. 1 LVwG-E bezieht sich seinem Wortlaut nach nur auf Abs. 3. Damit können auf der höheren Eingriffsstufe insbesondere auch Daten aus Wohnraumüberwachungen in Betracht kommen. Entsprechendes gilt für Daten aus einem verdeckten Zugriff auf informationstechnische Systeme.

§ 98e StPO-E erfasst hingegen andere Datenbestände. Zulässig sind insbesondere Vorgangs- und Falldaten, Daten aus polizeilichen Informationssystemen und dem polizeilichen Informationsaustausch sowie unter zusätzlichen Voraussetzungen Daten aus anderen eingriffsintensiven Maßnahmen und aus Asservaten. Ausdrücklich ausgeschlossen sind jedoch Daten aus Online-Durchsuchungen und akustischen Wohnraumüberwachungen nach §§ 100b und 100c StPO in anderen Strafverfahren sowie aus entsprechenden Maßnahmen nach anderen Gesetzen.

Auch eine unmittelbare Anbindung der Analyseplattform an nichtpolizeiliche Register ist nach § 98e StPO-E ausgeschlossen. Ergebnisse konkreter Registerabfragen und im Einzelfall erhobene Internetdaten können dagegen in die Analyse einfließen.

Mit Blick auf die einzubeziehenden Quelldaten bestehen damit erhebliche Unterschiede. Daten aus gefahrenabwehrrechtlichen Wohnraumüberwachungen und Online-Durchsuchungen sind der Analyse nach § 98e StPO-E entzogen, können aber nach § 188c Abs. 4 LVwG-E in die präventive Analyse einbezogen werden.

### c) Zulässige Analysemethoden

Auch hinsichtlich der eingesetzten Analysemethoden unterscheiden sich beide Entwürfe.

§ 188c Abs. 6 LVwG-E schließt für sämtliche Analysen die Verarbeitung biometrischer Daten sowie selbstlernende Systeme aus. Der Landesgesetzgeber begrenzt damit bewusst die Leistungsfähigkeit des Systems und senkt auf diese Weise das Eingriffsgewicht der Analyse.

§ 98e StPO-E enthält dagegen kein entsprechendes generelles Verbot künstlicher Intelligenz oder selbstlernender Systeme. Die Gesetzesbegründung geht ausdrücklich davon aus, dass innerhalb der gesetzlich zugelassenen Analysemethoden auch KI-Systeme und Sprachmodelle eingesetzt werden können.[24] Begrenzt wird ihr Einsatz insbesondere dadurch, dass die Analyse anlassbezogen und manuell ausgelöst werden muss, die Suchparameter aus einem konkreten Sachverhalt abzuleiten sind und keine ausschließlich automatisierte Entscheidung mit nachteiligen Rechtsfolgen getroffen werden darf.

Für eine gemeinsam genutzte Plattform hat dieser Unterschied unmittelbare technische Bedeutung. Stellt das System für die Strafverfolgung selbstlernende Verfahren bereit, müssen diese für eine Analyse nach § 188c LVwG-E zuverlässig ausgeschlossen werden.

### d) Anordnung und Kontrolle

Besonders deutlich unterscheiden sich die Vorschriften bei der Anordnungszuständigkeit.

Für die Analyse nach § 188c Abs. 3 LVwG-E verlangt § 188c Abs. 8 LVwG-E eine qualifizierte polizeiliche Anordnung nach Maßgabe des § 186 Abs. 2 LVwG. Anordnungsbefugt sind insbesondere die Leitungen des Landespolizeiamtes, des Landes-

[24] Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, 01.07.2026, BT-Drucks. 21/6806, S. 22.

kriminalamtes oder einer Polizeidirektion sowie besonders beauftragte Personen des Polizeivollzugsdienstes.
Die weitergehende Analyse nach § 188c Abs. 4 LVwG-E steht dagegen unter Richtervorbehalt. Soll darüber hinaus ein Verhaltensprofil nach § 188c Abs. 7 LVwG-E erstellt werden, muss dies ausdrücklich von der Anordnung umfasst sein.

§ 98e StPO-E sieht demgegenüber weder einen Richtervorbehalt noch eine Anordnung durch die Staatsanwaltschaft vor, die nach der strafprozessualen Grundentscheidung der StPO eigentlich „Herrin des Ermittlungsverfahrens“ ist. Der Entwurf verlangt lediglich eine Begründung und Protokollierung der Analyse, überträgt die Entscheidung über ihren Einsatz aber weder einer besonders qualifizierten externen oder staatsanwaltschaftlichen Stelle noch einem Richter. Dies ist insbesondere deshalb bemerkenswert, weil § 98d StPO-E für den unmittelbar benachbarten automatisierten biometrischen Internetabgleich immerhin einen Staatsanwaltschaftsvorbehalt vorsieht.

Für eine gemeinsame Plattform ergibt sich daraus ein weiterer Unterschied: Eine weitreichende präventive Analyse kann einer richterlichen Anordnung bedürfen, während eine technisch vergleichbare repressive Analyse auf derselben Plattform ohne jegliche vorherige Kontrolle durchgeführt werden kann.

**e) Kennzeichnung, Nachvollziehbarkeit und Protokollierung**

Insbesondere mit Blick auf einen möglichen zweckübergreifenden Datenbestand gewinnen Kennzeichnung, Zugriffskontrolle und Protokollierung besondere Bedeutung.

§ 188d LVwG-E enthält hierzu vergleichsweise detaillierte Vorgaben. Die Vorschrift verlangt insbesondere die Kennzeichnung der einbezogenen Daten, eine anlassbezogene und nach Personenkategorien differenzierte Verarbeitung, die Nachvollziehbarkeit des automatisierten Verfahrens, die Beschränkung des Zugangs auf besonders qualifizierte Beschäftigte sowie Zugriffskontrollen und Protokollierungen.
Die technischen und organisatorischen Einzelheiten sollen durch eine veröffentlichte Verwaltungsvorschrift konkretisiert werden. Dies betrifft insbesondere die Zweckbindung und Kennzeichnung der Daten, die Suchkriterien, die Nachvollziehbarkeit

des Verfahrens, die Zugangs- und Berechtigungskonzepte sowie die Speicherdauer. Die grundrechtswesentlichen Entscheidungen – Eingriffsschwellen, zulässige Datenbestände, ausgeschlossene Datenarten und Anordnungszuständigkeiten – verbleiben dagegen im Gesetz. Dies entspricht dem Ansatz des BVerfG, technische Einzelheiten angesichts der Entwicklungsdynamik solcher Systeme untergesetzlicher Konkretisierung zu überlassen, die wesentlichen Grenzen des Eingriffs aber gesetzlich festzulegen.[25]

Daneben greifen die allgemeinen datenschutzrechtlichen Protokollierungspflichten. Für die polizeiliche Datenverarbeitung des Landes folgen sie aus den Vorschriften zur Umsetzung von Art. 25 der Richtlinie (EU) 2016/680. Für das Strafverfahren gelten § 500 Abs. 1 StPO i.V.m. § 76 BDSG.

Hinzu treten für § 98e StPO-E besondere Begründungs- und Protokollierungspflichten. Nach § 98e Abs. 5 S. 1 StPO-E sind die Voraussetzungen des konkreten Einsatzes und bei Einbeziehung besonders sensibler Daten auch deren Erforderlichkeit zu begründen. Über § 98e Abs. 5 S. 2 i.V.m. § 98d Abs. 2 StPO-E sind zudem die eingesetzte Anwendung, der Zeitpunkt, die einbezogenen Daten und die ausführende Organisationseinheit zu protokollieren. Nach der Gesetzesbegründung soll dadurch insbesondere nachvollziehbar bleiben, welche Datenbestände wann und warum einbezogen wurden.[26] Die Gesetzesbegründung erfasst dagegen nicht ausdrücklich den für eine gemeinsam genutzte Plattform besonders bedeutsamen Wechsel zwischen präventiver und repressiver Funktion und eine etwaige Überführung der gewonnenen Erkenntnisse in das jeweils andere Aufgabenregime.

### 3. „Befugnishopping“ und Zweckwechselkreislauf

Die dargestellten Unterschiede zwischen präventiver und repressiver Datenanalyse bergen ein Risiko: Für technisch vergleichbare Auswertungen stehen unterschiedliche Rechtsregime mit unterschiedlichen materiellen und formellen Voraussetzungen zur Verfügung. Dieses Problem setzt nicht voraus, dass beide Aufgaben auf einer einzigen

[25] BVerfGE 165, 363, Rn. 112 ff.

[26] Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, 01.07.2026, BT-Drucks. 21/6806, S. 23.

gemeinsamen Analyseplattform wahrgenommen werden. Es besteht auch bei technisch getrennten Analysebeständen, wenn dieselben Bediensteten über denselben Arbeitsplatz auf beide Systeme zugreifen und zwischen präventiver und repressiver Analyse wechseln können. Entscheidend ist deshalb weniger die physische Trennung der Systeme als die Frage, wie der jeweilige Verarbeitungszweck festgelegt, der Zugriff gesteuert und ein Wechsel zwischen beiden Aufgabenbereichen kontrolliert wird.
Für sich genommen ist es unbedenklich, dass für Gefahrenabwehr und Strafverfolgung unterschiedliche Befugnisse bestehen. Die Wahl der Rechtsgrundlage darf sich jedoch nicht danach richten, welches Regelungsregime im konkreten Fall den leichteren Zugriff eröffnet.

Die Unterschiede zwischen § 188c LVwG-E und § 98e StPO-E verdeutlichen die Gefahr eines solchen „Befugnishoppings“ besonders deutlich. Fehlt etwa der für § 98e StPO-E erforderliche qualifizierte Verdacht einer auch im Einzelfall schwerwiegenden Straftat nach § 100a Abs. 2 StPO, können gleichwohl die gefahrenabwehrrechtlichen Voraussetzungen des § 188c LVwG-E erfüllt sein. Umgekehrt kann ein hinreichend konkretisierter Verdacht einer bereits begangenen schweren Straftat eine Analyse nach § 98e StPO-E ermöglichen, obwohl die für § 188c LVwG-E erforderliche Gefahrenlage nicht besteht. Hinzu treten Unterschiede bei den zulässigen Datenbeständen und Analysemethoden: § 188c Abs. 4 LVwG-E eröffnet unter gesteigerten Voraussetzungen teilweise weitergehende Datenbestände, während § 98e StPO-E insbesondere Daten aus gefahrenabwehrrechtlichen Wohnraumüberwachungen und Online-Durchsuchungen ausschließt. Umgekehrt lässt der Bundesentwurf Analysemethoden zu, die § 188c LVwG-E ausdrücklich begrenzt. Auch die formellen Sicherungen unterscheiden sich, weil die eingriffsintensive Analyse nach § 188c Abs. 4 LVwG-E richterlicher Anordnung bedarf, § 98e StPO-E dagegen keinen entsprechenden Richter- oder Staatsanwaltschaftsvorbehalt vorsieht.

Bei Sachverhalten mit zugleich präventivem und repressivem Bezug können damit Anreize entstehen, die Analyse dem jeweils weniger restriktiven Rechtsregime zuzuordnen. „Befugnishopping“ setzt dabei keinen bewussten Rechtsmissbrauch voraus. Ein Funktionswechsel wird in der Praxis bereits dadurch erleichtert, dass

dieselbe Person an demselben Arbeitsplatz Zugriff auf einen präventiven und einen repressiven Analysebestand hat. Eine gemeinsame Plattform verstärkt dieses Problem lediglich.

Hinzu kommt die Gefahr eines Zweckwechselkreislaufs. Strafprozessual erhobene Daten können unter den gesetzlichen Voraussetzungen in einen gefahrenabwehrrechtlichen Verwendungszusammenhang gelangen, dort mit weiteren Daten verknüpft und zur Gewinnung neuer Erkenntnisse genutzt werden. Ergeben sich daraus Hinweise auf eine bereits begangene Straftat, besteht erneut ein Interesse an einer strafprozessualen Verwendung. Ein solcher Wechsel zwischen beiden Rechtsregimen ist nicht schlechthin unzulässig (dazu III. 3.). Er darf aber nicht dazu führen, dass die jeweils strengeren Voraussetzungen durch den zwischenzeitlichen Wechsel des Verarbeitungszwecks umgangen werden.

## VI. Zweckänderung bei Ausgangsdaten, Analysebeständen und Analyseergebnissen

Auf Grundlage der dargestellten Regelungskonzepte und Befugnisse ist nunmehr zu prüfen, unter welchen Voraussetzungen Daten und Erkenntnisse zwischen Gefahrenabwehr und Strafverfolgung verwendet werden dürfen. Die in Abschnitt IV. beschriebenen Unterschiede werden damit auf ihre rechtlichen Folgen für den Zweckwechsel untersucht. Entsprechend der eingangs eingeführten Unterscheidung betrifft dies die zweckändernde Verwendung einzelner Ausgangsdaten (1.), die Nutzung des zusammengeführten Analysebestands (2.) und die Weiterverwendung der erst durch die Analyse erzeugten Erkenntnisse (3.).

### 1. Zweckänderung der Quell- und Ausgangsdaten

Auf der ersten Ebene geht es um die Zweckänderung der Quell- und Ausgangsdaten selbst. Insoweit gelten zunächst die allgemeinen Regeln, die für jede weitere Nutzung personenbezogener Daten gelten – unabhängig davon, ob anschließend eine automatisierte Datenanalyse erfolgt. Der Wechsel zwischen Gefahrenabwehr und Strafverfolgung setzt daher nach dem Doppeltürmodell eine gesetzliche Öffnung auf

Herkunfts- und Verwendungsseite voraus. Bei eingriffsintensiv erhobenen Daten gilt zudem der Grundsatz der hypothetischen Datenneuerhebung (dazu oben III. 3.). Das gilt auch beim bloßen Funktionswechsel innerhalb derselben Polizeibehörde.

### a) Daten aus dem Strafverfahren für Zwecke der Gefahrenabwehr

§ 481 Abs. 1 StPO öffnet auf strafprozessualer Seite die Übermittlung strafprozessual erhobener Daten an die Polizei; die korrespondierende Öffnung für ihre zweckändernde Weiterverarbeitung enthält in Schleswig-Holstein § 188a Abs. 2 LVwG. Bei besonders eingriffsintensiv erhobenen Daten sind zudem die Verwendungsbeschränkungen des § 479 Abs. 2 StPO zu beachten.

### b) Daten aus der Gefahrenabwehr für Zwecke der Strafverfolgung

Für den umgekehrten Wechsel von der Gefahrenabwehr zur Strafverfolgung ist die Regelung weniger eindeutig. Bei § 188a LVwG hat der Schleswig-Holsteinische Gesetzgeber seinerzeit bewusst darauf verzichtet, die landesrechtliche „erste Tür“ für eine strafprozessuale Weiterverwendung näher auszugestalten.[27] Zur Begründung verweist er auf die Gesetzgebungskompetenz des Bundes für das Strafverfahren. Die Bundeskompetenz erfasst jedoch nur die strafprozessuale Anschlussverwendung, also die zweite Tür. Unbeantwortet bleibt damit die vorgelagerte Frage, unter welchen Voraussetzungen das Landesrecht die zu präventiven Zwecken erhobenen Daten aus ihrer bisherigen Zweckbindung entlässt.

Als erste Tür des Doppeltürmodells kommt insoweit § 188 Abs. 1 S. 3 LVwG in Betracht. Danach ist eine Verarbeitung zu anderen Zwecken zulässig, soweit sie in anderen Rechtsvorschriften vorgesehen ist. Es handelt sich folglich um eine dynamische Verweisungsregel, die die Entscheidung über die Reichweite der landesrechtlichen Zweckbindung ohne Not dem Bundesgesetzgeber überlässt.

Ohne dies an dieser Stelle näher vertiefen zu können, fehlt es auch in der StPO an einer allgemeinen, ausdrücklich als solche ausgestalteten Einlassklausel, die im Bild des

[27] Schleswig-Holsteinische Landesregierung, LT-Drs. 19/2118, S. 97.

Doppeltürmodells die zweite Tür öffnet.[28] Nach h.M. wird hierfür auf § 161 Abs. 1 StPO unter Beachtung der Verwendungsbeschränkungen des § 161 Abs. 3 StPO für die Nutzung zu Beweiszwecken zurückgegriffen.[29] Eine eigenständige Befugnis zur automatisierten Datenanalyse folgt daraus nicht; hierfür soll § 98e StPO-E die besondere Rechtsgrundlage schaffen.

### 2. Nutzung des gefahrenabwehrrechtlichen Analysebestands für Strafverfolgungszwecke

Da der Bundesgesetzgeber auf der strafprozessualen Ebene, wie bereits ausgeführt, keinen eigenen Datenanalysebestand schaffen will, stellt sich auf der zweiten Ebene die Frage nach der Nutzung des gefahrenrechtlich zusammengeführten Analysebestands. Zwar können einzelne zu Gefahrenabwehrzwecken erhobene Quelldaten unter den soeben dargestellten allgemeinen Voraussetzungen für Strafverfolgungszwecke weiterverwendet werden. Davon zu unterscheiden ist jedoch die Zweckbindung des nach § 188c Abs. 2 LVwG-E gebildeten Analysebestands.

Insoweit ist zunächst festzuhalten, dass der nach § 188c Abs. 2 LVwG-E gebildete Analysebestand auf gefahrenabwehrrechtliche Zwecke beschränkt ist. Die Anlassbindung folgt aus § 188c Abs. 2 S. 1 LVwG-E. § 188c Abs. 2 S. 1 LVwG-E bestimmt ferner, dass der zusammengeführte Datenbestand ausschließlich zu den in den Absätzen 3 und 4 genannten Zwecken verarbeitet werden darf. Diese Zwecke sind präventiver Natur. § 188c Abs. 2 S. 2 LVwG-E stellt dies zusätzlich ausdrücklich klar, indem er eine Verarbeitung des zusammengeführten Datenbestandes zu anderen Zwecken ausschließt.

Daran ändert auch die Verweisung des § 188c Abs. 2 LVwG-E auf § 188a Abs. 1 und 2 LVwG sowie auf § 479 Abs. 2 S. 2 Nr. 1 und 2 StPO nichts. Zwar spricht die Gesetzesbegründung insoweit von einer einheitlichen Sicherung der präventiven und repressiven Datenverarbeitung.[30] Die in Bezug genommenen Vorschriften öffnen jedoch

[28] So ausdrücklich auch Specht/Mantz DatenschutzR-HdB/*Roggenkamp,* 1. Aufl. 2019, § 21 Rn. 72.
[29] Grundlegend zu den Verwendungsregeln s. *Singelnstein,* ZStW 120 (2008), 854 ff.
[30] Schleswig-Holsteinische Landesregierung, LT-Drs. 20/4284, S. 50.

gerade nicht die erste Tür gefahrenabwehrrechtlich erhobener Daten in das Strafverfahren.

§ 188a Abs. 1 und 2 LVwG regelt ausschließlich die Weiterverarbeitung vorhandener Daten zu gefahrenabwehrrechtlichen Zwecken. Die Vorschrift betrifft damit die Verwendung von Daten innerhalb des Gefahrenabwehrrechts und nicht deren Nutzung für Zwecke der Strafverfolgung.

Auch die Verweisung auf § 479 Abs. 2 S. 2 Nr. 1 und 2 StPO führt zu keinem anderen Ergebnis. Sie betrifft vielmehr den umgekehrten Datentransfer. Ausgangspunkt ist insoweit § 481 Abs. 1 StPO, der grundsätzlich die Übermittlung strafprozessual erhobener Daten an Polizeibehörden für Zwecke außerhalb des Strafverfahrens ermöglicht. § 479 Abs. 2 S. 2 Nr. 1 und 2 StPO begrenzt diese Verwendung für Daten, die durch besonders eingriffsintensive strafprozessuale Maßnahmen erlangt wurden.
Eine Befugnis für die Verwendung des nach § 188c Abs. 2 LVwG-E gebildeten Analysebestandes zu Zwecken der Strafverfolgung lässt sich aus den Verweisungen auf § 188a LVwG und § 479 Abs. 2 S. 2 StPO demnach gerade nicht ableiten. Dafür bedürfte es einer eigenständigen Öffnung auf gefahrenabwehrrechtlicher Seite, etwa vergleichbar mit § 9b Abs. 1 S. 2 BKAG-E.

§ 188c Abs. 2 S. 2 LVwG-E schließt darüber hinaus die Verarbeitung dieses Datenbestands zu anderen Zwecken ausdrücklich aus. Die Zulässigkeit einer zweckändernden Verwendung einzelner Quelldaten eröffnet daher keinen Zugriff auf den präventiv gebildeten Analysebestand für Zwecke der Strafverfolgung.
Auch ein Rückgriff auf § 188 Abs. 1 S. 3 LVwG führt zu keinem anderen Ergebnis, weil § 188c Abs. 2 S. 2 LVwG-E die speziellere Regelung enthält und § 188 Abs. 1 S. 3 LVwG mithin sperrt.

Damit tritt in Schleswig-Holstein die Konstellation ein, vor der der Bundesrat gewarnt hat. § 98e StPO-E setzt in der Fassung des Regierungsentwurfs einen bereits zusammengeführten polizeilichen Analysebestand voraus. Die Gesetzesbegründung verlangt deshalb „spiegelbildliche“ landesrechtliche Regelungen, die dessen Nutzung für

die Strafverfolgung ermöglichen. Der Schleswig-Holsteinische Entwurf trifft jedoch die entgegengesetzte Anordnung: Ein nach § 188c Abs. 2 LVwG-E gebildeter Bestand darf nicht für die Strafverfolgung genutzt werden. **§ 98e StPO-E könnte daher in Schleswig-Holstein nicht angewendet werden, weil der dafür erforderliche Analysebestand nicht zur Verfügung stünde.**

Hinzu kommt, dass die Öffnung auch strukturell nicht ohne Weiteres in das Landeskonzept passte. Der nach § 188c Abs. 2 LVwG-E gebildete Bestand entsteht anlassbezogen für eine konkrete gefahrenabwehrrechtliche Analyse und darf nach § 188d Abs. 5 LVwG-E nur so lange vorgehalten werden, wie dies für deren Zweck erforderlich ist. Ein solcher Bestand ist kein dauerhaft verfügbarer Grunddatenbestand. Eine Öffnung für die Strafverfolgung würde daher zusätzlich eine Abstimmung mit der zeitlichen Begrenzung des § 188d Abs. 5 LVwG-E erfordern. Ohne eine solche Öffnung bedürfte es für eine repressive Analyse einer eigenständigen Zusammenführungsbefugnis und eines rechtlich gesonderten Bestands – wie es der Bundesrat forderte –, während der Bundesentwurf gesonderte Zusammenführungen für beide Aufgaben gerade vermeiden will.

Der Landesgesetzgeber hat sich erkennbar bewusst gegen einen dauerhaft vorgehaltenen Analysebestand entschieden. Die Zusammenführung soll vielmehr anlassbezogen erfolgen und zeitlich durch den jeweiligen gefahrenabwehrrechtlichen Zweck begrenzt bleiben. Darin liegt eine Abweichung vom bundesrechtlichen Modell eines dauerhaft verfügbaren zusammengeführten Datenbestands. Ob damit zugleich unterschiedliche technische Plattformen für Gefahrenabwehr und Strafverfolgung vorgesehen werden sollen, lässt sich dem Entwurf hingegen nicht entnehmen. Die unterschiedliche Konzeption der Datenvorhaltung zwingt jedenfalls nicht zu einer solchen technischen Trennung, sofern die Datenbestände und Zugriffsrechte nach ihrem jeweiligen Zweck getrennt bleiben (dazu VII. 2.).

Die darüberhinausgehende Sperre für eine strafprozessuale Nutzung des bereits zusammengeführten Analysebestands erscheint dagegen als unbeabsichtigte Folge des § 188c Abs. 2 S. 2 LVwG-E. Dafür spricht, dass die Gesetzesbegründung ausdrücklich

auch die repressive Datenverarbeitung anspricht, die Vorschrift deren Ermöglichung aber gerade entgegensteht.

### 3. Zweckfremde Nutzung des Analyseergebnisses zur Strafverfolgung

Auf der dritten Ebene stellt sich die Frage nach der weiteren Verwendung der erst durch die Analyse gewonnenen Erkenntnisse. Für sie ist gesondert zu prüfen, welche Zweckbindungen fortwirken.

Praktisch stellt sich die Frage etwa dann, wenn eine gefahrenabwehrrechtliche Analyse einen bislang unbekannten Zusammenhang aufdeckt, der zugleich den Verdacht einer bereits begangenen Straftat begründet: Darf diese Erkenntnis in das Strafverfahren übernommen werden?

Die Analyseergebnisse sind weder mit einzelnen Quelldaten noch mit dem zusammengeführten Datenbestand gleichzusetzen. § 188c Abs. 2 S. 2 LVwG-E erfasst ausdrücklich nur den „zusammengeführten Datenbestand“. Ob die daraus gewonnenen Analyseergebnisse ebenfalls der dort angeordneten Zweckbindung unterliegen, bleibt offen.

Damit bleibt eine eigenständige Frage der Zweckänderung im vorliegenden Gesetzesentwurf ungeklärt. Für ihre Beantwortung kommt es zugleich darauf an, ob die Herkunft der Analyseergebnisse so weit nachvollziehbar bleibt, dass fortwirkende Zweckbindungen und Verwendungsbeschränkungen der Quelldaten geprüft werden können. Welche Anforderungen sich daraus für die Zugriffsarchitektur ergeben, wird unter VII. 2. d) erörtert; der gesetzgeberische Regelungsbedarf folgt unter VIII. 2.

## VII. Anforderungen an die Zugriffsarchitektur

### 1. Getrennte oder gemeinsame Analyseinfrastruktur

Die bisherigen Ausführungen betreffen die Reichweite und das Zusammenspiel der vorgesehenen Befugnisse. Davon zu unterscheiden ist die hier aufzuwerfende rechtspolitische Frage, ob getrennte oder gemeinsam genutzte Analysestrukturen vorzugswürdig sind. Ausgangspunkt der Abwägung ist die unter VI. 2. herausgearbeitete Konsequenz: Der nach § 188c Abs. 2 LVwG-E gebildete Analysebestand steht für eine Nutzung nach § 98e StPO-E in der Fassung des Regierungsentwurfs nicht zur Verfügung.

Daraus folgt eine rechtliche Trennung der Bestände, jedoch noch keine Entscheidung für technisch getrennte Plattformen.
Diese grundsätzliche Zurückhaltung in Bezug auf die dauerhafte Speicherung des Analysebestandes erscheint im Ausgangspunkt nachvollziehbar. Der Entwurf setzt die Vorgaben des Palantir-Urteils erkennbar restriktiv um: Er bindet die Zusammenführung an einen konkreten Anlass, begrenzt ihre Dauer, staffelt die Eingriffsschwellen nach dem Gewicht der Analyse und schließt biometrische Verfahren sowie selbstlernende Systeme aus. Er vermeidet damit gerade den dauerhaft vorgehaltenen Universalbestand, den das – insoweit auch viel kritisierte – Bundesmodell voraussetzt.

Eine zusätzliche technische Doppelstruktur könnte allerdings mit erheblichen Nachteilen verbunden sein: Es besteht aus strafprozessualer Perspektive ein legitimes und zunehmendes Bedürfnis nach leistungsfähiger automatisierter Datenanalyse. Die stetig wachsenden Datenmengen in komplexen Ermittlungsverfahren lassen sich nicht unbegrenzt durch eine entsprechende Ausweitung personeller Ressourcen auffangen. Ein Rechtsstaat muss nicht nur rechtswidrige oder übermäßige Datenverarbeitung verhindern. Er muss Strafverfolgungsbehörden auch in die Lage versetzen, die ihnen nach dem Legalitätsprinzip übertragenen Aufgaben tatsächlich wahrzunehmen. Bei weiter wachsender Datenmenge kann deshalb auch ein Verzicht auf leistungsfähige Analyseinstrumente die praktische Verwirklichung des Legalitätsprinzips gefährden.

Darin liegt das eigentliche Spannungsverhältnis. Weder überzeugt eine technisch möglichst weitgehende Zusammenführung unter der Prämisse, die Strafverfolgung könne ohne Weiteres auf eine präventiv geschaffene „Superdatenbank“ zurückgreifen, noch erscheint es sachgerecht, automatisierte Analysemöglichkeiten durch strikt getrennte und möglicherweise nicht miteinander kompatible Strukturen faktisch erheblich zu erschweren.
Aus strafverfahrensrechtlicher Perspektive erscheint deshalb eine gemeinsame oder jedenfalls technisch anschlussfähige Infrastruktur vorzugswürdig. Voraussetzung hierfür sind allerdings hohe, technisch abgesicherte Schutzstandards, die die rechtliche Trennung von Gefahrenabwehr und Strafverfolgung innerhalb dieser Infrastruktur wirksam gewährleisten.

## 2. Anforderungen an eine gemeinsam genutzte Analyseinfrastruktur

Gerade bei rechtlich getrennten Beständen setzt die gemeinsame Nutzung technischer Infrastruktur voraus, dass die unterschiedlichen rechtlichen Bindungen der Daten und die jeweiligen Analysebefugnisse auch innerhalb der Plattform wirksam bleiben. Die folgenden Anforderungen konkretisieren diesen Maßstab für die Zugriffsarchitektur.

### a) Zweckbezogene Arbeitsbereiche und Rollen

Erforderlich sind zunächst getrennte präventive und repressive Nutzungskontexte. Jede Analyse muss einem konkreten Zweck, einer Rechtsgrundlage und einem bestimmten Vorgang zugeordnet werden. Die Plattform darf daher nicht als einheitlicher Datenraum ausgestaltet sein, in dem die rechtliche Zuordnung erst nachträglich über die Protokollierung erfolgt.

Auch die Rollen- und Rechteverwaltung muss dieser Trennung Rechnung tragen. Wer in gefahrenabwehrrechtlicher Funktion auf die Plattform zugreift, darf nicht allein aufgrund einer allgemeinen personenbezogenen Berechtigung zugleich auf repressive Analysefunktionen oder nur hierfür freigegebene Datenbestände zugreifen. Ein Wechsel zwischen beiden Funktionen muss technisch erkennbar und dokumentiert sein.

Dies gilt auch dann, wenn dieselbe Person sowohl Aufgaben der Gefahrenabwehr als auch der Strafverfolgung wahrnimmt. Entscheidend ist – wie bereits ausgeführt – nicht die Identität der handelnden Person, sondern die rechtliche Funktion und der Zweck der konkreten Datenverarbeitung. Anderenfalls würde ein „Befugnishopping“ durch die technische Ausgestaltung gerade erleichtert.

### b) Herkunftskennzeichnung und Fortwirkung von Verwendungsbeschränkungen

Die Herkunft und der rechtliche Status der einbezogenen Daten müssen innerhalb der Analyseplattform erkennbar bleiben. Die gemeinsame technische Speicherung lässt die unterschiedlichen rechtlichen Bindungen der Daten unberührt. Dass präventiv und repressiv erhobene Daten in demselben Informationssystem gespeichert sind, rechtfertigt daher nicht, sie für beide Aufgabenbereiche gleichermaßen verfügbar zu machen. Herkunft, Erhebungszweck und besondere Verwendungsbeschränkungen müssen deshalb technisch mitgeführt werden.

§ 188d LVwG-E trägt diesem Gedanken bereits Rechnung, indem die Vorschrift insbesondere Kennzeichnung, Nachvollziehbarkeit, Zugangsbegrenzung und Protokollierung verlangt. Für eine gemeinsam genutzte Analyseplattform müssten diese Vorgaben so konkretisiert werden, dass die rechtliche Verfügbarkeit der Daten bereits bei ihrer Einbeziehung in die Analyse geprüft werden kann.

Dabei genügt es nicht, rechtlich nicht verwendbare Daten lediglich aus der späteren Ergebnisanzeige auszublenden. Sind Daten für den konkreten Zweck nicht verfügbar, dürfen sie auch nicht zuvor in die Berechnung oder Verknüpfung einfließen und dadurch mittelbar das Analyseergebnis prägen.

**c) Anlassbindung und Protokollierung**

Jeder Einsatz der Analyseplattform muss einem dokumentierten Anlass zugeordnet werden. Die Protokollierung sollte jedenfalls erkennen lassen, wer in welcher Funktion, auf welcher Rechtsgrundlage und zu welchem Zweck eine Analyse durchgeführt hat und welche Datenbestände hierbei einbezogen wurden.

Von besonderer Bedeutung sind Wechsel zwischen präventiver und repressiver Nutzung. Sie sollten als eigenständige Vorgänge nachvollziehbar sein. Dies gilt sowohl für den Zugriff auf Daten aus dem jeweils anderen Regelungsregime als auch für die Übernahme von Analyseergebnissen.

Eine solche Protokollierung dient nicht nur der nachträglichen Kontrolle einzelner Zugriffe. Sie muss auch ermöglichen, wiederholte Zweckwechsel und auffällige Zugriffsketten zu erkennen.

**d) Nachvollziehbarkeit der Analyseergebnisse**

Für jedes Ergebnis muss in dem für die rechtliche Kontrolle erforderlichen Umfang nachvollziehbar bleiben, aus welchen Datenkategorien und Verarbeitungsschritten es hervorgegangen ist. Nur so lässt sich beurteilen, ob fortwirkende Verwendungsbeschränkungen der Ausgangsdaten der Weiterverwendung entgegenstehen. Die gebotene Nachvollziehbarkeit darf allerdings keinen umfassenden Zugriff auf sämtliche Ausgangsdaten eröffnen; auch für die Herkunftsprüfung gelten die jeweiligen Zugriffs- und Verwendungsbeschränkungen fort.

## VIII. Regelungsbedarf im Gesetzentwurf

Aus den vorstehend begründeten Schutzanforderungen ergeben sich für §§ 188c und 188d LVwG-E drei gesetzgeberische Aufgaben: die Entscheidung über das Verhältnis zu § 98e StPO-E (1.), eine eigenständige Regelung für Analyseergebnisse (2.) und die verbindliche Absicherung der Zwecktrennung innerhalb einer gemeinsam genutzten Plattform (3.).

### 1. Entscheidung über das Verhältnis zu § 98e StPO-E

Der Landesgesetzgeber hat sich gegen einen dauerhaft vorgehaltenen Analysebestand entschieden. Klärungsbedarf besteht daher nicht hinsichtlich dieser Grundentscheidung, sondern hinsichtlich ihrer Reichweite. Insbesondere sollte ausdrücklich geregelt werden, ob der anlassbezogen für Zwecke der Gefahrenabwehr gebildete Analysebestand auch für eine spätere strafprozessuale Nutzung gesperrt bleiben soll.

Die unter VI. 2. herausgearbeitete Abweichung von § 98e StPO-E betrifft neben der unterschiedlichen Konzeption der Bestandsbildung insbesondere die Frage der zweckändernden Nutzung eines bereits gebildeten Analysebestandes. Diese Folge sollte im weiteren Gesetzgebungsverfahren ausdrücklich aufgegriffen und mit dem bundesrechtlichen Regelungsmodell abgestimmt werden.

Soll an der offenbar unbeabsichtigten Zwecktrennung gleichwohl festgehalten werden, muss zugleich geklärt werden, auf welcher rechtlichen und technischen Grundlage in Schleswig-Holstein künftig eine automatisierte Datenanalyse zu Strafverfolgungszwecken stattfinden soll. Soll dagegen derselbe präventiv gebildete Analysebestand auch für Strafverfolgungszwecke nutzbar sein, bedarf es einer ausdrücklichen Öffnung des § 188c Abs. 2 Satz 2 LVwG-E für eine Nutzung nach Maßgabe des § 98e StPO-E. Ein Verweis auf § 479 Abs. 2 S. 2 StPO trägt diese Öffnung nicht (dazu VI. 2.). Zusätzlich müsste geregelt werden, ob und wie lange der Bestand nach Wegfall des präventiven Zwecks für eine zulässige strafprozessuale Nutzung vorgehalten werden darf; § 188d Abs. 5 LVwG-E wäre entsprechend abzustimmen.

Gerade weil §§ 188c, 188d LVwG-E und § 98e StPO-E nahezu gleichzeitig entstehen und potentiell dieselben technischen Datenverarbeitungsstrukturen betreffen, sollte diese Grundentscheidung bereits im Gesetzgebungsverfahren abgestimmt werden. Es vermag wenig zu überzeugen, miteinander nicht abgestimmte gesetzliche Konzepte erst nach ihrem Inkrafttreten durch technische Lösungen oder Verwaltungsvorschriften miteinander in Einklang bringen zu wollen. Dabei geht es nicht darum, die restriktiveren landesrechtlichen Schutzstandards an den Bundesentwurf anzupassen, sondern darum, bewusst festzulegen, welche technische Infrastruktur gewollt ist und wie innerhalb dieser Infrastruktur die unterschiedlichen rechtlichen Grenzen beider Aufgabenbereiche wirksam werden sollen.

**2. Eigenständige Regelung für Analyseergebnisse**

Daneben sollte das Gesetz mit Blick auf zweckändernde Öffnungsklauseln ausdrücklich zwischen den Ausgangsdaten, dem zusammengeführten Analysebestand und den hieraus neu erzeugten Analyseergebnissen unterscheiden.

Für Analyseergebnisse sollte geregelt werden, ob und unter welchen Voraussetzungen sie für einen anderen Zweck verwendet werden dürfen. Dabei muss gewährleistet sein, dass besondere Verwendungsbeschränkungen der zugrunde liegenden Daten nicht durch die Erzeugung eines neuen Analyseergebnisses umgangen werden können.

Für die Prüfung dieser Anschlussverwendung sollte das Gesetz eine hinreichende Herkunftskennzeichnung verbindlich vorsehen. Sie muss die unter VII. 2. d) beschriebene Kontrolle fortwirkender Verwendungsbeschränkungen ermöglichen, ohne einen darüber hinausgehenden Zugriff auf die Ausgangsdaten zu eröffnen.

**3. Verbindliche Anforderungen an die Zwecktrennung innerhalb der Plattform**

§ 188d LVwG-E enthält bereits wesentliche technische und organisatorische Schutzvorkehrungen. Für den Fall einer gemeinsamen oder technisch verbundenen präventiven und repressiven Analyse sollten diese jedoch gezielt ergänzt werden.

Gesetzlich abzusichern sind insbesondere zweckbezogene Nutzungskontexte, kontextabhängige Rollen und Berechtigungen, die technische Sperrung nicht zulässiger Daten und Analysefunktionen sowie die Protokollierung von Zweck- und

Rollenwechseln. Die technische Ausgestaltung im Einzelnen kann einer Verwaltungsvorschrift überlassen bleiben. Die grundlegende Entscheidung, dass die jeweilige Rechtsgrundlage den technisch verfügbaren Daten- und Funktionsumfang steuern muss, ist dagegen grundrechtswesentlich und muss daher in einem Parlamentsgesetz festgeschrieben werden. Die automatisierte Datenanalyse zeigt damit exemplarisch, dass technische Architektur und rechtliche Befugnisordnung nicht getrennt voneinander geregelt werden können.

## IX. Ergebnisse

Bund und Land verfolgen unterschiedliche Regelungskonzepte: Der Bund setzt auf einen dauerhaft vorbereiteten, grundsätzlich auch für die Strafverfolgung nutzbaren Analysebestand; § 188c LVwG-E bindet die Zusammenführung dagegen an einen konkreten gefahrenabwehrrechtlichen Anlass.

Die Zweckbindung des § 188c Abs. 2 S. 2 LVwG-E steht der vom Regierungsentwurf zu § 98e StPO-E vorausgesetzten strafprozessualen Nutzung des präventiven Analysebestands entgegen. Der Landesgesetzgeber muss ausdrücklich klären, ob auch diese Sperre gewollt ist oder unter abgestimmten Voraussetzungen eine strafprozessuale Anschlussnutzung zugelassen werden soll.

Eine gemeinsame oder technisch anschlussfähige Infrastruktur ist aus strafverfahrensrechtlicher Perspektive vorzugswürdig, sofern die Zwecktrennung durch hohe rechtliche und technische Schutzstandards wirksam gewährleistet wird.

Ausgangsdaten, zusammengeführter Analysebestand und neu gewonnene Analyseergebnisse sind bei jedem Zweckwechsel gesondert zu beurteilen. Für die zweckändernde Verwendung der Analyseergebnisse bedarf es einer ausdrücklichen Regelung unter Wahrung fortwirkender Verwendungsbeschränkungen.

Das Gesetz muss die gewählte Zwecktrennung durch verbindliche Vorgaben für Datenverfügbarkeit, Analysefunktionen, Zugriffsrechte und die Nachvollziehbarkeit von Zweckwechseln absichern.