Hochschule des Bundes
für öffentliche Verwaltung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 F

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Prof. Dr. Markus Löffelmann
HAUSANSCHRIFT Habersaathstr. 51, 10115 Berlin
POSTANSCHRIFT Postfach 40527, 10063 Berlin
TEL 030 – 22 00 89 – 85513
E-MAIL markus.loeffelmann@hsbund-nd.de

DATUM Berlin, 17.04.2024

BETREFF **Schriftliche Stellungnahme zur öffentlichen Sachverständigenanhörung am 22. April 2024 zu BT-Drs. 20/9495**

Stellungnahme zum Antrag der Fraktion der CDU/CSU

Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren

BT-Drs. 20/9495

A. Vorbemerkung

Die Notwendigkeit, den Sicherheitsbehörden in Deutschland moderne und leistungsfähige Instrumente der Datenverarbeitung und -analyse zur Verfügung zu stellen, dürfte auf Bundes- und Länderebene in allen politischen Lagern übergreifend anerkannt sein. [1]

Unklar und umstritten war lange Zeit hingegen der verfassungsrechtliche Rahmen für den Einsatz solcher Instrumente.[2] Eine erste Einordnung nahm der Erste Senat des BVerfG in seiner Entscheidung zur erweiterten Nutzung von Daten der Antiterrordatei im Jahr 2020 vor. Er führte dort aus, dieser Nutzungsart komme eine „gesteigerte Belastungswirkung“ zu, weil sie „nicht nur eine Informationsanbahnung nach Maßgabe des Fachrechts, sondern als Ergebnis einer automatisierten Verknüpfung und Analyse der von verschiedenen Behörden in die Antiterrordatei eingespeisten Daten auch die Erzeugung neuer Erkenntnisse und Zusammenhänge (‚Data-mining‘), die eine erhebliche Persönlichkeitsrelevanz aufweisen können“, möglich mache.[3] Diese Belastungswirkung erfordere „hinreichend konkretisierte Eingriffsschwellen für die erweiterte Nutzung zu Zwecken der Gefahrenabwehr, Strafverfolgung sowie der Aufgabenerfüllung von nicht operativ tätig werdenden Behörden wie den Nachrichtendiensten auf der Grundlage normenklarer Regelungen“.[4] In seiner nachfolgenden Judikatur zu sicherheitsbehördlichen Datenerhebungen und -verarbeitungen entwickelte der Erste Senat diese Maßstäbe fort und konturierte dabei ein Stufenmodell einander korrespondierender Eingriffsgewichte und legitimierender Eingriffsschwellen und Rechtsgüter.[5] Dieses System bildet auch den gedanklichen Rahmen der Entscheidung vom 16.2.2023 zur automatisierten Datenanalyse nach den Polizeigesetzen von Hessen und Hamburg. Darin skizziert das Gericht zahlreiche Abwägungsparameter und fordert den Gesetzgeber auf, „die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch

[1] Zu den mit dem Einsatz einer solchen Software verbundenen Erwartungen HessLT-Drs. 19/6501, S. 40 f.
[2] Vgl. vor der jüngsten Rspr. des BVerfG etwa Singelnstein, NStZ 2018, 1 ff.; Rademacher/Perkowski, JuS 2020, 713 ff.; Kuhlmann/Trute, GSZ 2021, 103 ff.; Arzt in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G Rn. 1144 ff., 1179 ff.; jew. m.w.N.
[3] BVerfGE 156, 11, 52 f. (Rn. 107, 109 f.).
[4] BVerfGE 156, 11, 55 (Rn. 117).
[5] BVerfGE 162, 1, 87, 92 ff. (Rn. 181, 192 ff.).

Gesetz vorgeben“ zu müssen.[6] Angesichts des Umstands, dass eine solche gesetzliche Regelung von der Art und Leistungsfähigkeit der angestrebten automatisierten Datenverarbeitung abhängig ist, dabei komplexe Abwägungen erforderlich sind und die Rechtsprechung des BVerfG dem Gesetzgeber breite Gestaltungsspielräume inhaltlicher aber auch regelungstechnischer Art einräumt, ist die Frage der Auswahl einer bestimmten Analysesoftware untrennbar mit den Anforderungen an die rechtliche Ausgestaltung ihres Einsatzes verknüpft.

Im Folgenden soll vor diesem Hintergrund versucht werden, Eckpunkte eines Regelungskonzepts zu skizzieren, die für die Frage, welche Analysesoftware erworben oder beauftragt werden soll, hilfreich sein können.

II. Anforderungen an ein Regelungskonzept

In seiner Entscheidung vom 16.2.2023 zeigt das BVerfG zahlreiche Gesichtspunkte auf, die die verfassungsrechtliche Zulässigkeit des Einsatzes von Analysesoftware determinieren, legt sich dabei aber nur auf wenige verfassungsrechtlich gebotene Beschränkungen fest. Einige Problempunkte, wie die Frage, ob die angegriffenen Normen ausreichende Regelungen zu den zu schützenden Rechtsgütern sowie zu Zweckbindung, Transparenz und Rechtsschutz enthielten, blieben zudem mangels insoweit gegebener Zulässigkeit der Verfassungsbeschwerde offen.[7] Das eröffnet einen breiten Gestaltungsspielraum für den Gesetzgeber.

1. Unzulässige Einsatzweisen

Schlechthin unzulässig ist nach den Vorgaben des BVerfG eine gänzlich anlasslose automatisierte Auswertung personenbezogener Daten zur vorbeugenden Bekämpfung von Straftaten.[8] Diese Bindung an einen Anlass bei Ermächtigungen zu Eingriffen in das Recht auf informationelle Selbstbestimmung entspricht der ständigen

[6] BVerfGE 165, 363, 414 (Rn. 112).
[7] BVerfGE 165, 363, 387 (Rn. 48).
[8] BVerfGE 165, 363, 412 (Rn. 108).

Rechtsprechung des Gerichts seit dem „Volkszählungsurteil“.[9] Erforderlich ist danach die Bindung des Einsatzes von Analysesoftware an den Anfangsverdacht einer Straftat oder die Prognose einer Rechtsgutsverletzung. Die Eingriffsschwellen müssen dabei der Eingriffsintensität der Datenverarbeitung, die je nach Art der verwendeten Daten, den Analysemethoden und anderen Kriterien stark divergieren kann, entsprechen. Ebenfalls unzulässig sind die Erstellung *umfassender* Persönlichkeitsprofile[10] sowie Eingriffe in den Kernbereich privater Lebensgestaltung, wobei die „Verletzungsgeneigtheit“[11] der automatisierten Datenanalyse von der Leistungsfähigkeit des Systems und der Art der verwendeten Daten abhängt. Beide Beschränkungen machen eine Auswahl erforderlich, in welchem Umfang welche Art von Daten verarbeitet werden soll. Die Einbeziehung personenbezogener Daten ist vor diesem Hintergrund grundsätzlich problematisch.

2. Verarbeitung großer Datenmengen und Einsatz Künstlicher Intelligenz

Besondere Vorkehrungen sind nach den Vorgaben des BVerfG bei der automatisierten Verarbeitung großer Datenmengen erforderlich. Ohne eingrenzende Vorgaben zur Verarbeitungs*methode* sei eine automatisierte Durchsuchung großer Bestände personenbezogener Daten auf bislang unbekannte Gesetzmäßigkeiten und gefahrenabwehrrechtlich bedeutende Zusammenhänge unzulässig.[12] Bei einer Auswertung auf statistische Zusammenhänge hin sei eine ausreichende Datenqualität sicherzustellen und müssten Vorkehrungen dagegen getroffen werden, dass die Auswahl der einbezogenen Daten unangemessen verzerrende, diskriminierende Wirkungen entfalten könne.[13] Mit anderen Worten muss einer nach Art. 3 Abs. 3 GG unzulässigen Diskriminierung betroffener Personen wirksam vorgebeugt werden.[14] Dies gilt insbesondere für den Einsatz lernfähiger Systeme, also Künstlicher Intelligenz.[15]

---

[9] BVerfGE 65, 1, 46.
[10] BVerfGE 65, 1, 43; 112, 304, 319; 109, 279, 323; 141, 220, 280, 317; 162, 1, 131 u.ö.; st.Rspr.
[11] BVerfGE 141, 220, 276 ff., 313 ff.; 154, 152, 262 ff.
[12] BVerfGE 165, 363, 407 (Rn. 95).
[13] A.a.O.; näher zu Diskriminierungsrisiken durch algorithmenbasierte Systeme Nink, Justiz und Algorithmen, 2021, S. 167 ff.
[14] BVerfGE 165, 363, 400 f. (Rn. 77).
[15] BVerfGE 165, 363, 408 (Rn. 98).

Der Gesetzgeber ist bei einer entsprechenden Leistungsfähigkeit der Analysesoftware also gehalten, wirksame rechtliche Vorkehrungen zu schaffen, ohne dass der Rechtsprechung des BVerfG hierfür ein Regelungsmuster entnommen werden kann. Alternativ wäre es denkbar, eine Auswertung auf statistische Zusammenhänge hin und den Einsatz Künstlicher Intelligenz gesetzlich auszuschließen[16], was allerdings die Leistungsfähigkeit solcher Systeme stark beschneidet.

3. Stufensystem der Eingriffsintensität

Das BVerfG benennt zahlreiche Parameter, die die Eingriffsintensität des Einsatzes von Analysesoftware beeinflussen können. Beispiele sind

- die Menge und das Format der in die Analyse einbezogenen Daten[17],
- die Nähe der Daten zum persönlichen Lebensbereich[18],
- die Art der Analysemethode[19],
- die Möglichkeit der Erstellung von Bewegungs- und Persönlichkeitsprofilen[20],
- die Einbeziehung von Daten Unbeteiligter[21],
- etwaige Diskriminierungsrisiken[22],
- die Fehleranfälligkeit der Analyse[23],
- die Ausgestaltung von Zugriffsrechten[24] oder
- die Gefahr eines etwaigen Missbrauchs der Daten[25].

Diese und andere[26] Parameter muss der Gesetzgeber gewichten und in ein Stufensystem zu den mittels der Datenanalyse verfolgten Zwecken stellen. Dabei ist nicht

[16] So Art. 61a Abs. 5 Nr. 2 BayPAG-E zur Verwendung selbstlernender Systeme (BayLT-Drs. 19/725 S. 47).
[17] BVerfGE 165, 363, 399, 401, 404 (Rn. 76, 78, 87).
[18] BVerfGE 165, 363, 399, 401 (Rn. 76, 78).
[19] BVerfGE 165, 363, 399 f., 404 ff., 408 (Rn. 76, 77, 88, 90-93, 100).
[20] BVerfGE 165, 363, 397, 400, 407 (Rn. 70, 77, 96-98).
[21] BVerfGE 165, 363, 399 f., 403, 406 (Rn. 76, 77, 84, 94); vgl. auch bereits die in BVerfGE 115, 320 aufgestellten hohen Hürden für die Rasterfahndung.
[22] BVerfGE 165, 363, 400, 405, 408 (Rn. 77, 90, 100).
[23] BVerfGE 165, 363, 409 (Rn. 102).
[24] BVerfGE 165, 363, 402, 404 (Rn. 80, 89).
[25] BVerfGE 165, 363, 399, 405, 408 f. (Rn. 76, 90, 100 f.).
[26] Vgl. Löffelmann, JR 2023, 331, 341 f.

nur eine Gewichtung auf Seiten der Eingriffsintensität ausgesprochen anspruchsvoll, sondern auch die Stufung der legitimierenden Gründe.[27]

4. Differenzierte Eingriffsschwellen

Diese Gewichtung muss durch den Gesetzgeber schließlich in Eingriffsschwellen und Rechtsgutskategorien übertragen werden. Auch dabei besteht ein erheblicher gesetzgeberischer Gestaltungsspielraum, den das BVerfG nur exemplarisch andeutet. So kann etwa eine Begrenzung auf den Zweck der Erkenntniserlangung über gefährliche oder gefährdete Orte niedrigere Anforderungen an den Rechtsgüterschutz legitimieren.[28] Im Bereich der Strafverfolgung kann die Verwendung auf bestimmte Delikte begrenzt werden. In Betracht komme zum Beispiel die Anwendung auf solche Straftaten, „die regelmäßig in Serie begangen werden, so dass aus der Begehung einer Straftat unter bestimmten Umständen auf die Begehung weiterer Straftaten geschlossen werden“ kann.[29] Das ermöglicht etwa die Datenanalyse zum Zweck von Strukturermittlungen bei Wohnungseinbrüchen, wo sie in der Vergangenheit bereits erfolgreich praktiziert wurde.[30] Analog kann auch im Bereich der Gefahrenabwehr der Einsatz auf bestimmte Rechtsgüter begrenzt werden. Welche Straftaten und Rechtsgüter dabei einer bestimmten Kategorie zuzuordnen sind, ist nur zum Teil verfassungsrechtlich vorgegeben, was eine gesetzgeberische Priorisierung und Gewichtung von Einsatzzwecken erforderlich macht.

5. Prozedurale Flankierungen

Das BVerfG fordert für bestimmte Formen der automatisierten Datenanalyse prozedurale Schutzvorkehrungen, um einem etwaigen Missbrauch der verarbeiteten und neu erzeugten Daten zu begegnen. So ist der Zugriff auf solche Daten durch eine

---

[27] Vgl. zu dieser Problematik näher Löffelmann, Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz, 2022, S. 57 ff.
[28] BVerfGE 165, 363, 407, 412, 418 (Rn. 97, 108, 121).
[29] BVerfGE 165, 363, 433 (Rn. 159 f.).
[30] Vgl. BT-Drs. 19/23700, S. 221.

Regelung von Zugriffsrechten für „entsprechend qualifizierte“ Mitarbeiter der Sicherheitsbehörden zu begrenzen.[31] Um welche Art von Qualifikation es sich dabei handeln muss, ist durch den Gesetzgeber zu spezifizieren. Ergänzend sind organisatorische und technische Vorkehrungen zur Begrenzung des Zugriffs erforderlich, deren wesentliche Funktion ebenfalls der Gesetzgeber zu bestimmen hat. Lediglich „technische Einzelheiten“ können in zu veröffentlichenden Verwaltungsvorschriften geregelt werden.[32] Das BVerfG hebt ausdrücklich hervor, dass der Verwendung von Software privater Anbieter und ausländischer Stellen ein erhöhtes Missbrauchsrisiko innewohne[33], dem folglich durch entsprechend anspruchsvollere Schutzvorkehrungen – wie etwa eine unabhängige Zertifizierung und fortlaufende Kontrolle des Quellcodes – Rechnung zu tragen ist. Auch eine angemessene aufsichtliche Kontrolle muss gewährleistet sein, ohne dass das BVerfG aber deren Ausprägung näher spezifiziert.[34]

6. Regelungstechnische Ausgestaltung

Das BVerfG lässt dem Gesetzgeber bei alledem einen Spielraum, auf welche Weise er seinem Gestaltungsauftrag nachkommen will. So könne er die Verwaltung „zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen“.[35] Dies müsse dann nachvollziehbar dokumentiert und veröffentlicht werden.[36] Vom Gesetzgeber selbst zu bestimmen sei der Kreis der einzubeziehenden Datenbestände und das Ausmaß ihrer automatisierten Auswertung. Auch hier eröffnet das BVerfG aber die Möglichkeit einer untergesetzlichen abstrakt-generellen Regelung.[37] Bei einem Einsatz im Gefahrenvorfeld müsse das Gesetz „in grundlegenden Zügen“ einschränkende Vorgaben zur Methode der Analyse enthalten.[38] Außerdem müsse der Gesetzgeber selbst „grundlegende Maßgaben zur Begrenzung des Automatisie-

[31] BVerfGE 165, 363, 416 (Rn. 117).
[32] A.a.O.
[33] BVerfGE 165, 363, 408 (Rn. 100) m.d.H.a. Wissenschaftlicher Dienst des Deutschen Bundestags, WD3-3000-018/20 S. 8 m.w.N.
[34] BVerfGE 165, 363, 412 f. (Rn. 109).
[35] BVerfGE 165, 363, 414 (Rn. 112).
[36] BVerfGE 165, 363, 414 (Rn. 113).
[37] BVerfGE 165, 363, 415 (Rn. 114).
[38] BVerfGE 165, 363, 418 (Rn. 120).

rungsgrades treffen“.[39] Ferner müsse der Einsatz selbstlernender Systeme und die Verwendung von Daten aus einer Wohnraumüberwachung oder Online-Durchsuchung außerhalb des Zwecks der Abwehr einer dringenden Gefahr im Gesetz ausgeschlossen sein.[40] Die Vorgaben des BVerfG zum Regelungsauftrag des Gesetzgebers machen es dabei in weiten Teilen notwendig, sich zunächst Klarheit darüber zu verschaffen, worin die „wesentlichen Grundlagen“ zur Begrenzung der automatisierten Datenanalyse überhaupt bestehen.

III. Schlussfolgerung

Die Analyse der verfassungsgerichtlichen Vorgaben zur automatisierten Datenanalyse zeigt unmissverständlich – namentlich auch in ihrer Genese aus dem datenschutzrechtlichen Zweckbindungsgrundsatz und der in diesem Zusammenhang in ständiger Rechtsprechung erhobenen Forderung nach „präzisen und bereichsspezifischen“ gesetzlichen Regelungen[41] –, dass das BVerfG bei der gesetzgeberischen Einhegung von Möglichkeiten der automatisierten Datenanalyse eine sorgfältige, verantwortungsbewusste und maßnahmenspezifische Abwägung einfordert. Auffällig ist dabei, dass das Gericht – anders als in zahlreichen anderen Judikaten zu sicherheitsrechtlichen Themen – keine konkreten und ins Detail gehenden Vorgaben macht, sondern anhand von zahlreichen in Betracht kommenden Abwägungsgesichtspunkten in groben Zügen vorzeichnet, welchen Fragen sich der Gesetzgeber zu stellen hat. Angesichts der Komplexität und vielfältigen Einsatzmöglichkeiten solcher Systeme liegt diese Zurückhaltung in der Natur der Sache.

Den Gesetzgeber stellt dies vor eine große Herausforderung, insbesondere auch, weil es in diesem Bereich einerseits bislang kaum Regelungsvorbilder, andererseits aber „vielfältige Möglichkeiten“[42] der Gestaltung gibt. All dies macht einen aufwändigen, gut strukturierten parlamentarischen Prozess erforderlich, in dem die sicherheitsbehördlichen Bedarfe und technischen Spezifitäten im Lichte der verfassungs-

[39] BVerfGE 165, 363, 418 (Rn. 121).
[40] BVerfGE 165, 363, 392, 394, 416 (Rn. 59, 64, 118).
[41] Etwa BVerfGE 100, 313, 360, 389; 115, 166, 191; 118, 168, 187 f.; 162, 1, 95, 155; st.Rspr.
[42] BVerfGE 165, 363, 409 (Rn. 103).

gerichtlichen Maßstäbe zu würdigen sind. Letzten Endes sind der normative Rahmen für den Einsatz von Methoden der automatisierten Datenanalyse und deren technische Leistungsfähigkeit so eng miteinander verschränkt, dass die Entwicklung des normativ Erlaubten, technisch Machbaren und sicherheitsbehördlich Erforderlichen Hand in Hand gehen sollten. Vor diesem Hintergrund erscheint die gegenständliche Entscheidung, nicht auf ein von einem US-amerikanischen Unternehmen angebotenes System zurückzugreifen, sondern ein solches selbst zu entwickeln, gut nachvollziehbar. Auf diese Weise kann außerdem die gebotene Transparenz der Funktionsweise besser gewährleistet[43] und dem ausdrücklich vom BVerfG thematisierten Missbrauchsrisiko bei der Verwendung von Software privater und ausländischer Hersteller (o. II.5.)[44] – auch mit Blick auf etwaige künftige Erweiterungen der Funktionalität – leichter begegnet werden kann.

Die enormen Herausforderungen, die mit dem Schaffen adäquater Rechtsgrundlagen verbunden sind, werden auch durch die aktuellen Entwicklungen in den Ländern belegt.[45] So gibt es – soweit ersichtlich – gegenwärtig in mehr als der Hälfte der Bundesländer noch keine konkreten Vorhaben zur Einführung einer automatisierten Datenanalyse. In Bayern liegt ein aktueller Gesetzentwurf (Art. 61a BayPAG-E) vor[46], der bei vorläufiger Würdigung jedenfalls in wesentlichen Teilen verfassungsrechtlichen Bedenken begegnet[47]; einzelne Länder prüfen offenbar, sich dieser Regelung anzuschließen. Einen eigenständigen, bislang nicht veröffentlichten Regelungsansatz verfolgt aktuell Rheinland-Pfalz. Die Novellierung der Rechtsgrundlage im Hessischen Polizeirecht (§ 25a HSOG[48]) erfolgte im Rahmen eines ausgesprochen un-

[43] So auch Kugelmann/Buchmann, GSZ 2024, 1, 6.
[44] Vgl. zu insoweit thematisierten – und dort ausgeräumten – Bedenken auch den Zwischenbericht des Untersuchungsausschusses im Hessischen Landtag, HessLT-Drs. 19/6864 S. 67 ff.
[45] Vgl. hierzu die Darstellung unter https://netzpolitik.org/2024/automatisierte-datenanalyse-bei-der-polizei-bundeslaender-nicht-scharf-auf-palantir/ vom 03.01.2024.
[46] BayLT-Drs. 19/725.
[47] Dies betrifft neben der Verwendung des – ohnehin umstrittenen – Anlasses der „drohenden Gefahr“ (Art. 61a Abs. 1 S. 1 Alt. 2, Abs. 2 S. 1 Nr. 2 Alt. 2 PAG-E), den Rang der zu schützenden Rechtsgüter (Art. 61a Abs. 2 S. 1 Nr. 2 PAG-E), die Einschränkung der Art der zu verarbeitenden Daten (Art. 61a Abs. 2 S. 3 und 4, Abs. 3 S. 1 PAG-E), das Fehlen von Beschränkungen für die Verarbeitung großer Datenmengen und für statistische Auswertungen, die undifferenzierte Einbeziehung von Daten dritter (unverdächtiger, geschädigter etc.) Personen sowie das Fehlen gesetzlicher Schutzvorkehrungen zur Vermeidung von Diskriminierung.
[48] GVBl. 2023 S. 456, 468 f.; dazu HessLT-Drs. 20/8129, 20/10821, 20/8130, 20/10821, 20/11194, 20/11235, 20/11292.

übersichtlichen und hastigen Gesetzgebungsverfahrens[49] und hat erneut eine rechtstechnisch und verfassungsrechtlich angreifbare Norm hervorgebracht.[50] Gegen die von Anfang an umstrittene Regelung zum Data-Mining nach § 23 Abs. 6 PolG NW wurde eine – nach den bisher vom BVerfG entwickelten Maßstäben wohl nicht aussichtslose – Verfassungsbeschwerde angebracht.[51]

All dies macht deutlich, dass in diesem Bereich ein ausgeprägter rechtlicher und auch technischer Diskussionsbedarf besteht.[52] Da es das erklärte Ziel des Projekts „Polizei 2020“ ist, ein einheitliches Produkt für alle Polizeibehörden auf Bundes- und Länderebene zu schaffen, wäre die logische Voraussetzung hierfür, zunächst eine Konsolidierung der erforderlichen Rechtsgrundlagen und Anforderungen an den Algorithmus herbeizuführen, anstatt ein Produkt „auf Vorrat“ zu erwerben, das dann möglicherweise aus rechtlichen Gründen nicht oder nur eingeschränkt Verwendung finden kann. Ein erster Schritt für eine solche erforderliche Konsolidierung könnte die Einrichtung einer Bund-Länder-Arbeitsgruppe zur Umsetzung der Rechtsprechung des BVerfG zur automatisierten Datenanalyse sein.

[redacted]

(Prof. Dr. Markus Löffelmann)

[49] S. die Kritik bei Bäuerle in: Möstl/Bäuerle (Hrsg.), BeckOK Polizei- und Ordnungsrecht Hessen, 32. Edition, Stand 1.3.2024, HSOG § 25a Rn. 16 ff.
[50] Vgl. die Kritik bei Bäuerle, a.a.O., Rn. 22 ff., 31 ff., 60.
[51] Vgl. https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-NRW/2022-10-05-PolG_NRW_Palantir_Website_geschwaerzt_Punkte.pdf; vgl. auch die Kritik bei Arzt in: Möstl/Kugelmann (Hrsg.), Ordnungsrecht Nordrhein-Westfalen, PolG NRW § 23 Rn. 50i ff.
[52] Ähnl. aktuell Kugelmann/Buchmann, GSZ 2024, 1 ff. mit Vorschlägen zu Regelungsansätzen.