

Michael Bäuerle,  
Kai Denker,  
Christian Geminn,  
Bettina Schöndorf-  
Haubold (Hg.)

*Big Data und KI  
bei der Polizei*

Das Palantir-Urteil in  
der interdisziplinären  
Diskussion



## Big Data und KI bei der Polizei

*Michael Bäuerle* ist Professor für Öffentliches Recht an der Hessischen Hochschule für öffentliches Management und Sicherheit. *Kai Denker* ist Wissenschaftlicher Mitarbeiter (PostDoc) im Institut für Philosophie der Technischen Universität Darmstadt. *Christian Geminn* ist Privatdozent für Öffentliches Recht und Recht der digitalen Gesellschaft an der Universität Kassel. *Bettina Schöndorf-Haubold* ist Professorin für Öffentliches Recht an der Justus-Liebig-Universität Gießen.

Michael Bäuerle, Kai Denker, Christian Geminn,  
Bettina Schöndorf-Haubold (Hg.)

# Big Data und KI bei der Polizei

Das Palantir-Urteil in der interdisziplinären Diskussion

Schriftleitung: Christopher Giogios

Campus Verlag  
Frankfurt/New York

Der Themenband veröffentlicht die Ergebnisse der Projektgruppe »Big Data und KI im Bereich der deutschen Sicherheitsbehörden« am Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI). Das Zentrum wird gefördert durch das Hessische Ministerium für Digitalisierung und Innovation.

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Der Text dieser Publikation wird unter der Lizenz »Creative Commons Namensnennung-Nicht-kommerziell-Weitergabe unter gleichen Bedingungen 4.0 International« (CC BY-NC-SA 4.0) veröffentlicht. Den vollständigen Lizenztext finden Sie unter: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de>

Verwertung, die den Rahmen der CC BY-NC-SA 4.0 Lizenz überschreitet, ist ohne Zustimmung des Verlags unzulässig. Die in diesem Werk enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Quellenangabe/Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen. Die Beltz Verlagsgruppe behält sich die Nutzung ihrer Inhalte für Text und Data Mining im Sinne von § 44b UrhG ausdrücklich vor.



ISBN 978-3-593-52211-1 Print

ISBN 978-3-593-46400-8 E-Book (PDF)

DOI 10.12907/978-3-593-46400-8

Trotz sorgfältiger inhaltlicher Kontrolle übernehmen wir keine Haftung für die Inhalte externer Links. Für den Inhalt der verlinkten Seiten sind ausschließlich deren Betreiber verantwortlich.

© 2025 Einige Rechte im Campus Verlag in der Beltz Verlagsgruppe GmbH & Co. KG, Werderstr. 10, 69469 Weinheim, [info@campus.de](mailto:info@campus.de).

Umschlaggestaltung: Beltz Verlagsgruppe GmbH & Co. KG

Satz: le-tex xerif

Druck und Bindung: Beltz Grafische Betriebe GmbH, Bad Langensalza

Beltz Grafische Betriebe ist ein Unternehmen mit finanziellem Klimabeitrag (ID 15985-2104-1001).

Printed in Germany

Campus Verlag® / [www.campus.de](http://www.campus.de)

# Inhalt

Polizei-Software als Politikum? Das »Palantir-Urteil« des Bundesverfassungsgerichts .....	7
<i>Michael Bäuerle, Kai Denker, Christian Geminn, Bettina Schöndorf-Haubold</i>	

## Teil I: Das Urteil des Bundesverfassungsgerichts zur automatisierten Datenanalyse

Das Urteil zur automatisierten Datenanalyse (BVerfGE 165, 363) – Besprechung des Urteils und seiner sicherheitsverfassungsrechtlichen Implikationen .....	15
<i>Lea Rabe</i>	

Ein Schritt zurück, zwei nach vorn? Die Reform(en) des HSOG im Kontext des Urteils zur automatisierten Datenanalyse .....	45
<i>Christopher Giogios</i>	

Automatisierte Datenanalysen zwischen DS-GVO, JI-RL und KI-VO .....	71
<i>Lea Rabe, Christian Geminn, Paul Johannes</i>	

Das Gericht, seine Sprache und die kritischen Schwellenwerte von Softwaretechnik – Zur begrifflich ambivalenten Fassung polizeilicher Big Data-Analysen durch das »Palantir-Urteil« des Bundesverfassungsgerichts .....	99
<i>Petra Gehring</i>	

Neue Informationen, neue Erkenntnisse, alte Daten .....	117
<i>Kai Denker</i>	

Risikoabwägungen und Abwägungsrisiken – Zur Einordnung automatisierter Datenanalysen durch das Bundesverfassungsgericht anhand von Risikokalkulationen und damit einhergehenden Risiken selektiver Bewertung .....	137
<i>Andreas Brenneis</i>	
Automatisierte Datenverarbeitung und Individualisierung .....	163
<i>Andreas Brenneis, Bettina Schöndorf-Haubold</i>	
<b>Teil 2: Sicherheit vor KI und Sicherheit durch KI</b>	
Sicherheit durch KI oder Sicherheit vor KI – Regelungsstrategien für den polizeilichen Einsatz künstlicher Intelligenz .....	189
<i>Bettina Schöndorf-Haubold</i>	
hessenDATA in rechtssoziologischer Perspektive – Rechtstatsächliche Aspekte der automatisierten Datenanalyse durch die hessischen Polizeibehörden .....	213
<i>Michael Bäuerle</i>	
Data is Power – Code is Ideology: Selbstmarketing und politische Positionierungen an der Spitze von Palantir .....	225
<i>Andreas Brenneis, Kai Denker, Petra Gehring</i>	
Rechtspolitischer Rück- und Ausblick – hessenDATA und der schmale Grat zwischen polizeilicher Effizienz und Grundrechtsschutz .....	251
<i>Michael Bäuerle</i>	
Mitglieder der Projektgruppe, Autorinnen und Autoren .....	263

# Polizei-Software als Politikum?

## Das »Palantir-Urteil« des Bundesverfassungsgerichts

*Michael Bäuerle, Kai Denker, Christian Geminn,  
Bettina Schöndorf-Haubold*

»Werden gespeicherte Datenbestände mittels einer automatisierten Anwendung zur Datenanalyse oder -auswertung verarbeitet, greift dies in die informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) aller ein, deren Daten bei diesem Vorgang personenbezogen Verwendung finden.« (Leitsatz 1, BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 – 1 BvR 2634/20)

Mit der bereits im Jahr 2017 getroffenen Entscheidung des Landes Hessen, eine Software anzuschaffen, die zuvor unverbundene Datenbanken der Landespolizeibehörden durchgängig durchsuchbar macht, hat eine bundesweite Kontroverse über die Reichweiten und Grenzen der digitalen Möglichkeiten der Polizei begonnen. Angeheizt wurde die Debatte einerseits durch Sorgen um den Datenschutz, andererseits durch die Tatsache, dass ausgerechnet ein Softwareprodukt des durch den in der Kritik stehenden Tech-Milliardär Peter Thiel geleiteten US-amerikanischen Unternehmens Palantir zum Einsatz kam. *Big Data* in der Polizeiarbeit – führt das nicht zu einer massenhaften Nutzung von Daten im konkreten Fall gänzlich unverdächtigter Bürgerinnen und Bürger? »Weiß« die Polizei so nicht einfach zu viel? Auf dieses Problem richteten sich einerseits viele Fragen. Und andererseits steht die Kooperation der Polizeibehörden eines demokratischen Landes mit einem Softwareanbieter, der für antidemokratische Botschaften bekannt ist, in der Kritik.

Angesichts neuer Bedrohungen für Staat und Gesellschaft wurden die deutschen Sicherheitsbehörden seit geraumer Zeit zentralisiert, ausgebaut und erhielten neue Aufgaben. Ihre Tätigkeit wandelte sich sukzessive von reaktivem Einzelfallbezug hin zu einem strukturierten operativen Vorgehen, das Risiken frühzeitig erkennen und ihnen entgegenwirken soll. Je mehr es gilt, Gefahren rechtzeitig zu antizipieren, desto stärker sind die Sicherheitsbehörden – technologiegestützt – auf die Gewinnung und Verarbeitung von Daten angewiesen. Diese Entwicklung findet unter den Bedingungen der Digitalisierung privater und staatlicher Räume statt und geht mit einer weitgehenden Datafizierung von Kommunikation und gesellschaftlichem Handeln einher, sodass inzwischen auch das sicherheitsbehördliche Handeln durch einen zunehmenden

(und geplanten) Einsatz von Big-Data-Analysen und Künstlicher Intelligenz (KI) gekennzeichnet ist. Die Verarbeitung großer Datenmengen zum Zweck der Erkenntnisgewinnung und Wissensgenerierung ist damit zentraler Bestandteil sicherheitsbehördlicher Tätigkeit im Rahmen der Gefahrenabwehr und der Strafverfolgung. In der Folge ist in den vergangenen Jahren nicht nur eine Zunahme von Big-Data-Analysetechniken zu beobachten, sondern jüngst auch die Bereitstellung von Rechtsgrundlagen für den Einsatz künstlicher Intelligenz bei der Datenverarbeitung.

Nach Hessen haben sich später auch Nordrhein-Westfalen, Bayern und jüngst Baden-Württemberg entschieden, die Palantir-Software »Gotham« zur »Effektuierung« der polizeilichen Datenverarbeitung einzusetzen. Im Hessischen Gesetz über die öffentliche Sicherheit und Ordnung und im Hamburger Gesetz über die Datenverarbeitung der Polizei wurde hierzu erstmals eine landesrechtliche Befugnis geschaffen. In Hamburg geschah dies, obwohl das Land die Software bis heute nicht beschafft hat und einsetzt. Die beiden Regelungen sind in den Jahren 2022/2023 umgehend Gegenstand einer umfassenden, größtenteils erfolgreichen Verfassungsbeschwerde geworden. Während das Land Hessen die umstrittene Software unter dem Namen »hessenDATA« bereits nutzte, erging am 16. Februar 2023 die Entscheidung des Bundesverfassungsgerichts, in der das Gericht die Teile der angegriffenen Regelungen als verfassungswidrig beanstandete.

Der Text des Urteils setzt sich ausführlich vor allem mit den datenschutzrechtlichen Aspekten, aber auch mit der Veränderung der Polizeimethodik durch *Big Data*-Analysen auseinander.

Das vorliegende Buch nimmt das Urteil des Bundesverfassungsgerichts zum Ausgangspunkt eingehender Analysen, die das komplexe Thema kritisch ausleuchten. Die Zugänge sind teils rechtswissenschaftlicher Art, teils aber auch durch interdisziplinäre Diskussionen geprägt, in denen sich sozialwissenschaftliche, informatische und technikphilosophische Perspektiven verbinden. Ziel der Beiträge ist es, Rahmenbedingungen für eine Regulierung von *Big Data*-Analysen in den Polizeibehörden auf den Prüfstand zu stellen und grundsätzlich zu durchdenken. Dabei werden auch Zukunftsperspektiven, etwa das sogenannte *Predictive Policing* und europäische Entwicklungen rund um den AI-Act in den Blick genommen. Diskutiert wird ebenso, was in der Entscheidung des Gerichts kaum Erwähnung findet: die Rolle privater Unternehmen im Bereich der Sicherheitsgewährleistung.

## Teil I: Das Urteil des Bundesverfassungsgerichts zur automatisierten Datenanalyse

Zunächst stellt **Lea Rabe** das Urteil des Bundesverfassungsgerichts zur automatisierten Datenanalyse aus dem Februar 2023 eingehend vor und ordnet dieses sowohl in den verfassungsrechtlichen als auch den einfachgesetzlichen Kontext ein.

**Christopher Giogios** knüpft an die Kernaussagen des Urteils an und beleuchtet insbesondere mit einem Fokus auf die hessische Rechtslage die Folgen, die sich aus dem Urteil ergeben haben. Dieses hat im Ergebnis nicht nur zu einer zweifachen Änderung des hessischen Polizeigesetzes mitsamt eines nunmehr ausdrücklich erlaubten KI-Einsatzes geführt, sondern auch eine erneute Verfassungsbeschwerde hervorgerufen. Darüber hinaus lässt sich insbesondere in jüngster Zeit beobachten, dass zahlreiche weitere Bundesländer die Verabschiedung entsprechender Rechtsgrundlagen sowie die Nutzung von Palantir-Produkten beabsichtigen. Dies wirft vor allem die Frage auf, ob die Länder, aber auch der Bundesgesetzgeber mit den gegenwärtigen Initiativen den vom Bundesverfassungsgericht vorgegebenen Gestaltungsspielraum in zulässiger Art und Weise ausschöpfen.

Im Anschluss gehen **Lea Rabe**, **Christian Geminn** und **Paul Johannes** auf rechtliche Fragen ein, die eine automatisierte Datenanalyse im Kontext des Datenschutzes und der KI-Regulierung aufwirft. Mit der KI-Verordnung wurde rechtliches Neuland betreten, und gerade das Zusammenspiel mit dem Datenschutzrecht ist an vielen Stellen noch unklar. Diese Probleme verschärfen sich, wo beide Regularien in Form der automatisierten Datenanalyse bei der Polizei auf einen Regulierungsgegenstand treffen, der selbst hochinnovativ ist und eigene Unschärfen aufweist.

**Petra Gehring** unterzieht die Bundesverfassungsgerichtsentscheidung einer Tiefenlektüre, die auf die begriffliche Modellierung dessen abzielt, was das Gericht als das eigentlich Neue der umstrittenen Software ansieht. Dabei zeigen sich Unschärfen. Der Software wird einerseits die Rolle eines Werkzeugs zugewiesen, andererseits aber doch zur Last gelegt, die Polizeimethodik in kritischer Weise zu verändern und sogar »neues Wissen« zu produzieren. Dies könnte als (unge-  
wollte) Überschätzung einer womöglich unkontrollierbaren Macht von Technik politisch letztlich bedenklich sein.

Sodann nimmt **Kai Denker** eine »definitionsarchäologische Untersuchung« des Urteils vor: Er entdeckt, dass der Informationsbegriff zwischen den Polen »Daten« und »neuen Erkenntnissen« changiert. Die hier ausgemachte Doppeldeutigkeit eröffnet ein Feld, in dem das Urteil über datenschutz- und polizeirechtliche Erwägungen hinaus Eigenschaften informationstechnischer Verarbeitungsmethoden deutlicher als zuvor adressiert. Sie reichen vom bloßen Datenabgleich in Form einer Suche bis hin zu avancierten und entsprechend eingriffsintensiven statistischen Auswertungen, auch mit Mitteln der künstlichen Intelligenz.

**Andreas Brenneis** analysiert die durch das Urteil vorgenommene Definition und Abwägung von Risiken und zeigt dabei, dass durch diese Risikoabwägung selbst Risiken entstehen – nämlich hinsichtlich Unklarheiten der Grundrechtsdogmatik, Verkürzungen technischer Arrangements durch Ausblendung ihrer sozialen Eingebundenheit sowie unbotmäßige Restriktionen polizeilicher Aufgabenerfüllung. Hierzu werden die Argumente für und wider einen Einsatz automatisierter Datenanalyse seitens der Polizeibehörden und der Beschwerdeführenden vor dem Hintergrund der Risikokalkulation dargestellt und auf den zentralen Begriff des »neuen Wissens« bezogen sowie die Differenzierung zwischen dem Aufdecken und dem Generieren von Anhaltspunkten als der zentrale Knackpunkt der Argumentation des Bundesverfassungsgerichts rekonstruiert und informationstechnisch eingeordnet.

**Andreas Brenneis und Bettina Schöndorf-Haubold** fragen, ob die technischen Möglichkeiten im Bereich der automatisierten Datenverarbeitung – insbesondere im polizeilichen Kontext – tatsächlich bereits im (alltagssprachlichen wie rechtsdogmatischen) Vorfeld so stark eingeschränkt werden müssen, wie es das Urteil nahelegen scheint, oder ob sich nicht alternative Wege denken lassen, die eine differenziertere Abwägung zwischen gesteigerter technischer Effektivität und dem Schutz des Grundrechts auf informationelle Selbstbestimmung ermöglichen. Dazu loten sie aus, ob und inwiefern eine noch stärker ausdifferenzierte Bewertung und Gestaltung der Schritte und Schwellen in der Datenverarbeitung – insbesondere bei Initiierung und Einsatz der Datenverarbeitung sowie beim Übergang der Analyseergebnisse in die polizeiliche Verwertung – dazu beitragen kann, Technikpotenziale auszunutzen, ohne den Schutz der informationellen Selbstbestimmung zu unterlaufen. Als zentrale Ansatzpunkte werden individualisierte von nicht-individualisierten Eingaben und Ergebnissen unterschieden sowie Optionen der Qualitätssicherung und mögliche Rollenkonzepte diskutiert.

## Teil 2: Sicherheit vor KI und Sicherheit durch KI

**Bettina Schöndorf-Haubold** behandelt zu Beginn des zweiten Teils unterschiedliche rechtliche Regelungsansätze für automatisierte Datenverarbeitungsmethoden und künstliche Intelligenz in der und durch die Polizei im Bereich der Zuständigkeit unterschiedlicher legislativer, exekutiver und judikativer Akteure im unionalen Mehrebenensystem. Noch vor der Frage der verfassungsrechtlichen Zulässigkeit wird die Frage nach der föderalen Zuständigkeit zunächst im deutschen Bundesstaat und darüber hinaus in der Europäischen Union aufgeworfen, die ergänzende und zum Teil verdrängende Produktsicherheits- und Datenschutzstandards auch und gerade im Bereich der Sicherheitsgewährleistung erlassen hat. Die Regelungsansätze auf den unterschiedlichen Ebenen variieren zwischen der Effektivierung der Sicherheitsgewährleistung durch KI und dem Grundrechts- und Datenschutz vor KI, zu denen sich auch der risikobasierte produktsicherheitsrechtliche Ansatz des EU-Rechts nicht eindeutig verhält.

**Michael Bäuerle** untersucht die polizeiliche Anwendungspraxis anhand der vorliegenden Daten unter rechtssoziologischen Gesichtspunkten. Dabei geht es insbesondere um die Frage, inwieweit sich das normative Konzept der auf die Abwehr erheblicher Gefahren gerichteten Datenanalyse in der tatsächlichen Anwendung durch die Polizeibehörden widerspiegelt.

**Andreas Brenneis, Kai Denker** und **Petra Gehring** skizzieren die Ideologie hinter der Unternehmensspitze von Palantir. Sie zeigen wie die prima facie marktliberalen Haltungen Peter Thiels und Alexanders Karp auf einen autoritären Libertarismus rekurren, der seinerseits von den extrem rechten Diskursströmungen der Neoreactionism und der Dark Enlightenment ununterscheidbar wird. Die Frage, ob sich eine liberale Demokratie wie die Bundesrepublik von einem Softwareanbieter abhängig machen sollte, dessen CEOs Demokratie und Freiheit für miteinander unverträglich halten, steht aus Sicht der Autoren definitiv im Raum.

Abschließend erörtert **Michael Bäuerle** anhand der bisherigen Gesetze und Gesetzentwürfe zu automatisierten Datenanalysen die rechtspolitische Perspektive polizeilicher Big-Data- und KI-Anwendungen vor dem Hintergrund der Datifizierung aller Lebensbereiche. Insoweit stellt sich insbesondere die Frage, ob die Rechtspolitik an dem bisherigen individuellen Eingriffsabwehrkonzept des Rechts perspektivisch festhalten sollte.

Ein Buch ist immer das Werk vieler. Neben den Autorinnen und Autoren danken wir dem Zentrum verantwortungsbewusste Digitalisierung (ZEVEDI) des Landes

Hessen, das die Forschungen der Projektgruppe *Big Data und KI im Bereich der deutschen Sicherheitsbehörden* ermöglicht hat, deren Ergebnisse wir hiermit vorlegen. Ebenso danken wir Dr. Simon Egbert, Thomas Hering, Franziska Görlitz, Prof. Dr. Dieter Kugelmann, Dirk Peglow, Stephan Ursuleac und besonders Dr. Nora Jansen für inspirierende Diskussionen, Burak Türkmén für tatkräftige Unterstützung und dem Campus Verlag für die gute Zusammenarbeit.

Teil 1:  
Das Urteil des Bundesverfassungsgerichts  
zur automatisierten Datenanalyse



# Das Urteil zur automatisierten Datenanalyse (BVerfGE 165, 363) – Besprechung des Urteils und seiner sicherheitsverfassungsrechtlichen Implikationen

*Lea Rabe*

Mit Urteil vom 16. Februar 2023 erklärte das Bundesverfassungsgericht die Rechtsgrundlagen für die Verfahren zur automatisierten Datenanalyse im hessischen und hamburgischen Polizeirecht für verfassungswidrig.<sup>1</sup> Doch zeigte sich der Senat durchaus technologieoffen: Die gesetzliche Implementierung von *Big Data*-Analysen sowie folgerichtig auch ihre Anwendung durch die Behörden ist aus verfassungsgerichtlicher Sicht damit zwar möglich, muss aber eine Reihe grundrechtsschonender Voraussetzungen erfüllen. Die Rechtsetzung sieht sich daher vor die Aufgabe gestellt, zwischen der Garantie von Individualrechten und der Öffentlichen Sicherheit zu vermitteln. Rechtspolitisch aufgeworfen ist die Frage nach der persönlichen Freiheit in der sogenannten Sicherheitsgesellschaft.

In der Sache geht es um automatisierte Datenanalyse. Mit dem Bundesverfassungsgericht handelt es sich hierbei um automatisiertes *Data Mining* zur Informationsgewinnung – mit dem Datenanalyseurteil also um »eine von Algorithmen gesteuerte datei-, format-, und datenbankübergreifende Recherche und Analyse von personenbezogenen Daten zur Generierung neuen Wissens und neuer Erkenntnisse«<sup>2</sup>.<sup>3</sup> In der Regel kommt Künstliche Intelligenz (KI) zum Einsatz. Neues Wissen entsteht hier als Verknüpfungs- und Sortierungswissen.<sup>4</sup> Automatisierte Datenanalysen können sich auf einfache Abgleichfunktionen beschränken. Überschreiten sie aber durch die Fähigkeit zu komplexeren Formen des Datenabgleichs die herkömmlichen Erkenntnismöglichkeiten der Polizei – schlichtweg durch ihren Umfang oder aber durch den Einsatz spezifischer Methoden wie Mustersuchen oder maschinelle Sachverhaltsbewertungen – ist ihnen

---

1 BVerfGE 165, 363.

2 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 26; vgl. auch BT-Drs. 17/11582, aufgegriffen in BVerfGE 156, II (40).

3 BT-Drs. 17/11582, S. 2.

4 BVerfGE 165, 363 (396).

ein spezifisches Eingriffsgewicht inhärent, das verfassungsrechtlich besonders zu behandeln ist.<sup>5</sup>

Die Maßstäbe, an denen sich automatisierte Datenanalysen messen lassen müssen – das gilt für ihre einfachgesetzlichen Ermächtigungsnormen ebenso wie für den jeweiligen Einzelakt – ergeben sich zuvörderst aus dem Verfassungsrecht. Mit dem Urteil zur automatisierten Datenanalyse vom 16. Februar 2023 liegt eine hierfür unmittelbar einschlägige Entscheidung vor. Dieses sattelt auf einer bis dato entwickelten datenschutzverfassungsrechtlichen Sonderdogmatik<sup>6</sup> auf. Das vorliegende Kapitel rekapituliert das Urteil und seine Rezeption und stellt die sich abzeichnenden verfassungsrechtlichen Parameter für automatisierte Datenanalysen dar.

## 1. Das Urteil des Bundesverfassungsgerichts: Datenanalyse ja – aber wie?

Im Datenanalyseurteil arbeitet der Erste Senat minutiös die Anforderungen an Ermächtigungsgrundlagen heraus – und warum § 25a HSOG a. F. und § 49 HmbPolDVG diese verfehlten. Bei diesen handelte es sich um die jeweiligen spezifischen Ermächtigungsnormen für automatisierte Datenanalysen im Landesrecht. Als Schlagworte für die Prüfung seien hier schon vorab die Grundsätze der Zweckbindung und Zweckänderung und die Kalibrierung des »spezifischen Eingriffsgewichts«<sup>7</sup> automatisierter Analyseverfahren genannt. Der Senat setzte sich mit der Verfassungskonformität der aufgezümmten Eingriffsschwellen auseinander – und kam für beide Normen zu einem Negativbefund.<sup>8</sup> Maßstab war einzig das Grundrecht auf informationelle Selbstbestimmung (Art. 1 i. V. m. Art. 2 I GG); die Beschwerdeführenden hatten ihr Vorbringen hinsichtlich möglicher Verletzungen der Art. 13 I GG und 10 I GG nicht hinreichend substantiiert.<sup>9</sup> Eine gesonderte Prüfung des Art. 3 III 1 GG unterblieb, weil dieser nicht vom Beschwerdevorbringen umfasst war.<sup>10</sup> Das Urteil wird nachfolgend anhand einer cursorischen Gesamtschau nachvollzogen. Im Anschluss werden jene Aussagen gewürdigt, die besondere Aufmerksamkeit verdienen. Hierzu zählen die Erfordernisse effektiver Datenkennzeichnung und der Reduzierung des Daten-

5 BVerfGE 165, 363 (428 f.).

6 Als solche bezeichnet bei Buchheim, in: Barczak 2023, § 9 BKAG Rn. 18.

7 BVerfGE 165, 363 (LS. 2 und 3).

8 BVerfGE 165, 363 (388); Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 13 f.

9 BVerfGE 165, 363 (387).

10 BVerfGE 165, 363 (375 f.).

umfangs sowie Maßgaben für Künstliche Intelligenz und auch das Gebot der Normklarheit.

Welche Textgrundlage wurde also besehen? Der hessische Landesgesetzgeber hatte das HSOG im Mai 2018 umfassend novelliert, um es an die Vorgaben der DSGVO und der JI-RL und der höchstrichterlichen Rechtsprechung zum BKA-Gesetz anzupassen.<sup>11</sup> Die Generalklausel für die Weiterverarbeitung polizei- und gefahrenabwehrbehördlicher Daten ist, damals wie heute, § 20 HSOG.<sup>12</sup> § 25a HSOG a. F. wurde nachträglich, nämlich mit Gesetz vom 25. Juni 2018 eingefügt.<sup>13</sup> Mit § 25a HSOG a. F. setzte der Erste Senat sich erst in einem zweiten Schritt auseinander. Vorher setzte er bekannte dogmatische Grundsätze in Bezug zu automatisierten Datenanalysen. Der materiellrechtliche Teil des Urteils ist also zweigligdrig. Dementsprechend enthält das Urteil neben landesrechtsspezifischen Aussagen auch verallgemeinerbare Maßgaben zur verfassungskonformen Regelung automatisierter Datenanalyseverfahren.

### 1.1 Grundsätzliches und spezifisches Eingriffsgewicht der Datenverarbeitung

Bei der Prüfung der informationellen Selbstbestimmung setzte der Senat die verfassungsrechtlichen Anforderungen an die Rechtfertigung des § 25a a. F. HSOG aufgrund der großen Reichweite der Eingriffsnorm streng an.<sup>14</sup> Um auch die interdisziplinäre Leser:innenschaft an dieser Stelle mit ins sprichwörtliche Boot zu holen: eine verfassungsrechtliche Grundrechteprüfung hat ein festes Prüfschema. Bestimmt wird zunächst das betroffene Grundrecht, dann der Eingriff in dasselbe und dessen Schwere. Es schließt sich eine Rechtfertigungsprüfung an. Die Belastung eines Grundrechts kann daher verfassungsrechtlich hinnehmbar sein, wenn sie einem legitimen Zweck dient, zur Erreichung dieses Zwecks geeignet und erforderlich und auch im engeren Sinne angemessen ist. Die Angemessenheitsprüfung bedeutet eine Abwägung der relevanten Rechte und Rechtsgüter.

Das Bundesverfassungsgericht prüfte also das Grundrecht auf informationelle Selbstbestimmung. Dieses ist eine bereichsspezifische Konkretisierung des allgemeinen Persönlichkeitsrechts<sup>15</sup> und weitestgehend Produkt der Bundesverfassungsrechtsprechung. Erstmals am 15. Dezember 1983, im sogenannten Volkszählungsurteil, bemühte der Erste Senat einen Schutz gegen unbegrenzte

---

11 Bäuerle, in: Möstl/Bäuerle 2025, § 20 HSOG Rn. 8, II.

12 Bäuerle, in: Möstl/Bäuerle 2025, § 20 HSOG Rn. 3.

13 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 1.

14 BVerfGE 165, 363 (388).

15 Barczak, in: Dreier 2023, Art. 2 I GG Rn. 91.

Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten unter den Bedingungen der modernen Datenverarbeitung. Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis der Betroffenen, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen.<sup>16</sup> Das bedeutet, dass alle Maßnahmen innerhalb des Datenkreislaufs (Erhebung, Verarbeitung, Nutzung, Zweckänderung, Übermittlung) einen Eingriff begründen können – sogar wenn es sich in der Sache um bereits erhobene Daten handelt oder diese im Binnenraum der Verwaltung verbleiben.<sup>17</sup> Zudem hat das Grundrecht auf informationelle Selbstbestimmung eine demokratische Funktion: Bürger:innen dürfen nicht einem »Gefühl ständigen Überwachtwerdens« ausgesetzt werden, sonst droht ein chilling effect für Wahrnehmung der grundrechtlich verbürgten Freiheiten.<sup>18</sup>

Im Fall der automatisierten Datenanalyse nun lägen zwei Grundrechtseingriffe vor<sup>19</sup>. Zunächst durch die Weiternutzung der bereits erhobenen Daten über den ursprünglichen Anlass hinaus. Die Belastung sei breit gestreut. In den Worten des Senats: würden »gespeicherte Datenbestände gemäß § 25a HSOG [...] mittels einer automatisierten Anwendung zur Datenanalyse oder -auswertung verarbeitet, [greife] dies in die informationelle Selbstbestimmung (Art. 2 Abs 1 i. V. m. Art. 1 Abs. 1 GG) aller ein, deren Daten bei diesem Vorgang personenbezogene Verwendung finden.«<sup>20</sup> Eingriffsqualität habe zudem auch die Erlangung grundrechtsrelevanten, gänzlich »neuen Wissens«. Damit würdigte der Erste Senat ein dem data mining inhärentes spezifisches Eingriffsgewicht.<sup>21</sup> Das begründete Karlsruhe wie folgt: zunächst sei eine intensivere Datenerschließung möglich. Entsprechende Technologien erlaubten eine Verarbeitung großer und komplexer Informationsbestände. Der Umfang reiche über die Möglichkeiten »klassischer« Polizeiarbeit weit hinaus.<sup>22</sup> Und außerdem könnten weitere persönlichkeitsrelevante Informationen, die ansonsten so nicht zugänglich wären,

16 BVerfGE 65, 1 (I, 1. LS.); 113, 29 (46); 130, 151 (183); Vasel 2023, S. 1175.

17 BVerfGE 130, 151 (183 f.); Barczak, in: Dreier 2023, Art. 2 I GG Rn. 100.

18 StRspr, BVerfGE 150 244 (268) m.w.N.; siehe auch EuGH, Urt. v. 08.04.2014, C-293/12, C-594/12, Digital Rights Ireland Ltd gegen Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, ECLI:EU:C:2014:238, Rn. 37; Müller/Schwabenbauer, in: Lisken/Denninger 2021, Rn. 1346. – Kritische Tendenz m.w.N. bei Rademacher, in: Zimmer 2021, S. 254 f.

19 Schulenberg, in: Barczak 2023, § 12 BKAG Rn. 2; Hartmann/Cipierre/Beeck 2023, S. 147.

20 BVerfGE 165, 363 (388); vgl. Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 9.

21 Löffelmann 2023, S. 342; Hartmann/Cipierre/Beeck 2023, S. 148; so auch bei Schulenberg, in: Barczak 2023, § 12 BKAG Rn. 2. – Der Schutz durch das Grundrecht auf informationelle Selbstbestimmung erstreckt sich dabei auf die Generierung personenbezogener neuen Wissens; ortsbezogene Verfahren aber sind nicht notwendigerweise persönlichkeitsrelevant und entbehren somit einer spezifischen Eingriffsintensität, BVerfGE 165, 363 (412).

22 BVerfGE 165, 363 (396 f.).

gewonnen werden.<sup>23</sup> Das näherte sich, wie vor dem Senat schon von der Kriminologin Sommerer beobachtet, einem Profiling an.<sup>24</sup> Insgesamt beobachtet der Senat, es werde »[e]in herkömmliches Verfahren, die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit, [...] mit viel größerer Durchschlagkraft versehen«<sup>25</sup>. Dieser Überwindung der Erkenntnisgrenzen klassischer Polizeiarbeit seien besondere Gefahren für Individualrechtsgüter inhärent.<sup>26</sup> Das bedeutet im Umkehrschluss, dass Datenanalysen – auch personenbezogene – denen eine derartige spezifische Eingriffsintensität abgeht, schon nach den Grundsätzen der Zweckbindung gerechtfertigt sein können.<sup>27</sup> Das ist dem Senat zufolge der Fall wenn »eine auf die Befugnis gestützte Maßnahme nicht zu tieferen Einsichten in die persönliche Lebensgestaltung der Betroffenen führt als sie die Behörde, wenngleich aufwendiger und langsamer, auch ohne automatisierte Anwendung realistisch erlangen könnte«<sup>28</sup>. Datenanalysen mit spezifischem Eingriffsgewicht unterliegen aber besonderen verfassungsrechtlichen Anforderungen. Die Eingriffe können unter Bedingungen, die das Bundesverfassungsgericht sodann konkretisiert, gerechtfertigt sein.

Sinn, als rechtstechnisch gesprochen »legitimer Zweck«, für Ermächtigungen zur automatisierten Datenanalyse sei die Steigerung der Wirksamkeit der vorbeugenden Straftatbekämpfung vor dem Hintergrund der informationstechnischen Entwicklung, insbesondere die effektive Handhabung heterogener und händisch unter Zeitdruck manuell kaum auswertbarer Datenaufkommen.<sup>29</sup> Das entspricht seitens der Verantwortlichen im hessischen Vergabeverfahren artikulierten Bedürfnissen. Vorherige Verfahren zur Datenstrukturierung, -zusammenführung und -auswertung seien überwiegend manuell vorgenommen worden, dies »zeitintensiv, fehleranfällig und teilweise wenig zielführend« gewesen.<sup>30</sup> Von der technischen Veränderung versprach sich die hessische Polizei grundlegende Verbesserungen.

Wenig überraschend ging der Senat so auch von der Geeignetheit und insbesondere Erforderlichkeit aus: »weil durch eine automatisierte Datenanalyse oder -auswertung für die Verhütung von Straftaten relevante Erkenntnisse erschlossen werden können, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären«<sup>31</sup>. Angemessen sei eine Regelung, die

---

23 BVerfGE 165, 363 (397).

24 BVerfGE 165, 363 (396 f., 400).

25 BVerfGE 165, 363 (397).

26 BVerfGE 165, 363 (397 f.); weitsichtig schon Golla 2021, S. 671.

27 BVerfGE 165, 363 (412).

28 BVerfGE 165, 363 (412).

29 BVerfGE 165, 363 (398); vgl. auch Kugelmann/Buchmann 2024, S. 3 f.

30 LT-Drs. 19/6864, S. 28.

31 BVerfGE 165, 363 (389).

Eingriffsgewicht, Eingriffsschwelle und Rechtsgüterschutz austariere. Die Zulässigkeit der Datenweiternutzung zunächst bemesse sich an den Grundsätzen der Zweckbindung und Zweckänderung.<sup>32</sup> Der Senat lässt letztlich offen, ob der hessische Gesetzgeber diesen hinreichend genüge getan hatte und richtet die Bewertung der Verfassungskonformität der Regelung am spezifischen Eingriffsgewicht des automatisierten Verfahrens aus.<sup>33</sup> Es gelten folgende Grundsätze:<sup>34</sup>

*Je weniger die verwendbaren Daten der Art nach eingeschränkt seien, umso größer sei die zur Verarbeitung gelangende Datenmenge und umso höher sei das tendenzielle Eingriffsgewicht.*

*Die Art der Daten (Stichwort: Persönlichkeitsrelevanz) sei auch für sich genommen für das Eingriffsgewicht von Bedeutung.*

*Art und Umfang der Daten sowie deren Auswirkungen auf das Gewicht der Grundrechtseingriffe könnten durch verschiedene Vorkehrungen näher bestimmt und beschränkt werden.*

Diese Grundsätze schlagen sich sodann in kleinteiligen »Vorschlägen«<sup>35</sup> zur Regulierung des spezifischen Eingriffsgewichts nieder. Das Eingriffsgewicht könne zunächst gemindert werden durch eine Reduzierung des Datenumfangs, insbesondere gesetzliche Regelungen zur Datenherkunft<sup>36</sup>, zum Datensubjekt<sup>37</sup>, zur Speicherdauer (jedenfalls von Verkehrsdaten<sup>38</sup>)<sup>39</sup> zum Datenformat (insbesondere dem Ausschluss biometrischer Daten)<sup>40</sup> sowie zur Zugriffssteuerung<sup>41</sup> und Sichtbarkeit<sup>42</sup>. Weiterhin ließe sich die Eingriffsintensität durch Auswahl zugelassener Analysemethoden (Komplexität des Abgleichs, konkreter Suchanlass oder offene Suche, Einsatz von Künstlicher Intelligenz) regulieren.<sup>43</sup> In diesem Kontext eingriffsintensitätsmildernd wirkten sich auch die Sicherstel-

32 BVerfGE 165, 363 (390); interessanterweise vertritt der Senat hier die Auffassung, dass sich der für eine verfassungskonforme hypothetische Datenneuerhebung erforderliche konkrete Ermittlungsansatz für die Weiterverwendung bereits erhobener Daten auch aus diesen Daten selbst ergeben kann, BVerfGE 165, 363 (390).

33 BVerfGE 165, 363 (394 f.).

34 BVerfGE 165, 363 (401).

35 Zur »Regelungshypertrophie« im Datenschutzrecht siehe unter 3.

36 BVerfGE 165, 363 (404).

37 BVerfGE 165, 363 (403).

38 Hierin liegt ein Bezug zur Rechtsprechung zur Vorratsdatenspeicherung.

39 BVerfGE 165, 363 (403).

40 BVerfGE 165, 363 (404).

41 BVerfGE 165, 363 (404).

42 »Sekundenschneller Datenabgleich«, BVerfGE 165, 363 (403 f.).

43 BVerfGE 165, 363 (404 f.).

lung von Nachvollziehbarkeit der automatisierten Prozesse und Regeln zur Art der Suchergebnisse (orts-, statt personenbezogen, Ausschluss von *Predictive Policing*) aus.<sup>44</sup> In Bezug auf die Eingriffsschwelle wiederum rekurriert der Senat einmal mehr auf Altbekanntes. Bemerkenswert ist hier gleichwohl der Einbezug in den Kreis »besonders gewichtiger Rechtsgüter« von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist (wesentliche Infrastruktureinrichtungen und sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen)<sup>45</sup>. Der Schutz besonders gewichtiger Rechtsgüter sei bei besonders grundrechtsintensiven Analyseverfahren erforderlich. Der Eingriffsanlass (also die Gefahrenschwelle) müsse in solchen Fällen ebenfalls als mindestens konkretisierte Gefahr angesetzt werden, bei weniger eingriffsintensiven Maßnahmen reiche es, wenn die Ermächtigungsnorm entweder die hohe Gefahren- oder Rechtsgüterschwelle ansetze.<sup>46</sup> Heimliche Maßnahmen führten zur Erhöhung der Eingriffsintensität.<sup>47</sup> Aus dem Verhältnismäßigkeitsgrundsatz ergäben sich damit zusammenhängend zudem Anforderungen an Transparenz, individuellen Rechtsschutz<sup>48</sup>, staatliches Monitoring der eingesetzten Software und aufsichtsrechtliche Kontrolle: Praxisgerecht sei in Hinblick auf letztere auch ein stichprobenartiges Vorgehen.<sup>49</sup> Schließlich müsse eine Regelung den Geboten des Vorbehalts des Gesetzes, der Bestimmtheit und Normenklarheit genügen.<sup>50</sup> Der Gesetzgeber könne aber, sofern eine detaillierte einfachgesetzliche Regelung angesichts der raschen technischen Fortentwicklung für den Grundrechtsschutz nicht praktikabel sei, die Verwaltung zur Ausgestaltung durch Verwaltungsvorschriften ermächtigen.<sup>51</sup>

## 1.2 Verdikt: Verfassungswidrigkeit des § 25a HSOG a. F.

Der Regelung der automatisierten Datenanalyse in Hessen durch § 25a HSOG konkret attestiert das Urteil eine hohe Eingriffsintensität, die Eingriffsvoraussetzungen seien unzureichend eingegrenzt.<sup>52</sup> Zunächst liege ein intensiver Eingriff vor.<sup>53</sup> Denn die Art und Menge der einsetzbaren Daten sei kaum begrenzt,

---

44 BVerfGE 165, 363 (407 f.).

45 BVerfGE 165, 363 (410).

46 BVerfGE 165, 363 (410 f.).

47 BVerfGE 165, 363 (369 f.).

48 Bäuerle 2024, S. 13 ff.

49 BVerfGE 165, 363 (412 f.).

50 BVerfGE 165, 363 (398).

51 BVerfGE 165, 363 (412 f.).

52 BVerfGE 165, 363 (419, 430).

53 BVerfGE 165, 363 (419).

insbesondere unterbliebe eine Unterscheidung zwischen Daten Unbeteiligter (etwa Opfern oder Zeug:innen) und strafrechtlich schon auffälligen Personen.<sup>54</sup> Des Weiteren sehe die Norm keine Vorkehrungen zur Beschränkung der einzubeziehenden Datenbestände vor.<sup>55</sup> Große Besorgnis galt hier Daten aus den öffentlich einsehbaren Teilen des Internets. Es sei zudem uneindeutig, ob § 20 IX 3 HSOG a. F. (der den automatisierten Einbezug von Daten aus der gesamten Vorgangsverwaltung in die Analyseplattform ermöglichte) die allgemeinen Zweckbindungsregeln des § 20 HSOG abbedinge und somit schon systematisch gegen den Zweckbindungsgrundsatz verstoße.<sup>56</sup> Insofern fehle es, so der Senat, an der gebotenen Normklarheit. Schließlich erschwere die (teil-) automatisierte Einbeziehung von Daten die Prüfung der Einbeziehungsvoraussetzungen im Einzelfall.<sup>57</sup> Eine Kennzeichnungs- oder Aussonderungspflicht für besonders sensible, personenbezogene Daten fehle.<sup>58</sup> Entsprechendes gelte für den Einbezug von eingriffssintensiven Daten aus Funkzellenabfragen und für Verkehrsdaten.<sup>59</sup> Schließlich würden auch die zugelassenen Methoden der Datenverarbeitung nicht rechtlich beschränkt; automatisierte Gefährlichkeitsbewertungen und der Einsatz selbstlernender KI bliebe möglich.<sup>60</sup>

Hinsichtlich der Inverhältnissetzung von Eingriffsgewicht und Eingriffsanlass meint Karlsruhe, das insgesamt potenziell sehr hohe spezifische Eingriffsgewicht der mit § 25a HSOG a. F. ermöglichten automatisierten Datenanalyse sei mit der unzureichenden Konkretisierung des Eingriffsanlasses unverträglich.<sup>61</sup> In Anbetracht des hohen Eingriffsgewichts könne einzig die restriktive Eingriffsschwelle des Erfordernisses konkretisierter Gefahr zu einem verhältnismäßigen Rechtsgüterausgleich führen.<sup>62</sup> Dem stehe das Erfordernis der »vorbeugenden Bekämpfung von [...] Straftaten« in § 25a I 1. Alt. HSOG a. F. nach.<sup>63</sup> Im Straftatatalog seien auch Vorfeldtatbestände einbezogen, somit auf das Vorliegen einer konkreten oder konkretisierten Gefahr aber verzichtet worden.<sup>64</sup> Insgesamt stelle die Norm daher keinen angemessenen Ausgleich zwischen Eingriffsschwelle

---

54 BVerfGE 165, 363 (419 f.).

55 BVerfGE 165, 363 (420); das bedeutet, dass nicht nur polizeilich erhobene Daten, mithin solche aus heimlichen Überwachungsmaßnahmen, verarbeitet werden könnten, sondern auch solche, die von anderen staatlichen oder nicht öffentlichen Stellen stammen.

56 BVerfGE 165, 363 (423 f.).

57 BVerfGE 165, 363 (424).

58 BVerfGE 165, 363 (424, 427 f.).

59 BVerfGE 165, 363 (426).

60 BVerfGE 165, 363 (428 f.).

61 BVerfGE 165, 363 (431 f.).

62 BVerfGE 165, 363 (431).

63 BVerfGE 165, 363 (431).

64 BVerfGE 165, 363 (438).

und Eingriffsgewicht her. Das Bundesverfassungsgericht erklärte deswegen § 25a I 1. Alt. HSOG für verfassungswidrig und gab eine Neuregelung bis zum 30. September 2023 auf.<sup>65</sup> Bis dahin war der Normgebrauch einschränkenden, grundrechtschonenden Maßgaben unterworfen.<sup>66</sup>

### 1.3 Rezeption: Technologieoffenheit und »Regelungshypertrophie«

Im Nachgang gelobt wurde die Technologieoffenheit des Urteils. Der Erste Senat habe »zugunsten feingliedriger Differenzierungen auf allzu pauschale Wertungen verzichtet«<sup>67</sup>. Der Verzicht auf ein Totalverbot von Analyseverfahren wurde begrüßt.<sup>68</sup> Datenschutzakteur:innen – so der Bundesbeauftragte für Datenschutz Ulrich Kelber und die an der Beschwerde maßgeblich beteiligte Gesellschaft für Freiheitsrechte – lobten andererseits die Grundrechtsorientiertheit des Ersten Senats.<sup>69</sup> Einigermaßen hart hingegen liest sich das Urteil von Markus Hartmann, Paula Cipierre<sup>70</sup> und Leonie Beek, die meinen, mit einer »Eingrenzung dieser Art stürbe das Instrument [der automatisierten Datenanalyse, Anmerkung L. R.] den stillen Tod der Bedeutungslosigkeit«<sup>71</sup>. In der Bewertung etwas milder, aber dennoch in die gleiche »Kerbe« schlagend, meint auch Johann Justus Vasel, der Ausschluss der Analyse im Gefahrenvorfeld sei deswegen problematisch, weil der Vorteil von Big Data-Technologien gegenüber manuellen Verfahren ja gerade in der effektiven Aufbereitung großer und heterogener Datenbestände bei unklarem Suchziel liege.<sup>72</sup> Zwar ist der Beitrag von Hartmann, Cipierre und Beek überzeichnet, doch spiegelt sich hier, wie auch bei Vasel, die grundsätzliche Antinomie zwischen Big Data und Daten- beziehungsweise Grundrechtsschutz.

Ferner stand in der Kritik die, wenn man so will, Rechtserzeugungstechnik. Moniert wurde der Umfang und die Detailliertheit der verfassungsgerichtlich

---

65 BVerfGE 165, 363 (441).

66 BVerfGE 165, 363 (441).

67 Manns 2023, S. 144; Vasel 2023, S. 1177; Löffelmann 2023, S. 341.

68 Vasel 2023, S. 1176.

69 S. LTO, »Polizei-Software Hessendata verfassungswidrig«, legal tribune online, 16.02.2023. <https://www.lto.de/recht/nachrichten/n/bverfg-1bvr154719-1bvr263420-einsatz-software-hessendata-durch-polizei-verfassungswidrig> (01.10.2025); beck-aktuell, »Nach BVerfG-Urteil zur automatisierter Datenanalyse: Neue Software erforderlich?«, beck-aktuell, 17.02.2023. <https://rsw.beck.de/aktuell/daily/meldung/detail/nach-bverfg-urteil-zu-automatisierter-datenanalyse-neue-software-erforderlich> (01.10.2025).

70 Cipierre war zum Zeitpunkt der Veröffentlichung Bereichsleiterin bei Palantir Technologies.

71 Hartmann/Cipierre/Beek 2023, S. 151.

72 Vasel 2023, S. 1177; bereits Rademacher, in: Zimmer 2021, S. 255.

herausgearbeiteten Vorgaben an den Gesetzgeber.<sup>73</sup> Das resoniert mit Bedenken hinsichtlich einer vermeintlichen »Regelungshypertrophie«<sup>74</sup> des Datenschutzrechts. Hierunter begreift die Literatur die Tendenz, dass zunehmend detailliertere verfassungsgerichtliche Regelungsaufträge den einfachen Gesetzgeber insbesondere aufgrund ihrer Praxisferne vor Herausforderungen stellen, die dieser regelmäßig schlichtweg durch eine nahezu wortgetreue Übernahme von Rechtsprechungsinhalten in Gesetzestexte zu meistern suche.<sup>75</sup> Dem ist hier in Bezug auf das Datenanalyseurteil nur teilweise zuzustimmen. Den Kritiker:innen ist einerseits zwar zuzugeben, dass das Normvolumen durch diese Rechtsprechungspraxis tatsächlich ansteigt. Auch die nach dem Urteil erlassene (alte) Neufassung des § 25a HSOG war um einiges umfangreicher als die Vorgängerversion und zumal ersichtlich darauf ausgelegt, den verfassungsgerichtlichen »Stichwortgeber« zufriedenzustellen.<sup>76</sup> Diese Regelungsweise ist insofern paradox, als sie der Normklarheit zwar im Sinne des Gesetzesvorbehalts nachkommt, die resultierende Normkomplexität der Verständlichkeit aber abträglich ist.<sup>77</sup> Gleichwohl ist dies nicht zwingende Folge des als allzu detailverliebt empfundenen »Rechtsprechungsstils« – sofern man überhaupt von einem Stil im eigentlichen Sinne sprechen kann: Denn letztlich obliegt dem Bundesverfassungsgericht im Verfassungsbeschwerdeverfahren die Begutachtung und Bewertung konkreter Hoheitsakte. Der durch Art. 94 I Nr. 4a GG verfassungsmäßig auferlegten Prüfpflicht wird der Senat also überhaupt erst durch die notwendig detaillierte Auseinandersetzung mit Eingriffsnormen gerecht. Wie Gesetzgebungsorgane die stets fallbezogene Rechtsprechung im Rahmen von Neuregelungen umsetzen, ist ihnen aber höchstselbst überlassen.

Generell und auch speziell im Fall Hessen drängt sich der Verdacht auf, dass die »Hypertrophie« von Gesetzestexten mehr der Ausgestaltung und insbesondere Terminierung von Gesetzgebungsverfahren geschuldet ist (denn unzureichender verfassungsgerichtlicher Vorarbeit), konkret: einer nicht nachvollziehbaren Verknappung der parlamentarischen Bearbeitungszeit. Das Bundesverfassungsgericht hatte dem Gesetzgeber eine sechsmonatige »Frist« für die Neufassung eingeräumt, bis zum 30. September galt der verfassungswidrige § 25a HSOG a. F. noch fort. Die (alte) Neufassung des § 25a HSOG wurde aber in das einjährige Gesetzgebungsverfahren nur neun Tage vor der Beschlussfassung durch den Landtag eingebracht.<sup>78</sup> Den Abgeordneten blieben lediglich

---

73 Vasel 2023, S. 1176.

74 Rademacher/Perkowski 2020, S. 719.

75 Vasel 2023, S. 1176.

76 S. zu den Neufassungen von § 25a HSOG den Beitrag von Giogios in diesem Band.

77 Vasel 2023, S. 1176.

78 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 19.

zwei Tage, den 853 Worte starken Entwurfstext nebst amtlicher Begründung (37 Normseiten à 1800 Zeichen inklusive Leerzeichen), durchzusehen.<sup>79</sup> Dies wirft nach dem Eilbeschluss des Bundesverfassungsgerichts zum sogenannten Heizgesetz vom 5. Juli 2023<sup>80</sup> weiterführende Fragen zum Recht der Abgeordneten auf Informationsverarbeitung aus Art. 38 I GG bzw. den entsprechenden landesverfassungsrechtlichen Normen auf.<sup>81</sup> Jedenfalls ist die enge Orientierung an verfassungsrichterlichen Vorgaben bei einer derartig verknappten Bearbeitungszeit im Parlament wenig verwunderlich. Eine Kritik der Ausdehnung und Unverständlichkeit von Normen wäre also an die parlamentarischen Entscheidungskräfte, nicht an die Rechtsprechung zu richten.<sup>82</sup>

#### 1.4 Reaktion: Verfehler Nachbesserungsversuch als »nachlaufende« Gesetzgebung

Bedenken gegenüber der (alten) Neufassung bestehen auch inhaltlicher Art. Mit der erneuten Novelle des HSOG nur wenige Monate später setzt sich *Christopher Giogios* in diesem Band auseinander.<sup>83</sup> Die (alte) Neufassung war schwer zugänglich: Nicht nur war sie mit 853 Worten sehr umfangreich – was insbesondere dadurch verstärkt wurde, dass erst eine etwa dreimal so lange Verwaltungsvorschrift (VV § 25a HSOG)<sup>84</sup> Begriffe und Verfahren näher erläuterte – sondern darüber hinaus auch überaus abstrakt. Das Gebot der Normklarheit wurde damit verfehlt. Das Normsetzungsverfahren war einmal mehr »nachlaufender«<sup>85</sup> Natur. Es war dem hessischen Gesetzgeber ersichtlich nicht darum gegangen, eine tatsächlich abstrakte Regelung für jegliche Anwendungen zu schaffen. Der Erlass der ersten Neufassung – zumal überschnellt, um die vom Bundesverfassungsgericht gesetzte Frist einzuhalten<sup>86</sup> – diente ganz offensichtlich dem Zweck, den möglichst unveränderten Weiterbetrieb von hessenDATA sicherzustellen.<sup>87</sup> *Michael Bäuerle* hat insofern zutreffend angemerkt, die Regelung lese

---

79 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 20.

80 BVerfGE 166, 304; weiterführend Meinel 2023.

81 BVerfG 166, 304 (329 ff.); weiterführend: Meinel 2023.

82 So bei Löffelmann 2023, S. 344.

83 S. den Beitrag von Giogios in diesem Band.

84 Verwaltungsvorschrift zur Ausführung des § 25a des Hessischen Gesetzes über die Sicherheit und Ordnung vom 12.07.2023, StAnz. 2023, S. 946.

85 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 25.

86 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 19 ff.: die Landtagsabgeordneten hatten zur Lektüre des Gesetzentwurfs nebst amtlicher Begründung (37 Seiten) zwei Tage Zeit; weiterführend zum Recht der Abgeordneten auf Mitwirkung am Gesetzgebungsverfahren BVerfGE 166, 304.

87 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 25.

sich »über weite Strecken als Deskription der bisherigen internen Regelungen für das konkret im Betrieb befindliche System«<sup>88</sup>. Dem hessischen Gesetzgeber war es misslungen, die Maßgaben des Urteils umzusetzen. Aufgrund der »nachlaufenden« Gesetzgebung überrascht es wenig, dass die als »wortreiche Scheinbeschränkung«<sup>89</sup> bezeichnete Neufassung die vom Senat gerügten Mängel wiederholte.

Zunächst wurden schon die Grundsätze der Zweckbindung und Zweckänderung verfehlt, insbesondere weil es nach wie vor an einer Datenkennzeichnung, die Rückschlüsse auf den Erhebungszweck zulässt, fehlt. § 20a I HSOG sieht zwar eine ordnungsgemäße Kennzeichnung vor. Gekennzeichnet werden das Mittel der Erhebung (einschließlich der Markierung als verdeckte/offene Maßnahme), bei Grunddatenerhebung die Kategorie der Person, zu schützende Rechtsgüter und die Erhebungsstelle. Doch findet praktisch aufgrund der Ausnahmeklausel des § 20a IV HSOG keine Kennzeichnung statt. Damit lässt sich auch nicht feststellen, ob ein ursprünglicher Erhebungszweck bei der Datenweiterverarbeitung realisiert, gewahrt oder geändert wird. Grundrechtsschonend – und -konform wäre daher ein Verarbeitungsverbot in § 25a HSOG für nicht gekennzeichnete Daten oder alternativ eine Streichung des § 20a IV 2 2. Var. HSOG (Ausnahme von der Kennzeichnungspflicht bei »unverhältnismäßigem Aufwand«) gewesen.

Jedenfalls § 25a III Nr. 3 HSOG entsprach verfassungsrechtlichen Maßstäben nicht. Denn Eingriffsgewicht und zugelassene Methode standen in keinem angemessenen Verhältnis zueinander. Vor allem wurde der Einsatz selbstlernender Systeme im Gefahrenvorfeld nicht normenklar ausgeschlossen.<sup>90</sup> Auch der Komplexitätsbegriff des § 25a II Nr. 2 a) 2 HSOG lief völlig ins Leere und enthielt insofern keine hinreichend klare Vorsteuerung der Eingriffsintensität. Denkbar wäre es etwa gewesen, die Komplexität einer Datenanalyse von ihrer Leistungsfähigkeit, etwa an den für das Training verwendeten Berechnungen festzumachen. Vorbild für eine solche Regelung ist Art. 51 II KI-VO. In der damaligen Fassung war die Vorschrift die Komplexität betreffend jedenfalls vollkommen unverständlich. Insgesamt genügte die Neufassung des § 25a HSOG also den in der Rechtsprechung konturierten Anforderungen an die verfassungskonforme Regelung von Verfahren zur automatisierten Datenanalyse nicht.<sup>91</sup> Dementsprechend dürfte die noch gegen die alte Neufassung am 21. Juni 2024 erhobene Verfassungsbeschwerde<sup>92</sup> Aussicht auf Erfolg haben.

---

88 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 24.

89 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 73.

90 Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 29.

91 Wie hier: Bäuerle, in: Möstl/Bäuerle 2025, § 25a Rn. 47 ff.; Löffelmann 2024, S. 10.

92 Singelstein 2024.

## 2. Verfassungsrechtliche Anforderungen an automatisierte Datenanalysen

Mit dem Urteil vom 16. Februar 2023 hat das Bundesverfassungsgericht klargestellt, dass sich ein Totalvorbehalt automatisierter Datenanalysen aus dem Verfassungsrecht nicht herleiten lässt. Gleichwohl hat der Senat sich schützend vor die Grundrechtssubjekte gestellt, indem er, wiederholt, die personenbezogene Gefahrenvorhersage »ins Blaue hinein« als verfassungswidrig eingestuft hat. Welche Parameter lassen sich also aus dem Urteil für die zukünftige Regulierung des Einsatzes von *Big Data* bei der Polizei erkennen?

Das Bundesverfassungsgericht unterscheidet abstrakt drei verschiedene Schweregrade des spezifischen Eingriffsgewichts von automatisierten Datenanalysen: besonders schwerwiegende und weniger gewichtige Eingriffe in die informationelle Selbstbestimmung sowie Datenanalysen ohne spezifisches Eingriffsgewicht, also solche, die die personenbezogenen Erkenntnismöglichkeiten manueller Auswertungen nicht überschreiten oder lediglich ortsbezogen sind.<sup>93</sup> Der Schweregrad korrespondiert mit dem notwendigen Eingriffsanlass, das heißt der erforderlichen Gefahrenschwelle.

### 2.1 Analyseverfahren ohne spezifisches Eingriffsgewicht

Liegt kein spezifisches Eingriffsgewicht vor, reicht eine Bindung an den Zweckbindungssatz aus. Das ist bei personenbezogenen Analysen der Fall, wenn die praktischen Erkenntnisgrenzen klassischer Polizeiarbeit nicht überschritten werden, ergo kein »neues Wissen«<sup>94</sup> produziert wird.<sup>95</sup> Auch Analysen, die kein personenbezogenes Wissen generieren, also ortsbezogen sind, entbehren einer spezifischen Belastung für das Grundrecht auf informationelle Selbstbestim-

---

<sup>93</sup> BVerfGE 165, 363 (411 f.); Bartsch 2024.

<sup>94</sup> Die Software vereinfacht, beschleunigt und zentralisiert Datenanalyseverfahren bei der Polizei; vgl. LT-Drs. 19/6864, S. 19. Unübersichtliche Datenmengen werden strukturiert und vereinheitlichend aufbereitet. Dadurch entsteht neues Wissen einerseits als sortiertes Wissen, da die aus den Datensammlungen abgeschöpften Informationen Zusammenhängen zugeordnet und so für Beamte einsehbar, bereifbar und verwaltbar gemacht werden. Andererseits kann auch neues Wissen als Verknüpfungswissen entstehen, wenn durch die automatisierte Datenanalyse »in den Daten angelegte, aber zunächst mangels Verknüpfung verborgene Erkenntnisse« (BVerfGE 165, 363 [396]) hervortreten. Gemeint ist die Herstellung von Persönlichkeits-, Beziehungs- oder Ortsprofilen. Werden solche nicht nur durch die Datenzusammenführung erzeugt, sondern durch »algorithmisch errechnete Annahmen über Beziehungen und Zusammenhänge ergänzt« (BVerfGE 165, 363 [397]), bedeutet das eine Generierung neuer Informationen aus den vorhandenen Daten.

<sup>95</sup> BVerfGE 165, 363 (397).

mung und damit eines spezifischen Eingriffsgewichts.<sup>96</sup> Solche Analysen sind bei Wahrung des Zweckbindungsgrundsatzes gerechtfertigt. Voraussetzung für die Weiterverwendung bereits erhobener Daten in der Analyseplattform ist dann also, dass diese durch dieselbe Behörde, im Rahmen derselben Aufgabe und zum Schutz derselben Rechtsgüter erfolgt. Der Eingriffsanlass entfällt, das heißt, die Weiterverwendung der Daten ist auch ohne Vorliegen einer konkreten Gefahr erforderlich. Praktisch kann man sich das so vorstellen, dass die Polizei die Daten von Tätern und Verdächtigen nutzen möchte, um heat maps oder andere ortsbezogene Visualisierungen oder Wahrscheinlichkeitsberechnungen abzufragen, ohne dass Hinweise auf eine konkretisierte Gefahr (vereinfacht gesagt: eine baldige Tatbegehung) vorliegen. So können besonders verbrechensgeneigte Orte oder raumbezogene Behebungsmuster erkannt werden.

Der Erste Senat ist nicht ausdrücklich darauf eingegangen, ob eine Datenweiternutzung bei Analysen, denen ein spezifisches Eingriffsgewicht abgeht, auch nach dem Grundsatz der hypothetischen Datenneuerhebung zulässig ist. Es ist jedoch nicht ersichtlich, warum von diesen dogmatischen Grundsätzen abgewichen werden sollte, sofern das Eingriffsgewicht der Datenweiterverarbeitung demjenigen herkömmlicher Methoden entspricht. Das bedeutet, dass die Daten auch außerhalb derselben Aufgabenstellung weitergenutzt werden dürfen, wenn ein konkreter Ermittlungsansatz vorliegt. Das ist der Fall, wenn konkrete Anhaltspunkte für eine im Einzelfall vorliegende Gefahr für vergleichbar gewichtige Rechtsgüter vorliegen. Diese Anhaltspunkte können sich auch aus den Daten selbst ergeben. Wichtig ist hier aber die chronologische Reihenfolge. Der Ermittlungsansatz ist Voraussetzung für die Analyse. Das heißt, dass auch eine Analyse ohne spezifisches Eingriffsgewicht nicht zur Gewinnung eines Gefahrenverdachts eingesetzt werden darf, ergo Verdachtsgewinnungsmaßnahmen »ins Blaue hinein« ausgeschlossen sind.

Notwendig für die Einhaltung der Zweckbindungsregeln ist in jedem Fall eine effektive Markierung der Daten bei der Erhebung, da die Zweckwahrung sonst nicht sichergestellt werden kann, beziehungsweise sich nicht feststellen lässt, ob vergleichbar gewichtige Rechtsgüter betroffen sind. Werden Daten aufgrund von Ausnahmeregeln zu Datenkennzeichnungsvorschriften – wie in Hessen – nicht markiert, kann ein effektiver Grundrechtsschutz nicht gewährleistet werden. Das betrifft nicht nur das Grundrecht auf informationelle Selbstbestimmung. Die Schutzwirkung auch anderer durch die Datenerhebung möglicherweise betroffener Grundrechte, also neben Art. 3 III 1 GG vor allem Art. 10 I GG, Art. 13 I GG und das IT-Grundrecht (Art. 2 I GG i. V. m. Art. 1 I GG)

---

<sup>96</sup> BVerfGE 165, 363 (412).

umfasst auch die Datenübermittlung.<sup>97</sup> Es sind daher effektive Datenaussonderungen erforderlich. Einen besonders schwerwiegenden Eingriff stellt die Analyse von Daten dar, die aus besonders eingriffintensiven Maßnahmen wie der Wohnraumüberwachung oder Online-Durchsuchungen stammen. Solche werden mitunter unter Belastung des Art. 13 I GG erlangt. Eine Weiterverwendung für automatisierte Datenanalysen ist in jedem Fall für die vorbeugende Straftatenbekämpfung unzulässig.<sup>98</sup> Fehlt es an einer solchen Kennzeichnung, dann ist die automatisierte Datenanalyse als verfassungswidrig einzustufen, weil sie den Zweckbindungsgrundsatz verfehlt.<sup>99</sup>

Auch für Analysen ohne spezifisches Eingriffsgewicht folgen aus dem Verhältnismäßigkeitsgrundsatz Transparenz-, Rechtsschutz- und Kontrollerfordernisse.<sup>100</sup> Das soll auch einer »diffusen Bedrohlichkeit geheimer staatlicher Beobachtung«<sup>101</sup>, also den sogenannten chilling effects behördlicher Informationsverarbeitung in der sich kontinuierlich weiter ausprägenden Sicherheitsgesellschaft<sup>102</sup>, entgegenwirken. Ausreichend sind stichprobenartige Kontrollen. Unabhängige und innerbehördliche Datenschutzbeauftragte können diese arbeitsteilig wahrnehmen.<sup>103</sup>

## 2.2 Analyseverfahren mit spezifischem Eingriffsgewicht

Die Rechtmäßigkeitsanforderungen für Analysen mit spezifischem Eingriffsgewicht sind deutlich komplexer. Personenbezogene Analysen sind stets von derartigem Eingriffsgewicht, denn das Analyseergebnis ist neues personenbezogenes Wissen. Im Urteil angelegt ist eine Ausdifferenzierung dieses »neuen Wissens« in Sortierungswissen, Verknüpfungswissen oder »Wissen« prognostischer Natur. Aufgrund der zahlreichen Faktoren, die in dem Urteil zur automatisierten Datenanalyse für die Vermittlung zwischen Eingriffsgewicht und Eingriffsschwelle bei Datenanalysen mit spezifischem Eingriffsgewicht von Bedeutung sind, kann der nachfolgende Abschnitt nur die Grenzen zulässiger Analysepraktiken sowie ih-

---

97 BVerfGE 100, 313 (360); 100, 279 (374 f.); 155, 119 (205 f.).

98 BVerfGE 165, 363 (416).

99 Vgl. BVerfGE 100, 279 (379 f.).

100 BVerfGE 165, 363 (410, 412 f.); Kugelmann/Buchmann 2024, S. 9; Ruf 2024, S. 9.

101 BVerfGE 141, 220 (282).

102 Sicherheitsdiskurse interagieren mit dem technologischen Fortschritt und treiben diesen letztlich weiter an. Die Kriminologen Tobias Singelstein und Peer Stolle haben diese Dynamik als »Sicherheitsgesellschaft« bezeichnet. Sie verstehen darunter die Herstellung sozialer Ordnung durch die angestrebte, aber nie erreichbare und sich daher als kontinuierliche Legitimationsgrundlage eignende Ausrichtung auf (subjektive) Sicherheit; Singelstein/Stolle 2012, S. 123.

103 BVerfGE 165, 363 (412 f.).

rer Regulierung aufzeigen. Die Abstimmung zwischen den einzelnen Parametern (Reduzierung des Datenumfangs, zugelassene Analyseverfahren, Justierung der Eingriffsschwelle) im Rahmen zulässigen Technikeinsatzes wurde nämlich weitestgehend der Gesetzgebung überlassen.

Jedenfalls erforderlich ist eine normklare Rechtsgrundlage.<sup>104</sup> Zudem gilt das Erfordernis der Verfahrenssicherung auch hier. Dem Staat fällt bei besonders leistungsstarken Systemen eine Pflicht zum Monitoring der eingesetzten Software zu.<sup>105</sup> Systeme müssen für Laien verständliche Erklärungen ihrer Entscheidungsprozesse mit dem Analyseergebnis direkt mit ausgeben, um die Nachvollziehbarkeit durch Nutzer:innen, externe Kontrollstellen (Datenschutzbeauftragte) und Adressaten abzusichern. Auf das Problem, dass dies bei weiterlernenden Systemen nicht vollends möglich ist, wird noch zurückzukommen sein.

### 2.2.1 Grenzen personenbezogener Datenanalyse zur vorbeugenden Straftatenbekämpfung

Einige klare Maßgaben enthält das Urteil für die vorbeugende Straftatenbekämpfung, also für den Einsatz automatisierter Datenanalysen bevor eine konkrete Gefahr vorliegt. Ausgeschlossen sind diese bei besonders eingriffsintensiven Analyseverfahren. Ein erhöhtes spezifisches Eingriffsgewicht, das den Einsatz im Gefahrenvorfeld ausschließt, liegt vor bei:

- maschinellen Sachverhaltsbewertungen, wenn also die Analyse über die bloße Anzeige von Übereinstimmungen hinausgeht,<sup>106</sup>
- dem Einsatz selbstlernender Systeme,<sup>107</sup>
- der Erstellung von Verhaltens-, Beziehungs-, und Bewegungsprofilen,<sup>108</sup>
- dem Einbezug von Daten Unbeteiligter (allerdings gelten Ausnahmen beim sogenannten sekundenschnellen Datenabgleich in Nichttrefferfällen),<sup>109</sup>
- bei Bestehen spezifischer Diskriminierungsrisiken,<sup>110</sup>
- bei einer Verknüpfung mit dem Internet,<sup>111</sup>
- bei offenen Suchen in personenbezogenen Daten zur Mustererkennung.<sup>112</sup>

104 BVerfGE 165, 363 (415 f.); Kuhlmann/Trute 2021, S. 107.

105 BVerfGE 165, 363 (412 f.).

106 BVerfGE 165, 363 (407).

107 BVerfGE 165, 363 (408, 418).

108 BVerfGE 165, 363 (398).

109 BVerfGE 165, 363 (400, 403 f.).

110 BVerfGE 165, 363 (400 f.).

111 BVerfGE 165, 363 (404).

112 BVerfGE 165, 363 (407).

Diese Analysen sind im Gefahrenvorfeld nicht zulässig. In Hinblick auf die Erstellung von Verhaltens-, Bewegungs- und Beziehungsprofilen ist zudem an Art. 11 JI-RL zu erinnern, der erstens vollautomatisierte Entscheidungen untersagt und zweitens ein Diskriminierungsverbot aufstellt. Auf die Unzulässigkeit diskriminierungssensibler Verfahren wird noch zurückzukommen sein. Im Folgenden werden Sonderfälle besprochen, in denen sich aus dem Zusammenspiel von Technik, Verfassungs- und Datenschutzrecht konkretere Vorgaben für die Zulässigkeit automatisierter Datenanalysen ergeben.

### *2.2.2 Hinzuziehung der Daten Unbeteiligter und »sekundenschneller Datenabgleich«*

Ein Sonderfall ist die Hinzuziehung der Daten Unbeteiligter in die Analyse. Unbeteiligte in diesem Zusammenhang sind (mutmaßliche) Opfer, Zeug:innen und Hinweisgebende.<sup>113</sup> Dass schon in der Übermittlung dieser Daten aus den angeschlossenen Datentöpfen an die Analyseplattform eine Verarbeitung im Sinne des Datenschutzrechts vorliegt, thematisierte der Erste Senat nicht. Eine Rechtsgrundlage für diese Übermittlung liegt nicht vor, müsste also parallel zu oder mit der Verarbeitungsvorschrift geschaffen werden. Der Senat ist der Auffassung, dass sich das Eingriffsgewicht automatisierter Datenanalysen erhöht, wenn sich durch die eingesetzte Technik das Risiko für Unbeteiligte, Ziel weiterer polizeilicher Maßnahmen zu werden, erhöht.<sup>114</sup> Das bedeutet auch, dass die Hinzuziehung von Daten Unbeteiligter im Rahmen eines »sekundenschnellen Datenabgleichs«<sup>115</sup> – sofern eine Weiterverarbeitungsgrundlage vorliegt – auch für die Verarbeitung sogar im Gefahrenvorfeld zulässig wäre. Denn erst die Generierung neuen personenbezogenen Wissens erzeugt das spezifische Eingriffsgewicht. Beim »sekundenschnellen Datenabgleich« werden die Daten für Beamte im Analyseergebnis nicht sichtbar (beziehungsweise wäre dafür bei der technischen Ausgestaltung Sorge zu tragen). Es wird also kein neues personenbezogenes Wissen generiert, sodass der Analyse kein erhöhtes spezifisches Eingriffsgewicht inhärent ist. Darauf, inwieweit diese Maßgaben auf weiterlernende Systeme übertragbar sind, wird sogleich eingegangen. Ist ein solcher sekundenschneller Datenabgleich nicht (fehlerfrei) eingerichtet, sondern werden die Daten Unbeteiligter sichtbar, so bleibt es bei der Zulässigkeit nur im Rahmen der Abwehr konkreter Gefahren für besonders hochrangige Rechtsgüter.

Eine darüber hinausreichende Auswertungsbefugnis von Daten Unbeteiligter bei Vorliegen einer Gefahr für weniger gewichtige Rechtsgüter ergibt sich auch

---

113 Bartsch 2024.

114 BVerfGE 165, 363 (400).

115 BVerfGE 165, 363 (403 f.).

nicht aus der europäischen Rechtsprechung zur Vorratsdatenspeicherung. Bis dato war eine Vorratsdatenspeicherung auch von Daten Unbeteiligter nach der Rechtsprechung des EuGH bei Vorliegen einer konkreten – das heißt realen, aktuellen aber zumindest vorhersehbaren Gefahr für die nationale Sicherheit erlaubt.<sup>116</sup> Eine allgemeine oder ständige Gefahr, wie sie durch prävalente Terrorismusdiskurse inszeniert wird, ist nicht ausreichend.<sup>117</sup> Jüngst, nämlich im Urteil vom 30. April 2024, senkte der Gerichtshof allerdings die Eingriffsschwelle für Vorratsdatenspeicherungen nach Art. 15 I der Datenschutzrichtlinie für elektronische Kommunikation<sup>118</sup> ab. Eine unterschiedslose Vorratsdatenspeicherung soll demnach schon für die Bekämpfung von Straftaten im Allgemeinen und nicht nur für schwere beziehungsweise schwerste Kriminalität zulässig sein.<sup>119</sup> Unabhängig von der Frage der verfassungskonformen Umsetzung dieser Rechtsprechung lässt sich diese gleichwohl nicht auf den vorliegenden Bearbeitungskontext übertragen. Denn Rechtmäßigkeitsvoraussetzung einer unterschiedslosen Vorratsdatenspeicherung ist dem EuGH zufolge eine strikte Trennung der verschiedenen Kategorien der auf Vorrat gespeicherten Daten: »Um sicherzustellen, dass eine [solche] genaue Schlüsse auf das Privatleben der betreffenden Person ermöglichende Kombination von Daten ausgeschlossen ist«<sup>120</sup>. Eine solche Zusammenführung von Daten wird aber durch automatisierte Datenanalysen gerade bezweckt. Daher sind die Maßgaben des EuGH-Urteils vom 30. April 2024 auf diese nicht anwendbar.

Wie auch bei der Vorratsdatenspeicherung kommt es für die Verfassungskonformität des Einbezugs von Daten Unbeteiligter entscheidend darauf an, dass Löschfristen<sup>121</sup> für die sich im Analysesystem befindenden Daten gewahrt werden. Zudem sind fachgerichtliche und aufsichtsrechtliche Kontrolle sicherzustellen.<sup>122</sup> Hier wäre, wie bei der Vorratsdatenspeicherung, bei Maßnahmen mit gro-

---

116 EuGH, Urt. v. 20.09.2022, C-793/19, C-794/19, Bundesrepublik Deutschland gegen SpaceNet AG und Telekom Deutschland GmbH, ECLI:EU:C:2022:702, Rn. 93.

117 EuGH, Urt. v. 20.09.2022, C-793/19, C-794/19, Bundesrepublik Deutschland gegen SpaceNet AG und Telekom Deutschland GmbH, ECLI:EU:C:2022:702, Rn. 93.

118 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

119 EuGH, Urt. v. 30.04.2024, C-470/21, La Quadrature du Net u. a. gegen Premier Ministre, Ministre de la Culture, ECLI:EU:C:2024:370, Rn. 82.

120 EuGH, Urt. v. 30.04.2024, C-470/21, La Quadrature du Net u. a. gegen Premier Ministre, Ministre de la Culture, ECLI:EU:C:2024:370, Rn. 84.

121 EuGH, Urt. v. 06.10.2020, C-511/18, C-512/18, C-520/18, La Quadrature du Net u. a. gegen Premier ministre u. a., ECLI:EU:C:2020:791, Rn. 148; BVerfGE 155, 119 (225 f.).

122 BVerfGE 155, 119 (227).

ßer Streubreite auch an eine Vorabgenehmigung durch eine unabhängige Stelle, ergo: eine richterliche Anordnung, zu denken.<sup>123</sup>

### 2.2.3 Verfahrens- und aufsichtsrechtliche Sicherungen beim Einsatz Künstlicher Intelligenz

Der Einsatz Künstlicher Intelligenz ist mit besonderen Risiken behaftet. Der Senat unterscheidet zwischen weiterlernenden (»selbstlernenden«) und ausgelernten (»deterministischen«) Systemen.<sup>124</sup> In beiden Fällen mangelt es an einer Nachvollziehbarkeit der Systemausgaben. Mustererkennung, -entwicklung und -anwendung durch ML-basierte Software sind, verstärkt noch bei weiterlernenden Systemen, mitunter selbst für Spezialist:innen nicht mehr nachvollziehbar (blackbox).<sup>125</sup> Wenn aber die Nachvollziehbarkeit nicht gewährleistet ist, ist auch eine Kontrolle des Analyseergebnisses unmöglich.<sup>126</sup> Während diese Unsicherheit bei ausgelernten Systemen durch Test- und Anpassungsprozesse abgemildert werden kann, ist bei weiterlernenden Systemen schlicht nicht zu gewährleisten, dass die Ausgabe eines weiterlernenden Systems sachlich zutreffend ist. Dem Senat zufolge schadet das aber nicht, sofern Sicherungen verfahrensrechtlicher Art bestehen, um ein hinreichendes Schutzniveau zu sichern.<sup>127</sup> Es ist allerdings zweifelhaft, ob solche überhaupt effektiv implementiert werden können, da ja der bestechende Vorteil von automatisierten Datenanalysen, zumal KI-gestützter, doch gerade die maschinelle Überflügelung menschlicher Sichtung- und Beurteilungsfähigkeit ist. Mit dem Bundesverfassungsgericht ist in jedem Fall – entsprechend Art. 11 I JI-RL (§ 54 I BDSG) – eine menschliche Überprüfungsinstanz (human in the loop) zwischen die automatisierte Entscheidung und Rechtsakte mit Außenwirkung zu »schalten«. Das korrespondiert mit dem datenschutzrechtlichen Grundsatz der Datenrichtigkeit aus § 5 I d) DSGVO, Art. 4 I d) JI-RL (§ 47 Nr. 4 BDSG). Allerdings garantiert auch diese menschliche Supervision die inhaltliche Richtigkeit der Entscheidung nicht. Erinnerung sei

---

123 EuGH, Urt. v. 21.12.2016, C-203/15, C-698/15, *Tele2 Sverige AB gegen Post -och telestyrelsen und Secretary of State for the Home Department gegen Tom Watson u. a.*, ECLI:EU:C:2016:970, Rn. 120; vgl. auch EuGH, Urt. v. 21.06.2021, C-817/19, *Ligue de droits humains gegen Conseil de ministres*, ECLI:EU:C:2022:491, Rn. 215; BVerfGE 155, 119 (229 ff.).

124 BVerfGE 165, 363 (408 f.).

125 EuGH, Urt. v. 21.06.2021, C-817/19, *Ligue de droits humains gegen Conseil de ministres*, ECLI:EU:C:2022:491, Rn. 195; BVerfGE 115, 320 (343); Rademacher/Perkowski 2020, S. 716 f.; Sommerer 2020, S. 195 f., 202 f.

126 Ferguson 2017, S. 1170 f.; Kugelmann/Buchmann 2024, S. 9 f.

127 BVerfGE 165, 363 (408 f.).

einerseits an den automation bias.<sup>128</sup> Als automation bias bekannt ist das Phänomen des regelmäßigen Vertrauensvorschlusses für die vermeintlich objektive Technizität von Entscheidungsunterstützungssystemen und ihren Ausgaben (nun auch Art. 14 IV b) KI-VO). Ob ein solcher Vertrauensvorschluss gerechtfertigt ist oder ob möglicherweise Verdrängungs- und Ausnutzungseffekte sowie reproduzierte Verzerrungen die Effektivität der Anwendung mindern<sup>129</sup>, können Nutzer:innen nur bei hinreichender Transparenz der maschinellen Entscheidungsfindungsprozesse überprüfen.<sup>130</sup> Die Signifikanz auch nur einer bloßen Systemempfehlung für menschliche Letztentscheidungen sollte daher nicht unterschätzt werden. Andererseits liegt der bestechende Vorteil automatisierter Datenanalysen ja gerade in der Produktion »neuen« und daher durch einzelne Beamte nur schwer eigens erzeugbaren Wissens. Es fehlt also am rein menschlich erzeugten Vergleichswissen. Daher muss der Verfahrensschutz deutlich weiterreichen. Vorgeschlagen wurde mitunter ein grundsätzliches Verbot nicht nachvollziehbarer Systeme.<sup>131</sup> Ein solches wäre zweifelsfrei die einfachste und sicherste Option, um nachteiligen Folgewirkungen aufgrund intransparenter Erwägungen künstlicher Agenten vorzubeugen. Dies entspricht aber nicht dem Urteil zur automatisierten Datenanalyse. Als hinreichend zu erachten wäre daher eine behördeninterne und externe Kontrolle (sprich: Datenschutzbeauftragte), die wiederum Grundlage für den Individualrechtsschutz ist.<sup>132</sup> Zu ergänzen wäre dies durch substanzielle Schulungen des zur Analyse befugten Personals, jedenfalls hinsichtlich der Funktionsweise der Software und des *automation bias*.

### 2.2.3.1 Ausschluss kontinuierlich weiterlernender Systeme

Mehr noch erfahren wir aus dem Datenanalyseurteil zu Künstlicher Intelligenz: Selbstlernende Systeme dürfen nicht im Gefahrenvorfeld eingesetzt werden. Und außerdem ist der Einsatz solcher Systeme auch zur Abwehr konkretisierter Gefahren nur unter einschränkenden Bedingungen möglich. Vor allem dürfen weiterlernende Systeme dem Senat nach nur zum Einsatz kommen, wenn besondere verfahrensrechtliche Vorkehrungen ein hinreichendes Schutzniveau trotz der eingeschränkten Nachvollziehbarkeit der Systeme sichern.<sup>133</sup> Es ist also letztlich nur ein sehr beschränktes, punktuelles Weiterlernen möglich. Das wäre praktisch

128 Ferguson 2012, S. 402 f.; Singelstein 2018, S. 4; Haouache, in: Beck/Stember 2020, S. 28; Rademacher/Perkowski 2020, S. 717; Rademacher, in: Zimmer 2021, S. 250 f.; Psychologische Einordnung bei Bahner 2008, S. 40 ff.

129 Singelstein 2018, S. 4.

130 Rademacher, in: Zimmer 2021, S. 250.

131 Rademacher/Perkowski 2020, S. 720; Ruf 2024, S. 9.

132 Singelstein 2018, S. 7.

133 BVerfGE 165, 363 (408).

so vorzustellen: Bei Vorliegen einer konkretisierten Gefahr für besonders hochrangige oder gewichtige Rechtsgüter löst eine Beispielpolizistin eine Analyse aus, die sich aus den zugänglichen Datentöpfen personenbezogene Daten »zieht« (die Schaffung einer Verarbeitungsgrundlage vorausgesetzt: auch Daten Unbeteiligter<sup>134</sup>). Im Laufe des Analyseprozesses lernt die Software weiter, untersucht also die Datenmengen nach Mustern, normativiert sie und wirft anhand der erkannten Muster Ergebnisse aus (Stichwort: offene Suchen in personenbezogenen Daten zur Mustererkennung zum Zweck der Gefahrenabwehr). Die Anwenderin kann aber nicht nachvollziehen, wie die Software zu ihrem Ergebnis gekommen ist. Dem Senat zufolge schadet das nicht, sofern hinreichende Sicherungen verfahrensrechtlicher Art bestehen (s.o.). Die erlernten Muster müssten allerdings gleich wieder verworfen werden. Denn wenn diese weiterverwendet werden, entfällt der konkrete Gefahrenbezug, und es liegt ein unzulässiger Gefahrenvorfeld-eingriff vor, bei dem der Einsatz selbstlernender Systeme seitens des Ersten Senats ausgeschlossen wurde (s.o.). Kontinuierliches Weiterlernen, mitunter mit Polizeidaten Unbeteiligter, ist somit untersagt.

#### *2.2.3.2 Ausschluss selbstständiger Recherchen im Internet*

Auch Analysetools mit Internetzugriff müssen als unzulässig betrachtet werden. Zunächst dürfte eine derartige Software deutlich anfälliger für Angriffe von außen sein, sodass die System- und Datenintegrität (Art. 5 I DSGVO, Art. 4 JI-RL, § 47 BDSG, § 42 HDSIG) nicht gewährleistet werden kann. Verfassungsrechtlich einschlägig wäre insofern das IT-Grundrecht. Mit einem weiten Verständnis des Telekommunikationsgeheimnisses, das den Schutzbereich auf netzwerköffentliche Kommunikation erstreckt, wären auch social media Daten vor der Durchsichtung und Weiterverarbeitung durch Analysetools geschützt.

#### *2.2.4 Umgang mit spezifischen Diskriminierungsrisiken*

Besonders eingriffsintensiv sind zudem auch Datenanalysen, denen spezifische Diskriminierungsrisiken inhärent sind. Dem Ersten Senat lag mit der Verfas-

---

<sup>134</sup> Auch weiterlernende Systeme erzeugen kein neues personenbezogenes Wissen, selbst wenn sie anhand der Daten Unbeteiligter weiterlernen. Das bedeutet, dass die Daten Unbeteiligter auch hier eingespielt werden dürfen. Denn durch den maschinellen Lernprozess findet eine »Übersetzung« der personenbezogenen Daten in mathematische Variablen statt, die einen unmittelbar nachvollziehbaren Personenbezug auflöst, vgl. Hüger 2024, S. 277 f. zu LLMs, mitunter auch zum Problem des overfittings. Das bedeutet, dass nach den Maßgaben des Urteils zur automatisierten Datenanalyse keine spezifische Eingriffsintensität vorliegt, die das Weiterlernen mit Daten Unbeteiligter per se ausschließen würde. Es fehlt gleichwohl an einer Verarbeitungsgrundlage.

sungsbeschwerde kein »Auftrag« für die Prüfung von Gleichheitsrechten vor. Dennoch erwähnt das Datenanalyseurteil Diskriminierungsrisiken ausblickhaft. Diese seien »verfassungsrechtlich umso weniger hinzunehmen [...], je mehr sich die Wirkungen der automatisierten Datenanalyse oder -auswertung einer nach Art. 3 Abs. 3 GG unzulässigen Benachteiligung annähern könnten«<sup>135</sup>. Konkretere Vorgaben macht der Senat nicht und lässt insbesondere offen, ob nur erhöhte Rechtfertigungsanforderungen bestehen oder ob, beziehungsweise ab wann Analysen mit diskriminierender Wirkung den Rahmen des verfassungsrechtlich duldbaren überschreiten. Es lohnt sich gleichwohl, hier etwas genauer hinzuschauen. Denn der künftige Einsatz von Big Data bei der Polizei wird sich auch am Antidiskriminierungsrecht messen lassen müssen.

#### 2.2.4.1 Spezifische Diskriminierungsrisiken in der Trainingsphase

Der automatisierten Datenanalyse inhärent sind spezifische Diskriminierungsrisiken. Um dies zu begreifen, ist ein zumindest rudimentäres Verständnis der zugrundeliegenden Technik erforderlich. Wichtig ist hier die Unterscheidung zwischen ausgelerntem und lernendem System. Bei ersterem ist das Training vor Auslösung der Datenanalyse abgeschlossen. Die Analysesoftware durchsucht und sortiert Daten nur nach bereits bekannten Mustern. Das hohe Diskriminierungsrisiko liegt in jedem Fall (lernendes und ausgelerntes System) in der Normativierung von erkannten Mustern begründet. Während des Trainings werden Technologien zur Mustererkennung instruiert, vorliegend in Bezug auf Muster die im Trainingsprozess als Indikatoren für einen polizeilich relevanten Umstand ausgewiesen wurden.<sup>136</sup> Bereits hier, das heißt bei der Datensammlung, -auswahl und dem data-object linking, finden Auswahlprozesse statt, die regelmäßig diskriminierungsrelevant verzerrt sind.<sup>137</sup> Dem System wird ein algorithmischer bias antrainiert: Denn zunächst funktioniert Software besonders gut für Daten, mit denen trainiert wurde.<sup>138</sup> Enthalten also die Trainingsdaten beispielsweise überwiegend Informationen zur Täterhistorie von Menschen mit geringem Bildungsabschluss, wird das System solche später gut erkennen können, Akademiker:innen jedoch tendenziell übersehen.<sup>139</sup> Künstliche Intelligenz, genauer: ML, sucht im Trainingsprozess zudem selbst nach neuen mathematischen Formeln für die erkannten Zusammenhänge (vereinfacht: Achim + Petry

---

135 BVerfGE 165, 363 (400 f.).

136 Rademacher/Perkowski 2020, S. 716.

137 Singelstein 2018, S. 5; Sommerer 2020, S. 174 f.; Lauscher/Legner 2022, S. 371.

138 Lauscher/Legner 2022, S. 371.

139 Calo 2017, S. 412.

+ Bonn = Schlagersänger) und generiert so Suchmuster.<sup>140</sup> Während des Trainingsprozesses, also der Datensammlung, -auswahl und -verlinkung, gehen daher Kontextwissen und damit Feindifferenzierungen zunehmend verloren.<sup>141</sup> Die Algorithmen verarbeiten ergo nur eine simplifizierte, bruchstückhafte Wirklichkeitswahrnehmung. Der Rechtswissenschaftler *Dan Burk* von der UC Irvine formulierte insofern, Muster und Bewertungen würden weniger entdeckt als konstruiert.<sup>142</sup> Diese Konstruktionen können diskriminierungssensibel sein. Vereinfacht: Erkennt eine Künstliche Intelligenz Achim als Vornamen für eine männliche Person und zudem noch Roland, Rex und Roy, dann verknüpft sie das Attribut »Schlagersänger:in« möglicherweise mit dem männlichen Geschlecht. Man spricht hierbei vom *overfitting*, was die Ableitung allgemeingültiger Kausalitätsbeziehungen aus Korrelationen durch den Algorithmus meint.<sup>143</sup> Eine Helene wird aus der Kategorie dementsprechend ausgeschlossen, Männer wahrscheinlicher als Schlagersänger eingeordnet. Was für Schlagerfans allemal bedauernswert sein dürfte, bedeutet fernab von diesem harmlosen Beispiel für Menschen mit dem Namen Amri, Muhammad oder Husain realiter schlechthin ein erhöhtes Potential, Ziel algorithmischer Beobachtung zu werden.

Das ist mit dem Diskriminierungsverbot nach Art. 3 III 1 GG in dieser Generalität schwer vereinbar. Diskriminierung kann also schon »vorprogrammiert« sein, nämlich wenn der Algorithmus in die Zielfunktion Variablen einbezieht, die an die nach Art. 3 III 1 GG verbotenen Merkmale anknüpfen.<sup>144</sup> Eine entsprechende Anknüpfung an *proxies*<sup>145</sup> muss als mittelbare Diskriminierung gelten. Es muss daher überwacht werden, wie die Software im Rahmen ihrer Wirklichkeitskonstruktion diskriminierungssensible Zusammenhänge normativiert.

#### 2.2.4.2 Diskriminierungsanfälligkeit des »neuen Wissens«

Auch das »neue Wissen« an sich ist diskriminierungsanfällig. Analysetools wirken zunächst aufmerksamkeitssteuernd. Wenn etwa *heat maps* spezifische Orte als verbrechensgeneigt kennzeichnen, werden Beamte nachvollziehbarerweise geneigt sein, diese Orte verstärkt zu kontrollieren. Dann werden andere Orte möglicherweise nicht mehr kontrolliert. Das bedeutet, dass durch Big Data-Analysen selektiv jene Phänomene stärker kontrolliert werden, die ohnehin schon der Kontrolle unterliegen.<sup>146</sup> Bei diesem »technologischen Generalverdacht« kann

140 Hölzer/Natterer, in: Kersting/Lampert/Rothkopf 2019, S. 141; Burk 2021, S. 1159.

141 Burk 2021, S. 1158.

142 Burk 2021, S. 1158.

143 Sommerer 2020, S. 175.

144 Lauscher/Legner 2022, S. 372.

145 Lauscher/Legner 2022, S. 372; wohl a. A. bei Rademacher, in: Zimmer 2021, S. 264.

146 Ferguson 2012, S. 401 f.

es Überschneidungen zu Diskriminierungsmerkmalen geben. Aus den USA bekannt ist das Problem der häufigen Korrelation von Wohnorten mit Hautfarbe.<sup>147</sup> Problematisch in Deutschland wäre im Hinblick auf das Verbot von Diskriminierungen aufgrund religiöser Zugehörigkeit und rassistischer Diskriminierung eine dementsprechende Aufmerksamkeitsverschiebung auf muslimische Glaubensstätten und ihr Umfeld. Das ist angesichts eines prävalenten Anti-Terror-Diskurses<sup>148</sup> nicht unwahrscheinlich.

Die aufgezeigten Probleme entstehen bei beiden Varianten der Produktion »neuen Wissens«, also Verknüpfungs- und Sortierungswissen. Sowohl »ausgelernte« als auch weiterlernende Systeme werden Daten zunächst nach den dargestellten Parametern strukturieren und aufbereiten. Das sortierte Wissen ist biased, da Zielfunktionen für verschiedene soziale Gruppen unterschiedlich (gut) funktionieren. Bei Verknüpfungswissen besteht diese Gefahr ebenso: Die als »Vorstufe«<sup>149</sup> zum Predictive Policing erzeugten Sach- und Personendossiers enthalten als Produkte der dargestellten technischen Prozesse notwendigerweise Verzerrungen. Algorithmische Sachverhaltsergänzung bedeutet zusätzliche Aggravation. Gemeint ist der Fall der Generierung neuer Informationen aus den vorhandenen Daten, etwa bei der Ergänzung von Persönlichkeits- oder Bewegungsprofilen oder »echter« prädiktiver Funktionen wie der Generierung von »Gefährderscores«<sup>150</sup>. Denn ein erzeugtes digitales inter alias ist mehr ein lückenhafter Abriss der dahinterstehenden Person als ein vorhersagesicheres Kriminalprofil<sup>151</sup>; personenbezogene Gefährlichkeitsaussagen sind diskriminierungs- und fehleranfällig.

#### 2.2.4.3 Verbot diskriminierender Analyseverfahren

Europa- und Verfassungsrecht enthalten ein Verbot diskriminierender Analyseverfahren. Der europarechtlich vorgeprägte Profiling-Begriff aus Art. 11 III JI-RL umfasst zunächst jede Verwendung personenbezogener Daten, mit der persönliche Aspekte analysiert oder vorhergesagt werden. Dieser ist prozessbezogen.<sup>152</sup> Automatisierte Analysen personenbezogener Daten fallen unter den Profiling-Begriff. Damit gilt das Diskriminierungsverbot des Art. 11 III JI-RL. Die Umsetzungsakte der JI-RL haben gleichwohl nur den Rang einfachen Rechts; es verbie-

147 Rademacher/Perkowski 2020, S. 716.

148 Hiller/Schneider 2018, S. 246 ff.

149 Sommerer 2020, S. 97.

150 hessenDATA generiert keine Gefährderscores, der Hinweis bezieht sich auf Big Data-Analysen im Allgemeinen.

151 Burk 2021, S. 1160.

152 Vgl. Singelstein 2018, S. 8.

tet sich normhierarchisch grundsätzlich, aus dem einfachen Recht verfassungsrechtliche Maßgaben abzuleiten.

Die Grundrechte wirken allerdings entsprechend. Art. 3 III 1 GG stellt auf Benachteiligungen und Bevorzugungen, mithin auf Unterscheidungen ab. Im vorliegenden Kontext ist fraglich, ob eine solche Unterscheidung schon in Gestalt der Datenverarbeitung oder erst beim Tätigwerden der Behörde gegenüber Grundrechtsträger:innen vorliegt. Parallel zur Dogmatik zum Grundrecht auf informationelle Selbstbestimmung ist schon die Verarbeitung sensibler Daten als Hoheitsakt mit Eingriffsqualität zu werten. Daraus folgt ein zweistufiger Schutz gegen Diskriminierung. Zunächst muss das System von Verzerrungen und bias befreit werden. Das gilt auch für die Unterscheidungen anhand von proxies.<sup>153</sup> Automatisierte Datenanalysen, die auf der Basis von ML trainiert wurden, sind, wie oben erläutert, besonders diskriminierungsanfällig. Daher sind bereits im Trainingsprozess Vorkehrungen gegen diskriminierende Musterbildung und Zuschreibungen zu treffen. Auch das Analyseverfahren selbst muss dann frei von Diskriminierung sein. Analysen, die anhand verbotener Merkmale unterscheiden, stellt das Benachteiligungsverbot unter Rechtfertigungsvorbehalt.<sup>154</sup> Die Verwendung diskriminierender Kategorien und ihrer proxies muss jedenfalls zur Erreichung eines legitimen Zwecks erforderlich sein. Die Rechtfertigung der Ungleichbehandlung ist nur durch kollidierendes Verfassungsrecht möglich – wozu allerdings die Öffentliche Sicherheit durchaus zählt. Demnach müssten entsprechende Verfahren bei Vorliegen einer hinreichend konkretisierten Gefahr für die Öffentliche Sicherheit zulässig sein.<sup>155</sup> Doch kann man den verfassungsrechtlichen Diskriminierungsschutz auch umfassender verstehen.<sup>156</sup> Ausgelegt als asymmetrisches Gleichheitsrecht enthält Art. 3 III 1 GG ein Verbot menschenwürderelevanter Unterscheidungen. Parallel zum Diskriminierungsverbot der JI-RL wären solche dann nicht rechtfertigungsfähig. Das bedeutet, dass Unterscheidungen, die soziale Ungleichheiten aktualisieren, also etwa eine Benachteiligung aufgrund rassistischer, religiöser oder Geschlechtszuschreibung, nicht gerechtfertigt werden können. Daher dürfen automatisierte Datenanalysen nicht entlang dieser diskriminierungssensiblen Kategorien durchgeführt werden.<sup>157</sup> Zum Vergleich könnte das FlugDaG herangezogen werden: In § 4 III 7 FlugDaG heißt es, dass »Angaben zur rassischen oder ethnischen Herkunft, zu den politischen Meinungen, zu den religiösen oder weltanschaulichen

---

<sup>153</sup> Arzt 2023, S. 999.

<sup>154</sup> Baer/Markard, in: Huber/Voßkuhle 2024, Art. 3 Abs. 2 und 3 GG, Rn. 432 f.

<sup>155</sup> BVerfGE 165, 363(4. LS); Ruf 2024, S. 9.

<sup>156</sup> Eingehend zur Gleichheitsdogmatik und insbesondere der Herausbildung eines materialen, das heißt wirklichkeitsbezogenen Diskriminierungsbegriffes Rabe 2024, S. 91 ff.

<sup>157</sup> Rademacher 2017, S. 406 f.

Überzeugungen, zur Mitgliedschaft in einer Gewerkschaft, zum Gesundheitszustand, zum Sexualleben oder zur sexuellen Orientierung einer Person« nicht Gegenstand eines durch die Muster herausgebildeten Prüfungsmerkmals des automatisierten Datenabgleichs sein dürfen. Gleiches muss für automatisierte Datenanalysen zur Gefahrenabwehr gelten. Wo hier die Grenze zu ziehen ist, ist allerdings schwer zu bestimmen, da letztlich alle Diskriminierungsmarker des Art. 3 III 1 GG mit der Menschenwürde verknüpft sind. Art. 3 III 1 GG ist kein verfassungsrechtlicher »Trumpf«. Letztlich muss es also bei einer Rechtfertigungsprüfung und damit einer Abwägungsentscheidung zwischen dem individuellen Diskriminierungsschutz und der Erforderlichkeit der jeweiligen Analysemaßnahme für den akuten Schutz der Öffentlichen Sicherheit bleiben. Mit dem obiter dictum des Ersten Senats ist Art. 3 III 1 GG aber sehr ernst zu nehmen und im Zweifel stärker zu gewichten.

### 3. Ausblick

Abseits der dargestellten Zulässigkeitsgrenzen verbleibt gesetzgeberischer Ausgestaltungsspielraum. Es bleibt abzuwarten, wie die Bundesländer und auch der Bund selbst diesen nutzen. Der hessische Landtag versuchte eine Neuregelung durch das »Gesetz zur Stärkung der Inneren Sicherheit in Hessen«<sup>158</sup> bereits im Dezember 2024. Unter anderem die Befugnisse zum Einsatz von Künstlicher Intelligenz wurden durch dieses ausgeweitet. Dass verfassungsrechtliche Vorbehalte auch gegenüber dieser »neuen« Neufassung bestehen, führt *Christopher Giogios* in seinem Beitrag zu diesem Band aus. Die Lage ist dynamisch. Die Gesellschaft für Freiheitsrechte hat auch gegen die (alte) Neufassung des § 25a HSOG Verfassungsbeschwerde erhoben.<sup>159</sup> Die Vorschrift wird abermals am Verfassungsrecht, das heißt neben dem Grundrecht auf informationelle Selbstbestimmung auch an den Grundsätzen der Wesentlichkeit, Normklarheit und Bestimmtheit sowie Art. 10 GG zu messen sein (Art. 3 GG wurde von den Beschwerdeführenden nicht gerügt). Da auch andere Bundesländer und die Bundespolitik derzeit (Verbund-)Lösungen für Analysesysteme diskutieren, wird der Diskurs um *Big Data* und die Grundrechte so schnell nicht abreißen. Ein weiterer Streitpunkt hierbei ist die Herkunft von Programmen. *hessenDATA* ist ein Ableger der Software *Gotham* des amerikanischen Unternehmens *Palantir*. Die deutsche Tochterfirma

---

158 GVBl. HE, Nr. 83.

159 Verfassungsbeschwerde v. 21.06.2024, abrufbar unter <https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf> (01.10.2025).

Palantir Technologies GmbH hat Medienberichten zufolge im Jahr 2019 eine Umsatzsteigerung von 133 %, das heißt auf 28,3 Millionen Euro, erwirtschaftet.<sup>160</sup> Palantir könnte sich bei Abruf durch Bund und Länder unter dem mit der bayerischen Polizei abgeschlossenen Mantelrahmenvertrag zum Monopolisten mit absoluter Preishoheit im Bundesgebiet entwickeln. Der Senat mahnte insoweit im Datenanalyseurteil an, dass beim Softwareankauf aus privater Hand zahlreiche Opazitätsprobleme bestünden, nämlich eine Gefahr »unbemerakter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte«<sup>161</sup>. Das kann auch beim Ankauf von Palantir-Produkten nicht ausgeschlossen werden.<sup>162</sup> Insoweit ist die Feststellung<sup>163</sup> der Innenministerkonferenz, dass eine digital souveräne Lösung anzustreben sei, zu begrüßen.

## Quellen und Literatur

- Arzt, Clemens, »Polizeiliche Verarbeitung »besonderer Kategorien personenbezogener Daten«, in: *Die Öffentliche Verwaltung (DÖV)* 2023, S. 991–1002.
- Barczak, Tristan (Hg.), *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*, Baden-Baden 2023.
- Bahner, Jennifer Elin, *Übersteigertes Vertrauen in Automation: Der Einfluss von Fehlererfahrungen auf Complacency und Automation Bias*, Berlin 2008.
- Bartsch, André, »Welche Daten? Zur geplanten Einführung automatisierter Datenanalysen bei BKA, Bundespolizei und Staatsanwaltschaften«, in: *Verfassungsblog*, 30.8.2024. <https://verfassungsblog.de/bka-gesetz-referentenentwurf-automatisierte-datenanalyse/> (01.10.2025).
- Bäuerle, Michael, *Das Informationsrecht der Sicherheitsbehörden zwischen Konstitutionalisierung und Europäisierung*, Frankfurt a. M. 2024.

---

160 S. POLICE-IT, »Fragen an deutsche Polizeibehörden zu Big-Data-Analysesystemen von Palantir«, POLICE-IT, 07.09.2021. <https://police-it.net/fragen-an-polizeibehoerden-zu-palantir-analysesystemen> (01.10.2025); der Bericht stellt auf den im Unternehmensregisterverzeichnis nicht mehr einsehbaren Jahresabschlussunterlagen ab.

161 BVerfGE 165, 363 (407).

162 Zwar konnte das Fraunhofer Institut für Sichere Informationstechnologie bei der bayerischen »Softwareschwester« VeRA keine sogenannte Backdoor (Funktionen im Softwareprogramm, die bei einer Anmeldung an, ggf. selten verwendeten, Ports unter Umgehung der üblichen Autorisierungsmechanismen Zugriff gewähren) identifizieren, so das Bayerische Landeskriminalamt in einer Pressemitteilung v. 8.3.2023. Die (nicht veröffentlichte) Untersuchung bezog sich aber nur auf Teile der Software und kann insbesondere Aktualisierungen technisch nicht abdecken; vgl. Ruf 2024, S. 10. Das bedeutet, dass Datenabflüsse weder während des Softwarebetriebs noch im Rahmen der Anpassungsarbeiten seitens Palantir ausgeschlossen werden können.

163 IMK, Beschlüsse, 2025, S. 33.

- Burk, Dan L., »Algorithmic Legal Metrics«, in: *Notre Dame Law Review* 96 (2021), S. 1147–1203.
- Calo, Ryan, »Artificial Intelligence Policy: A Primer and Roadmap«, in: *UC Davis Law Review* 51 (2017), S. 399–435.
- Dreier, Horst (Begr.), *Grundgesetz Kommentar*, hrsg. v. Frauke Brosius-Gersdorf, Bd. 1, 4. Auflage, Tübingen 2023.
- Ferguson, Andrew Guthrie, »Big Data and Predictive Reasonable Suspicion«, in: *University of Pennsylvania L. Rev.* 163 (2012), S. 329–410.
- ders., »Policing predictive Policing«, in: *Washington University L. Rev.* 94 (2017), S. 1115–1194.
- Golla, Sebastian, »Algorithmen, die nach Terroristen schürfen – »Data-Mining« zur Gefahrenabwehr und zur Strafverfolgung«, in: *Neue Juristische Wochenschrift* (NJW) 2021, S. 667–672.
- Haouache, Gerold, »Digitalisierung der Verwaltung: Der Einsatz Künstlicher Intelligenz im staatlichen Bereich in Gestalt von Assistenz- und vollautomatisierten Entscheidungssysteme«, in: Beck, Joachim/Stember, Jürgen (Hg.): *Der demographische Wandel*, Baden-Baden 2020, S. 19–34
- Hartmann, Markus/Cipierre, Paula/Beeck, Leonie, »Datamining in der Strafjustiz?«, in: *Recht der Datenverarbeitung (RDV)* 2023, S. 147–152.
- Hiller, Jens/Schneider, Josua, »War on Terror revisited? Das War on Terror-Narrativ als Legitimationsquelle des Syrieneinsatzes im bundesdeutschen Diskurs nach den Terroranschlägen von Paris«, in: *Zeitschrift für Friedens- und Konfliktforschung* (ZeFKo) 2018, S. 246–277.
- Hölzer, Christian/Natterer, Elena, »Big Data, Viele Daten – viel Wissen?«, in: Kersting, Kristian/Lampert, Christoph/Rothkopf, Constantin (Hg.): *Wie Maschinen lernen, Künstliche Intelligenz verständlich erklärt*, Wiesbaden 2019, S. 141–147.
- Huber, Peter M./Voßkuhle, Andreas (Hg.), *Grundgesetz Kommentar*, begründet von v. Mangoldt, Hermann, fortgeführt von Klein, Friedrich und Starck, Christian, 3 Bd.; Bd. 1, 8. Auflage, München 2024.
- Hüger, Jakob, »Die Rechtmäßigkeit von Datenverarbeitungen im Lebenszyklus von KI-Systemen, Zum datenschutzrechtlichen Rechtfertigungsbedürfnis im Rahmen der Entwicklung und des Einsatzes von KI-Systemen nach der DS-GVO und der neuen KI-Verordnung«, in: *Zeitschrift für Digitalisierung und Recht* (ZfDR) 2024, S. 263–291.
- IMK, Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 223. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 11. bis 13.06.25 in Bremerhaven, 2025. [https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2025-06-13\\_DOK/beschluesse.pdf?\\_\\_blob=publicationFile&v=1](https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2025-06-13_DOK/beschluesse.pdf?__blob=publicationFile&v=1) (01.10.2025).
- Kugelman, Dieter/Buchmann, Antonia, »Der Algorithmus und die Künstliche Intelligenz als Ermittler, Zum Rechtsrahmen für sicherheitsbehördliche Datenanalysen und für den Einsatz von Verfahren künstlicher Intelligenz«, in: *Zeitschrift für das Gesamte Sicherheitsrecht* (GSZ) 2024, S. 1–10.
- Kuhlmann, Simone/Trute, Hans-Heinrich, »Predictive Policing als Formen polizeilicher Wissensgenerierung«, in: *Zeitschrift für das Gesamte Sicherheitsrecht* (GSZ) 2021, S. 103–111.
- Lauscher, Anne/Legner, Sarah, »Künstliche Intelligenz und Diskriminierung«, in: *Zeitschrift für Digitalisierung und Recht* (ZfDR) 2022, S. 367–390.
- Löffelmann, Markus, »Verfassungsrechtliche Anforderungen an automatisierte Datenanalysen durch Sicherheitsbehörden«, in: *Juristische Rundschau* (JR) 2023, S. 331–344.
- Löffelmann, Markus, 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) für die mündliche Anhörung des im Innenausschuss des Deutschen Bundestages am 22. April 2024, Ausschussdr. 20(4)418 F, Berlin 2024.
- Manns, Luca, »Automatisierte Datenanalyse für die vorbeugende Bekämpfung von Straftaten«, in: *Legal Tech – Zeitschrift für die digitale Anwendung (LTZ)* 2023, S. 122–144.
- Meinel, Florian, »Legitimation contra Verfahren: Der Beschluss des BVerfG zur parlamentarischen Beratung des Gebäudeenergiegesetzes«, in: *Verfassungsblog*, 09.07.2023. <https://verfassungsblog.de/legitimation-contra-verfahren/> (01.10.2025).
- Möstl, Markus/Bäuerle, Michael (Hg.), *BeckOK Polizei und Ordnungsrecht Hessen*, 34. Edition, München 2025.
- Müller, Michael W./Schwabebauer, Thomas, »Informationsverarbeitung im Polizei- und Strafverfahrensrecht – Ausblick: Chancen und Herausforderungen digitalisierter Polizeiarbeit«, in: Liskan, Hans/Denninger, Erhard (Hg.): *Handbuch des Polizeirechts*, München 2021, Rn. 1336–1350.
- Rabe, Lea, *Nach Parität: Vulnerabilität und Demokratie*, Tübingen 2024.
- Rademacher, Timo, »Predictive Policing im deutschen Polizeirecht«, in: *Archiv des öffentlichen Rechts (AöR)* 2017, S. 366–416.
- ders., »Verdachtsgewinnung durch Algorithmen. Maßstäbe für den Einsatz von predictive policing und retrospective policing bei Gefahrenabwehr bzw. Strafverfolgung«, in: Zimmer, Daniel (Hg.): *Regulierung für Algorithmen und Künstliche Intelligenz*, Tagung an der Universität Bonn am 7. und 8. September 2020, Baden-Baden 2021, S. 229–268.
- Rademacher, Timo/Perkowski, Lennart, »Staatliche Überwachung, neue Technologien und die Grundrechte«, in: *Juristische Schulung (JuS)* 2020, 713–720.
- Ruf, Simone, Stellungnahme zu dem Antrag der Fraktion 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) für die mündliche Anhörung des im Innenausschuss des Deutschen Bundestages am 22. April 2024, Ausschussdr. 20(4)418 D, Berlin 2024.
- Singelstein, Tobias, »Predictive Policing: Algorithmbasierte Straftatprognosen zur vorausschauenden Kriminalintervention«, in: *Neue Zeitschrift für Strafrecht (NStZ)* 2018, S. 1–9.
- Singelstein, Tobias/Stolle, Peer, *Die Sicherheitsgesellschaft*, Soziale Kontrolle im 21. Jahrhundert, 3. Auflage, Wiesbaden 2012.
- ders.: Verfassungsbeschwerde v. 21.06.2024. <https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf> (01.10.2025).
- Sommerer, Lucia, *Personenbezogenes Predictive Policing, Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose*, Baden-Baden 2020.
- Vasel, Johann Justus, »Verfassungsgerichtliche Fesseln? – Das Karlsruher Urteil zur automatisierten Datenanalyse«, in: *Neue Juristische Wochenschrift (NJW)* 2023, 1174–1178.



# Ein Schritt zurück, zwei nach vorn? Die Reform(en) des HSOG im Kontext des Urteils zur automatisierten Datenanalyse

*Christopher Giogios*

## 1. Einleitung

Am 16.02.2023 hat der erste Senat des Bundesverfassungsgerichts zwei Rechtsgrundlagen für die automatisierte Datenanalyse in den Landespolizeigesetzen von Hessen (§ 25a des Hessischen Gesetzes über die Öffentliche Sicherheit und Ordnung) und Hamburg (§ 49 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei für unvereinbar mit dem Recht auf informationelle Selbstbestimmung und damit für verfassungswidrig erklärt.<sup>1</sup> Neben der Feststellung, dass die streitgegenständlichen Vorschriften keine dem spezifischen Eingriffsgewicht solcher Datenanalysen angemessene Eingriffsschwelle enthielten, hat das Gericht auch – am Rande – die Frage des Einsatzes künstlicher Intelligenz adressiert.<sup>2</sup> Die Entscheidung reflektiert daher grundlegende rechtliche und gesellschaftspolitische Herausforderungen: Welches Maß an technologischer Leistungsfähigkeit und Befugnissen der Polizeibehörden ist überhaupt gewollt? Wie kann das Spannungsfeld zwischen notwendiger technischer Ausstattung und der Sorge vor einer Orwell'schen Polizei austariert werden? Und wie lassen sich die zunehmenden technischen Möglichkeiten – vor allem im Bereich der künstlichen Intelligenz – im Polizeirecht sinnvoll gesetzgeberisch abbilden und möglicherweise auch einhegen?

Für diese kontrovers diskutierten Fragen hat sich Hessen auch nach dem Urteil des Bundesverfassungsgerichts als Brennpunkt erwiesen: Zwei Änderungen des HSOG<sup>3</sup> als Reaktion auf das Urteil sowie die europäische KI-Verordnung<sup>4</sup> haben im Ergebnis den Einsatz künstlicher Intelligenz im Bereich der Datenanalyse

---

1 BVerfGE 165, 363.

2 BVerfGE 165, 363 (408, 418).

3 Gesetz zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei v. 29.06.2023, GVBl. HE, S. 456 und Gesetz zur Stärkung der Inneren Sicherheit in Hessen v. 18.12.2024, GVBl. HE, Nr. 83.

4 Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften über künstliche Intelligenz.

(§ 25a HSOG n.F.) sowie der Videoüberwachung (§ 14 HSOG n.F.) im hessischen Polizeirecht ausdrücklich ermöglicht. Mit den neuen Regelungen reißt auch die Kritik nicht ab: Neben kritischen Stimmen in der Rechtswissenschaft hat auch die Gesellschaft für Freiheitsrechte (bereits aufseiten der Beschwerdeführer an der Verfassungsbeschwerde beteiligt, die zum Urteil im Jahre 2023 führte) am 21.06.2024 erneut Verfassungsbeschwerde gegen § 25a HSOG in seiner damaligen Fassung erhoben.

Dieser Beitrag wird die Kernaussagen des Urteils als Ausgangspunkt nehmen, um die verfassungsrechtlichen Anforderungen an solche Systeme und das KI-Verständnis des Bundesverfassungsgerichts aufzuzeigen (2.). Anschließend werden schwerpunktmäßig die Auswirkungen des Urteils diskutiert: Die Neufassungen des HSOG und der diesbezügliche Einfluss der KI-Verordnung werden dabei ebenso in den Blick genommen wie die erneute Verfassungsbeschwerde gegen § 25a HSOG (3.). Schließlich soll versucht werden, innerhalb größerer rechtlicher Entwicklungslinien einen Ausblick auf künftige Regulierungsvorhaben aufzuzeigen (4.).

## 2. Nach »Automatisierte Datenanalyse I«

### 2.1 Hintergrund der Entscheidung: die Software hessenDATA und ihre Rechtsgrundlage

Die Entscheidung des Bundesverfassungsgerichts betraf in Hessen mit § 25a HSOG a. F. eine Vorschrift, die in dieser Fassung im Jahre 2018 in Kraft getreten war und als Rechtsgrundlage für die bereits seit 2017 verwendete Analysesoftware hessenDATA diente. Technisch handelt es sich hierbei um die hessische Ausführung des Produkts »Gotham« des US-amerikanischen Softwareanbieters Palantir Technologies Inc.<sup>5</sup> Nach § 25a a. F. konnten die Polizeibehörden zur vorbeugenden Bekämpfung von schweren Straftaten im Sinne von § 100a Abs. 2 der Strafprozessordnung oder zur Abwehr von Gefahren für besonders wichtige Rechtsgüter (z. B. die Sicherheit des Bundes, aber auch Leib, Leben oder Freiheit einer Person) ihre bereits vorhandenen personenbezogenen Daten<sup>6</sup> mithilfe einer automatisierten Datenanalyse weiterverarbeiten (Abs. 1). Die automatisierte

---

<sup>5</sup> Vgl. HessDrs. 19/6864, S. 17; zu Palantir und der politischen Positionierung seiner Unternehmensführung s. Brenneis/Denker/Gehring, in diesem Band, S. 225 ff.

<sup>6</sup> Entscheidend ist dabei, dass auf Grundlage von § 25a HSOG bzw. mithilfe von hessenDATA keine neuen Daten erhoben werden; es handelt sich also nicht um eine Befugnisnorm zur Erhebung neuer personenbezogener Daten, vgl. HessDrs. 19/6502, S. 41.

Datenanalyse selbst wurde zwar nicht gesetzgeberisch definiert, zumindest aber in Abs. 2 das Ziel solcher Daten(weiter)verarbeitungsmaßnahmen formuliert: Diese sollten es den Polizeibehörden ermöglichen, neues Wissen in Form von Beziehungen oder Zusammenhängen zwischen Personen oder Personengruppen, aber auch Objekten und Sachen zu erzeugen und gleichzeitig unbedeutende Informationen auszuschließen (Abs. 2).

In der Gesetzesbegründung hat der Gesetzgeber schon seinerzeit deutlich gemacht, dass es bei der Nutzung von hessenDATA in erster Linie darum gehe, das »unverbundene Nebeneinander« zahlreicher polizeilicher Informationssysteme zu beenden und die Vernetzung und Durchsuchung verschiedener Datentöpfe zu erleichtern.<sup>7</sup> Plastisch ausgedrückt: Mit Hilfe von hessenDATA können mit einer einzigen Abfrage verschiedene Datenbestände der Polizei (insbesondere: POLAS, das polizeiliche Auskunftssystem für »repressive Daten«, CRIME, eine Datenbank für »präventive« Daten zukünftiger Ermittlungsverfahren, ComVor, das polizeiliche Vorgangsbearbeitungssystem, in dem alle polizeilichen Vorgänge geführt werden, sowie weitere externe Datenquellen, also Daten aus Funkzellenabfragen oder forensische Extrakte aus sichergestellten Mobilfunkgeräten)<sup>8</sup> gleichzeitig durchsucht werden, anstatt mehrere Abfragen der einzelnen Datenbestände durchführen zu müssen. Daten aus sozialen Netzwerken werden zwar nicht automatisch in das System einbezogen, können allerdings ebenfalls händisch eingepflegt werden.<sup>9</sup>

Während Palantir Gotham in Hessen auf Grundlage von § 25a HSOG a. F. bereits seit geraumer Zeit im Einsatz war, gab es in Hamburg mit § 49 HmbPolDVG

---

7 S. HessDrs. 19/6502, S. 40; vgl. auch Zeugenaussage einer Palantir-Mitarbeiterin im Untersuchungsausschuss 19/3, HessDrs. 19/6864, S. 17: »Wir haben eine Software entwickelt, die strukturierte und unstrukturierte Daten integriert und somit Kunden unterstützt, ihre eigenen Daten, ihre bereits vorhandenen Daten, besser verstehen und besser anwenden zu können.«

8 S. HessDrs. 19/6864, S. 18.

9 Vgl. Arzt 2021, Rn. 1304.

lediglich eine nahezu wortgleiche<sup>10</sup> Rechtsgrundlage, jedoch noch keinen auf dieser Vorschrift beruhenden Einsatz der Software.<sup>11</sup>

## 2.2 Eingriffsgewicht und Eingriffsschwelle als gesetzgeberische Stellschrauben

Im Rahmen der für diesen Beitrag maßgeblichen Prüfung der verfassungsrechtlichen Rechtfertigung der automatisierten Datenanalyse als rechtfertigungsbedürftigem Grundrechtseingriff geht das Bundesverfassungsgericht zweischrittig vor. Es verortet das Eingriffsgewicht der automatisierten Datenanalyse insgesamt einerseits im Gewicht der vorgeschalteten Datenerhebungseingriffe, attestiert darüber hinaus aber auch der automatisierten Datenanalyse selbst ein eigenes Eingriffsgewicht.<sup>12</sup> Wie von *Lea Rabe* bereits an anderer Stelle treffend beschrieben,<sup>13</sup> wiederholt das Gericht im ersten Schritt daher zunächst die Grundsätze seiner Judikatur zum Recht auf informationelle Selbstbestimmung und legt dabei die bekannten Rechtfertigungsanforderungen nach den Grundsätzen der zweckwahren und zweckändernden Weiternutzung von bereits erhobenen Daten dar.<sup>14</sup>

10 Der in Hamburg verwendete Begriff der »Datenauswertung« anstelle der hessischen Formulierung der »Datenanalyse« sollte ausweislich der Hamburger Regierungsfractionen zum einen der Klarstellung dienen, dass im Rahmen von § 49 kein Datenabgleich »in einer unüberschaubaren Anzahl von Fällen« durchgeführt werden sollte, zum anderen, dass keine intelligenten Systeme zur Anwendung kommen, die eine eigene inhaltliche Bewertung eines Datensatzes vornehmen, vgl. Hmb. Innenausschuss Drs. 21/40, Anlage 1, S. 6; dies warf schon seinerseits die Frage auf, ob diese Begrifflichkeit eine solche Klarstellung leisten kann, wenn das System tatsächlich hinsichtlich seiner technischen Leistungsfähigkeit eine Vielzahl von Datenabgleichen durchführt. Mit Wirkung zum 05.02.2025 hat der Hamburger Gesetzgeber eine neue Fassung von § 49 verabschiedet, die nunmehr (ohne nähere Begründung) die hessische Definition der automatisierten Datenanalyse verwendet, GVBl. HH Nr. 6 v. 22.01.2025, S. 183.

11 Auch in Nordrhein-Westfalen wird »Gotham« seit 2020 unter der Bezeichnung »Datenbankübergreifende Analyse und Recherche« (DAR) genutzt, vgl. NRW Drs. 18/1400, S. 1; mit § 23 Abs. 6 PolG NRW wurde im April 2022 nachträglich eine Rechtsgrundlage geschaffen, gegen die ebenfalls aktuell eine Verfassungsbeschwerde der Gesellschaft für Freiheitsrechte anhängig ist, s. Gesellschaft für Freiheitsrechte, Pressemitteilung v. 06.10.2022. <https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-stop-data-mining> (01.10.2025); in Bayern befindet sich »Gotham« nach einer Pilotphase seit dem 25.12.2024 im Echtbetrieb, vgl. Stock, »Palantir als Interimslösung: Bundesrat fordert schnellen Einsatz für die Polizei«, in: *heise online*, 24.03.2025. <https://www.heise.de/news/Palantir-als-Interimslösung-Bundesrat-fordert-schnellen-Einsatz-fuer-die-Polizei-10325605.html> (01.10.2025).

12 BVerfGE 165, 363 (390); treffend Löffelmann 2023b, S. 342: »Die Datenanalyse besitzt somit ein janusköpfiges Aussehen. Sie ist einerseits Datenweiterverarbeitung, andererseits aber auch Datenneugenerierung.«

13 S. Rabe, in diesem Band, S. 17 f.

14 BVerfGE 165, 363 (390 ff.), v.a. mit Verweis auf die Maßstäbe aus dem Urteil zum Bundeskriminalamtgesetz, BVerfGE 141, 220.

Von besonderem Interesse sind allerdings die Belastungseffekte, die einer automatisierten Datenanalyse nach Ansicht des Gerichts immanent sind. Diese seien einerseits im Wesen der automatisierten Analyse selbst begründet, durch die derart große Datenmengen ausgewertet werden können, dass das hierdurch gewonnene neue Wissen »händisch« nicht in vergleichbarer Art und Weise hervorgebracht werden könne.<sup>15</sup> Die Möglichkeit, Daten hierdurch viel intensiver als zuvor zu erschließen und dadurch umfassendere Persönlichkeitsbilder und personenbezogene Vorhersagen zu erstellen (sog. Predictive Policing),<sup>16</sup> erlaube es nicht, diesen neuen Methoden lediglich mit dem Grundsatz der Zweckbindung Rechnung zu tragen.<sup>17</sup> Stattdessen werden eine Reihe von Faktoren genannt, die für die Bestimmung des Eingriffsgewichts maßgeblich sind, und dabei insbesondere auf Art, Umfang und Verwendung der Daten abgestellt.<sup>18</sup> Korrespondierend zu diesem Eingriffsgewicht stellt das Gericht schließlich Maßstäbe für die Ermittlung der jeweiligen Eingriffsschwellen auf, die sich wiederum aus dem mit einer Maßnahme zu schützenden Rechtsgut und dem Anlass einer Maßnahme zusammensetzen.<sup>19</sup> Mit dem Urteil zeigt das Bundesverfassungsgericht daher zwei wesentliche Stellschrauben auf, mit deren Hilfe der Gesetzgeber eine verfassungskonforme Rechtsgrundlage der automatisierten Datenanalyse feinjustieren könne:

- Eine Verringerung des Eingriffsgewichts durch Regelungen, die die Herkunft der Daten beschränken (etwa durch den Ausschluss von Daten aus sozialen Netzwerken), die Datenmenge reduzieren (etwa durch eine Begrenzung von Daten dergestalt, dass sie unbeteiligte Dritte möglichst ausschließt), Einschränkungen bei der technischen Methode vorsehen (etwa einfache Abgleiche, statt mehrstufige Analysen), aber auch durch begleitende Regelungen wie Aufbewahrungs- und Löschrufen.<sup>20</sup>
- Regelungen, die dem Eingriffsgewicht entsprechende Eingriffsschwellen vorsehen und hierdurch einerseits eine anlasslose automatisierte Datenanalyse zur vorbeugenden Bekämpfung von Straftaten ausschließen, andererseits bei schweren Eingriffen in das Recht auf informationelle Selbstbestimmung

---

15 Diesen Belastungseffekten durch das Zusammenführen großer Datenmengen hat das Gericht erstmals in seiner zweiten Entscheidung zum Antiterrordateigesetz Rechnung getragen, s. BVerfGE 156, 11 (56), vgl. Kugelmann/Buchmann 2024a, S. 4; kritisch zu der Annahme, dass eine größere Datenmenge auch ein größeres Eingriffspotential mit sich bringt: Trute 2020, S. 110.

16 Grundsätzlich zum Thema Predictive Policing: Sommerer 2020; Hofmann 2020.

17 BVerfGE 165, 363 (397 f.).

18 BVerfGE 165, 363 (399 ff.).

19 BVerfGE 165, 363 (409).

20 BVerfGE 165, 363 (403); eine anschauliche Umsetzung dieser Regelungsmöglichkeit könnte die neue Hamburger Fassung des § 49 HmbPolDVG darstellen, s. sogleich unter 4.

zumindest eine hinreichend konkretisierte Gefahr für besonders gewichtige Rechtsgüter verlangen.<sup>21</sup>

Gerade das Fehlen einer durch den Gesetzgeber in diesem Sinne ausgestalteten hinreichenden Eingriffsschwelle führte zur Verfassungswidrigkeit der beiden Streitgegenständlichen Vorschriften.<sup>22</sup>

### 2.3 »Ja, aber...«-Entscheidung<sup>23</sup> auch für den KI-Einsatz?

Die Frage des Einsatzes künstlicher Intelligenz im Rahmen der Datenanalyse adressiert das Gericht nur am Rande.<sup>24</sup> Dies hat im Wesentlichen zwei Gründe: Zum einen wurde hessenDATA in seiner damaligen Ausprägung nicht KI-gestützt eingesetzt, weshalb es aus Sicht des Gerichts keine dringende Veranlassung gab, ausführlich zu diesem Thema Stellung zu beziehen; zum anderen gelang es den Beschwerdeführern nicht, substantiiert vorzutragen, dass der Gesetzgeber keine hinreichenden Regelungen getroffen habe, um den Einsatz künstlicher Intelligenz (der nach ihrer Auffassung aufgrund der Methodenoffenheit der Vorschrift durchaus schon seinerzeit möglich gewesen sei) ausreichend organisations- und verfahrensrechtlich abzusichern.<sup>25</sup> Bezogen auf diese Rechtsfrage scheiterten die Beschwerdeführer folglich an den Zulässigkeitschürden des Gerichts.

Gleichwohl nutzte das Bundesverfassungsgericht die Gelegenheit, um zunächst anzudeuten, dass künstliche Intelligenz hinsichtlich des ihr innewohnenden Eingriffsgewichts eine Steigerung der automatisierten Datenanalyse darstelle.<sup>26</sup> Dabei bringen die Richterinnen und Richter ein KI-Verständnis zum Ausdruck, das sich insbesondere durch die Charakteristik des weiterlernenden Systems (im Gegensatz zu deterministischen Systemen), den Grad der Nachvollziehbarkeit des Ergebnisses einer KI-Abfrage durch den Anwender (sog. »black-box«-Phänomen)<sup>27</sup> sowie durch die der Technik inhärenten Diskrimi-

---

21 BVerfGE 165, 363 (4. Leitsatz).

22 BVerfGE 165, 363 (430 f.).

23 Angelehnt an Bäuerle 2025, S. 129.

24 BVerfGE 165, 363 (408).

25 Vgl. Bäuerle 2025, S. 129.

26 BVerfGE 165, 363 (387): »[...] mit Blick auf komplexe Formen automatisierten Datenabgleichs bis hin zu selbstlernenden Systemen (Künstliche Intelligenz, »KI«) [...]«.

27 Zum Problem der »black box« und zum Lösungsansatz der »Explainable Artificial Intelligence« (XAI) vgl. Mehta, »Erklärbare KI: Das Geheimnis der Blackbox lüften«, in: Fraunhofer IAO Blog, 21.11.2023. <https://blog.iao.fraunhofer.de/erklaerbare-ki-das-geheimnis-der-blackbox-lueften/> (01.10.2025).

nierungsrisiken auszeichnet.<sup>28</sup> Dieses KI-Verständnis fügt sich insoweit in die Entscheidungen des Bundesverfassungsgerichts zur Frage der Verknüpfung von Daten(töpfen) ein: Während der Umgang mit der Verarbeitung großer Datenmengen kein gänzlich neues rechtliches Problem darstellt,<sup>29</sup> liegt der Fokus in dieser Entscheidung stärker auf der *Methodik* der Zusammenführung und die dadurch entstehende Belastungswirkung,<sup>30</sup> die nach dem vorliegenden KI-Verständnis durch den Einsatz von KI geradezu zwangsläufig weiter zunimmt. Diesbezüglich stand das Gericht auch unter dem Eindruck eines erst kurz zuvor ergangenen Urteils des Europäischen Gerichtshofs zur Verwendung von Fluggastdaten (sog. PNR-Daten): Hier hatte sich der EuGH explizit mit dem Verweis auf die unzureichenden menschlichen Einwirkungs- und Kontrollmöglichkeiten eines KI-basierten Bewertungsprozesses (und damit verbunden auch die fehlenden Rechtsschutzmöglichkeiten) gegen den Einsatz solcher Technologien ausgesprochen.<sup>31</sup>

Auch wenn sich das Gericht in der Folge nicht weiter zur Frage der künstlichen Intelligenz auslässt, wird zumindest klargestellt, dass der Einsatz solcher Systeme im Vorfeld einer hinreichend konkretisierten Gefahr ausgeschlossen sein muss.<sup>32</sup> Insofern ist es nicht ganz von der Hand zu weisen, wenn *Petra Gehring* an dieser Stelle des Urteils eine gewisse Vagheit beobachtet,<sup>33</sup> die man aus rechtlicher Sicht zwar mit dem klar umfassten Prüfungsgegenstand erklären kann, im Übrigen aber wichtige Fragen aufwirft: Welche Regelungsmöglichkeiten verbleiben dem Gesetzgeber, wenn Technizität zwangsläufig zu einem gesteigerten Eingriffsgewicht führt?<sup>34</sup>

---

28 Zum Umgang mit Diskriminierungsrisiken s. ausführlich den Beitrag von Rabe, in diesem Band, S. 36 ff.

29 Vgl. nur die Entscheidung zur Rasterfahndung, BVerfGE 115, 320 (349 f.).

30 Schon angedeutet in BVerfGE 156, 11 (56), vgl. Fußnote 15.

31 S. EuGH, Urteil vom 21.06.2022, C-817/19, Rn. 194 f.

32 BVerfGE 165, 363 (418); kritisch Vasel 2023, S. 1177, der den Nutzen des KI-Einsatzes gerade im Gefahrenvorfeld bei unbestimmten Suchzielen und großen Datenbeständen verortet.

33 S. Gehring, in diesem Band, S. 109 f.

34 Vgl. Rademacher/Perkowski 2020, S. 715 ff., die bereits einige Zeit vor dem Urteil Kategorien und Kriterien zur Beurteilung solcher Technologien im Polizeieinsatz formuliert haben.

### 3. Vor »Automatisierte Datenanalyse II«

#### 3.1 Erste Neufassung des § 25a HSOG

Die Entscheidung des Bundesverfassungsgerichts hatte neben der Verfassungswidrigkeit der Vorschrift auch die Anordnung ihrer vorübergehenden Fortgeltung lediglich bis zum 30.09.2023 zur Folge. Anschließend wäre die Norm nicht mehr anwendbar gewesen, was den hessischen Gesetzgeber vor die Aufgabe stellte, innerhalb von sieben Monaten eine Rechtsgrundlage für die Weiternutzung von hessenDATA zu präsentieren. Die Neufassung wurde mit dem »Gesetz zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei« vom 29.06.2023<sup>35</sup> geschaffen. Das Gesetz beruhte auf einem Gesetzentwurf zu umfassenderen Änderung des HSOG, der bereits im März 2022 eingebracht worden war.<sup>36</sup> Die nun notwendige Überarbeitung von § 25a HSOG hingegen wurde erst nach dem Urteil und damit am Ende des Gesetzgebungsverfahrens eingeführt; gerade einmal neun Tage vor der Beschlussfassung.<sup>37</sup> Diese zeitliche Dimension wurde auch vor dem Hintergrund der Komplexität der Neuregelung scharf kritisiert und dabei die Frage aufgeworfen, inwieweit die Abgeordneten überhaupt in die Lage versetzt worden sind, sich ein umfassendes Bild von dem Abstimmungsgegenstand machen zu können.<sup>38</sup>

Diese Kritik steht auch in engem Zusammenhang mit dem Umfang der Neufassung, die eine der längsten Vorschriften des gesamten HSOG darstellt. Die Vorschrift in Gänze darzustellen, ginge über die Grenzen dieses Beitrags hinaus; insofern sei auf die Einzelkommentierung von *Michael Bäuerle* sowie die kritische Würdigung von *Lea Rabe* in diesem Band verwiesen.<sup>39</sup> Die neue Regelung sieht nunmehr eine Beschreibung der »automatisierten Anwendung zur Datenanalyse« in Abs. 1 vor und nennt in Abs. 2 die einbezogenen Datenkategorien sowie die Eingriffsschwellen für den Einsatz der Datenanalyse. Abs. 3 enthält die Verpflichtung, eine Verwaltungsvorschrift zu schaffen, die Rollen- und Rechtekonzepte sowie die Kategorisierung und Kennzeichnung von Daten näher ausgestaltet. Der

<sup>35</sup> GVBl. HE, S. 456.

<sup>36</sup> HessDrs. 20/8129 v. 22.03.2022; seinerzeit war für § 25a HSOG zunächst nur eine kleinere redaktionelle Änderung vorgesehen.

<sup>37</sup> HessDrs. 20/11292 v. 27.06.2023

<sup>38</sup> Zum Gesetzgebungsverfahren und seiner zeitlichen Dimension ausführlich und kritisch Bäuerle 2024, Rn. 16 ff.; nur wenige Tage später wurde eine vergleichbare Streitfrage im vielbeachteten Beschluss des Bundesverfassungsgerichts in einem Eilantrag zum Gebäudeenergiegesetz dahingehend entschieden, dass die Teilhabe an der parlamentarischen Willensbildung durch eine zeitlich derart knappe Ausgestaltung des Gesetzgebungsverfahrens durchaus verletzt sein kann, s. BVerfG, Beschluss v. 05.06.2023, 2 BvE 4/23, Rn. 89 ff.

<sup>39</sup> Bäuerle, in: Möstl/Bäuerle 2025, § 25a Rn. 76 ff.; Rabe, in diesem Band, S. 25 ff.

Einsatz der automatisierten Datenanalyse wird sodann in Abs. 4 durch formelle Anforderungen wie eine Zugriffskontrolle sowie Protokollierungs- und Begründungspflichten flankiert und in Abs. 5 schließlich der Anordnung durch eine Behördenleitung sowie der vorherigen Anhörung des hessischen Datenschutzbeauftragten unterworfen.

Ein besonderes Augenmerk soll hier auf die gesetzgeberische Beschreibung der »automatisierten Anwendung zur Datenanalyse« gelegt werden. Diese wird in § 25a Abs. 1 S. 1 und S. 2 als Zusammenführung verschiedener Datentöpfe und die anschließende Weiterverarbeitung zusammengeführter Daten in Form der Verknüpfung, Aufbereitung, Auswertung sowie Anwendung für statistische Zwecke umschrieben.<sup>40</sup> Die so legaldefinierte Methodik soll daher nach dem Verständnis des Gesetzgebers lediglich ein technisches Hilfsmittel der Polizeibehörden darstellen (S. 3). Darüber hinaus soll die automatisierte Datenanalyse gemäß S. 4 und 5 immer anhand anlassbezogener und zielgerichteter Suchkriterien erfolgen, wird in diesem Zusammenhang manuell ausgelöst und läuft regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ab (zum letzten Halbsatz und der jüngsten Änderung s. unter 3.3.1). Diese bloße Beschreibung des eingesetzten Verfahrens macht die vorgenannte politische und zeitliche Problematik des Gesetzgebungsverfahrens deutlich. Der Wortlaut lässt vermuten, dass es dem Gesetzgeber darum ging, hessenDATA in seiner bestehenden Form möglichst nahtlos weiterverwenden zu können und dabei im Wesentlichen eine Beschreibung der gegenwärtigen Funktionsweise in Gesetzes- und Verordnungsform<sup>41</sup> zu gießen, statt die polizeiliche Datenanalyse abstrakt und im Einklang mit den verfassungsrechtlichen Vorgaben zu regeln.<sup>42</sup>

### 3.2 Alte Probleme, neue Verfassungsbeschwerde: § 25a HSOG erneut auf dem Prüfstand

Mit Datum vom 21.06.2024 haben sechs Beschwerdeführerinnen und Beschwerdeführer aus dem Kreis der *Gesellschaft für Freiheitsrechte e. V.*, wie schon im ersten Verfahren vertreten durch den Strafrechtler und Kriminologen *Prof. Dr. Tobias Sin-*

---

40 Auch wenn die Zusammenführung (S. 1) und die anschließende Weiterverarbeitung (S. 2) in § 25a Abs. 1 in verschiedenen Sätzen aufgeführt wird, spricht viel dafür, erst den gesamten Vorgang aus Zusammenführung und Weiterverarbeitung als »automatisierte Anwendung zur Datenanalyse« zu verstehen, ähnlich Weingarten 2024, S. 8.

41 S. VV § 25a HSOG, HessStAnz. 2023, 946.

42 So auch Bäuerle, in: Möstl/Bäuerle 2025, § 25a Rn. 22 f.

*gelstein*, Verfassungsbeschwerde gegen die Neuregelung von § 25a HSOG erhoben.<sup>43</sup>

### 3.2.1 *Im Mittelpunkt der Kritik: zu hohes Eingriffsgewicht, zu unbestimmte Eingriffsschwellen*

Die Beschwerdeführerinnen und Beschwerdeführer bewegen sich, wie in Verfahren im Informationssicherheitsrecht üblich, in unterschiedlichen gesellschaftlichen Bereichen, die (teils auch aufgrund gesicherter Erkenntnisse, dass von ihnen Daten in polizeilichen Datenbanken gespeichert sind) die Vermutung zulassen, dass sie mit einiger Wahrscheinlichkeit Zielperson einer Datenanalyse im Rahmen von § 25a geworden sind und damit ihre Beschwerdebefugnis darlegen können: Personen, die in politischen Strukturen oder der organisierten Fußballszene aktiv sind, Strafverteidigerinnen und Strafverteidiger sowie Journalistinnen und Journalisten, die beruflich als Kontaktpersonen betroffen sein könnten, aber auch Kontaktpersonen aus dem privaten Umfeld der genannten Personen.<sup>44</sup>

Im Kern rügen die Beschwerdeführerinnen und Beschwerdeführer, dass auch die Neufassung von § 25a insbesondere aufgrund der Daten- und Methodenoffenheit der Vorschrift das hohe Eingriffsgewicht von Maßnahmen der Datenanalyse nicht ausreichend einzudämmen vermag. Folglich wird eine Verletzung des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), aber auch des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) geltend gemacht, soweit im Rahmen der Datenanalyse auch Daten aus einer Telekommunikationsüberwachung betroffen sind. Schließlich wird mit Verweis auf das unzureichende datenschutzrechtliche Kontrollkonzept in § 25a auch eine Verletzung der Rechtsschutzgarantie aus Art. 19 Abs. 4 GG gerügt.

Die Verfassungsbeschwerde orientiert sich auf der Ebene der Begründetheit an der bekannten »Waage« von Eingriffsgewicht und Eingriffsschwelle und ist folglich dem Urteil entsprechend zweistufig aufgebaut. Eine wirksame Reduzierung des Eingriffsgewichts können die Beschwerdeführenden nicht erkennen. Nach ihrer Ansicht lasse die neue Regelung vielmehr nahezu alle Gelegenheiten aus, um das Eingriffsgewicht in angemessener Weise zu verringern. Dies zeige sich schon bei den einbezogenen Daten, wofür hier zwei Beispielsfälle zur Veranschaulichung der vorgetragenen Argumentation dienen sollen:

43 s. Gesellschaft für Freiheitsrechte, Verfassungsbeschwerde v. 21.06.2024. <https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf> (01.10.2025).

44 S. Verfassungsbeschwerde v. 21.06.2024, S. 19 ff.; insofern wird auch bereits an dieser Stelle mit der großen Streubreite von derartigen Datenanalyseverfahren argumentiert, die für eine wahrscheinliche Betroffenheit der Beschwerdeführerinnen und Beschwerdeführer sprechen soll, S. 23.

So enthalte § 25a Abs. 2 S. 2 zwar eine abschließende Aufzählung der einbezogenen Datenbestände, diese sei jedoch unzureichend. Es wird vor allem die Einbeziehung von Vorgangsdaten (in Hessen: ComVor, s. unter 2.1.) beanstandet, da gerade ein Vorgangsbearbeitungssystem typischerweise auch Daten von Dritten (z. B. Zeugen oder Unfallbeteiligte) erfasse.<sup>45</sup> Zwar sieht § 25a Abs. 3 Nr. 2 a) S. 4 einen Ausschluss von »Unbeteiligten« vor, worunter der Gesetzgeber Personen versteht, die mit einem polizeilichen Sachverhalt nur zufällig in Berührung stehen.<sup>46</sup> Diese Erläuterung überzeugt die Beschwerdeführenden allerdings nicht, da nach ihrer Ansicht etwa eine Anzeigenerstatterin auch eine »unbeteiligte« Person (also eine Person, die keine Gefahr verursacht oder einer Straftat verdächtig ist) darstelle, gleichzeitig aber auch nicht zufällig in Berührung mit einem relevanten Sachverhalt stehe.<sup>47</sup>

Die behauptete Verletzung des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG (die im ersten Verfahren nicht weiter behandelt wurde, weil die Möglichkeit einer Grundrechtsverletzung nicht ausreichend dargelegt wurde und das Gericht die Prüfung daher an den Hürden der Zulässigkeit scheitern ließ) wird hingegen mit der Einbeziehung von Daten aus Telekommunikationsüberwachungsmaßnahmen begründet (§ 25a Abs. 2 S. 2). Die Weiterverarbeitung solcher Daten sei nicht nur aufgrund der Heimlichkeit ihrer Erhebung besonders schwerwiegend, sondern auch, weil dabei regelmäßig Daten von unbeteiligten Gesprächspartnern einbezogen werden. Auch wenn der Gesetzgeber diesbezüglich in seiner Begründung angegeben hat, dass Inhalte aus solchen Maßnahmen erst nach einer polizeilichen Bewertung in die automatisierte Analyse einbezogen werden und damit einer menschlichen (Inhalts-)Kontrolle unterliegen,<sup>48</sup> bemängeln die Beschwerdeführenden dennoch die fehlende gesetzliche Verankerung dieser Vorgehensweise.<sup>49</sup>

In ähnlicher Weise sei auch die vom Bundesverfassungsgericht geforderte Kennzeichnung von Daten unzureichend: Hierfür existiere im HSOG mit § 20a zwar eine Rechtsgrundlage, die in § 25a jedoch nicht in Bezug genommen werde.<sup>50</sup> Auch das in § 25a Abs. 3 Nr. 2 implementierte Konzept zur Kennzeichnung

---

45 S. Verfassungsbeschwerde v. 21.06.2024, S. 49.

46 S. HessDrs. 20/11235, S. 16.

47 S. Verfassungsbeschwerde v. 21.06.2024, S. 55; man verweist an dieser Stelle auch auf die Ausführungen des hessischen Innenministeriums in der mündlichen Verhandlung des vorausgegangenen Verfahrens. Hier hatte das Ministerium noch vorgetragen, dass es keine polizeilich »Unbeteiligten« gebe, da alle in einem Vorgangssystem eingespeicherten Personen bereits durch den Dokumentationsvorgang »Beteiligte« darstellen würden.

48 S. HessDrs. 20/11235, S. 13.

49 S. Verfassungsbeschwerde v. 21.06.2024, S. 50 f.

50 S. Verfassungsbeschwerde v. 21.06.2024, S. 63; zu den diesbezüglichen Anforderungen des Gerichts s. BVerfGE 165, 323 (424).

erfülle die verfassungsgerichtlichen Anforderungen nicht. Dieses sehe zwar eine differenzierte Bewertung der Kategorisierung und Kennzeichnung personenbezogener Daten anhand des jeweiligen Veranlassungszusammenhangs (je gewichtiger der Veranlassungszusammenhang, desto komplexer darf die automatisierte Datenanalyse erfolgen) und der Grundrechtsrelevanz der erhobenen Daten vor;<sup>51</sup> jedoch legen die Beschwerdeführenden hier wie an anderen Stellen einen besonderen Fokus darauf, neben ihren schwerpunktmäßigen Ausführungen zum Eingriffsgewicht und den unzureichenden Eingriffsschwellen der automatisierten Datenanalyse auch die verfassungsrechtlichen Grundsätze der Wesentlichkeit, Bestimmtheit und Normenklarheit zu bemühen.<sup>52</sup> Insoweit wird grundsätzlich der Standpunkt vertreten, dass sich der an den untergesetzlichen Normgeber übertragene Regelungsbereich lediglich auf organisatorische und technische Details beziehen könne.<sup>53</sup> Hinsichtlich des nach § 25a Abs. 3 S. 2 und 3 durch eine Rechtsverordnung zu regelnden Rollen- und Rechtekonzepts wird sodann gleich in doppelter Hinsicht gerügt, dass der Gesetzgeber nicht nur die Einzelheiten dieser Regelungen umfangreich an den Ordnungsgeber delegiert habe (anstatt die wesentlichen Entscheidungen selbst zu treffen), sondern zusätzlich bereits die Abstraktheit der Vorschrift eine hinreichende Normenklarheit für die betroffenen Bürgerinnen und Bürger vermissen lasse.<sup>54</sup>

Auf der anderen Seite werden auch unzureichende Eingriffs- und Rechtsgüterschwellen bemängelt. Wird die in § 25a Abs. 2 Nr. 1 aufgeführte konkrete Gefahr für besonders gewichtige Rechtsgüter noch als angemessen befunden, kommen die Beschwerdeführenden bei den beiden anderen Eingriffsschwellen für den Einsatz der automatisierten Datenanalyse (die Abwehr konkretisierter Gefahren in § 25a Abs. 2 Nr. 2 sowie die vorbeugende Bekämpfung von Straftaten in § 25a Abs. 2 Nr. 3) zu einem Negativbefund.<sup>55</sup> Dieses Ergebnis stützt sich bei der ersten Variante auf die Straftaten, die dem Wortlaut nach einbezogen sein könnten (nämlich auch bloße Vergehen, die sich »lediglich« gegen bedeutende Sach- oder Vermögenswerte richten). In der Variante der vorbeugenden

---

51 Vgl. zum Veranlassungszusammenhang VV § 25a HSOG, HessStAnz. 2023, 946: »Zentrales Element des Konzepts der Kennzeichnung und Kategorisierung personenbezogener Daten ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen.«

52 Grundsätzlich zu den Grundsätzen von Bestimmtheit und Normenklarheit im Recht auf informationelle Selbstbestimmung Eichberger 2024, Rn. 293 ff.

53 S. Verfassungsbeschwerde v. 21.06.2024, S. 45; solche Details könnten etwa in Bestimmungen zu sehen sein, die die Organisation von Updates des Systems regeln.

54 S. Verfassungsbeschwerde v. 21.06.2024, S. 68 ff.; hier werden insbesondere die Unbestimmtheit der Begriffe des »Gewichts der zu schützenden Rechtsgüter« und der »Dringlichkeit des polizeilichen Einschreitens« als Maßstab des Rollen- und Rechtekonzepts kritisiert.

55 S. Verfassungsbeschwerde v. 21.06.2024, S. 87 ff.

Bekämpfung von Straftaten hingegen sehen die Beschwerdeführenden eine derartige Vorverlagerung in das Gefahrenvorfeld, dass sie einer »anlasslosen automatisierten Auswertung personenbezogener Daten« gleichkäme.<sup>56</sup>

### 3.2.2 Zwischen verfassungsrechtlichen und technischen Herausforderungen

Es dürfte nicht überrascht haben, dass eine erneute Verfassungsbeschwerde nach dem Urteil zu »Automatisierte Datenanalyse I« und der anschließenden Reform des § 25a HSOG nicht lange auf sich warten ließ.<sup>57</sup> Dies folgt einerseits aus dem überwiegend erfolgreichen letzten Verfahren, das einmal mehr sehr weitgehende Vorgaben, aber auch Gestaltungsmöglichkeiten, hervorgebracht hat. Die Verfassungsbeschwerde ist aber auch logische Konsequenz einer Neuregelung, der das schwierige Spannungsfeld zwischen Grundrechtsschutz und zunehmend technologisierter Polizeiarbeit sowie der gesetzgeberische Zeitdruck durchaus anzusehen ist.<sup>58</sup> An dieser Stelle offenbart sich die grundlegende rechtspolitische Herausforderung, verfassungsgerichtliche Entscheidungen nicht bloß mal mehr, mal weniger wortgetreu in polizeirechtliche Ermächtigungsgrundlagen zu übernehmen, sondern auch ihre zugrundeliegenden Wertungen zu beachten.<sup>59</sup> Die vorliegende Regelungstechnik, die sich hier im umfangreichen, sehr beschreibenden Normtext und einer extensiven Verwaltungsvorschrift niederschlägt,<sup>60</sup> bietet zahlreiche Anknüpfungspunkte für kritische Auseinandersetzungen wie die von den Beschwerdeführenden angemahnten Verstöße gegen verfassungsrechtliche Grundsätze wie den Gesetzesvorbehalt oder das Bestimmtheitsgebot.<sup>61</sup> Dies vorangestellt, ist es nicht unwahrscheinlich, dass das Bundesverfassungsgericht auch den zweiten Versuch des hessischen Gesetzgebers, eine taugliche Rechtsgrundlage für die automatisierte Datenanalyse zu schaffen, beanstanden wird. Insbesondere die fehlende Begrenzung des Eingriffsgewichts durch die Daten- und Methodenoffenheit des § 25a und Eingriffsschwellen auch unterhalb der konkretisierten Gefahr deuten nicht darauf hin, dass sich der Einsatz von hessenDATA durch die Neuregelung wieder einem »einfachen Datenabgleich«<sup>62</sup> angenähert haben könnte – was in tatsächlicher Hinsicht vermutlich auch nicht beabsichtigt war.

56 S. Verfassungsbeschwerde v. 21.06.2024, S. 93.

57 Vgl. nur Vasel 2023, S. 1176; Bäuerle, in: Möstl/Bäuerle 2025, § 25a Rn. 31.

58 Vgl. Bäuerle 2024, Rn. 60: »wortreiche Scheinbeschränkung«.

59 Vgl. Löffelmann 2023b, S. 92.

60 Ausführlich Bäuerle, in: Möstl/Bäuerle 2025, § 25a Rn. 22 ff.

61 Zu den Anforderungen des Bundesverfassungsgerichts s. Beschluss v. 28.09.2022, 1 BvR 2345/13, Rn. 110 ff.

62 BVerfGE 165, 363 (405).

In beiden Punkten wird die grundlegende Schwierigkeit deutlich, technisch sehr leistungsfähige Instrumente wie die automatisierte Datenanalyse unter Berücksichtigung hergebrachter datenschutzrechtlicher Grundsätze überhaupt sinnvoll einsetzen zu können. Dies zeigt sich exemplarisch bei der Kennzeichnung von Datensätzen: Hier sind sich Gericht, Beschwerdeführende und Gesetzgeber gleichermaßen einig, dass eine solche Kennzeichnung zur Einhaltung des Zweckbindungsgrundsatzes zwar durchaus sinnvoll wäre, technisch hingegen kaum praktikabel abgebildet werden kann.<sup>63</sup> Auch Regelungen zu Zugriffsbeschränkungen (§ 25a Abs. 3 Nr. 1 HSOG; 4.1 VV HSOG) verdeutlichen dieses Spannungsfeld. Aus praktischer Sicht leuchtet es ein, dass eine Zentralisierung von hessenDATA bei speziell geschulten Analyse- und Auswertungsstellen einen begrenzteren und zielgerichteteren Zugriff auf die personenbezogenen Daten ermöglicht und somit eine Verringerung des Eingriffsgewichts bedeuten könnte.<sup>64</sup> Gleichwohl wird in der Verfassungsbeschwerde (in Einklang mit Stimmen aus der Literatur) vertreten, dass eine derartige Begrenzung des Anwenderkreises nicht zwangsläufig zu einer Verringerung des grundrechtsrelevanten neuen Wissens führen müsse, sondern dieses durch die besondere Expertise des eingesetzten Personals sogar ansteigen könnte.<sup>65</sup> Offen bleibt dabei einmal mehr die Frage, wie der Gesetzgeber angesichts dieser grundlegenden Skepsis seinen Gestaltungsspielraum sinnvoll nutzen könnte: Würde eine Software wie hessenDATA unterschiedslos in allen Polizeibehörden von allen Mitarbeitenden genutzt, wäre die Kritik an der großen Streubreite dieses Einsatzes folgerichtig; wenn man demgegenüber lediglich besonders geschultem Personal den Zugriff gestatten würde, bliebe die Befürchtung einer alles durchleuchtenden, nachrichtendienstähnlichen »Spezialeinheit« bestehen.

Eine Entscheidung ist im Jahre 2025 jedenfalls nicht zu erwarten, zumindest ist das Verfahren nicht in den geplanten Entscheidungen des ersten Senats aufgeführt.<sup>66</sup> Die ursprüngliche Verfassungsbeschwerde war damit hinsichtlich eines Vorbringens zum Einsatz künstlicher Intelligenz auf Grundlage von § 25a schon im Dezember 2024 überholt (s. unter 3.3). Zwar haben die Beschwerdeführenden bereits in der nunmehr alten Fassung von § 25a Abs. 1 S. 5 keinen wirksamen Ausschluss von künstlicher Intelligenz ausmachen können;<sup>67</sup> dass die hessische Landesregierung nur wenige Monate nach der Verfassungsbeschwerde den Einsatz

---

63 S. BVerfGE 165, 363 (427); Verfassungsbeschwerde v. 21.06.2024, S. 65; s. auch § 20a Abs. 4 HSOG.

64 So auch vom Bundesverfassungsgericht in den Raum gestellt, s. BVerfGE 165, 363 (404).

65 Vgl. Verfassungsbeschwerde v. 21.06.2024, S. 52 f.; Bäuerle 2024, Rn. 59; Vasel 2023, S. 1176.

66 S. Bundesverfassungsgericht, Geplante Entscheidungen für das Jahr 2025. [https://www.bundesverfassungsgericht.de/DE/Aktuelles/GeplanteEntscheidungen/geplante-Entscheidungen\\_node.html](https://www.bundesverfassungsgericht.de/DE/Aktuelles/GeplanteEntscheidungen/geplante-Entscheidungen_node.html) (01.10.2025).

67 S. Verfassungsbeschwerde v. 21.06.2024, S. 80 ff.

selbstlernender Systeme in § 25a sogar explizit ermöglichen würde, war mit Blick auf die Gesetzesbegründung für die vorherige Änderung aus dem Jahre 2023 jedoch noch nicht zu erwarten.<sup>68</sup>

### 3.3 Erneute HSOG-Novelle: künstliche Intelligenz auf dem Vormarsch

Mit Beschluss der Fraktionen CDU und SPD im hessischen Landtag vom 12.12.2024 kam es durch das »Gesetz zur Stärkung der Inneren Sicherheit in Hessen«<sup>69</sup> zu einer erneuten umfangreichen Änderung des HSOG. In der Begründung des Gesetzentwurfs wird vor allem das durch islamistische und rechtsextremistische Anschläge beeinträchtigte Sicherheitsgefühl der Bürgerinnen und Bürger als Anlass für die Notwendigkeit der Modernisierung des Polizeirechts aufgeführt.<sup>70</sup> Als Lösungsansatz wird (unter anderem) die Erweiterung der Videoüberwachung an besonders gefährdeten Orten (z.B. in der Nähe von religiösen Einrichtungen, aber auch im Zusammenhang mit sogenannten Angsträumen) präsentiert. Den hierdurch erhofften Sicherheitsgewinn möchte der Gesetzgeber unter anderem mit einer KI-gestützten automatisierten Datenanalyse und dem Einsatz künstlicher Intelligenz im Rahmen der intelligenten Videoüberwachung erreichen.<sup>71</sup>

In Bezug auf die Ausweitung von Techniken künstlicher Intelligenz in den einzelnen Rechtsgrundlagen weist das Gesetzgebungsverfahren Parallelen zur ersten umfassenden Änderung von § 25a nach dem Urteil des Bundesverfassungsgerichts auf. Erst mit dem letzten Änderungsantrag vom 05.12.2024 – also eine Woche vor der entscheidenden Abstimmung im Parlament – wurde die KI-gestützte Videoüberwachung in § 14 Abs. 8–11 sowie die KI-gestützte Datenanalyse in § 25a Abs. 1 S. 5 eingefügt.<sup>72</sup> Entsprechend kritisch haben sich Vertreterinnen und Vertreter der Oppositionsfraktionen in der Parlamentsde-

---

68 S. HessDrs. 20/11235, S. 7:

69 GVBl. HE, Nr. 83.

70 HessDrs. 21/1151 v. 01.10.2024, S. 1; s. auch Innenminister Roman Poseck (CDU) in der zugehörigen Pressemitteilung v. 12.12.2024: »Die Sicherheitslage ist angespannt. Dazu tragen aktuelle Entwicklungen maßgeblich bei. [...] Die Bürgerinnen sollen sicher sein und sich sicher fühlen.« <https://hessen.de/presse/gesetz-zur-modernisierung-des-polizeirechts-beschlossen> (01.10.2025); insofern bildet es den gegenwärtigen öffentlichen Diskurs um die innere Sicherheit ab, dass die Novelle auch Regelungen über Identitätsfeststellungen in sog. Waffenverbotszonen enthält, HessDrs. 21/1151 v. 01.10.2024, S. 10. Grundlegend zur Frage, ob das Sicherheitsgefühl der Bevölkerung als Schutzgut der öffentlichen Sicherheit dienen kann: Schewe 2009.

71 HessDrs. 21/1151 v. 01.10.2024, S. 1.

72 HessDrs. 21/1448 v. 05.12.2024, S. 4, S. 7 ff.; leider konnten die zahlreichen Sachverständigen sich aus diesem Grund auch nicht mehr zu den Regelungen äußern, die KI-gestützten Anwendungen vorsehen.

batte zu den Möglichkeiten geäußert, sich in der Kürze der Zeit noch adäquat mit solch umfassenden Änderungen auseinandersetzen zu können.<sup>73</sup> Auch diese zeitliche Dimension des Gesetzgebungsverfahrens führte im Juni 2025 schließlich zu einem Normenkontrollantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN beim Staatsgerichtshof, mit dem sechs Bestimmungen des neuen Gesetzes – darunter § 25a und § 14 HSOG – verfassungsrechtlich überprüft werden sollen.<sup>74</sup> Demgegenüber haben Vertreter der Regierungskoalition den Vorstoß (nicht ganz zu Unrecht, s. unter 4.) als wegweisend im deutschen Polizeirecht bezeichnet,<sup>75</sup> handelt es sich um Vorschriften, die zu diesem Zeitpunkt in keinem anderen Landespolizeigesetz enthalten waren. Im Übrigen wurde jedoch keine weitere Erklärung geliefert, weshalb man trotz der weitreichenden Ergänzungen weder eine erneute Sachverständigenanhörung noch mehr Zeit für die parlamentarische Debatte vorgesehen hatte.

### 3.3.1 KI-gestützte Datenanalyse

Obwohl eine Ausweitung der automatisierten Datenanalyse im ersten Gesetzentwurf nicht als einer der zentralen Lösungsansätze für die genannten Herausforderungen und Bedrohungen angesehen wurde, hat § 25a eine inhaltlich bedeutsame Neufassung erfahren. Diese sieht vor, in § 25a Abs. 1 S. 5 die bisherige Einschränkung zu streichen, wonach eine automatisierte Datenanalyse »regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten« abzulaufen hat. Stattdessen bleibt es fortan bei der knappen Feststellung: »Sie (also die automatisierte Datenanalyse, Anm. d. Verf.) wird manuell ausgelöst«.

Durch diese sprachlich nur geringfügige Änderung wird also fortan klar gestellt, dass die automatisierte Datenanalyse zwar weiterhin vom Menschen manuell veranlasst werden muss, anschließend aber auch KI-basiert arbeiten kann. Weitere Analyseschritte müssen demnach nicht mehr nach einer menschlich definierten Abfolge erfolgen. Der hessische Gesetzgeber verweist für diese Ausweitung der Einsatzmöglichkeiten von hessenDATA auf den Rechtsrahmen der KI-VO und verspricht sich davon, Datenformate schneller zusammenführen zu können, Tat- und Täternetzwerke schneller zu identifizieren, Hinweise aus unstrukturierten Daten schneller zu erkennen sowie komplexe Analyseschrit-

---

73 S. nur Redebeitrag von Vanessa Gronemann (Bündnis 90/Die Grünen), Plenarprotokoll 21/27, S. 1780.

74 S. Normenkontrollantrag vom 18.06.2025. [https://www.gruene-hessen.de/landtag/wp-content/blogs.dir/2/files/2025/06/Normenkontrollantrag-StGH-Hessen-Endfassung-28.05.2025\\_1.pdf](https://www.gruene-hessen.de/landtag/wp-content/blogs.dir/2/files/2025/06/Normenkontrollantrag-StGH-Hessen-Endfassung-28.05.2025_1.pdf) (01.10.2025).

75 S. nur Lisa Gnadl, innenpolitische Sprecherin der SPD-Fraktion: »Ja, mit diesem Gesetzentwurf betreten wir ein Stück weit Neuland.«, Plenarprotokoll 21/27, S. 1781.

te zu vereinfachen und für die Polizeibehörden nutzbar zu machen.<sup>76</sup> Das ist freilich ein gänzlich neuer Ansatz als die vorherige Fassung, die sich nicht nur durch manuell *ausgelöste* Analysevorgänge auszeichnete, sondern auch in den anschließenden Verarbeitungsschritten vom Menschen vorab festgelegte »Wenn-Dann-Operatoren« vorsah.<sup>77</sup> Hatte man sich 2023 noch das KI-Verständnis des Bundesverfassungsgerichts zu eigen gemacht (s. unter 2.3.)<sup>78</sup> und mit einem Schwerpunkt auf deterministischen Systemen eine Abgrenzung zur künstlichen Intelligenz verdeutlichen wollen, erfolgt nun eine direkte Bezugnahme auf den KI-Begriff der europäischen KI-Verordnung.<sup>79</sup>

Der in diesem Zusammenhang neu eingefügte § 25a Abs. 6 versucht dem vom Bundesverfassungsgericht geforderten Schutzniveau beim KI-Einsatz zumindest in Ansätzen gerecht zu werden. Nach dieser neuen Vorschrift sollen die Polizeibehörden sicherstellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Ausweislich der Gesetzesbegründung soll zur Einhaltung dieser Maßgabe eine unabhängige Stelle (wohl in Anlehnung an die nach der KI-VO einzurichtenden Behörden) beteiligt werden, gleichwohl ist zum gegenwärtigen Zeitpunkt nicht klar, wer diese Aufgabe übernehmen soll – auch, weil eine aktualisierte Verwaltungsvorschrift noch nicht bekannt gegeben wurde.<sup>80</sup>

### 3.3.2 KI-gestützte Videoüberwachung und Bildanalyse

Der zweite große Bereich des HSOG, der durch die Implementierung künstlicher Intelligenz ausgeweitet wird, betrifft die Videoüberwachung und Bildanalyse im öffentlichen Raum im Rahmen von § 14 HSOG. Die Vorschrift sah bereits in ihrer vorherigen Fassung unterschiedliche Einsatzfelder vor, die von ereignisbezogener Videoüberwachung im Zusammenhang mit öffentlichen Veranstaltungen und Versammlungen (Abs. 1), der Abwehr konkreter Gefahren (Abs. 3 Nr. 1), der

---

76 S. HessDrs. 21/1448 v. 05.12.2025, S. 10; auf die Ausweitung von hessenDATA hatte man sich bereits im Koalitionsvertrag verständigt, s. Koalitionsvertrag zwischen CDU und SPD für die 21. Legislaturperiode, S. 38. [https://hessen.de/sites/hessen.hessen.de/files/2024-01/koalitionsvertrag\\_fuer\\_die\\_21.\\_legislaturperiode.pdf](https://hessen.de/sites/hessen.hessen.de/files/2024-01/koalitionsvertrag_fuer_die_21._legislaturperiode.pdf) (01.10.2025).

77 S. HessDrs. 20/11235, S. 7; hierzu auch Bäuerle 2025, S. 130.

78 Hier ist einschränkend hinzuzufügen, dass der Gesetzgeber in der Begründung von § 25a Abs. 1 a. F. den KI-Einsatz (bzw. seinen Ausschluss) auch nicht direkt adressiert hat, sondern lediglich bei der Beschreibung der damaligen Funktionsweise einen starken Fokus auf deterministische und vom Menschen gesteuerte Abläufe gelegt hat und hierdurch offenbar einen KI-Ausschluss suggerieren wollte; an diese nicht ganz eindeutige Begründung knüpfte dementsprechend auch die bereits dargestellte Skepsis der Beschwerdeführenden und Teile der Literatur an.

79 S. HessDrs. 21/1448, S. 10.

80 Zum Verwaltungsorganisationsrecht nach der KI-VO grundsätzlich Roth-Isigkeit 2024, Rn. 1 ff.

auf tatsächlichen Anhaltspunkten beruhende Annahme, dass Straftaten drohen (Abs. 3 Nr. 2) bis hin zu ortsbezogener Videoüberwachung reichen. Die Einstufung solcher Orte erfolgt anhand verschiedener Kriterien: Teils werden gewisse Orte schon vom Gesetzgeber als besonders gefährdet eingestuft – wie etwa Flughäfen, Bahnhöfe, Sportstätten (Abs. 3a) oder religiöse Einrichtungen (Abs. 4 Nr. 1). In der Neufassung reicht aber auch die bloße Annahme, dass bestimmte Orte von der Bevölkerung gemieden werden, weil sie aufgrund ihrer Lage, Einsehbarkeit und Frequentierung günstige Gelegenheiten für Straftaten mit erheblicher Bedeutung bieten (Abs. 3 Nr. 3). Letztere Orte werden in der Gesetzesbegründung als »Angsträume« bezeichnet, wobei deren Eignung als Schutzgut der öffentlichen Sicherheit bereits durch die Sachverständigen im Gesetzgebungsverfahren aufgrund mangelnder objektiv nachvollziehbarer Maßstäbe deutlich in Zweifel gezogen wurde.<sup>81</sup>

Für den KI-Bezug interessant sind hingegen die neuen Absätze 8 bis 11. Nach § 14 Abs. 8 besteht nun die Möglichkeit, intelligente Bildanalysesoftware einzusetzen, um Mustererkennungen in zwei Konstellationen vorzunehmen: Bewegungsmuster, die auf die Begehung einer Straftat hindeuten, aber auch die Identifizierung von Waffen oder anderen gefährlichen Gegenständen. Für den Einsatz dieser Technik ist ein Stufenmodell vorgesehen, welches auf der ersten Stufe die Mustererkennung (S. 1) und die anschließende unverzügliche (menschliche) Überprüfung der Polizeibehörden vorsieht, ob aufgrund der erkannten Muster Straftaten mit erheblicher Bedeutung zu erwarten sind (S. 2).<sup>82</sup> Die zweite Stufe (S. 3) besteht darin, eine automatisierte Nachverfolgung (sog. KI-Tracking) der festgestellten verantwortlichen Person zu veranlassen, um diese etwa in einer größeren Menschenmenge identifizieren und verfolgen zu können. Auf der letzten Stufe dieses Stufenmodells implementiert schließlich Satz 4 die biometrische Echtzeit-Fernidentifizierung im engeren Sinn. Liegt demnach eine erhebliche gegenwärtige Gefahr für besonders gewichtige Rechtsgüter (Leben oder körperliche Unversehrtheit) vor, kann die Polizei mithilfe von KI einen schnellen Abgleich und eine Identifizierung der verantwortlichen Person anhand polizeilicher Auskunfts- und Fahndungssysteme durchführen.<sup>83</sup>

---

81 S. nur Arzt, Stellungnahme zur Anhörung im Innenausschuss des Hessischen Landtages, S. 4, der vor allem die Frage aufwirft, nach welcher empirischen Methode im Sinne von Abs. 3 S. 2 »ermittelt« werden soll, ob an einem gewissen Ort die geforderte Vermeidungshandlung vorliegt. Eine Eingrenzung des ursprünglichen Entwurfs lag darin, diese Tatbestandsalternative in der finalen Fassung auf Straftaten mit erheblicher Bedeutung zu beschränken, so auch vorgeschlagen von Bäuerle, Stellungnahme v. 07.11.2024, S. 3.

82 S. Gesetzesbegründung, HessDrs. 21/1448, S. 7 f.

83 S. Gesetzesbegründung, HessDrs. 21/1448, S. 8.

Außerhalb dieses Stufenmodells sieht § 14 Abs. 9 zwei Möglichkeiten vor, in denen die biometrische Echtzeit-Fernidentifizierung auch ohne die vorherigen Schritte eingesetzt werden kann: die gezielte Suche nach Personen, die eine terroristische Gefahr verursachen (S. 1) sowie die gezielte Suche nach Opfern von Straftaten oder vermissten Personen (S. 2). Absätze 10 und 11 der Vorschrift flankieren diese Regelungen mit verfahrensrechtlichen Sicherungen, etwa eine umfangreiche Protokollierungs- (Abs. 10 S. 1) und Begründungspflicht (Abs. 10 S. 2). Außerdem unterliegt jeglicher Einsatz der biometrischen Echtzeit-Fernidentifizierung einem Richtervorbehalt (Abs. 11), der in dringlichen Ausnahmefällen auch durch eine Anordnung einer Behördenleitung ersetzt werden kann, dann aber innerhalb von 24 Stunden richterlich bestätigt werden muss.

### 3.3.3 Einfluss der europäischen KI-Verordnung auf den hessischen KI-Vorstoß

Wie bereits angedeutet, sind die beiden dargestellten Einsatzfelder künstlicher Intelligenz in der HSOG-Novelle maßgeblich von der KI-Verordnung der Europäischen Union geprägt. Weil die Verordnung auf einer produktsicherheitsrechtlichen Konzeption basiert, macht sie künstliche Intelligenz in Form des legaldefinierten KI-Systems zum Regelungsgegenstand und beansprucht damit durch den KI-Einsatz in unterschiedlichen Bereichen sektorübergreifend Geltung.<sup>84</sup> Ungeachtet der eingeschränkten Kompetenz der Union für das Sicherheitsrecht enthält die Verordnung auch zahlreiche Vorgaben für den KI-Einsatz der Polizeibehörden.<sup>85</sup> Dabei verfolgt die Verordnung einen risikobasierten Ansatz, stellt also an die unterschiedlichen Einsatzbereiche und Ausprägungen von KI-Systemen auch unterschiedlich hohe Anforderungen, um deren Risiken einzuhegen.<sup>86</sup>

Nach diesen Risikostufen der KI-VO ließe sich die nunmehr KI-basierte automatisierte Datenanalyse in § 25a HSOG n.F. mit guten Argumenten als Hochrisiko-KI i. S. v. Art. 6 Abs. 2 KI-VO i. V. m. Anlage 2 Nr. 6 lit. e) einstufen.<sup>87</sup> Eine

84 Vgl. Wendt/Wendt 2024, § 3 Rn. 36 f.; zum KI-Begriff der Verordnung s. Art. 3 Nr. 1 KI-VO: »Ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können«.

85 Zur Frage der Kompetenz der Union für den KI-Einsatz im Sicherheitsrecht kritisch Peuker 2023, S. 384; abweichend argumentierend Schöndorf-Haubold/Verf. 2024.

86 Vgl. Ruschemeier 2024a, Rn. 2 ff.

87 So auch Buchmann/Kugelmann 2024b; gleichwohl kann man hiergegen einwenden, dass Anlage 2 Nr. 6 lit. e) KI-VO als maßgebliches Kriterium für die Einstufung der automatisierten Datenanalyse als Hochrisiko-System den »bestimmungsgemäßen« Einsatz zur Erstellung von Persönlichkeitsprofilen bestimmt; demgegenüber stellt das Profiling zumindest in der Sprache des Bundesverfassungsgerichts

Einstufung als Hochrisiko-System hat einige Beschränkungen zur Folge, die von prozeduralen (z.B. Genehmigungsvorbehalte) bis hin zu organisatorischen (z.B. Dokumentationspflichten) Anforderungen reichen, aber auch Vorgaben für die Entwicklung und das Training von KI-Systemen enthalten.<sup>88</sup>

Die Regelungen zur biometrischen Echtzeit-Fernidentifizierung hingegen sind im Wesentlichen ein Abbild der Bestimmungen in Art. 5 KI-VO, wie auch die Gesetzesbegründung und der explizite Verweis in § 14 Abs. 11 HSOG auf die richterliche Anordnung »nach Maßgabe« von Art. 5 Abs. 3 UAbs. 2 KI-VO deutlich macht. Im Gefüge der KI-VO handelt es sich bei den Vorschriften zur biometrischen Echtzeit-Fernidentifizierung um einen politisch und rechtlich hoch umstrittenen Teil der Verordnung, der aufgrund tiefgehender Eingriffe in die Rechte der Betroffenen nicht zu Unrecht als Ausnahmetatbestand des Art. 5 KI-VO formuliert wurde, in dem eigentlich die verbotenen KI-Praktiken aufgezählt sind.<sup>89</sup>

#### 4. Ausblick: Von Pionierarbeit und Schnellschüssen

Wenn die Regierungskoalition in Hessen die jüngste Änderung des HSOG als »Pionierarbeit« bezeichnet,<sup>90</sup> mag das als parlamentarisches »Marketing« abgetan werden. Tatsächlich gibt es jedoch auf Landes- und Bundesebene derzeit keine vergleichbaren Rechtsgrundlagen für den KI-Einsatz bei der automatisierten Datenanalyse und der biometrischen Echtzeit-Fernidentifizierung.<sup>91</sup> Gleichwohl sind gegenwärtig zahlreiche Initiativen auf Bundes- und Landesebene zu beobachten, die der hessischen Gesetzeslage gleichkommen.

---

erst das Resultat einer (zu) intensiven Erschließung personenbezogener Datenbestände durch eine automatisierte Datenanalyse dar. Ob bei einer solchen Lesart davon gesprochen werden kann, dass das Profiling z.B. im Falle von hessenDATA in jedem Fall auch der erforderliche »bestimmungsgemäße« (i. S. v. »ausschließliche«) Zweck der automatisierten Datenanalyse i. S. v. Anlage 2 Nr. 6 lit. e) KI-VO darstellt, kann zumindest in Frage gestellt werden, ähnlich Ruschemeier 2024b, Rn. 75 f. Der Verweis des Gesetzgebers auf die »Einschränkungen der zukünftig geltenden KI-VO« legt hingegen eine Einordnung als Hochrisiko-System nahe, HessDrs. 21/1448, S. 10, ähnlich auch Bäuerle 2025, S. 131.

<sup>88</sup> Zu den Anforderungen an Hochrisiko-Systeme vgl. Pilniok 2024, S. 589 f.; Krönke 2024, S. 532.

<sup>89</sup> Vgl. Wendehorst 2024, Rn. 136 f.

<sup>90</sup> S. Plenarprotokoll 21/29, S. 1918; dem entgegenend Moritz Promny (FDP): »Das ist ein Schnellschuss und nichts anderes.«

<sup>91</sup> Zur Situation rund um den Einsatz von »Gotham« in Nordrhein-Westfalen s. Fußnote 11.

#### 4.1 Bundespolizei, BKA und das bundesweite Datenhaus

In den letzten Zügen der vergangenen Legislaturperiode haben auf Bundesebene die verbliebenen beiden Regierungsfractionen SPD und Bündnis 90/Die Grünen einen (erneuten) Anlauf gestartet, um für das Bundeskriminalamt und die Bundespolizei Befugnisse für eine KI-gestützte automatisierte Datenanalyse und den biometrischen Datenabgleich zu schaffen. Damit sollte insbesondere auch die Rolle des BKA als Zentralstelle im polizeilichen Informationssystem gestärkt werden.<sup>92</sup> Bereits bei erster Betrachtung des Entwurfs zur automatisierten Datenanalyse in § 16a BKAG-E wird deutlich, dass die Vorschrift hinsichtlich ihrer Systematik und Formulierung stark an § 25a HSOG angelehnt ist – Gleiches gilt aber auch für die Zweifel an der Verfassungsmäßigkeit der Vorschrift hinsichtlich der einbezogenen Datenbestände und der korrespondierenden Eingriffsschwellen.<sup>93</sup> Im Zuge der Einführung einer Rechtsgrundlage für das BKA wird auch die Diskussion um ein bundesweites »Datenhaus« wieder lauter. Dieser Vorschlag, der bereits im Jahre 2023 intensiv diskutiert wurde, sieht eine bundesweite Analyseplattform auf Basis von »Gotham« vor, die allen Polizeibehörden des Bundes und der Länder gleichermaßen einen Zugriff auf die verschiedenen polizeilichen Datenbanken ermöglichen soll.<sup>94</sup> Im März 2025 wurde diese Debatte im Bundesrat auf Initiative der Landesregierungen in Bayern und Sachsen-Anhalt wieder aufgegriffen und eine entsprechende Entschließung gefasst.<sup>95</sup> Zwei Ende Juli 2025 von *netzpolitik.org* lancierte Entwürfe deuten an, dass die geplante Einführung einer Rechtsgrundlage für das Bundeskriminalamt und die Bundespolizei auch unter der aktuellen Bundesregierung wieder an Fahrt aufnimmt.<sup>96</sup>

---

92 Im September 2024 kam es bereits zu einem ersten Versuch einer Änderung des BKAG durch die damalige Bundesregierung, seinerzeit noch gemeinsam mit der FDP, s. BTDRs. 20/12806; der zweite Gesetzesentwurf datiert auf den 28.01.2025, BTDRs. 20/14704.

93 In diese Richtung auch die (heftige) Kritik (»Super-Datenbank«) der Bundesdatenschutzbeauftragten zum ersten Entwurf, die trotz einiger Änderungen noch große Teile des aktuellen Entwurfs abbildet, s. Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit v. 11.09.2014, S. 7 ff.

94 Mitte 2023 wurde auf Bundesebene von CDU/CSU der (sofortige) Einsatz von »Palantir Gotham« im Rahmen der Einführung einer bundesweiten »Verfahrensübergreifenden Recherche- und Analyseplattform« (»Bundes-VeRa«) gefordert; die damalige Innenministerin Faeser entschied sich jedoch gegen den Einsatz dieser Software und für die Entwicklung eines eigenen Analysetools; die hiergegen gerichtete Kritik geht dahin, dass die Entwicklung einer hauseigenen Lösung voraussichtlich Jahre in Anspruch nehmen würde, vgl. BTDRs. 20/9495, S. 1 f.

95 S. BRDRs. 58/25.

96 S. Meister, »Innenminister Dobrindt plant neues Sicherheitspaket«, in: *netzpolitik.org*, 23.07.2025, <https://netzpolitik.org/2025/gesichtserkennung-und-ki-innenminister-dobrindt-plant-neues-sicherheitspaket/> (01.10.2025).

## 4.2 Heterogene Gesetzesinitiativen auf Länderebene

Auf Landesebene ist die Situation von unterschiedlichen Entwicklungen geprägt. Während in Hessen, Nordrhein-Westfalen und jüngst auch in Bayern (wo »Gotham« seit Dezember 2024 im Einsatz ist)<sup>97</sup> Verfassungsbeschwerden anhängig sind, haben zahlreiche Bundesländer noch Anfang 2024 angegeben, keine entsprechenden Pläne zu verfolgen.<sup>98</sup> Jüngst gewinnen derartige Vorhaben jedoch – wie etwa in Baden-Württemberg gut zu beobachten ist – deutlich an Dynamik. Dort hatte die Landesregierung im September 2024 zunächst ein Maßnahmenpaket vorgestellt, in dem der Bedarf an einem KI-gestützten Datenanalysetool formuliert wurde.<sup>99</sup> Ende Juli 2025 wurde sodann bekannt, dass das Innenministerium in Baden-Württemberg im März 2025 einen Vertrag mit Palantir unterzeichnet hatte und bereits ab Herbst 2025 gegenüber dem Unternehmen zahlungspflichtig ist.<sup>100</sup> Schließlich wurde im August 2025 mit dem »Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften« auch der Vorschlag für eine Rechtsgrundlage präsentiert.<sup>101</sup>

Hierbei ist zu beobachten, dass immer wieder auf terroristische Anschläge wie in Mannheim, Solingen oder Magdeburg Bezug genommen wird und sich derartige Taten offensichtlich als Beschleuniger dieser Prozesse erweisen. Zudem wird aber deutlich, dass die öffentliche Debatte in aller Regel weniger die rechtliche Zulässigkeit der automatisierten Datenanalyse an sich adressiert, sondern sich vielmehr um den Einsatz einer Software des umstrittenen Unternehmens

97 Mit § 61a PAG wurde nachträglich auch eine Rechtsgrundlage geschaffen, s. BayDrs. 19/1557, S. 8, S. 23 ff; zur Verfassungsbeschwerde s. Gesellschaft für Freiheitsrechte, Verfassungsbeschwerde v. 22.07.2024. [https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Verfassungsbeschwerde-Art.-61a-BayPAG/2025-07-23-Verfassungsbeschwerde-Art.-61a-BayPAG\\_geschwaerzt.pdf](https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Verfassungsbeschwerde-Art.-61a-BayPAG/2025-07-23-Verfassungsbeschwerde-Art.-61a-BayPAG_geschwaerzt.pdf) (01.10.2025).

98 S. Kurz, »Bundesländer nicht scharf auf Palantir«, in: *netzpolitik.org*, 03.01.2024. <https://netzpolitik.org/2024/automatisierte-datenanalyse-bei-der-polizei-bundeslaender-nicht-scharf-auf-palantir/> (01.10.2025).

99 Maßnahmenpaket »Sicherheit stärken, Migration ordnen, Radikalisierung vorbeugen«, 24.09.2024, S. 2 f. [https://stm.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Anlagen\\_PMs\\_2024/240924\\_Massnahmenpaket\\_Sicherheit-staerken\\_Migration-ordnen\\_Radikalisierung-vorbeugen.pdf](https://stm.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Anlagen_PMs_2024/240924_Massnahmenpaket_Sicherheit-staerken_Migration-ordnen_Radikalisierung-vorbeugen.pdf) (01.10.2025)

100 S. Pfäfflin, »Steuerzahlern in BW droht Millionenverlust durch Kauf von Polizei-Software«, in: SWR, 24.07.2025. <https://www.swr.de/swraktuell/baden-wuerttemberg/palantir-software-hohe-kosten-drohen-100.html> (01.10.2025)

101 S. »Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften«. [https://beteiligungsportal.baden-wuerttemberg.de/fileadmin/redaktion/beteiligungsportal/Dokumente/250730\\_Entwurf\\_Aenderung\\_Polizeigesetz.pdf](https://beteiligungsportal.baden-wuerttemberg.de/fileadmin/redaktion/beteiligungsportal/Dokumente/250730_Entwurf_Aenderung_Polizeigesetz.pdf) (01.10.2025); § 47a PolG BaWü-E soll zukünftig den Einsatz der automatisierten Datenanalyse regeln.

Palantir dreht. Wenngleich diesbezüglich auch die Innenministerkonferenz zu Protokoll gegeben hat, dass man sich ein »europäisch beherrschtes System« wünsche,<sup>102</sup> wird durch die Bezugnahme auf die »Erfahrungen im Einsatz entsprechender Systeme« der Palantir-Kunden Hessen, Bayern und Rheinland-Pfalz deutlich, dass Palantir-Anwendungen jedenfalls so lange das Mittel der Wahl bleiben, bis vergleichbar potente Instrumente deutscher oder europäischer Unternehmen zur Verfügung stehen.<sup>103</sup>

In Rheinland-Pfalz erinnert die neu geschaffene Rechtsgrundlage für eine automatisierte Datenanalyse in § 65a POG<sup>104</sup> von ihrer Struktur her stark an § 25a HSOG und beinhaltet die aus Hessen bekannten Eingriffsschwellen der konkreten Gefahr (Abs. 1 Nr. 1), der konkretisierten Gefahr (Abs. 1 Nr. 2) und der vorbeugenden Bekämpfung von Straftaten (Abs. 1 Nr. 3). Auch werden die gleichen Datentöpfe einbezogen, sodass auch die wegen ihrer Streubreite besonders sensiblen Vorgangsdaten in der Analyse enthalten sind (Abs. 3 S. 1) – wenngleich auch hier der Versuch unternommen wird, personenbezogene Daten von Unbeteiligten per Gesetz von der Datenverarbeitung auszunehmen (Abs. 6 S. 4). Auch wenn der KI-Einsatz nicht explizit ausgeschlossen wird, hat der rheinland-pfälzische Gesetzgeber rein maschinellen Sachverhaltsbewertungen eine Absage erteilt (Abs. 2 S. 2) und auch in seiner Begründung sichtlich Wert darauf gelegt, den »Faktor Mensch« in den Vordergrund zu rücken und daher immer wieder betont, dass der gesamte Datenverarbeitungsvorgang einer menschlichen Steuerung unterliegen soll.<sup>105</sup>

Derweil wird in Sachsen-Anhalt ein Gesetzesentwurf diskutiert, der mit § 30a SOG-E einen interessanten eigenen Regelungsansatz verfolgt.<sup>106</sup> Die Novelle sieht eine grundlegende Differenzierung zwischen einer operativen und einer strategischen Datenanalyse vor. Während die Datenanalyse im operativen Bereich den dargestellten Rechtsgrundlagen anderer Bundesländer ähnelt und daher für Prognosen und Entscheidungen im Einzelfall verwendet werden soll, beschreibt die Datenanalyse im strategischen Bereich vor allem die Erkennung gefährlicher Orte oder bestimmter Kriminalitätsphänomene, aber auch die Verarbeitung zu statistischen Zwecken (§ 30a Abs. 1, Abs. 2 SOG–E).<sup>107</sup> Der Entwurf etabliert damit von Beginn an zwei unterschiedliche Pfade für die Datenanalyse und erlaubt im Rahmen der strategischen Datenanalyse grundsätzlich nur die Verarbeitung anonymisierter oder pseudonymisierter Daten. Der Vorschlag in

---

102 Beschluss der Innenministerkonferenz vom 18.06.2025, S. 32.

103 Allgemein zum Gebot digitaler Souveränität Meyer 2025, S. 160 f.

104 Gesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes v. 25.02.2025, GVBl. RLP S. 15.

105 S. RPDrs. 18/1075, S. 83 f.

106 S. LSADrs. 8/5018, S. 31 ff.

107 Vgl. LSADrs. 8/5018, S. 57 f.

Sachsen-Anhalt sticht auch deshalb heraus, weil er deutlich konkretere Vorgaben zu den eingesetzten Techniken der Datenanalyse enthält. In diesem Kontext werden die Techniken »deskriptive Analytik, diagnostische Analytik, prädiktive Analytik, präskriptive Analytik, Data-Mining, maschinelles Lernen, Data Science und Sekundärdatenanalyse« genannt (§ 30a Abs. 5 SOG-LSA-E). Wenngleich die Gesetzesbegründung zu diesen technischen Methoden keine nähere Erklärung liefert (insoweit ist wohl die zugehörige Verwaltungsvorschrift abzuwarten), kann zumindest das maschinelle Lernen als wesentlicher Baustein von KI-Anwendungen identifiziert werden.

Auch in Hamburg wird weiterhin ein Sonderweg beschritten: Zwar hat man im Februar 2025 (also erst zwei Jahre nach dem Urteil) den vormals verfassungswidrigen § 49 HmbPolDVG geändert, jedoch ist von einem Einsatz einer (Palantir Gotham-basierten) Software bislang nichts bekannt – insofern hat sich der Gesetzgeber in Hamburg auch nicht dem gleichen Zeitdruck ausgesetzt, wie es in Hessen zu beobachten war. Dieses zurückhaltende Vorgehen schlägt sich auch in der neuen Rechtsgrundlage nieder. Diese entnimmt zwar dem hessischen Vorbild die Legaldefinition der automatisierten Datenanalyse, enthält aber unterhalb der Ebene der konkretisierten Gefahr keine mit § 25a Abs. 2 S. 3 HSOG vergleichbare Eingriffsschwelle. Zudem wird für lediglich konkretisierte Gefahren eine Herabsenkung des Eingriffsgewichts (z. B. hinsichtlich der einbezogenen Daten, § 49 Abs. 2 S. 6, S. 7 HmbPolDVG) bestimmt. Auch der KI-Einsatz wird jedenfalls nicht explizit ermöglicht; dahingehend befindet sich die Vorschrift (noch) auf dem »alten Stand« von § 25a HSOG.<sup>108</sup> Insgesamt lässt sich also festhalten, dass die aktuelle Hamburger Vorschrift zumindest im Vergleich mit dem hessischen Pendant weniger Anhaltspunkte für eine erneute Verfassungswidrigkeit zu enthalten scheint.<sup>109</sup>

Allein die Entwicklungen der vergangenen zwei Jahre zeigen, dass die rechtliche Gestaltung des polizeibehördlichen KI-Einsatzes durch nationale und europäische Gesetzgebung und verfassungsgerichtliche Rechtsprechung in einem ähnlich rasanten Tempo voranschreitet wie die Entwicklung dieser Technologien selbst. Dass nach »Automatisierte Datenanalyse I« vor »Automatisierte Datenanalyse II« sein würde, war dementsprechend keine Überraschung, jedoch hat sich die ohnehin schon dynamische Rechtslage im Bereich polizeilicher big data-Analysen durch die Verabschiedung der KI-Verordnung und durch den Vorstoß des hessischen Gesetzgebers weiter zugespitzt. Für das beim Bundesverfassungsgericht anhängige § 25a HSOG-Verfahren dürfte dies bedeuten, dass das

---

108 Vgl. auch die Gesetzgebungsbegründung zu § 49 HmbPolDVG, HmbDrs. 22/16042, S. 28 ff.

109 Sinnvolle Vorschläge zur Umsetzung der Anforderungen an Rechtsgrundlagen für automatisierte Datenanalysen liefern Kugelmann/Buchmann 2024a, S. 7 ff.

Gericht erstmals im großen Umfang zum polizeibehördlichen KI-Einsatz Stellung beziehen und diesbezügliche Mindestanforderungen formulieren wird.

Ob man der hessischen Landesregierung nun Pionierarbeit oder Schnellschüsse attestieren möchte: Wünschenswert wäre es, wenn sich im Zusammenspiel von Gesetzgebung und Verfassungsgerichtsbarkeit im Sicherheitsrecht eine Entwicklung einstellt, die tragfähigere Rechtsgrundlagen schafft, anstatt regelmäßige verfassungsgerichtliche Korrekturen notwendig zu machen.

## Quellen und Literatur

- Arzt, Clemens, »Praxis der polizeilichen Datenverarbeitung«, in: Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hg.), *Handbuch des Polizeirechts*, München 2021, S. 1108–1335.
- Bäuerle, Michael, »§ 25a HSOG«, in: Möstl, Markus/Bäuerle, Michael (Hg.), *Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen*, 34. Edition, München 2025, Rn. 1–139.
- Bäuerle, Michael, »Automatisierte und KI-gesteuerte Datenverarbeitung und -analyse bei den Sicherheitsbehörden«, in: *Zeitschrift für Datenschutz (ZD)* 2025, S. 128–132.
- Eichberger, Michael, »Grundgesetz Art. 2«, in: Voßkuhle, Andreas/Huber, Peter (Hg.), *Grundgesetz Kommentar*, München 2024, Rn. 1–377a.
- Hofmann, Henning, *Predictive Policing*. Berlin 2020.
- Ibrisagic, Irma/Dietz, Thorsten/Maier, Daniela/Weingarten, Dirk (Hg.), *Hessisches Gesetz über die Öffentliche Sicherheit und Ordnung Kommentar*, 26. Nachlieferung, Wiesbaden 2024.
- Krönke, Christoph, »Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten«, in: *Neue Zeitschrift für Verwaltungsrecht (NVwZ)* 2024, S. 529–534.
- Kugelmann, Dieter/Buchmann, Antonia, »Der Algorithmus und die Künstliche Intelligenz als Ermittler«, in: *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* 2024, S. 1–10.
- Kugelmann, Dieter/Buchmann, Antonia, »Big Brother is Analyzing You – Auswirkungen der KI-Verordnung auf Verfahren der automatisierten Datenanalyse«, in: *Verfassungsblog*, 11.12.2024. <https://verfassungsblog.de/big-brother-is-analyzing-you/> (01.10.2025).
- Kurz, Constanze, »Automatisierte Datenanalyse bei der Polizei. Bundesländer nicht scharf auf Palantir«, in: *netzpolitik.org*, 03.01.2024. <https://netzpolitik.org/2024/automatisierte-datenanalyse-bei-der-polizei-bundeslaender-nicht-scharf-auf-palantir/> (01.10.2025).
- Löffelmann, Markus, »Verfassungsrechtliche Anforderungen an automatisierte Datenanalysen durch Sicherheitsbehörden«, in: *Juristische Rundschau (JR)* 2023, S. 331–344.
- Löffelmann, Markus, »Eingriffsintensität und Eingriffsschwelle«, in: *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* 2023, S. 92–96.
- Mehta, Dharmil, »Erklärbare KI: Das Geheimnis der Blackbox lüften«, in: *Fraunhofer IAO Blog*, 21.11.2023. <https://blog.iao.fraunhofer.de/erklarbare-ki-das-geheimnis-der-blackbox-lueften/> (01.10.2025).
- Meister, Andre, »Innenminister Dobrindt plant neues Sicherheitspaket«, in: *netzpolitik.org*, 23.07.2025, <https://netzpolitik.org/2025/gesichtserkennung-und-ki-innenminister-dobrindt-plant-neues-sicherheitspaket/> (01.10.2025).

- Meyer, Simon Diethelm, »Der Einsatz künstlicher Intelligenz durch Sicherheitsbehörden«, in: *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* 2024, S. 156–161.
- Peuker, Enrico, »Datenschutz als Annexkompetenz – Zu Kompetenzgrenzen der europäischen KI-Regulierung im Bereich der Gefahrenabwehr und Strafverfolgung durch die Mitgliedstaaten«, in: *Zeitschrift für Digitalisierung und Recht (ZfDR)* 2023, S. 384–397.
- Pfäfflin, »Steuerzahlern in BW droht Millionenverlust durch Kauf von Polizei-Software«, in: *SWR*, 24.07.2025. <https://www.swr.de/swraktuell/baden-wuerttemberg/palantir-software-hohe-kosten-drohen-100.html> (01.10.2025).
- Pilniok, Arne, »Unionsrechtliche Regulierung des Einsatzes von KI-Systemen in der öffentlichen Verwaltung«, in: *Die Öffentliche Verwaltung (DÖV)* 2024, S. 581–592.
- Rademacher, Timo/Perkowski, Lennart, »Staatliche Überwachung, neue Technologien und die Grundrechte«, in: *Juristische Schulung (JuS)* 2020, S. 713–720.
- Roth-Isigkeit, David, »Art. 70 KI-VO – Benennung von zuständigen nationalen Behörden und zentrale Anlaufstelle«, in: Martini, Mario/Wendehorst, Christiane (Hg.), *Verordnung über künstliche Intelligenz Kommentar*, München 2024, Rn. 1–30.
- Ruschemeier, Hannah, »Art. 6 KI-VO – Einstufungsvorschriften für Hochrisiko-KI-Systeme«, in: Martini, Mario/Wendehorst, Christiane (Hg.), *Verordnung über künstliche Intelligenz Kommentar*, München 2024, Rn. 1–108.
- Ruschemeier, Hannah, »Anhang III KI-VO – Hochrisiko-KI-Systeme gemäß Artikel 6 Absatz 2«, in: Martini, Mario/Wendehorst, Christiane (Hg.), *Verordnung über künstliche Intelligenz Kommentar*, München 2024, Rn. 1–88.
- Schewe, Christoph S., *Das Sicherheitsgefühl und die Polizei*, Berlin 2009.
- Schöndorf-Haubold, Bettina/Giogios, Christopher, »KI im Einsatz für die Sicherheit – Innovation und Kontrolle im Spannungsfeld von europäischer Gesetzgebung und nationaler Souveränität«, in: *Verfassungsblog*, 10.12.2024. <https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/> (01.10.2025).
- Sommerer, Lucia, *Personenbezogenes Predictive Policing*, Baden-Baden 2020.
- Stock, Imke, »Palantir als Interimslösung: Bundesrat fordert schnellen Einsatz für die Polizei«, in: *heise online*, 24.03.2025. <https://www.heise.de/news/Palantir-als-Interimslösung-Bundesrat-fordert-schnellen-Einsatz-fuer-die-Polizei-10325605.html> (01.10.2025).
- Trute, Hans-Heinrich, »Zur Entwicklung des Polizei- und Ordnungsrechts 2013–2019«, in: *Die Verwaltung* 2020, S. 99–118.
- Vasel, Johann Justus, »Verfassungsgerichtliche Fesseln? Das Karlsruher Urteil zur automatisierten Datenanalyse«, in: *Neue Juristische Wochenschrift (NJW)* 2023, S. 1174–1178.
- Wendehorst, Christiane, »Art. 5 KI-VO – Verbotene Praktiken im KI-Bereich«, in: Martini, Mario/Wendehorst, Christiane (Hg.), *Verordnung über künstliche Intelligenz Kommentar*, München 2024, Rn. 1–195.
- Wendt, Janine/Wendt, Domenik (Hg.), *Das neue Recht der Künstlichen Intelligenz*, Baden-Baden 2024.

# Automatisierte Datenanalysen zwischen DS-GVO, JI-RL und KI-VO

*Lea Rabe, Christian Geminn, Paul Johannes*

## 1. Die Suche nach der Nadel im Heuhaufen

Die Ermittlungsarbeit der Polizei ist wie eine Suche nach der Nadel im Heuhaufen. Dieser Heuhaufen besteht im Kontext der automatisierten Datenanalyse grundsätzlich aus allen der Polizei zur Verfügung stehenden Daten.

Die Polizei- und Strafverfolgungsbehörden kämpfen damit, die Mengen, der ihnen zur Verfügung stehenden Daten zu überschauen und auszuwerten, die aus unzähligen heterogenen Quellen kommen. Das Problem ist hier nicht, an die Daten zu gelangen, sondern aus den bereits zur Verfügung stehenden Daten für die Ermittlungsarbeit nutzbare und nützliche Informationen zu gewinnen.

Es besteht zum einen für offene Datenquellen, wie das sichtbare, dokumentenbasierte Netz,<sup>1</sup> das Netz der sozialen Medien,<sup>2</sup> das Deep Web<sup>3</sup> und das Darknet.<sup>4</sup> Hinzutreten können kommerzielle Datenkataloge<sup>5</sup> sowie maschinenverständliche Daten aus offenen Quellen (Data Web) als Informationsquellen für Ermittlungen. Die Komplexität vervielfacht sich, wenn nicht nur Daten aus offenen Quellen analysiert werden, sondern zum anderen auch mit Daten aus in-

---

1 Das Internet, soweit es von Suchmaschinen indiziert wurde.

2 Soziale Netzwerke, die ggf. Einsicht nur in Abhängigkeit von gewährten Benutzerrechten und Schnittstellen (API) geben.

3 Große Datenhaltungen, z.B. von E-Commerce-Plattformen; auf diese kann nicht direkt zugegriffen werden, sondern nur über spezielle Schnittstellen; idR nicht durch öffentliche Suchmaschinen auffindbar; Inhalte sind auch Datenbanken, Intranets oder Fachwebseiten.

4 Webseiten im Darknet können nicht über konventionelle Internettools (Internet-Browser) erreicht werden und werden nicht von allen Suchmaschinenanbietern indiziert; der Betrieb und Zugang erfolgt über Anonymisierungsdienste- und -tools, die eine Zuordnung von Darknet-Inhalten zu Personen über Internetanschlüsse und IP-Adressen unmöglich machen sollen.

5 Z. B. Auskunftfeien oder Geldwäsche- und Risk-Screening-Datenbanken; auch dies sind offene Quellen, da sie gegen Entgelt von jedermann eingesehen werden können.

ternen Quellen der Polizei- und Ermittlungsbehörden<sup>6</sup> oder (beschlaggenommenen) Datensammlungen Dritter in Bezug gesetzt werden sollen.<sup>7</sup>

Eine Herausforderung für die Polizeiarbeit ist, dass Suche, Sammlung, Aggregation und Analyse solcher Datenquellen arbeitsintensiv ist und viel Zeit beansprucht. Hauptgrund dafür ist, dass man unterschiedliche Methoden und Werkzeuge braucht, um an diese diversifizierten Datenbestände zu kommen und daraus Informationen zu gewinnen. Ohne Fachwissen zur Datenanalyse ist ein Ermittler nicht in der Lage, alle verfügbaren Datenquellen zu nutzen und miteinander zu verknüpfen.

Die aus der Zusammenführung gewinnbaren Informationen (Suchtreffer) bilden selbst eine riesige, noch auszuwertende und zu bewertende Menge an Masendaten, die zum ganz überwiegenden Teil in unstrukturierter Form vorliegen. Außerdem basiert die meist frei verfügbare Suchtechnologie auf einfachen Stichworten (Indexierung), vernachlässigt aber Semantik und Kontext.

IT-Anwendungen zur Datenintegration und Datenanalyse versprechen diese Probleme zu adressieren. Sie sollen ermittlungsunterstützend eingesetzt werden können. Es sind Systeme, die Funktionen zur Extraktion, Integration, Kuratierung und Analyse unstrukturierter Daten bieten:<sup>8</sup>

Extraktions-Funktionen ermöglichen es, gleichzeitig in einer Vielzahl von Quellen und Datensammlungen nach Begriffen oder Personen zu suchen. So werden Medienbrüche vermieden und die Effizienz der Suche gesteigert. Dabei können automatisiert Entitäten, wie zum Beispiel Personen, Orte und Organisationen, aus einem breiten Korpus unstrukturierter Bild- oder Textdaten extrahiert werden.

Falls möglich, werden die gefundenen Entitäten automatisch mit anderen Datenquellen verknüpft und integriert (Datenintegration und Datenkuratierung). Sinn und Zweck der Datenintegration ist es, Entitäten aus unterschiedlichen Datenquellen zu identifizieren, die dasselbe wirkliche Objekt beschreiben. Bezieht man zum Beispiel Informationen über Personen aus zwei sozialen Netzen, so können sich unterschiedliche Entitäten auf dieselbe echte Person beziehen. Beim Zusammenführen so identifizierter Duplikate können Datenkonflikte auftreten, wenn unterschiedliche Werte für dieselbe Eigenschaft vorliegen. Zum Beispiel könnten zwei Quellen unterschiedliche Geburtsdaten für dieselbe Person nennen. Die Werkzeuge sollen Datenkonflikte durch Methoden der Feststellung und

---

6 Z. B. Vorgangs-, Fall- und sonstige Ermittlungsakten; aber auch öffentliche Register und Informationssysteme der Polizei- und Ermittlungsbehörden.

7 Dazu z. B. Johannes 2018, S. 151 ff.

8 Aggregations- und Analysewerkzeuge zur Ermittlungsunterstützung mit vergleichbaren Funktionen sind z. B. Palantir, Maltego, IBM i2 Analyst's Notebook oder Sentinel Visualizer.

Konsolidierung auflösen (helfen). Wenn dasselbe Objekt, zum Beispiel dieselbe Person, in mehreren Quellen gefunden wird und mit hinreichend vielen Attributen beschrieben ist, nutzen die Werkzeuge Verfahren zur Datenintegration, um die gefundenen Teilergebnisse zu einem Suchergebnis zusammenzuführen, welches dann über eine reichhaltigere Beschreibung verfügt.

Außerdem sollen diese Systeme Beziehungen der integrierten und kuratierten Daten analysieren. Erkannt werden können soll zum Beispiel, welche Pseudonyme als Verkäufer von Betäubungsmitteln im Darknet auftreten, wo diese Pseudonyme in sozialen Netzwerken zu finden sind und wie wahrscheinlich es ist, dass es sich um dieselben Personen handelt. Anwendungsabhängig werden die Ergebnisse der Analyse auch visualisiert, zum Beispiel in Beziehungsgeflechten und -graphen. Dies kann helfen, relevante Informationen für das Ermittlungsverfahren zu erhalten und Hinweise auf Mittäter oder weitere Opfer und Zeugen zu geben. Solche Anwendungen können auch weitergehend unterstützen, indem sie zum Beispiel versuchen, automatisiert in den Daten typische Muster von angebahnten Straftaten oder organisierter Kriminalität zu erkennen. Diese Aussagen sollten sich auf sog. PIOS-Objekte<sup>9</sup> beziehen – im Idealfall auch objektübergreifend, also auch bestehende Beziehungen zwischen diesen Objekten beschreiben. Die automatisierten Datenanalysen liefern grundsätzlich nur Wahrscheinlichkeitsergebnisse auf Grundlage statischer Inferenzen. Das bedeutet nahezu zwangsläufig, dass sie auch falsche Ergebnisse liefern. So können verdächtige Beziehungen nicht erkannt werden, das heißt, es kommt zu falsch-negativen Ergebnissen. Es könnte aber auch der Verdacht auf unbeteiligte Personen gelenkt werden, das heißt, es kommt zu falsch-positiven Ergebnissen.<sup>10</sup> Sofern solche Systeme zur automatisierten Datenanalyse im Einsatz oder in der Entwicklung personenbezogene Daten verarbeiten, sind die Vorgaben des Datenschutzrechts zu beachten. Diese müssen auch vom Gesetzgeber eingehalten werden, wenn eine Rechtsgrundlage für die Verwendung entsprechender Systeme geschaffen werden soll, und sind europarechtlich vorgeprägt. Ferner wurde mit der KI-Verordnung<sup>11</sup> ein weiterer unionaler Rechtsakt geschaffen,

---

<sup>9</sup> Personen, Institutionen, Orte, Sachen.

<sup>10</sup> Die im laufenden Betrieb notwendige und teilweise ohne menschliches Eingreifen (maschinelles Lernen) stattfindende Anpassung der Algorithmen zur Verringerung der Anzahl von falsch-negativen Ergebnissen führt in der Regel zur Vergrößerung der Anzahl von falsch-positiven Verdächtigungen. Umgekehrt führt die Anpassung zur Verringerung von falsch-positiven Ergebnissen zu Vergrößerung der Anzahl von falsch-negativen Ergebnissen.

<sup>11</sup> Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 2024/1689 vom 12.07.2024.

der das Datenschutzrecht flankiert<sup>12</sup> und auch über dessen Geltungsbereich (der Verarbeitung personenbezogener Daten) hinaus Vorgaben macht.

## 2. Rechtsrahmen: vom einen ins andere Regime

Datenschutzrechtliche Vorgaben ergeben sich zunächst sowohl aus der Datenschutz-Grundverordnung (DS-GVO)<sup>13</sup> als auch aus der Richtlinie für Justiz und Inneres (JI-Richtlinie).<sup>14</sup> Das private Unternehmen, das die Anwendung unter Verarbeitung von personenbezogenen Daten entwickelt oder trainiert, muss die Vorgaben der DS-GVO einhalten, während die Polizeibehörde die Vorgaben der JI-Richtlinie in Form ihrer Umsetzung<sup>15</sup> durch den nationalen Gesetzgeber beachten muss.

Der sachliche Anwendungsbereich des Polizeidatenschutzrechts auf Grundlage der JI-Richtlinie erstreckt sich nach Art. 1 JI-RL respektive § 45 BDSG, § 40 HDSIG auf die Straftatenverhütung, zu der auch Gefahrenabwehrmaßnahmen gehören.<sup>16</sup> Da die Datenverarbeitung zur Aufdeckung von Straftaten im Normsinne auch Verdachtsgewinnungsmaßnahmen, das heißt, solche zur Gewinnung von Ermittlungs- und Spurenansätzen im Gefahrenvorfeld, umfasst, sind vom Anwendungsbereich auch Big Data-Analysen zur vorbeugenden Straftatenbekämpfung umfasst.<sup>17</sup> Die Datenschutz-Grundverordnung ist gemäß Art. 2 Abs. 2 lit. d DS-GVO nicht einschlägig.<sup>18</sup> Die Umsetzungsakte sind im Anwendungsbereich auch *lex specialis* zum Verwaltungsverfahrensgesetz.<sup>19</sup> Spezialvorschriften mit Vorrangcharakter wiederum gegenüber den Datenschutzgesetzen sind

---

<sup>12</sup> Vgl. Art. 2 Abs. 7 KI-VO.

<sup>13</sup> Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119 vom 04.05.2016, S. 1–88.

<sup>14</sup> Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 04.05.2016, S. 89–131.

<sup>15</sup> In diesem Text werden als Beispiele für die Umsetzung die entsprechenden Normen des BDSG und des HDSIG bzw. HSOG benannt.

<sup>16</sup> Johannes/Weinhold 2018, § 1 Rn. 81.

<sup>17</sup> Braun, in: Gola/Heckmann 2022, § 45 BDSG Rn. 17.

<sup>18</sup> Zur Abgrenzung Arzt 2023, S. 992.

<sup>19</sup> Das gilt also auch für das Verbot vollautomatisierter Verwaltungsakte in § 35a VwVfG.

in den Fachgesetzen, etwa den Polizeigesetzen enthalten; BDSG und HDSIG beschränken die Ermächtigungsnormen des Fachrechts bereichsspezifisch.<sup>20</sup>

In der Anwendungsphase (siehe dazu 3.3) gilt das Rechtsregime der JI-RL beziehungsweise ihrer Umsetzungsakte. Die JI-Richtlinie gilt gemäß Art. 288 Abs. 3 AEUV in Deutschland nicht direkt. Der Bund ist der Umsetzungspflicht mit dem Bundesdatenschutzgesetz (BDSG)<sup>21</sup> nachgekommen. Auf Landesebene wurden, diesem entsprechende, allgemeine Datenschutzgesetze – wie das Hessische Datenschutz- und Informationsfreiheitsgesetz (HDSIG)<sup>22</sup> – oder Spezialgesetze erlassen oder aber Fachgesetze abgeändert.<sup>23</sup> Die einschlägigen Vorschriften in BDSG und HDSIG entsprechen sich weitestgehend, da Bund und Länder mitunter wörtlich die Vorgaben der JI-RL übernommen haben.<sup>24</sup> Inkongruenzen mit dem bisherigen nationalen Recht, insbesondere hinsichtlich der Abgrenzung von Prävention und Repression, sind dabei nicht ausgeblieben.<sup>25</sup> Die KI-Verordnung (KI-VO) ist ein umfassendes Regelwerk, das den Einsatz von Künstlicher Intelligenz (KI) reguliert. Sie legt erstmals EU-weit harmonisierte Vorschriften für KI fest und folgt einem risikobasierten Ansatz. Das bedeutet, dass die Anforderungen an KI-Systeme umso strenger sind, je höher das Risiko ist, das von ihnen ausgeht. Sie umfasst Regelungen für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der EU. Die Verordnung trat am 1. August 2024 in Kraft, wobei viele zentrale Bestimmungen jedoch erst ab dem 2. August 2026 wirksam werden.

Die KI-Verordnung lässt nach ihrem Art. 2 Abs. 7 Satz 2 bestehende Datenschutzregelungen der Union, wie die Datenschutz-Grundverordnung und die JI-Richtlinie unberührt. Sie ersetzt diese Regelungen also nicht, sondern stellt zusätzliche Anforderungen an den Einsatz von KI-Systemen, insbesondere wenn personenbezogene Daten verarbeitet werden, was Art. 2 Abs. 7 Satz 1 DS-GVO klarstellt. Die Datenschutzaufsichtsbehörden sind weiterhin zuständig und überwachen die Einhaltung der Datenschutzvorschriften im Zusammenhang mit KI-Systemen. Für die Aufsicht über die Durchsetzung der KI-Verordnung selbst sind von den Mitgliedstaaten nach Art. 70 KI-VO Marktüberwachungsbehörden zu bestimmen. In Deutschland ist dies zum Beispiel die Bundesnetzagentur.

---

20 Braun, in: Gola/Heckmann 2022, § 45 BDSG Rn. 3; Arzt 2023, S. 995.

21 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

22 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) vom 3. Mai 2018 (GVBl. S. 82) FFN 300–47, zuletzt geändert durch Art. 9 Drittes G zur Änd. dienstrechtl. Vorschriften vom 15. November 2021 (GVBl. S. 718).

23 Überblick über die Umsetzung in den Ländern bei Arzt 2023, S. 999; Bäuerle 2024, S. 64 f.

24 Arzt 2023, S. 999.

25 Weiterführend Braun, in: Gola/Heckmann 2022, § 45 BDSG Rn. 22; Arzt 2023, S. 999.

Die KI-Verordnung sieht vor, dass KI-Systeme, die als Hochrisiko-Systeme eingestuft werden, strengen Sicherheits- und Datenschutzmaßnahmen unterliegen. Dazu gehören beispielsweise die Pseudonymisierung oder Verschlüsselung von Trainingsdaten, um die Qualität und Sicherheit der Datenverarbeitung zu gewährleisten. Die KI-Verordnung sieht keine Anwendungsausnahme für den Bereich der Polizei- und Strafverfolgungsbehörden vor. Auch Polizeibehörden müssen sicherstellen, dass von ihnen betriebene KI-Systeme den Vorgaben der KI-Verordnung entsprechen und dass sie keine nach Art. 5 KI-VO verbotenen Anwendungen nutzen. Lediglich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit wird die Anwendbarkeit der KI-Verordnung nach Art. 2 Abs. 3 KI-VO ausgenommen.

Wenn ein privates Unternehmen eine KI-Anwendung für eine Polizeibehörde entwickelt, müssen beide Parteien die Anforderungen der KI-Verordnung und der DS-GVO einhalten. Die KI-Verordnung gilt nach Art. 2 Abs. 1 *expressis verbis* auch für Anbieter von KI-Systemen, die in der Union KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen, unabhängig davon, ob diese Anbieter in der Union oder in einem Drittland niedergelassen sind. Das private Unternehmen muss sicherstellen, dass die KI-Anwendung datenschutzkonform ist, soweit es selbst personenbezogene Daten verarbeitet, und die Polizeibehörde muss die Einhaltung der Vorschriften überwachen.

### 3. Phasen automatisierter Datenanalysen: Training, *fine-tuning*, Anwendung

Zentraler Anknüpfungspunkt des Datenschutzrechts sind Datenverarbeitungen. Im »Lebenszyklus« eines KI-Systems können nach Hüger drei datenschutzrechtlich relevante Verarbeitungsphasen unterschieden werden: die Erhebung vom Trainingsdaten und die Aufbereitung dieser Daten für das Training (3.1), die Trainingsphase (3.2) und der Einsatz und die Nutzung (3.3).<sup>26</sup> Eine solche Einteilung nach Phasen erlaubt es, die Verpflichtungen der jeweils datenschutzrechtlich Verantwortlichen beziehungsweise der Anbieter und Betreiber etc. im Sinne der KI-Verordnung chronologisch herauszuarbeiten. JI-Richtlinie und Datenschutz-Grundverordnung sind somit teilweise in unterschiedlichen Phasen, teilweise auch überlappend, von Relevanz.<sup>27</sup>

---

<sup>26</sup> Hüger 2024, S. 266 f.

<sup>27</sup> Beispiele zu überschneidenden Anwendungsbereichen bei Johannes 2020, S. 410 ff.

Für die Verarbeitungen in Phase 1 und 2 durch privatwirtschaftliche Anbieter wie Palantir Technologies Inc. ist grundsätzlich die Datenschutz-Grundverordnung einschlägig. Da Phase 2 auch das sog. fine-tuning umfasst, bei dem die Künstliche Intelligenz an die Bedürfnisse und Daten der Sicherheitsbehörden angepasst wird, könnte eine Auftragsverarbeitung vorliegen, bei der der privatwirtschaftliche Anbieter des KI-Systems im Auftrag und auf Weisung der fraglichen Sicherheitsbehörde tätig wird. Die Anwendung durch die Polizei in Phase 3 unterfällt der JI-Richtlinie beziehungsweise den nationalen Umsetzungsrechtsakten, denn die Richtlinie gilt spezifisch bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

In jeder Phase gelten die Verarbeitungsgrundsätze des Art. 5 DS-GVO respektive Art. 4 JI-RL. Neben dem Erfordernis einer Rechtsgrundlage (»Verbotsprinzip«<sup>28)</sup>) gelten die Grundsätze der Verarbeitung nach Treu und Glauben, der Transparenz, Zweckbindung, Datenminimierung, Datenrichtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit (Art. 5 Abs. 1 DS-GVO bzw. Art. 4 Abs. 1 JI-RL). Hinzu kommt die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO bzw. Art. 4 Abs. 4 JI-RL.<sup>29</sup>

Die Datenverarbeitungsgrundsätze können hier »vor die Klammer« gezogen werden. Automatisierte Datenanalysen laufen als Big Data-Technologien den hier normierten Grundsatzanliegen des Datenschutzrechts allerdings schon ganz grundsätzlich zuwider.<sup>30</sup> Denn Big Data-Technologien und damit auch automatisierte Datenanalysen zeichnen sich durch ihr »Volumen«, das heißt die Möglichkeit der Verarbeitung von Unmengen von Daten, aus, die als solche zunächst im Widerspruch zum Grundsatz der Datenminimierung stehen können. Hinzu kommt, dass die aus dem Transparenzgrundsatz erwachsenden Informationspflichten, die mit dem Rechtsschutz Betroffener<sup>31</sup> korrespondieren, in der Regel für diese Massendatenverarbeitungsverfahren nicht praktikabel sind. Insbesondere bei Weiterverarbeitungen besteht die Gefahr, dass der Zweckbindungsgrundsatz nicht immer gewahrt wird. Werden Daten aus dem Internet verwendet, kann die Sicherstellung der Datenrichtigkeit herausfordernd sein. Bei Machine-Learning-Technologien werden zudem möglicherweise fehlerhafte Muster ausgebildet und verzerrte Ausgaben produziert. Bei der Zusammenarbeit mit privaten Softwareanbietern ist weiterhin ungewiss, ob die Anforderungen an Vertraulichkeit und Datenintegrität eingehalten werden können. Schon diese

---

28 Schuh/Weiss 2024, S. 228.

29 Dazu insgesamt Johannes 2017.

30 Ashkar 2023, S. 524.

31 Art. 12 ff. DS-GVO, Art. 12 ff. JI-RL, §§ 55 ff. BDSG, §§ 31 HDSIG.

mehr kursorische Übersicht zeigt auf, dass erhebliche datenschutzrechtliche Bedenken in Bezug auf den Einsatz von automatisierten Datenanalysen bestehen müssen. Hinzu kommen spezifische Kollisionslagen in den einzelnen Phasen des KI-Lebenszyklus. Diese werden nachfolgend, zunächst allgemein für automatisierte Datenanalysen und daran anknüpfend konkret für hessenDATA besprochen.

### 3.1 Datensammlungs- und Trainingsphase für das Basismodell

Bei kommerziellen Softwareprodukten wie Gotham nebst Zusatzmodulen ist davon auszugehen, dass privatwirtschaftliche Anbieter ein Basismodell »vortrainieren«. Der Personenbezug der Trainingsdaten wird weit überwiegend zu bejahen sein,<sup>32</sup> soweit mit Daten realer Fälle bzw. aus echten Fall- und Vorgangsakten trainiert wird. Gleiches gilt für das Training mit offenen Daten aus dem Internet. Beides wird bei einem System für Predictive Policing oft notwendig sein. Findet das Training in der Verantwortung privater Akteure statt, greift die Datenschutz-Grundverordnung. Unternehmen sind also Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO, sofern sie dem räumlichen Anwendungsbereich (Art. 3 DS-GVO) unterfallen.<sup>33</sup>

Der Trainingsprozess »verzehrt« Mengen personenbezogener Daten. Schon bei Expertensystemen ist von einer Fallbasis von mehreren hundert bis tausend Personen auszugehen.<sup>34</sup> Automatisierte Datenanalysen als Big Data werden unter Einsatz von Verfahren des Maschinellen Lernens trainiert. Hier ist die Fallbasis technisch lediglich durch die zur Verfügung stehenden Rechenkapazitäten begrenzt.<sup>35</sup> Das Abrufen und Aufbereiten von Trainingsdaten erfüllt in der Regel eine Reihe der Verarbeitungstatbestände des Art. 4 Nr. 2 DS-GVO (jedenfalls das Auslesen, Abfragen, die Verwendung und Organisation von Daten).<sup>36</sup> Eine wirksame<sup>37</sup> Anonymisierung im Sinne des Art. 4 Nr. 1 DS-GVO ist bei Datenverarbeitungen im Stil von Big Data schwer möglich.<sup>38</sup>

Zunächst ist daher fraglich, welche Rechtsgrundlage für die Verarbeitung vorliegt. Einer solchen bedürfen Datenverarbeitungen grundsätzlich (Art. 5 Abs. 1 lit. a, 6 DS-GVO). Die Verarbeitung auf Basis von Einwilligung oder zu

---

<sup>32</sup> Vgl. Schuh/Weiss 2024, S. 253.

<sup>33</sup> Hüger 2024, S. 270 f.

<sup>34</sup> Sommerer 2020, S. 63.

<sup>35</sup> Sommerer 2020, S. 63.

<sup>36</sup> Hüger 2024, S. 268 f.

<sup>37</sup> Ashkar 2023, S. 524.

<sup>38</sup> Hüger 2024, S. 270; a. A. Schulz, in: Gola/Heckmann 2022, Art. 6 DS-GVO Rn. 153.

Vertragszwecken zu stützen ist im Fall von Big Data unpraktikabel, insbesondere wenn mit Internetdaten trainiert werden soll. In Betracht kommt daher als Verarbeitungsgrundlage in der Regel nur ein berechtigtes (auch kommerzielles<sup>39</sup>) Interesse der Verantwortlichen (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO). Sich auf ein solches überwiegendes Verarbeitungsinteresse zu stützen setzt die Beachtung hinreichender Datenschutzmaßnahmen – wirksame Anonymisierung, Begrenzung des Datenpools auf das erforderliche Maß – voraus.<sup>40</sup>

Dass bei Big Data-Verfahren der Miteinbezug sensibler Daten im Sinne des Art. 9 DS-GVO kaum auszuschließen ist, stellt eine zusätzliche rechtliche Hürde dar. Das betrifft die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Biometrische Daten dürften im polizeilichen Kontext eine hervorgehobene Rolle spielen. Eine Interessenabwägung wie in Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO ist bei der Verarbeitung sensiblen Daten jedoch ausgeschlossen. Vor allem Modelle, die Daten aus den öffentlich einsehbaren Teilen des Internets verarbeiten, dürften massenhaft sensible Daten abgreifen. Nach Art. 9 Abs. 2 lit. e DS-GVI ist die Verarbeitung personenbezogener Daten besonderer Kategorien allerdings dann nicht verboten, wenn sich die Verarbeitung auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat. Private Anbieter könnten also versuchen, die Konformität mit der Datenschutz-Grundverordnung durch eine effektive Aussonderung nicht-öffentlicher<sup>41</sup> sensibler Daten herzustellen.<sup>42</sup>

Auch im Trainingsprozess finden relevante Datenverarbeitungen statt. Das System selbst »lernt« mit wahrscheinlichkeitsrelevanten Werten. Bei der Übersetzung der vorliegenden Trainingsdaten in die algorithmische Lernsprache geht ihr Personenbezug insofern verloren, als er für Menschen nicht mehr rekonstruierbar ist.<sup>43</sup> Jedenfalls beim Test des KI-Systems unter Realbedingungen findet aber wieder ein Abgleich mit personenbezogenen Daten statt.<sup>44</sup> Wie im Rahmen

---

39 Schulz, in: Gola/Heckmann 2022, Art. 6 DS-GVO Rn. 61.

40 Ashkar 2023, S. 526; Hüger 2024, S. 271.

41 Die Veröffentlichung ist ein Realakt des Datensubjekts, Schulz, in: Gola/Heckmann 2022, Art. 9 DS-GVO Rn. 32 f.; Internetdaten sind insbesondere problematisch, weil von der Einsehbarkeit nicht auf die erforderliche subjektive Komponente der Veröffentlichung geschlossen werden kann.

42 Ashkar 2023, S. 527; Hüger 2024, S. 275.

43 Vergleiche Hüger 2024, S. 277, der aber vor allem auf das Training von Large Language Models abzustellen scheint; ebenfalls für LLMs Spies 2024, S. 290.

44 Hüger 2024, S. 279.

der Datenzusammenstellung ist von einer Einwilligung der betroffenen Personen zur Verarbeitung kaum auszugehen, da im Normalfall keine Kenntnis der Verarbeitung vorliegen wird. Insofern gelten die oben genannten Einwände auch hier. Hinzu kommt, dass gerade in Testverfahren regelmäßig sensible Daten im Sinne des Art. 9 DS-GVO eingespielt werden, um Diskriminierungseffekten bei der späteren Anwendung vorzubeugen.<sup>45</sup> Die Verwendung effektiv anonymisierter, pseudonymisierter oder künstlicher Daten ist vorzuzugswürdig, aber zu Trainingszwecken wohl nicht immer gleich geeignet.<sup>46</sup> Die Vermeidung von Diskriminierung durch das Endprodukt ist also nur durch die Verwendung diskriminierungssensibler Daten im Trainingsprozess möglich. Das wirkt zunächst paradox, veranschaulicht letztlich aber, dass Diskriminierung der Funktionsweise solcher Systeme zwangsläufig inhärent ist. Denn deren Aufgabe ist es schlechterdings, (vereinfachend) Klassifizierungen und Bewertung realweltlicher Phänomene vorzunehmen.

### 3.2 Verarbeitung von Behördendaten während des *fine-tunings*

Die datenschutzrechtlichen Anforderungen in der Phase des *fine-tunings* richten sich nach dem konkreten System und der vertraglichen Vereinbarung zwischen Behörde und Softwaredienstleisterin. Grundsätzlich ist davon auszugehen, dass in dieser Phase Daten, die die Behörde zur Verfügung gestellt hat, im Rahmen weiterer Trainingsprozesse zur Systemanpassung verarbeitet werden. Hier wirken also privatwirtschaftliche mit öffentlichen Akteuren zusammen. Dabei gilt die DS-GVO für den privatwirtschaftlichen Akteur, der kein Auftragsverarbeiter ist, und die JI-Richtlinie respektive ihre Umsetzungsakte für die Polizei- und Ermittlungsbehörden. Diskutiert wird, dass allein die Datenschutz-Grundverordnung einschlägig sei, da es sich in diesem Verfahrensstadium noch nicht um einen Verarbeitungsvorgang im Rahmen der Strafverfolgung etc. handelt, die nach Art. 2 Abs. 2 lit. d DS-GVO respektive Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 JI-RL den die JI-Richtlinie umsetzenden bundesrechtlichen und landesrechtlichen Regelungen unterfällt.<sup>47</sup> Dies folgt dem Argument, dass die Ausnahmetatbestände der Datenschutz-Grundverordnung eng auszulegen seien.<sup>48</sup> Datenverarbeitungen im Rahmen des *fine-tunings* bereiten die Anwendung des Systems zur Gefahrenabwehr lediglich vor, sind dieser also zeitlich wie technisch deutlich

---

<sup>45</sup> Kelber/Bortnikov 2023, S. 2002; Hüger 2024, S. 280.

<sup>46</sup> Kelber/Bortnikov 2023, S. 2002.

<sup>47</sup> Gola, in: Gola/Heckmann 2022, Art. 2 DS-GVO Rn. 28; Kelber/Bortnikov 2023, S. 2003.

<sup>48</sup> Erwgr. 3 ff., 10 DS-GVO; Kelber/Bortnikov 2023, S. 2003.

vorgelagert. Gegen diese Anschauung spricht aber, dass der Anwendungsbereich der JI-Richtlinie autonom auszulegen ist und nach dem Grundsatz der optimalen Wirkungskraft wohl gerade weit wirkt bzw. Art. 9 Abs. 2 JI-RL eng auszulegen ist. Entsprechend ist mit Art. 1 Abs. 3 JI-RL auch nur eine Mindestharmonisierung vorgesehen, was darauf hinweist, dass den Mitgliedstaaten im Bereich der JI-Richtlinie eher Regelungsräume eröffnet werden. Wichtigstes Argument ist aber: Das fine-tuning eines KI-Systems zu Zwecken der Gefahrenabwehr oder Strafverfolgung wirkt sich direkt auf die Funktion und Ergebnispräsentation des Systems aus. Es steht also im engsten Zusammenhang mit dem Zweck der damit einhergehenden Datenverarbeitung. Insoweit ist es nicht nur eine rein vorgelagerte Tätigkeit, wie zum Beispiel die Installation und Anpassung eines Textverarbeitungsprogramms. Dies gilt umso mehr, wenn das fine-tuning als kontinuierlicher bzw. nicht wiederholender Vorgang begriffen wird, der zur Verbesserung des sich im Einsatz befindlichen Systems dient. Auch die Regelungen nach Art. 7 JI-RL zur Unterscheidung zwischen personenbezogenen Daten und Überprüfung der Qualität der personenbezogenen Daten sowie Art. 11 JI-RL zur automatisierten Entscheidung im Einzelfall sprechen eher dafür, dass das fine-tuning für die zuständigen Behörden zur eigentlichen Verarbeitung im Anwendungsbereich der JI-Richtlinie gehört. Im Ergebnis spielt die Unterscheidung jedoch ohnehin nur in Details eine Rolle, da JI-Richtlinie und DS-GVO den Verantwortlichen weitgehend gleiche Pflichten und Rechte aufbürden bzw. einräumen.<sup>49</sup>

### 3.2.1 *Fine-tuning als Auftragsverarbeitung oder im gemeinsamen Verfahren*

Bei der Datenverarbeitung im Rahmen des fine-tunings kann es sich um eine Auftragsverarbeitung (Art. 28 DS-GVO respektive Art. 22 JI-RL) oder eine Verarbeitung in gemeinsamer Verantwortlichkeit (Art. 26 DS-GVO respektive Art. 21 JI-RL) handeln. Ein Auftragsverarbeiter ist nach Art. 4 Nr. 8 DS-GVO respektive Art. 3 Nr. 9 JI-RL eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Unterscheidungskriterium ist das Vorliegen eines Subordinationsverhältnisses: Auftragsverarbeitende werden nur weisungsgebunden tätig.<sup>50</sup> Da im Stadium des fine-tuning-Prozesses bereits ein schuldvertragliches Verhältnis zwischen der Behörde als Auftraggeber und dem IT-Entwickler als Auftragnehmer zustande gekommen ist, ist davon auszugehen, dass im Rahmen dieser

---

<sup>49</sup> Zu den Stellen, an denen die JI-Richtlinie und die DS-GVO im Detail »strenger« sind Johannes 2020, S. 413 ff.

<sup>50</sup> Gola, in: Gola/Heckmann 2022, Art. 4 DS-GVO Rn. 88; Ashkar 2023, S. 524.

Vertragsbeziehung für die hierfür erforderlichen Datenverarbeitungen auch regelmäßig ein Auftragsverarbeitungsvertrag (Art. 28 Abs. 3 DS-GVO respektive Art. 22 Abs. 3 JI-RL) zu schließen ist. Dann ist die auftraggebende Behörde allein Verantwortlicher im datenschutzrechtlichen Sinn. Das gilt nach Art. 22 Abs. 5 JI-RL respektive Art. 28 Abs. 10 DS-GVO nicht beim sogenannten Rollenexzess, also einer außervertraglichen Datenweitzernutzungen des IT-Entwicklers. Die Auftragsverarbeiterin ist nach Art. 28 Abs. 3 Nr. 2 DS-GVO respektive Art. 22 Abs. 3 lit. d JI-RL insbesondere zur Gewährleistung der Sicherheit und Vertraulichkeit sowie nach Beendigung des Auftragsverhältnisses zur Löschung der Daten verpflichtet. Die Sicherstellung der DS-GVO-Konformität obliegt aber hauptsächlich der Behörde als Auftraggeberin (Art. 28 Abs. 1 DS-GVO i. V. m. Art. 24 Abs. 1 DS-GVO respektive Art. 22 Abs. 1 JI-RL i. V. m. Art. 19 Abs. 1, 23 JI-RL). Richtigerweise ist die Datenweitergabe an die Auftragsverarbeiterin nicht als Übermittlung und somit Datenverarbeitung im Sinne des Art. 4 Nr. 2 DS-GVO respektive Art. 3 Nr. 2 JI-RL aufzufassen, da diese aufgrund der Weisungsgebundenheit »fiktive« interne Empfängerin ist. Somit entsprechen die datenschutzrechtlichen Verpflichtungen während des fine-tuning-Prozesses im Wesentlichen den oben genannten Maßgaben, richten sich allerdings an die Behörde. Liegt im konkreten Fall eine gemeinsame Verarbeitung vor, so gelten die Maßgaben des Art. 26 DS-GVO respektive Art. 21 JI-RL.

### 3.2.2 *Erfordernis einer Rechtsgrundlage für die Datenweiterverarbeitung*

Jede Datenverarbeitung zu Trainingszwecken im Rahmen des fine-tunings bedarf einer Rechtsgrundlage. Im Anwendungsbereich der Datenschutz-Grundverordnung kommt zunächst Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO in Betracht, also eine Verarbeitung im Rahmen der öffentlichen Aufgabenwahrnehmung. Generalklauselartige Ermächtigungsnormen sind Art. 3 BDSG beziehungsweise Art. 3 I HDSIG.<sup>51</sup> Die Datenverarbeitung hiernach muss jedoch erforderlich und auch angemessen sein, was erstens nur Datenverarbeitungen mit geringer Eingriffsintensität zulässt.<sup>52</sup> Zweitens gilt damit der Zweckbindungsgrundsatz.<sup>53</sup> Dessen Geltung ergibt sich, unabhängig von der Verarbeitungsgrundlage – in Betracht kommt neben Art. 6 Abs. 1 UAbs. 1 lit. e DS-GVO außerdem noch Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO als Verarbeitung zur Sicherstellung der Sicherheit der Datenverarbeitung<sup>54</sup> – bereits aus Art. 5 Abs. 1 DS-GVO. Regelmäßig wer-

---

51 Schulz, in: Gola/Heckmann 2022, Art. 6 DS-GVO Rn. 51.

52 Starnecker, in: Gola/Heckmann 2022, § 3 BDSG Rn. 26 ff.; Kelber/Bortnikov 2023, S. 2003.

53 Starnecker, in: Gola/Heckmann 2022, § 3 BDSG Rn. 35.

54 Kelber/Bortnikov 2023, 2003 f.

den die bei der Polizei gespeicherten Daten auf der Grundlage des § 45 BDSG (bzw. § 40 I HDSIG) zum Zweck der Strafverfolgung beziehungsweise Gefahrenabwehr erhoben worden sein. Werden diese Daten für das fine-tuning des KI-Systems verwendet, liegt also eine Zweckänderung vor, für die Art. 9 Abs. 1 JI-RL respektive § 49 Abs. 2 BDSG oder § 44 Abs. 2 HDSIG einschlägig ist.<sup>55</sup>

### 3.3 Anwendungsphase: Vorgaben der JI-Richtlinie und der Umsetzungsrechtsakte

#### 3.3.1 Allgemeine Datenverarbeitungsgrundsätze und Verfahrenssicherung

Die allgemeinen Grundsätze zur Datenverarbeitung statuieren unter anderem den bereits skizzierten Zweckbindungsgrundsatz, aus dem Vorgaben zur Datenlöschung und Systemintegrität resultieren (Art. 4 JI-RL, § 47 BDSG, § 42 HDSIG). Daten dürfen nicht länger als zur Zweckerreichung erforderlich gespeichert werden. Zudem erstreckt sich das Datenrichtigkeitsgebot (Art. 4 Abs. 1 lit. d JI-RL, § 47 Nr. 4 BDSG, § 42 Nr. 4 HDSIG) auch auf probabilistische Ausgaben automatisierter Prozesse.<sup>56</sup> Ein System muss erkennen lassen, ob es Tatsachen- oder Wahrscheinlichkeitsaussagen trifft. Auch sind Nutzende in die Lage zu versetzen, den maschinellen Erwägungsprozess nachzuvollziehen und gegebenenfalls kritisch einzuordnen. Datensicherheit wiederum ist mitunter durch geeignete technische und organisatorische Maßnahmen gegen unbefugte oder unrechtmäßige Verarbeitung zu gewährleisten. Gesichert werden soll hiermit die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme (weiter konkretisiert in Art. 29 JI-RL, respektive § 64 Abs. 2 BDSG, § 59 Abs. 2 HDSIG). Für automatisierte Verarbeitungen sind verschiedenste Kontrollen, etwa eine Zugangskontrolle oder die Datenträgerkontrolle, vorgesehen (Art. 29 Abs. 2 JI-RL, respektive § 64 Abs. 3 BDSG, § 59 Abs. 3 HDSIG). Sinn und Zweck ist die Absicherung gegen die Einsichtnahme Unbefugter und eine technisch fehlerfreie Datenverarbeitung.<sup>57</sup> Bei der Einführung neuer datenverarbeitender Technologien, die voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen begründen, ist vorab eine Datenschutz-Folgenabschätzung vorzunehmen (Art. 27 JI-RL, § 67 BDSG, § 62 HDSIG) und Datenschutzbeauftragte sind zu beteiligen.

---

<sup>55</sup> Schuh/Weiss 2024, S. 258 ff.

<sup>56</sup> Pesch/Böhme 2023, S. 921.

<sup>57</sup> Bäuerle, in: Möstl/Bäuerle 2025, § 20 HSOG Rn. 122 ff.

### 3.3.2 Verbot diskriminierenden Profilings

Eine Vorgabe zu Profiling und Predictive Policing enthält Art. 11 JI-RL beziehungsweise enthalten die §§ 54 I BDSG, 49 I HDSIG. Es gilt eine Zulässigkeitsbegrenzung vollautomatisierter Entscheidungen im Sinne eines grundsätzlichen Verbots. Der Verzicht auf den »human in the loop« steht im deutschen Recht unter Gesetzesvorbehalt und ist nach europarechtlichen Maßgaben nur im Ausnahmefall erlaubt. Grundsätzlich verboten ist, dass eine Entscheidung *ausschließlich* auf einer automatisierten Verarbeitung beruht und zudem mit einer nachteiligen Außenwirkung verbunden ist.

#### 3.3.2.1 Begriff der vollautomatisierten Entscheidung

Was damit gemeint ist, ist mitnichten eindeutig. Auch automatisierte Datenanalysen fallen möglicherweise hierunter.<sup>58</sup> Nach einem wirklichkeitsnahen Normverständnis aber scheint der europäische Gesetzgeber *prima facie* hier vollautomatisierte Sachverhaltsbewertung, etwa durch Expertensysteme, ohne menschliche Übersicht gemeint zu haben. Zum Beispiel die Bewertung, ob ein Anfangsverdacht zur Ermittlung gegen eine bestimmte Person vorliegt. Der Wortlaut ist dann aber doch weiter, stellen Art. 11 Abs. 1 JI-RL und die korrespondierenden Absätze des nationalen Rechts denn nicht nur auf »nachteilige Rechtsfolgen«, sondern zudem auf »erhebliche Beeinträchtigungen« ab. Solche nachteiligen automatisierte Entscheidungen können schon in Gestalt von Zwischenfestlegungen automatisierter Prozesse vorliegen. Führen sie zudem zu weiteren Datenverarbeitungsprozessen, liegen mitunter auch Beeinträchtigungen in Gestalt von Eingriffen in das Recht auf informationelle Selbstbestimmung, in Art. 10 Abs. 1, 13 Abs. 1 und/oder in Art. 3 Abs. 3 Satz 1 GG vor. *Kugelmann* und *Buchmann* haben daher für die Abgrenzung eine Unterscheidung von Systemen zur Wissensverdichtung beziehungsweise solchen zur Wissensgenerierung vorgeschlagen.<sup>59</sup> Das entspricht der Rechtsprechung des Bundesverfassungsgerichts zur spezifischen Eingriffsintensität der Herstellung »neuen Wissens«. Demzufolge wären automatisierte Datenanalysen durch ihre wissensgenerierende Funktion als automatisierte Entscheidungsfindung im Einzelfall zu verstehen und dem Gesetzesvorbehalt sowie den Anforderungen an Rechtsstaatlichkeit und Verfahrenssicherung des Art. 11 Abs. 1 JI-RL zu unterstellen.

Der Bundesgesetzgeber hat allerdings einen anderen Weg eingeschlagen; der Gesetzesbegründung zum BDSG ist zu entnehmen, dass interne Zwischenfestlegungen oder -auswertungen vollautomatisierter Prozesse nicht unter § 54 Abs. 1

---

<sup>58</sup> Kugelmann/Buchmann 2024, S. 3; a. A. Arzt 2023, S. 998.

<sup>59</sup> Kugelmann/Buchmann 2024, S. 3.

BDSG fallen sollen.<sup>60</sup> Die gesetzgeberische Entscheidung soll hier aber als gesetzt angenommen werden, zumal die besonders grundrechtssensiblen personenbezogenen automatisierten Datenanalysen ohnehin unter den Begriff des Profiling fallen.<sup>61</sup>

### 3.3.2.2 *Generierung neuen personenbezogenen Wissens durch automatisierte Datenanalysen als Profiling*

Anders als bei automatisierten Einzelfallentscheidungen sorgt die Legaldefinition des Art. 3 Nr. 4 JI-RL in Bezug auf Profiling dankenswerterweise für Normklarheit. Jenes ist demnach

»jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.«

Das entspricht der Rechtsprechung des Ersten Senats des Bundesverfassungsgerichts. Im Urteil zur automatisierten Datenanalyse vertrat dieser die Auffassung, dass sich Datenanalysen einem Profiling im Sinne des HDSIG beziehungsweise der JI-Richtlinie schon dann zumindest annähern, wenn sie eine intensivere Datenerschließung ermöglichen.<sup>62</sup> Das Urteil stellt eindeutig schon auf die automatisierte Wissensgenerierung, das heißt neuer, sonst nicht sicht- oder ermittelbarer persönlichkeitsrelevanter Erkenntnisse, als Profiling ab.<sup>63</sup> Das entspricht dem Vorschlag von *Kugelman* und *Buchmann*, die die automatisierte Natur von Sachverhaltsbewertungen im Fall von Big Data am Kriterium der Generierung neuen Wissens festmachen. Art. 11 Abs. 3 JI-RL (respektive § 54 Abs. 3 BDSG, § 49 Abs. 3 HDSIG) enthält ein diskriminierungsspezifisches Profiling-Verbot. Besonders sensible Daten dürfen nicht zum Profiling herangezogen werden. Für deren Verarbeitung im Rahmen von ortsbezogenen Analysen hingegen gilt Art. 10 JI-RL (respektive § 48 BDSG, § 20 HDSIG) und damit ein Gesetzes- und Erforderlichkeitsvorbehalt.

---

60 BT Drs. 18/1135, 112; BR Drs. 110/117, 115; ebenso Ashkar 2023, S. 530; kritisch Lauscher/Legner 2022, S. 381.

61 Arzt 2023, S. 998.

62 BVerfGE 165, 363 (396).

63 BVerfGE 165, 363 (396).

### 3.3.3 Weiterlernende Systeme

Auch das Weiterlernen von Machine-Learning-basierten Systemen mit personenbezogenen Daten der Sicherheitsbehörden ist demgemäß eine Verarbeitung im datenschutzrechtlichen Sinn. Dem steht die Rechtsprechung zur Rasterfahndung nicht entgegen. Das Bundesverfassungsgericht sprach hier einem »sekundenschnellen Datenabgleich«<sup>64</sup> Eingriffsqualität ab;<sup>65</sup> in einem späteren Urteil zur Kennzeichenkontrolle wurde wiederum ein Eingriff bejaht – jedoch mit dem Zusatz, dass wenn »der Datenabgleich in Sekundenschnelle durchgeführt wird und die erfassten Daten im Nichttrefferfall sofort vollständig wieder gelöscht werden, ohne einer Person bekannt zu werden« dies dem Eingriff »erheblich an Gewicht« nehme.<sup>66</sup> Gemeint war eine ungezielte und allein technikbedingte Datenerfassung, gefolgt von einer anonymen und spurlosen Datenwiederaussonderung.<sup>67</sup> Diese Rechtsprechung lässt sich nicht ohne weiteres auf die derzeitigen Verfahren zur automatisierten Datenanalyse übertragen. Der Rasterfahndung liegt ein simples positiv/negativ-Schema zugrunde: Das System zeigte einen Treffer an oder eben nicht.<sup>68</sup> Big Data-Analysen, zumal unter dem Rückgriff auf KI, sind bedeutend komplexer sowie spezifischer und nicht auf Datenaussonderung, sondern auf Aufbereitung und Sortierung angelegt.<sup>69</sup> Lernt das System mit den Polizeidaten weiter, werden diese für die Herausbildung neuer Entscheidungsregeln genutzt.<sup>70</sup> Selbst wenn Daten ausgesondert werden, hinterlassen sie also Spuren im System. Auf den schlichten Schutz vor menschlicher Sichtung kann es nicht ankommen; das behördliche Datennutzungsinteresse hat sich – mit der Terminologie des Rasterfahndungsbeschlusses<sup>71</sup> – schon grundrechtsrelevant verdichtet. In Bezug auf weiterlernende Systeme könnte man durchaus erwägen, den Begriff der automatisierten Einzelfallentscheidung entsprechend den obigen Überlegungen anzuwenden. Denn die Künstliche Intelligenz bildet neue Entscheidungsregeln

---

64 BVerfGE 116, 320 (375).

65 BVerfGE 115, 320 (343 f.): »An der Eingriffsqualität fehlt es lediglich, sofern Daten ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden. [...] Maßgeblich ist, ob sich bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist«.

66 BVerfGE 150, 244 (283).

67 BVerfGE 115, 320 (343).

68 Rademacher 2017, S. 395 f.

69 Rademacher 2017, S. 396.

70 BVerfGE 165, 363 (408).

71 BVerfGE 115, 320 (343).

aus, die aufgrund der algorithmischen Komplexität nicht mehr nachvollzogen werden können.<sup>72</sup>

In seiner Entscheidung zur Datensammlung über steuerliche Auslandsbeziehungen konkretisierte das Bundesverfassungsgericht diesen Schutzgedanken weiter.<sup>73</sup> Zwar stellte es erneut fest, dass es dem Staat nicht verwehrt ist, von jedermann zugänglichen Informationsquellen unter denselben Bedingungen wie jeder Dritte Gebrauch zu machen.<sup>74</sup> Es stellte jedoch ebenfalls klar, dass der staatliche Umgang mit personenbezogenen Daten, die für sich alleine genommen keine besondere Relevanz für die Freiheit und Privatheit des Betroffenen haben, je nach seinem Ziel und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben kann. Ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung ist deswegen auch anzunehmen, wenn die aus öffentlich zugänglichen Quellen stammenden Daten durch ihre systematische Erfassung, Sammlung und Verarbeitung einen zusätzlichen Aussagewert erhalten, aus dem sich die für das Grundrecht auf informationelle Selbstbestimmung spezifische Gefährdungslage für die Freiheitsrechte oder die Privatheit des Betroffenen ergibt. So kann es etwa liegen, wenn diese Daten mit anderen Daten verbunden werden und dadurch der Aussagegehalt der verknüpften Daten insgesamt zunimmt. In diesem Falle liegt keine »eingriffslose« Internetaufklärung vor, sondern eine Datenverarbeitung, für die es grundsätzlich einer Erlaubnis bedarf.<sup>75</sup>

Der Sinn der hier untersuchten automatisierten Datenanalyse liegt gerade darin, Daten, die ohnehin jederzeit und ohne Rücksicht auf Entfernungen in Sekundenschnelle aus offenen oder der Polizei zugänglichen Quellen abrufbar sind, so zu ordnen, dass sie beim Aufbau integrierter Informationssysteme mit anderen Datensammlungen der Polizei- und Strafverfolgungsbehörden zusammengesetzt werden können. Das Zusammenführen, das Abgleichen und die Auswertung von personenbezogenen Informationen ist ihr Zweck. Der Einsatz durch die Polizei und Strafverfolgungsbehörden greift daher in das Grundrecht auf informationelle Selbstbestimmung ein. Es kann dahinstehen, ob das Recht auf informationelle Selbstbestimmung vor der Erhebung jedes einzelnen Datums, das von der Verarbeitung erfasst wird, schützt, da die Verknüpfung der Daten aus unterschiedlichen (öffentlichen) Quellen eigenständigen Einblick in

---

72 EuGH, Urt. v. 21.06.2021, C-817/19, *Ligue de droits humains gegen Conseil de ministres*, ECLI:EU:C:2022:491, Rn. 195; BVerfGE 115, 320 (343).

73 BVerfGE 120, 351 (361).

74 So auch BVerfGE 142, 234 (251 f.).

75 BVerfGE 142, 234.

den Persönlichkeitsbereich oder sogar das Erstellen eines Persönlichkeitsprofils ermöglicht.<sup>76</sup>

Das würde bedeuten, dass sowohl personen- als auch ortsbezogene Analyseverfahren, die auf weiterlernender Software basieren, den Anforderungen des Art. 11 Abs. 1 JI-RL unterliegen. Werden besondere Kategorien personenbezogener Daten verwendet, sind spezifische Schutzmaßnahmen zu treffen (Art. 11 Abs. 2 JI-RL, entsprechend § 54 Abs. 2 BDSG, § 49 Abs. 2 HDSIG).

#### 4. Vorgaben der KI-Verordnung für personenbezogene Datenanalysen

Die KI-Verordnung gilt gemäß Art. 288 Abs. 2 AUEV in den Mitgliedstaaten unmittelbar. Ihr Zweck ist die Schaffung eines einheitlichen Rechtsrahmens für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der Union.<sup>77</sup> Menschbezogene und vertrauenswürdige KI soll gefördert werden.<sup>78</sup> Die Europäische Union sieht einen hohen Schutzstandard in Bezug auf Menschenrechte vor, der mit dem Interesse an Innovationsförderung in Einklang gebracht werden soll.<sup>79</sup> Der Ansatz der KI-Verordnung ist risikobasiert.<sup>80</sup> Sie gilt nach Art. 113 KI-VO vollständig ab dem 2. August 2026. Einige Regelungen gelten schon früher, allerdings nicht der hier einschlägige Art. 6 Abs. 2 KI-VO (Art. 113 lit. a KI-VO). Aus der KI-Verordnung ergeben sich daher ab Mitte 2026 weitere Vorgaben für automatisierte Datenanalysen. Diese gelten für bereits in Verkehr gebrachte oder sich auf dem Markt befindliche Hochrisiko-KI-Systeme gemäß Art. 111 Abs. 2 Satz 1 KI-VO nur dann, wenn diese Systeme wesentlich verändert werden. Gemeint sind Änderungen, die die Konformität mit den Anforderungen der Verordnung beeinträchtigen könnten, wie zum Beispiel Änderungen des Betriebssystems oder der Softwarearchitektur.<sup>81</sup> Die KI-Verordnung und das Datenschutzrecht gelten nebeneinander.<sup>82</sup> Die Überwachung von in Betrieb befindlichen Systemen geht mit Datenverarbeitungen im Sinne der Datenschutz-Grundverordnung einher, weil sie die Speicherung und gegebenenfalls auch Übermittlung von personenbezogenen

---

<sup>76</sup> Vgl. BVerfGE 115, 320 (342 f.).

<sup>77</sup> Erwgr. 1 KI-VO.

<sup>78</sup> Erwgr. 1, 6 KI-VO.

<sup>79</sup> Erwgr. 2, 8 KI-VO.

<sup>80</sup> Möller-Klapperich 2024, 338.

<sup>81</sup> Erwgr. 128, 177 KI-VO.

<sup>82</sup> Erwgr. 9 KI-VO.

Daten erfordert.<sup>83</sup> Rechtsgrundlage für die privatwirtschaftlichen Anbieter dafür könnte Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO sein. Hier greift also wiederum das Pflichtenprogramm des Art. 5 DS-GVO. Rechtsgrundlage für die Polizei- und Ermittlungsbehörden im Anwendungsbereich der JI-Richtlinie könnten Vorschriften zur Umsetzung von Art. 8 JI-RL in Verbindung mit Vorschriften zur Gewährleistung der Sicherheit der Datenverarbeitung zur Umsetzung von Art. 29 JI-RL sein.

Die Vorschriften der KI-Verordnung werden in absehbarer Zeit Relevanz für alle Verarbeitungsphasen entfalten. Sie verlaufen teilweise parallel zum Datenschutzregime, grundsätzlich sind hier aber Kollisionen angelegt; denn die Innovationsförderung von KI-Systemen bedeutet die Förderung von Big Data.

Polizeibehörden sind Strafverfolgungsbehörden im Sinne des Art. 3 Nr. 45 lit. a KI-VO. Personenbezogene automatisierte Datenanalysen unterfallen daher als Profiling-Methoden Nr. 6 lit. e Annex III KI-VO und beim Einsatz als Risikobewertungstools gegebenenfalls auch Nr. 6 lit. a Annex III KI-VO. Damit besteht die widerlegbare Vermutung, dass es sich um Hochrisiko-Systeme im Sinne des Art. 6 Abs. 3 KI-VO handelt.<sup>84</sup> Ortsbezogene Analysen hingegen fallen nicht unter Nr. 6 Annex III KI-VO; sie sind somit keine Hochrisiko-KI-Systeme. In Bezug auf sie ist die Befolgung der nachgenannten Vorgaben freiwillig (Art. 95 Abs. 1 KI-VO). Die Vorgaben der KI-VO richten sich sowohl an die Sicherheitsbehörden als Betreiberinnen (Art. 2 Abs. 1 lit. b i. V. m. Art. 3 Nr. 4 KI-VO) als auch private IT-Anbieter – wie Palantir Technologies – als Anbieter (Art. 2 Abs. 1 lit. a i. V. m. Art. 3 Nr. 3 KI-VO).

#### 4.1 Vorgaben für Anbieter:innen

Die Pflichten für Anbieter von Hochrisiko-KI-Systemen ergeben sich aus Art. 16 KI-VO. Einige dieser Pflichten gelten vor Inbetriebnahme, andere während des gesamten Lebenszyklus des KI-Systems. Art. 72 Abs. 2 KI-VO bestimmt gleichwohl, dass Anbieter im Rahmen einer post market surveillance die fortdauernde Konformität mit Art. 16 lit. a KI-VO anhand der von Betreibern zur Verfügung gestellten Informationen bewerten können müssen. Erforderlich ist die Einrichtung eines Risikomanagementsystems (Art. 9 KI-VO), die Sicherstellung einer hinreichenden Datenqualität im Rahmen des Trainings (Art. 10 KI-VO), eingedenk einer bias-Prävention, die technische Dokumentation sowie Protokollierung im Sinne einer automatischen Aufzeichnung von Ereignissen während

---

<sup>83</sup> Hüger 2024, S. 282.

<sup>84</sup> Möller-Klapperich 2024, S. 340.

des Betriebs des Systems (Art. 11 KI-VO), die Gewährleistung von Genauigkeit, Cybersicherheit und Robustheit (Art. 15 KI-VO) und schließlich auch die Ermöglichung effektiver menschlicher Aufsicht. Hinzu kommen Pflichten aus Art. 17 bis 20 und nach 43 ff. KI-VO im Rahmen des Notifizierungsverfahrens. Es drohen scharfe Sanktionen (Art. 99 KI-VO), die neben die Sanktionen etwa aus der Datenschutz-Grundverordnung treten.

Nach Art. 10 Abs. 4 KI-VO müssen Trainings-, Validierungs-, und Testdatensätze den geografischen und kontextuellen Parametern der Verwendung gerecht werden. Insofern kommt dem fine-tuning des Basismodells besondere Bedeutung zu. Möglicherweise können hier künftig auch die Maßnahmen für Innovationsförderungen nach den Art. 57 ff. KI-VO zwischen Datenschutzrecht und KI-Governance vermitteln.<sup>85</sup> Art. 59 Abs. 1 lit. a Var. i) KI-VO erlaubt die Weiterverarbeitung von für andere Zwecke erhobenen personenbezogener Daten zum Zweck des Trainings von KI-Systemen, die der öffentlichen Sicherheit dienen. Es gilt allerdings der Vorbehalt der Erforderlichkeit. Somit liegt in Zukunft eine Rechtsgrundlage für die Datenweiterverarbeitung im Rahmen von Trainingsprozessen vor. Diese ist gleichwohl an die Bedingungen des Art. 59 KI-VO geknüpft und damit, unter anderem, neben der Erforderlichkeit der Weiterverarbeitung auch an die Einhaltung von Sicherheitsvorkehrungen. Bemerkenswert ist in diesem Zusammenhang auch Art. 10 V KI-VO, der als Ausnahmenvorschrift zu Art. 9 Abs. 1 DS-GVO bzw. Art. 10 JI-RL die notwendige Verarbeitung von personenbezogenen Daten in der Trainingsphase zur Erkennung und Korrektur von *bias* erlaubt.<sup>86</sup> Die Verwendung künstlicher oder anonymisierter Daten ist sowohl nach Art. 59 KI-VO als Art. 10 Abs. 5 lit. a KI-VO vorzugswürdig.

Nach Art. 14 KI-VO müssen Anbieter (wie Palantir Technologies) auch während der Verwendung die wirksame menschliche Aufsicht gewährleisten. Diese Pflichten sind durch Bereitstellung aller notwendigen Informationen, etwa in der Betriebsanleitung, sicherzustellen.<sup>87</sup> Es gelten Sensibilisierungspflichten hinsichtlich der Funktionsweise des Systems, um Fehlfunktionen identifizieren zu können und zudem insbesondere in Bezug auf den automation bias (vergleiche Art. 14 Abs. 4 lit. a und b KI-VO). Die Interpretation von Ausgaben des KI-Systems soll mitunter durch Transparenz der Systeme erleichtert werden.<sup>88</sup> Das Thema Transparenz beziehungsweise Nachvollziehbarkeit fängt Forderungen nach explainable AI (XAI) ein.<sup>89</sup> Sie greifen mit dem Datenrichtigkeitsgebot (siehe Art. 5 Abs. 1 lit. d DS-GVO respektive Art. 4 Abs. 1.1 lit. d JI-RL, § 47 Nr. 4

---

<sup>85</sup> Hüger 2024, S. 286 ff.

<sup>86</sup> Müller-Peltzer/Tanczik 2023, S. 457.

<sup>87</sup> Ewgr. 72 f. KI-VO.

<sup>88</sup> Ewgr. 72 f. KI-VO.

<sup>89</sup> Rademacher 2021, S. 250.

BDSG, § 42 Nr. 4 HDSIG) ineinander. Problematisch ist hier insbesondere, wenn die Anbieter von KI-Systemen keine Berichtigung der Datensätze vornehmen können.<sup>90</sup>

Die Pflichten aus Art. 14 KI-VO lassen sich auf zwei verschiedene Aspekte der Anwendung zur automatisierten Datenanalyse beziehen. Offensichtlich ist zunächst der Umgang mit Analyseergebnissen (insbesondere Art. 14 Abs. 4 lit. b und lit. c KI-VO). Hier kann es nicht darauf ankommen, Nutzende in die Lage zu versetzen, die Mathematik hinter der Entscheidung des Systems nachzuvollziehen. Vielmehr sollte ein System eine Begründung darbieten, aus der die relevanten Entscheidungsaspekte und ihre Gewichtung ersichtlich wird.<sup>91</sup> Der zweite, damit zusammenhängende Aspekt der XAI ist die Systemüberwachung. Diese baut ebenfalls auf eine hinreichend kritische Haltung dem System gegenüber auf, setzt aber mehr technisches Knowhow voraus. Denn hier geht es auch um das Erkennen und Beheben von Anomalien, Fehlfunktionen und unerwarteter Leistung (Art. 14 Abs. 4 lit. a KI-VO).

#### 4.2 Vorgaben für Polizeibehörden als Betreiber:innen

Art. 26 KI-VO statuiert darüber hinaus Betreiberpflichten, die zum Teil mit den Anbieterpflichten ineinandergreifen. Betreiber:innen obliegen insbesondere die Überwachung und menschliche Aufsicht des Systems sowie eine Protokollierung nebst Aufbewahrung für mindestens sechs Monate. Das soll die *post market surveillance* nach Art. 72 KI-VO ermöglichen (Art. 26 Abs. 5 KI-VO), aber auch Transparenz und Rechtsschutz fördern, was allerdings nur durch eine Beachtung auch des einschlägigen Datenschutzrechts möglich ist. Natürliche Personen, die von Entscheidungen von Hochrisiko-KI-Systemen betroffen sind, sind über deren Einsatz zu informieren (Art. 26 Abs. 11 KI-VO i. V. m. Art. 13 JI-RL). Die Aufsichtspflicht wird nach Art. 26 Abs. 2 KI-VO natürlichen Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, übertragen. Das bedeutet, dass im Zweifelsfall IT-Spezialist:innen zur Prüfung des Systems zur Verfügung stehen müssen. Doch selbst versiertes Fachpersonal dürfte im Fall von Machine-Learning-basierten Systemen regelmäßig an der systemimmanenten Komplexität scheitern.<sup>92</sup> Insbesondere bei Analysetools, die während des

---

<sup>90</sup> Siehe dazu Beschwerde von noyb gegen OpenAI, 29.04.2024. [https://noyb.eu/sites/default/files/2024-04/OpenAI Complaint\\_DE\\_geschwärzt.pdf](https://noyb.eu/sites/default/files/2024-04/OpenAI%20Complaint_DE_geschwärzt.pdf) (01.10.2025).

<sup>91</sup> Haouache, in: Beck/Stember 2020, S. 29 f.; Rademacher 2021, S. 250; Sommerer 2020, S. 204 und 219 f.

<sup>92</sup> Ferguson 2017, S. 1170; Sommerer 2020, S. 200 ff.

Betriebs weiterlernen und somit neue Muster ausbilden, dürfte zum derzeitigen Stand der Technik hinreichende Transparenz kaum herzustellen sein.

Schließlich ist vor Inbetriebnahme eine Grundrechte-Folgenabschätzung vorzunehmen (Art. 27 KI-VO). Diese ist bei wesentlichen Änderungen zu wiederholen.<sup>93</sup> Die Polizei hat bei der Übermittlung von Daten im Rahmen der post market surveillance zudem datenschutzrechtliche Maßgaben zu beachten (Art. 26 Abs. 3 KI-VO). Vor allem sensible operative Daten sind von der Übermittlungspflicht nach Art. 72 KI-VO ausgeschlossen.

## 5. Parameter einer datenschutzrechtskonformen automatisierten Datenanalyse

Abschließend werden nun konkrete einfachrechtliche Vorgaben für die Regulierung und den Einsatz automatisierter Datenanalysen für die Gefahrenabwehr herausgearbeitet. Zur Systematisierung wird einmal mehr die Unterscheidung der KI-»Lebenszyklus«-phasen nach *Hüger* aufgegriffen. Es bietet sich teilweise auch ein Vergleich mit dem Fluggastdatengesetz an. Dieses erlaubt zum Zweck der Verhütung und Verfolgung terroristischer Straftaten und schwerer Kriminalität die automatisierte Analyse von Fluggastdaten (§ 1 Abs. 2, § 4 Abs. 2, 4 FlugDaG) und stellt hierfür verfahrensrechtliche Bedingungen auf. Auch hieraus lassen sich Maßgaben für die automatisierte Datenanalyse zur polizeilichen Gefahrenabwehr ableiten.

### 5.1 Notwendigkeit einer Rechtsgrundlage und KI-Reallabore

Erinnert sei hier insbesondere an die fehlende Rechtsgrundlage für das *fine-tuning* mit Polizeidaten. Eine zweckrealisierende Weiternutzung wird hier regelmäßig aufgrund des fehlenden konkreten Gefahren- bzw. Anlassbezugs ausscheiden, sodass die Erhebungsvorschrift nicht als Rechtsgrundlage herangezogen werden kann. Die Weiterverwendung von zu strafverfolgungs- bzw. Gefahrenabwehrzwecken erhobenen Polizeidaten zum Training einer Analysesoftware könnte mit einem sehr weiten Verständnis des Begriffs »derselben Aufgabe« zwar als zweckkonforme Weiternutzung begriffen werden. Die Objektive der Effektivierung des Grundrechtsschutzes spricht allerdings dagegen: Die Möglichkeit der zweckkonformen Weiternutzung darf nicht zu einem ausufernden »Datenrecy-

---

<sup>93</sup> Erwgr. 96 KI-VO.

cling« führen, da diesem die Gefahr einer voraussetzungslosen Weiterverwendung einmal – mitunter unter strengen verfassungs- und datenschutzrechtlichen Voraussetzungen – erhobener Daten inhärent ist. Die Zuständigkeit der Polizei ist die Gefahrenabwehr, der das fine-tuning einer Datenverarbeitungssoftware zwar dienlich, aber dennoch zeitlich weit vorgelagert ist. Das bedeutet, dass auch eine zweckändernde Weiternutzung, die eine zumindest auf mittlere Sicht drohende Gefahr voraussetzt, ausscheidet. Entsprechendes gilt für eine Weiterverarbeitung nach dem Grundsatz der hypothetischen Datenneuerhebung.

Das fine-tuning kann aber künftig nach Art. 59 KI-VO in sogenannten KI-Reallaboren zulässig sein. Auch die Schaffung einer anderen Rechtsgrundlage durch die Gesetzgebung ist nicht ausgeschlossen.<sup>94</sup> Ratsam dürfte allerdings die Aufgabenzuweisung an staatliche IT-Kompetenzzentren sein. Insgesamt bestehen erhebliche Bedenken, ob beim Training von Big Data-Analysen die Datenverarbeitungsgrundsätze (Datenminimierung, Transparenz, Datenrichtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) eingehalten werden können – und insbesondere bei Kooperationen mit privaten Anbietern auch eingehalten werden. Eine wirksame Anonymisierung von Trainingsdaten wäre daher empfehlenswert. Protokollierungs- und Dokumentationspflichten sind einzuhalten. Das ergibt auch ein Vergleich mit § 4 III FlugDaG, der Ermächtigungsnorm für die Fluggastdatenverarbeitung zur Mustergewinnung, der sehr konkret ist und dessen Detailliertheit zudem ein Mindestmaß für die Detailliertheit einfachrechtlicher Verarbeitungsgrundlagen vorgibt.

## 5.2 Phasenübergreifende Anforderungen: Verfahrenssicherung und Kontrolle

Schließlich gelten phasenübergreifende Rechtmäßigkeitsanforderungen. Aufgrund des Neuheitswertes von Verfahren zur automatisierten Datenanalyse und ihrer Grundrechtssensibilität ist eine Datenschutz-Folgenabschätzung zwingend. Die Protokollierungs- und Verfahrenssicherungspflichten korrespondieren mit dem Datenschutzrecht.

### 5.2.1 Protokollierung und Kennzeichnung

Protokollierungspflichten bei automatisierter Datenverarbeitung erwachsen aus Art. 25 JI-RL bzw. § 76 BDSG, § 49 HDSIG. Um die Rechtmäßigkeit der Verarbeitung zu überprüfen,<sup>95</sup> ist demnach die Protokollierung der Erhebung,

---

<sup>94</sup> Kelber/Bortnikov 2023, S. 2005.

<sup>95</sup> So Ehmman, in: Gola/Heckmann 2022, § 76 BDSG Rn. 6; a. A. Kugelmann/Buchmann 2024, S. 3.

Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung von Daten erforderlich. Datum, Uhrzeit, Bearbeiter:in und gegebenenfalls Datenempfänger:in sowie eine Begründung der Vorgänge sind anzugeben. Diese Protokollierungspflichten fördern zusammen mit den Auskunftsansprüchen der von Analyseverfahren Betroffener (Art. 13 ff. JI-RL, §§ 32 ff. BDSG, §§ 50 ff. HDSIG) den Individualrechtsschutz.

Besondere Relevanz für die grundrechtsverträgliche Ausgestaltung automatisierter Datenanalysen bzw. ihrer Rechtsgrundlagen hat auch die Kennzeichnung der zu verarbeitenden Daten anhand einer Unterscheidung verschiedener Kategorien betroffener Personen. Art. 6 JI-RL gibt hier eine Unterscheidung von Verdächtigen, verurteilten Straftäter:innen, (mutmaßlichen) Opfern, Zeug:innen, Hinweisgebenden und Kontaktpersonen vor. In § 72 BDSG und § 67 HDSIG hat diese Unterscheidung in präzisierter Form Niederschlag gefunden. Eine effektive Kennzeichnung erhobener Daten ist notwendig, um den Anforderungen des Zweckbindungsgrundsatzes und damit der Rechtfertigungsdogmatik zum Grundrecht auf informationelle Selbstbestimmung zu genügen.

### 5.2.2 Löschfristen

Löschfristen sind von hervorgehobener Bedeutung für den Grundrechtsschutz.<sup>96</sup> Das Fluggastdatengesetz etwa sieht eine Depersonalisierung von Daten nach sechs Monaten (§ 5 Abs. 1 FlugDaG) und eine Datenlöschung nach spätestens fünf Jahren vor (§ 13 FlugDaG). Der EuGH hat mittlerweile aber eine derartig langfristige Speicherung von Daten ohne objektiven Gefahrenbezug als unverhältnismäßig erachtet: Daher muss innerhalb der sechsmonatigen Speicherfrist eine Vorprüfung stattfinden, infolge derer unerhebliche Daten gelöscht werden.<sup>97</sup> Aufgrund des vergleichbaren Eingriffsgewichts ist eine derartige sechsmonatige Speicherfrist jedenfalls für die Daten Unbeteiligter (die ohnehin nur bei Vorliegen einer konkreten Gefahr für die nationale Sicherheit eingespeist werden dürfen) in polizeilichen Analyseplattformen anzusetzen. Das tariert im Zusammenspiel mit dem Verbot des Einbezugs dieser Daten in weiterlernende Systeme den Grundrechtsschutz Unbeteiligter und das Interesse an einer effektiven Gefahrenabwehr grundrechtskonform aus. Die Sechs-Monats-Frist muss als die maximale Speicherdauer und als eine Frist für Erheblichkeitsprüfung begriffen werden. Findet letztere statt und wird ein Nichttrefferfall ausgewiesen, müssen Daten unverzüglich wieder gelöscht werden (vergleiche § 13 Abs. 5 FlugDaG). Für

---

<sup>96</sup> BVerfGE 165, 363 (403).

<sup>97</sup> EuGH, Urt. v. 21.06.2021, C-817/19, Ligue de droits humains gegen Conseil de ministres, ECLI:EU:C:2022:491, Rn. 255 ff.

personenbezogene Daten von Personen mit objektivem Gefahrenbezug gibt die Verfassungsrechtsprechung keine konkreten Löschfristen vor. Allerdings dürfte ob des situativen Charakters der automatisierten Datenanalyse bei der Polizei, der sich in der Regel im Erfordernis einer mindestens konkretisierten Gefahr ausdrückt, zweifelhaft sein, ob eine dem Fluggastdatengesetz entsprechende Speicherdauer von fünf Jahren erforderlich und verhältnismäßig ist. Tendenziell dürften eher kürzere Speicherfristen angemessen sein.

## 6. Bewertung der Neufassung des § 25a HSOG

Auch die Neufassung des § 25a HSOG vom 29. Juni 2023 (1. Neufassung)<sup>98</sup> begegnet datenschutzrechtlich und in Hinblick auf die KI-Verordnung Bedenken.

Die Datenschutz-Grundverordnung ist auf die Datenzusammenstellung und das Training des Basismodells durch Palantir (Phase 1) anwendbar. Die Unternehmenstochter Palantir Technologies – Deutschland ist eine Niederlassung im Sinne des Art. 3 Abs. 1 DS-GVO.<sup>99</sup> Palantir gibt an, Kund:innendaten für das Training von KI-Modellen (Phase 2) zu verwenden.<sup>100</sup> Diese Daten würden jedoch außerhalb der Vertragsbeziehung nicht genutzt. Palantir Technologies – Deutschland agiert nach eigenen Angaben als Auftragsverarbeiter.<sup>101</sup> Auch die Dokumente zum hessischen Vergabeprozess legen diese Konstellation im Rahmen des *fine-tunings* nahe.<sup>102</sup> Ob dies praktisch auch zutrifft oder ob es sich um eine gemeinsame Verantwortung nach Art. 26 DS-GVO und Art. 21 JI-RL handelt, bei der auch Palantir datenschutzrechtliche Normadressatin wäre, ist eine Frage der konkreten Ausgestaltung des Vertragsverhältnisses und der tatsächlichen Verarbeitung.

Außerdem bedarf es einer gesetzlichen Grundlage, Daten zu Zwecken des *fine-tunings* zu verarbeiten und auch weiterzuverarbeiten. Diese ist bei systematischer Auslegung und dem Sinn und Zweck des Gesetzes in § 25a Abs. 1 Satz 1 HSOG zu finden: Die Daten dürfen zusammengeführt werden. Diese Zusammenführung muss das *fine-tuning* einschließen, ohne die die weiteren Ermächtigungen zur au-

---

98 GVBl. S. 456; s. LT-Drs. 20/11235. Weitere Änderungen durch Gesetz vom 13.12.2024 (GVBl. Nr. 83).

99 Erwgr. 22 DS-GVO; EuGH, Urt. v. 13.05.2014, C-131/12, Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, ECLI:EU:C:2014:317, Rn. 52; Piltz, in: Gola/Heckmann 2022, Art. 3 DS-GVO Rn. 12.

100 S. Palantir, »Palantir: Fragen und Antworten«, 12.04.2021. <https://blog.palantir.com/palantir-fragen-und-antworten-b3cb77b5ed91> (01.10.2025).

101 S. Palantir, »Palantir: Fragen und Antworten«, 12.04.2021. <https://blog.palantir.com/palantir-fragen-und-antworten-b3cb77b5ed91> (01.10.2025).

102 LT-Drs. 19/6864, 68 ff.

tomatisierten Datenanalyse (u.a. Verknüpfung, Aufbereitung, Auswertung) nach § 25a Abs. 1 Satz 2 ff. i. V. m. Abs. 2 bis 5 HSOG nicht möglich wären.

Es ist daneben fraglich, ob in praktischer Hinsicht die hier enthaltenen Anforderungen an die Systemintegrität gewahrt werden. Zugriffe durch Beschäftigte von Palantir im Zuge von Systemanpassungs- und Updateprozessen lassen sich nicht ausschließen. Die Zugangs- und Datenträgerkontrolle (Art. 29 Abs. 1 Nr. 2 a) und b) JI-RL respektive § 59 Abs. 2 Nr. 1 und 2 HDSIG) erscheint insoweit lückenhaft. Es besteht eine erhebliche Gefahr des Datenabflusses.

Erschwerend kommt hinzu, dass die erforderliche<sup>103</sup> Datenschutz-Folgenabschätzung nicht erfolgt ist oder wenigstens nicht an die Öffentlichkeit kommuniziert wurde.<sup>104</sup>

Besondere Bedenken bestehen zudem hinsichtlich der Kennzeichnungspflicht nach Art. 6 JI-RL beziehungsweise § 67 HDSIG, denn in Hessen wird nach § 20a Abs. 4 HSOG doch umfänglich von der Kennzeichnungspflicht befreit.

Auch die Einhaltung der Vorgaben nach der KI-Verordnung stehen in Frage. Da sich hessenDATA bereits im Betrieb befindet, gelten die Vorgaben der KI-Verordnung gemäß Art. 111 Abs. 2 KI-VO jedoch nur bei wesentlichen Änderungen des Systems. Für Palantir als Anbieter eines in der Union im Betrieb befindlichen KI-Systems sind die Pflichten aus Art. 11 KI-VO relevant. Die Pflichten aus Art. 14 KI-VO ließen sich durch zusätzliche Informationen zur algorithmischen Entscheidungsfindung und zum automation bias erfüllen. Zudem könnte ein Warnhinweis zum automation bias hilfreich sein. Die Nutzung von hessenDATA setzt nach 2.3 VV § 25a HSOG eine zweitägige Basisschulung voraus. Ob dies ausreichend ist, um Nutzer:innen entsprechend Art. 4 KI-VO zu sensibilisieren, geschweige denn ihnen hinreichendes Technikwissen für die Systemüberwachung zu vermitteln, ist zweifelhaft.

## Quellen und Literatur

- Arzt, Clemens, »Polizeiliche Verarbeitung ›besonderer Kategorien personenbezogener Daten«, in: *Die öffentliche Verwaltung* (DÖV) 2023, S. 991–1002.
- Ashkar, Daniel, »Wesentliche Anforderungen der DS-GVO bei Einführung und Betrieb von KI-Anwendungen«, in: *Zeitschrift für Datenschutz* (ZD) 2023, S. 523–530.
- Bäuerle, Michael, *Das Informationsrecht der Sicherheitsbehörden zwischen Konstitutionalisierung und Europäisierung*, Frankfurt a.M. 2024.

<sup>103</sup> Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 86.

<sup>104</sup> Arzt, Stellungnahme zur BT-Drs. 20/9495, 14.

- Ferguson, Andrew G., »Policing Predictive Policing«, in: Washington University Law Review 2017, S. 1109–1189.
- Gola, Peter/Heckmann, Dirk (Hg.), *Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, 3. Auflage, München 2022.
- Haouache, Gerold, »Digitalisierung der Verwaltung: Der Einsatz Künstlicher Intelligenz im staatlichen Bereich in Gestalt von Assistenz- und vollautomatisierten Entscheidungssysteme«, in: Beck, Joachim/Stember, Jürgen (Hg.): *Der demographische Wandel*, Baden-Baden 2020, S. 19–34.
- Hüger, Jakob, »Die Rechtmäßigkeit von Datenverarbeitungen im Lebenszyklus von KI-Systemen«, in: *Zeitschrift für Digitalisierung und Recht (ZfDR)* 2024, S. 263–290.
- Johannes, Paul C., »Die Gegenüberstellung – Allgemeine Grundsätze der Datenverarbeitung nach neuem BDSG, DS-GVO und JI-Richtlinie«, in: ZD-Aktuell 2017, 05757.
- Johannes, Paul C., »Analyse offener Datenquellen durch die Polizei: Entgrenzte Internet- und Darknetaufklärung in der Strafverfolgung«, in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hg.): *Die Fortentwicklung des Datenschutzes*, Wiesbaden 2018, S. 151–172.
- Johannes, Paul C., »Zertifizierung von Datenverarbeitungsvorgängen bei der Polizei«, in: *Die Polizei* 2020, S. 409–415.
- Johannes, Paul C./Weinhold, Robert, *Das neue Datenschutzrecht bei Polizei und Justiz*, Baden-Baden 2018.
- Kelber, Ulrich/Bortnikov, Vyacheslav, »Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten«, in: *Neue Juristische Wochenschrift (NJW)* 2023, S. 2000–2006.
- Kugelman, Dieter/Buchmann, Antonia, »Der Algorithmus und die Künstliche Intelligenz als Ermittler«, in: *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* 2024, S. 1–10.
- Lauscher, Anne/Legner, Sarah, »Künstliche Intelligenz und Diskriminierung«, in: *Zeitschrift für Digitalisierung und Recht (ZfDR)* 2022, S. 367–390.
- Möller-Klapperich, Julia, »Die neue KI-Verordnung der EU«, in: *Neue Justiz (NJ)* 2024, S. 337–342.
- Möstl, Markus/Bäuerle, Michael (Hg.): *Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen*, 34. Edition, München 2025.
- Müller-Peltzer, Phillip/Tanczik, Valentin, »Künstliche Intelligenz und Daten«, in: *Recht Digital (RD)* 2024, S. 452–458.
- Pesch, Pailiona/Böhme, Rainer, »Verarbeitung personenbezogener Daten und Datenrichtigkeit bei großen Sprachmodellen«, in: *Multimedia und Recht (MMR)* 2023, S. 917–923.
- Rademacher, Timo, »Predictive Policing im deutschen Polizeirecht«, in: *Archiv des Öffentlichen Rechts (AÖR)* 2017, S. 366–416.
- Rademacher, Timo, »Verdachtsgewinnung durch Algorithmen. Maßstäbe für den Einsatz von predictive policing und retrospective policing bei Gefahrenabwehr bzw. Strafverfolgung«, in: Zimmer, Daniel (Hg.): *Regulierung für Algorithmen und Künstliche Intelligenz*, Baden-Baden 2021, S. 229–268.
- Schuh, Mathias/Weiss, Erik, »Die Zweckbestimmung und Zweckbindung als Weichenstellung für die DSGVO-konforme Nutzung von Daten für KI-Systeme«, in: *Zeitschrift für Digitalisierung und Recht (ZfDR)* 2024, S. 225–262.
- Sommerer, Lucia, *Personenbezogenes Predictive Policing*, Baden-Baden 2020.
- Spies, Axel, »Wann passt die DS-GVO auf KI?«, in: *Multimedia und Recht (MMR)* 2024, S. 289–290.



# Das Gericht, seine Sprache und die kritischen Schwellenwerte von Softwaretechnik – Zur begrifflich ambivalenten Fassung polizeilicher Big Data-Analysen durch das »Palantir-Urteil« des Bundesverfassungsgerichts

*Petra Gehring*

## 1. Einleitendes

Im Februar 2023 hat das Bundesverfassungsgericht zwei landesgesetzliche Regelungen für die Nutzung einer Software des US-amerikanischen Herstellers Palantir zu Zwecken der polizeilichen Ermittlungsarbeit für verfassungswidrig erklärt.<sup>1</sup> Im Ergebnis beanstandet die Entscheidung vor allem den unbestimmten Charakter der überprüften Normen: weder legten diese Landesgesetze die zu tolerierenden Eigenschaften der Software hinreichend genau fest noch die Grenzen von deren legalem Einsatz.

Im Folgenden wird nicht diese Bewertung als solche diskutiert. Weitgehend beiseite lasse ich auch das juristische Erfordernis, dass Grundrechtseingriffe, die mit dem Einsatz neuer polizeilicher Methoden verbunden sind, zu allererst präzise einschätzbar sein müssen, bevor man sie (gegebenenfalls) für zulässig erklärt. Ein entsprechendes Präzisionsgebot auch für ein Gesetz, das auf solche neuen Methoden abhebt, ist plausibel. Im Juni 2023 hat das Land Hessen den beanstandeten § 25a HSOG daher auch überarbeitet, um ihn zu präzisieren. Zudem kam im Dezember 2024 eine Erweiterung der Bestimmungen zur Datenerhebung in öffentlichen und privaten Räumen hinzu. Die aktuell geltende Fassung des hessischen Gesetzes eröffnet überdies die Möglichkeit der Datenauswertung mittels »KI«.<sup>2</sup> Das Palantir-Urteil stellt also lediglich einen Zwischenschritt auf einem längeren Weg der rechtlichen Einordnung der Nutzung anspruchsvoller digitaler Verfahren in der polizeilichen Ermittlungsarbeit dar. Der Gesetzgeber treibt die Nutzung digitaler Verfahren energisch voran, und zugleich ändert sich die

---

1 BVerfG, Urt. v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 m. Anm. Vasel 2023, S. 1174. – Nachfolgend wird aus dem Urteil (unter Nachweis der Randnummern) im Fließtext zitiert.

2 Vgl. Gesetz zur Stärkung der inneren Sicherheit in Hessen (HSOG) vom 13.12.2024 (GVBl. Nr. 83)

Potenz dieser Verfahren (Stand der Algorithmik, neue Softwareprodukte, verfügbare Datenmengen) schnell. Folgen und Nebenfolgen für die Rechte Betroffener müssen dem Rechtsstaat wichtig sein.

Gehört das Verfassungsgericht grundsätzlich zu den Skeptikern einer »digitalen« Ausweitung polizeilicher Kompetenzen und Befugnisse, so ist das ebenfalls gut zu verstehen. Neben der Sorge um Grundrechtseingriffe hat dies auch demokratietheoretische Gründe. Krankheiten immer besser zu therapieren, Bildung zu verbessern: hierbei kann es nie zu viel Fortschritt geben. Niemand jedoch wünscht sich eine wirklich perfekte Polizei in einer freiheitlichen Demokratie. Sicherheit und Ordnung können nur Näherungswerte sein. Ziele wie eine hundertprozentige Aufklärung aller Straftaten, ein flächendeckendes präventives Wegsperrn potenzieller Täter oder gar die Abschaffung jeglichen Verbrechens sind mit einer liberalen Idee des menschlichen Zusammenlebens unvereinbar. Theoretisch muss echte Freiheit also auch die Freiheit zur Regelwidrigkeit umschließen – und praktisch kann ein perfekter Sanktionsstaat nur als Überwachungs- und Disziplinarstaat funktionieren. Er muss im Grunde Krieg gegen seine Bürger führen; er ist totalitär.<sup>3</sup>

Von daher stimmt man auch dem weitergehenden Grundgedanken, für den die BVerfG-Entscheidung vom Februar 2023 steht, ohne Weiteres zu – dem Gedanken nämlich, dass nicht nur Grundrechtseingriffe bedenklich sind, sondern dass auch Polizeiarbeit ein menschliches Maß behalten sollte. Ermittlungen haben prinzipielle Grenzen zu beachten. Dies gilt auch und gerade im Digitalzeitalter, in welchem aus Gründen einer stürmischen Fortentwicklung von Datengewinnung und Recherche »immer mehr geht«.

Der Schwerpunkt der nachfolgenden Überlegungen ist gleichwohl ein anderer. Mehr als das Ergebnis der Abwägungen des Gerichts (oder auch die grundrechtlichen Argumente auf dem Weg dorthin) interessiert mich die Begrifflichkeit, mittels welcher das Gericht den Gegenstand seiner Untersuchung und die mit ihm verbundenen, gewichtigen Problemstellungen zu erfassen versucht. Wie genau modelliert das Urteil die digitalen Innovationen, vor die es die Polizeiarbeit (und also auch sich) gestellt sieht? Allem voran möchte ich möglichst genau in den Blick nehmen, wie das Gericht die – aus seiner Sicht bedenkliche – *Wirkungsweise* der zur Diskussion stehenden Software bzw. datenbasierten Analytik einschließlich ihrer praktischen Spezifika beschreibt, und wie es diese für die Zwecke seiner spezifischen Betrachtung aufschlüsselt.

Von Interesse ist dabei einerseits der Blick des Datenschutzrechts auf Technik und andererseits das im Zuge der kleinteiligen Argumentation gezeichnete Bild neuer Schwellenwerte für das »Wissen«, welches die Polizei bei der Ermittlungs-

---

<sup>3</sup> Klassisch hierzu schon die Philosophie Hegels, vgl. für die Soziologie Popitz 1968.

arbeit (dank der verwendeten Auswertungssoftware oder vergleichbarer Produkte) gewinnt.

Wie »sieht« oder auch wie fasst bzw. stilisiert das Gericht die Besonderheiten der digitalen Neuerung – und welche Dynamiken sieht es bei seiner Antizipation der mit KI-Einsatz verbundenen Qualitätssprünge am Werk? Welche Kraft schreibt es den softwarebasierten erweiterten Datenauswertungen zu und wo bzw. inwiefern *verbessert* die Software die Polizeipraxis nicht nur, sondern *verändert* diese, *verfremdet* sie vielleicht gar? Schließlich: Wie steht aus Sicht des Gerichts überhaupt der Einsatz von Digitaltechnik zu dem, was es im Hinblick auf Polizeiarbeit »Methode« nennt?

Alle diese Fragen umkreisen gleichsam die begriffliche Lupe, die das Gericht zur Bewertung der Risiken der Software und ihres Einsatzes wählt. Meine abschließende Überlegung läuft darauf hinaus, dass diese Lupe Details in einer Weise in den Vordergrund rückt und überbewertet, die rechtspolitisch nicht wünschenswert ist – und zwar gerade, wenn man den Einsatz von digitalen Analysetechniken für bedenklich hält. Das Palantir-Urteil situiert die digitalen Analyseoptionen nicht in einem Kontext sich ausweitender, eventuell kritischer Verantwortlichkeiten oder in einem digitalpolitischen Kontext (etwa durch eine Bewertung der Provenienz von Software) oder auch nur in einem zunehmend digitalen Berufsbild der Polizei. Stattdessen beschränkt sich die Suche nach kritischen Schwellenwerten auf gleichsam das Innere und Innerste der Funktionsweise der neuen Technologie, um hier die Hauptgefahren für den Grundrechtsschutz zu suchen (und zu finden). So dämonisiert das Gericht die Technik selbst. Der Blick auf deren Herkunfts- und Einsatzkontexte sowie die Kompetenzen zu deren Einsatz wird, vermutlich ungewollt, verengt.

## 2. Neuheit

Wenig überraschend erinnert die BVerfG-Entscheidung zunächst – noch vor der näheren Betrachtung des Softwareeinsatzes – an die Kriterien des Datenschutzrechts und damit auch an diejenigen des Individualgrundrechts der informationellen Selbstbestimmung. Maßgeblich für eine Bewertung der in den beanstandeten Gesetzen erlaubten Datennutzung seien im Einzelfall demnach die Fragen nach

- der Art der verarbeiteten Daten
- dem Umfang (Menge) der verarbeiteten Daten
- der angewendeten Methode der Datenanalyse/-auswertung – sowie Möglichkeiten der Analyse/Auswertung.

Das Gericht setzt dann jedoch bei der *Neuheit* des zu beurteilenden Gegenstandes an. Den Besonderheiten der einzusetzenden Lösung des Herstellers Palantir Technologies werde ein Landesgesetzgeber nicht gerecht, wenn er deren Einsatz allzu pauschal erlaube.

Nicht sofort ersichtlich ist allerdings, wo die Neuheit eigentlich liegt: ob es um eine neue Qualität der Technologie selbst geht oder um deren bedenkliche Einsatzweise im Rahmen polizeilicher Ermittlungen oder um veränderte Arbeitsabläufe des Ermitteln – oder vielleicht um alles zugleich. Die Rede ist von »erweiterte[n] technische[n] Möglichkeiten, Informationstechnologie auch in der polizeilichen Arbeit zu nutzen« (Rn. 2). Diese Möglichkeiten bilden den Hintergrund der Zielstellung der zu prüfenden Gesetze,<sup>4</sup> »bisher unverbundene, automatisierte Dateien und Datenquellen in Analyseplattformen zu vernetzen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen, um die polizeiliche Aufgabenerfüllung auf diese Weise zu erleichtern und zu verbessern« (ebd.).

Die *Dateivernetzung* also sowie die dadurch mögliche Option der systematisch eingesetzten *Suche* und eine somit neuartige Option der *Erschließung* vorhandener Bestände zur *Erleichterung und Verbesserung* eines *spezifisch polizeilichen* Tuns: auf diesen Komplex richtet sich der kritische Blick des Gerichts.<sup>5</sup>

Hinzu kommt ein Zweites, nämlich die Option der »vorbeugenden Bekämpfung von Straftaten«, zu welcher die beanstandeten Normen ihre Landespolizei unter bestimmten Voraussetzungen (vgl. Rn. 3) ermächtigen wollen. Ein solcher prospektiver Gebrauchswert dessen, was die Software leistet, spielt für das Gericht neben der bloßen besseren Erschließung eine große Rolle – und auch auf dieser Ebene wird abgewogen, inwieweit die Technik etwas Neues mit sich bringt. Das Gericht bringt hier verschiedentlich (im Detail wenig erläutert) das Szenario eines »Predictive Policing« ins Spiel. Eine solche, Kriminalität bzw. eine erhöhte Wahrscheinlichkeit krimineller Vorfälle »vorhersagende« Funktion erörtert das Gericht nicht, weil die ihm vorliegende Klage diesen Vorwurf konkret bereits erheben würde, sondern weil die Richter eine solche Vorgehensweise mit den neuen technischen Möglichkeiten gleichsam am Horizont heraufkommen sehen. Tatsächlich hatte der hessische Gesetzgeber in der Anhörung die Einführung der Software (unter dem Namen hessenDATA) unter anderem mit dem Satz erläutert, die Polizei könne nun »über die bisherigen Erkenntnismöglichkeiten hinaus Zusammenhänge sowie Handlungsmuster und damit auch künftiges strafba-

---

4 Es geht um Gesetze aus Hamburg und Hessen; deren Vorgeschichte behandle ich hier nicht näher. Siehe aber die Beiträge von Lea Rabe und Christopher Giogios in diesem Band.

5 Die Beschwerdeführer haben – soweit im Urteil referiert – nicht das Wort »neu« genutzt, sondern sprechen von »erhöhter Eingriffsintensität«, vgl. Rn. 43.

res oder gefährliches Verhalten von Personen erkennen und geeignete präventive Maßnahmen treffen«. <sup>6</sup> Möglicherweise hat diese Aussage das Gericht zu seinen Ausführungen inspiriert.

Als »neu« erscheinen somit gleich drei entscheidungsrelevante Aspekte des Leistungsvermögens des Softwaresystems:

- die softwaregestützte polizeiliche Verfahrensweise oder auch die »Methode(n)«, die klassische Formen der Wissensgewinnung überschreiten (2.1),
- die Software (und das Wissen, das mit ihr erlangt werden kann) (2.2),
- die Option prospektiver Maßnahmen bzw. präventiver Umgangsweisen mit Verhalten bzw. Personen (2.3).

### 2.1 Veränderte »Methoden«

In den beanstandeten Landesgesetzen ist, für das, worum es geht, die Rede von »Auswertung«, genauer dann von »statistischem« Auswerten (vgl. Rn. 3 und die Landesgesetze) bzw. davon, »mittels einer automatisierten Anwendung zur Datenauswertung [zu] verarbeiten« (§ 49 HmbPolDVG), von »automatisierter Analyse« (Rn. 9) bzw. »automatisierter Datenanalyse« (Rn. 6) oder auch von der »Einrichtung und Nutzung eines automatisierten ›Analysetools«« (Rn. 7, Paraphrase der Hessischen Wortwahl) sowie vom »Einsatz« eines »Datenanalyseinstruments« (Rn. 10) und von der Nutzung einer »Analyseplattform« (Rn. 11). Das Gericht übernimmt diese Sprache nicht nur in seiner Sachdarstellung, sondern setzt sie auch im Rahmen seiner bewertenden Einschätzungen ein.

Die Begriffe »Datenanalyse« und »Datenauswertung«, so ist zu lesen, verwende das Gericht synonym. Von »Datenauswertung« zu sprechen, solle aber unterstreichen, dass hierbei lediglich ausgewertet würde, also dezidiert keine »KI« (›Einsatz von intelligenten, möglicherweise selbstlernenden Algorithmen«) zum Einsatz käme (vgl. Rn. 14, Paraphrase der Stellungnahme des Landes Hessen).

Es sind die Beschwerdeführer, die besonders deutlich methodische Veränderungen anprangern, welche die Verwendung der Palantir-Software mit sich bringt bzw. bringen würde. Sie ziehen eine Parallele zur sogenannten Rasterfahndung, einer Vorgehensweise, die seit den 1970er Jahren die juristische Diskussion beschäftigt und zu präventiven Zwecken 2006 durch eine Entscheidung des Bundesverfassungsgerichts auf das Vorliegen konkreter Gefahren begrenzt

---

<sup>6</sup> Vgl. Hessische Landtagsfraktionen CDU und BÜNDNIS 90/DIE GRÜNEN 2018, S. 40 f.

worden ist.<sup>7</sup> Das Gericht fasst den vorgetragenen – wenngleich bestrittenen<sup>8</sup> – Vorwurf so zusammen: Zu was die beanstandeten Regelungen ermächtigten, gehe »über die Rasterfahndung hinaus«, denn während jene immer noch durch ein begrenzendes Auswerteraster geprägt sei, würden jetzt »Systeme Daten auch unabhängig von einem Raster mit trainierten oder selbstlernenden Algorithmen ausgewertet« (Rn. 43). ML-Verfahren, welche die Gesetze nicht ausschlossen, seien zudem in ihren Ergebnissen nicht nachvollziehbar (vgl. ebda.). Anders gesagt, löse sich das neue System also vom bloßen »Raster« und es »lerne« womöglich sogar seine Auswertungskriterien selbst.

Das Gericht folgt dem nur bedingt, nämlich nicht im Sinne eines Verdikts gegen die Software als solche und auch nicht mittels jenes Rekurses auf nun nicht mehr vorhandene oder nötige »Raster«. Es moniert vielmehr, angesichts des weiterreichenden Wissens, welches die (auch als »Data-Mining« charakterisierte) Methodik liefere, seien die »Eingriffsschwellen« unzulänglich bestimmt, und es signalisiert Bedenken, was die Zielstellung einer vorbeugenden Verbrechensbekämpfung angeht.

Die Urteilsbegründung dröselte das (vom Datenschutzgedanken ausgehend) in einer Weise auf, die geradezu erkenntnistheoretische Züge hat, und setzt so tatsächlich den Zeiger auf methodische Aspekte. Das Urteil sieht nicht nur im Einklang mit früherer Rechtsprechung<sup>9</sup> einen begründungsbedürftigen Grundrechtseingriff in der *nochmaligen* – die Daten nun verknüpfenden – Verwendung von Daten, »sondern darüber hinaus in der Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die automatisierte Datenanalyse oder -auswertung geschaffen werden kann« (Rn. 50, 67 ff.). Somit ist der kritische Punkt eine bestimmte Praxis der Wissensgewinnung *mittels* Software (sowie die Neuheit des so erlangten Wissens – noch nicht so sehr die Softwareplattform selbst (vgl. hierzu dann aber 2.2.)). Auf die Gewinnung von »Erkenntnissen« käme es ihnen beim Einsatz von Palantirs Produkt Gotham an, so auch die Auskunft der Länder (vgl. Rn. 53).

Erlaubt der Einsatz der beanstandeten Softwarelösung aus Sicht des Gerichts also eine Art des epistemischen Vorgehens, das den polizeilichen Ermittlern vorher nicht möglich war? Immerhin fällt in der Entscheidung ganze 20 Mal der Ausdruck »Methode(n)«, dazu fallen jeweils einmal die Worte »Methodik« und »methodisch«. Mehrmals ist von »methodenoffen« und zweimal in einem nichtjuris-

---

7 Vgl. Beschluss des Ersten Senats vom 4. April 2006 (1 BvR 518/02).

8 Zumindest Hamburg hat in der Anhörung die viel spezifischere Art der durch das Tool ermöglichten Recherche stark gemacht: »Der Hamburger Innensenator erklärte, man plane kein mit der Rasterfahndung vergleichbares Instrument, sondern eher eine Art qualifizierten Datenabgleich (Hamburgische Bürgerschaft AusschussDrucks 21/39, S. 9 f., 32).« (Rn. 13).

9 Vgl. BVerfGE 156, 11: 39 f. Rn. 73 f.

tischen Sinne von »systematisch« die Rede: »durch Suchfunktionen systematisch [...] erschließen«, »systematisch betriebene Datenbanken«.

»Methoden der Analyse« scheinen jedenfalls durch Softwaresysteme wie hesenDATA verändert zu werden – und dies ist für das Erfordernis, andere Schwellenwerte für den Einsatz zu fixieren als bei der klassischen Datenbanknutzung – zentral. Im Detail freilich bleibt die Methodizität, auf die das Gericht hier abhebt, unbestimmt: Zum einen spricht es von »informationstechnisch mögliche[n] Methoden« (Rn. 90), was augenscheinlich doch wieder auf Technik, vielleicht ganz direkt auf Softwareleistungen abhebt.<sup>10</sup> Zum anderen scheint das Gericht eher die Vorgehensweisen der Polizeiarbeit im Auge zu haben und damit das, was Menschen mit der Softwarelösung ihrerseits dann machen. Methoden werden praxeologisch umschrieben – etwa: als »Suche«, »Erstellung von Bewegungs- und Verhaltens- oder Beziehungsprofilen oder noch umfassenderer Persönlichkeitsbilder« oder – ein »herkömmliches Verfahren« (Rn. 69) – »die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit« (Rn. 69).

Über Abschnitte hinweg erhält man tatsächlich den Eindruck, das neue Wissen entstehe im Wesentlichen im Wege von »Suchen« (und Finden), und die neue Qualität der beanstandeten Software liege darin, dass man im Rahmen der methodischen Polizeiarbeit mit ihrer Hilfe *anders sucht*. Und dann tauchen womöglich die »Raster« doch wieder auf, nämlich in Gestalt eines, wie es heißt, »polizeilichen Suchmusters« – und dieses, so wird man ergänzen dürfen, muss ein menschlich erdachtes Muster sein. Das Gericht unternimmt in dieser Hinsicht eine Art Vorher-Nachher-Vergleich: Bei einer herkömmlichen Suche steuerten »auch mit Erkenntnissen und Annahmen zum konkreten Sachverhalt gespeiste« »polizeiliche Suchmuster« (Rn. 93) das Vorgehen. Die neuen Systeme erlaubten hingegen eine Suche ohne bzw. nicht dem (konkreten) Sachverhalt entstammende Suchbegriffe – oder besser: Sie führten die suchbegriffslose Suche (oder auch das bloße »Entdecken« von »statistischen Auffälligkeiten«) in die herkömmliche Arbeitsweise – die herkömmliche Methode – ein. Und: »Weitere Abgleichsschritte« kämen hinzu.<sup>11</sup>

<sup>10</sup> »Rechtlich kann die handelnde Behörde aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen sowie aus der Auswertung neue Zusammenhänge erschließen.« (Rn. 67).

<sup>11</sup> Und »Schritte« bestehen darin, dass man jeweils treffergeleitet neu interessant gewordene Suchbegriffe nutzt, so jedenfalls reinterpretiere ich den folgenden Passus: »Das Eingriffsgewicht erhöht sich insbesondere, wenn die Datenanalyse oder -auswertung nicht auf einem Suchbegriff, jedenfalls nicht auf einem auf den bislang erkennbaren Sachverhalt bezogenen Suchbegriff gründet, sondern darauf zielt, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, die darüber hinaus (automatisiert) in weiteren Abgleichsschritten mit bestimmten Datenbeständen verknüpft werden und so zu weiteren Informationen führen können, nach denen zu suchen die Polizei zuvor keinen Anlass hatte.« (Rn. 93, Hervorh. d. Verf.).

Das »Suchen« scheint so aus Schritten des Abgleichens zu bestehen. Und durch das Hinzutreten der Software stehen »händische Suche oder einfache automatisierte Abgleiche« dem »komplexe[n] Abgleich« gegenüber, der viele Schritte umfasst – weswegen das Gericht dann bilanziert: »Die automatisierte Anwendung kann die Arbeitsweise und Erkenntnismöglichkeiten der Polizei somit entscheidend verändern.« (Rn. 70).

Einmal einfach abgleichen also, und zum anderen »komplex«? Halten wir zunächst fest: Die generische Vorstellung des *Abgleichs* von Daten spielt im Urteil in der Tat eine argumentativ wichtige Rolle. Denn der sogenannte »einfache« Abgleich scheint eine unproblematische (gleichsam händische) Vorgehensweise oder auch Methode zu sein. So heißt es im Text:

»Das Eingriffsgewicht wird geringer, je mehr der Vorgang der automatisierten Datenanalyse oder -auswertung methodisch einem einfachen Datenabgleich angenähert ist. Beim einfachen Abgleich erfolgt die Suche nach einem vorhandenen Datenbestand etwa über eine Person, indem im jeweiligen System die eingegebenen Daten des Betroffenen an den gespeicherten Daten vorbeigeführt werden; als automatisches Datenverarbeitungsverfahren führt der Dateiabgleich insoweit regelmäßig Datenbestände zusammen, um Übereinstimmungen der Daten festzustellen oder Daten des einen Bestands in den anderen zu überführen [...]. Der einfache Abgleich ist also ein suchender Vergleich von Daten zur Feststellung von Übereinstimmungen.« (Rn. 91).

Davon unterschieden werden »komplexe Formen des Datenabgleichs« als »eingriffsintensive Methoden der Datenauswertung« (Rn. 101) bezeichnet, welche die beanstandeten Gesetze erlauben:

»Die angegriffenen Vorschriften schließen auch komplexere Formen des Datenabgleichs nicht aus. Wenn § 25a HSOG und § 49 HmbPolDVG von der automatisierten Anwendung zur Datenanalyse oder zur Datenauswertung, also nicht etwa vom (automatisierten) Abgleich, sprechen, hebt sich das bereits gesetzessystematisch vom einfachen Abgleich (s. § 25 HSOG, § 48 Abs. 1 HmbPolDVG) ab. § 25a HSOG und § 49 HmbPolDVG ermöglichen demgegenüber ein »Data-Mining« (vgl. BVerfGE 156, 11 <40 Rn. 74>) bis hin zur Verwendung selbstlernender Systeme (KI). Dabei sind insbesondere auch offene Suchvorgänge zulässig (vgl. Rn. 93 ff.). Die Datenanalyse oder -auswertung darf darauf zielen, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, aus denen dann, möglicherweise auch mit Hilfe weiterer automatisierter Anwendungen, weitere Schlüsse gezogen werden. Die Vorschriften schließen auch bezüglich der erzielbaren Suchergebnisse nichts aus (vgl. Rn. 96 ff.); nach dem Wortlaut konnte das Suchergebnis in maschinellen Sachverhaltsbewertungen bestehen – bis hin zu Gefährlichkeitsaussagen über Personen im Sinne eines »predictive policing«. Es konnten also mittels Datenanalyse oder -auswertung neue persönlichkeitsrelevante Informationen erzeugt werden, auf die ansonsten kein Zugriff bestünde« (Rn. 147).

Der »automatisierte« *einfache* Abgleich würde demgemäß vielleicht noch unbedenklich sein, nicht aber die automatisierte »Anwendung zur Datenanalyse« insgesamt.

So ganz klar können wir allerdings nicht nachlesen, wo das Gericht denn nun wirklich die kritische Grenze sieht – die Grenze im Prozess der maschinell vollzogenen Analyseschritte (»Suche«, »Abgleich«) oder auch den kritischen Schwellenwert der mit ihrem Einsatz sich verändernden menschlichen »Methoden«. Zum einen scheint es auf die »neuen« Funde anzukommen, auf die man nur dank des »komplexen« automatischen Abgleichs stößt. Zum anderen scheint es – weitergehend – um die mit den maschinellen Suchvorgängen und Funden sich erschließenden »Zusammenhänge« zu gehen. Gerade bezogen auf Personen spricht das Gericht besorgt von einem »algorithmentypischen« Registrieren »bloßer Korrelationen«:

»Insoweit kann auch die Kombination personenbezogener und nicht personenbezogener Daten und gegebenenfalls die algorithmentypische Berücksichtigung bloßer Korrelationen neue, sonst nicht sicht- oder ermittelbare persönlichkeitsrelevante Aufschlüsse geben. Ein herkömmliches Verfahren, die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit, wird hierdurch mit einer viel größeren Durchschlagskraft versehen (vgl. BVerfGE 115, 320 <356 f.> m.w.N. – zur Rasterfahndung).« (Rn. 69).

Etwas dramatischer wird an einer anderen Stelle sogar das Bild von der *Methodenoffenheit* im Sinne von einer Art *Verlust* der (klassisch polizeilichen) Methoden gezeichnet. Dort heißt es:

»In ihrer *daten- und methodenoffenen Unbegrenztheit* erlauben die Regelungen der Polizei, mit einem Klick umfassende Profile von Personen, Gruppen und Milieus zu erstellen und auch zahlreiche rechtlich unbeteiligte Personen weiteren polizeilichen Maßnahmen zu unterziehen, die in irgendeinem Zusammenhang Daten hinterlassen haben, deren automatisierte Auswertung die Polizei auf die falsche Spur zu ihnen gebracht hat.« (R. 150, Hervorh. d. Verf.).

Mit der Rede vom »Algorithmentypischen« sowie vom »einen Klick« schließt sich freilich wieder der Kreis: das Kernproblem ist in dieser Perspektive dann doch wieder die zum Data Mining befähigende Software selbst. Sie übt Macht aus, wird zur Ursache. In der Technikphilosophie nennt man eine solche Annahme »Technikdeterminismus«: Die neuartige Technologie lässt die neuen Methoden entstehen.

## 2.2 Software(-Technik)

Die sich verändernden polizeilichen (Such-)Methoden sind ohne die »Analyseplattform« hessenDATA noch als »einfach« anzusehen. Kommt die Plattform zum Einsatz, bezeichnet das Gericht die Methoden aber als »komplex«. Das umreißt einerseits die methodisch neuen Qualitäten, neues Wissen sowie neue Möglichkeiten zur Vorausschau entstehen zu lassen. Veränderte Methoden sind es ande-

rerseits allein aber eben nicht. Vielmehr scheint die Kritikalität von hessenDATA aus Sicht des Gerichts sehr wohl auf das genuine Leistungsspektrum einer bestimmten Software und damit auf rein technische Gründe für die nun – als in zuvor unbekannter Weise komplex bezeichnete Vorgehensweisen – zurückzugehen.

Das Gericht geht zwar auf das umstrittene US-amerikanische Unternehmen Palantir Technologies kaum ein, und das Produkt Gotham charakterisiert es ebenfalls nicht. Die für das ganze Urteil charakteristische Idee vom datenschutzrechtlich relevanten »Eigengewicht« des genutzten Analysewerkzeugs lässt dennoch keinen Zweifel daran, dass es zumindest auch die Beschaffenheit des in Hessen eingesetzten (sowie von Bayern mit der Option andere Bundesländer zu beteiligen lizenzierten) Softwareprodukts ist, wegen der die Beschwerdeführer wie auch das Gericht in den beanstandeten Gesetzen einen Verfassungsverstoß sehen. Es wird also dezidiert nicht direkt über Gotham oder das angepasste Derivat hessenDATA verhandelt. Dennoch steht das Softwareprodukt paradigmatisch für das, was die Polizeibehörden der Länder Hessen, Hamburg und Bayern künftig legal nutzen dürfen sollen, und auch die unter 2.1 geschilderten Ausführungen des Gerichts zu den Polizeimethoden erhalten erst durch die Vorstellung einer Software ihren Sinn, die den Unterschied macht – im Sinne einer viel differenzierteren und durch Komplexität der Daten, der Pfadwahl etc. tiefergehenden, aber eben auch von der Technik abgeleiteten bzw. durch sie ermöglichten Vorgehensweise.

Schon die Unternehmenskommunikation jenes viel diskutierten Softwareanbieters, mit welchem man sich im Falle hessenDATA eingelassen hat, stimuliert die Phantasie in eine Richtung, die sich mit einer strengen Selbstbegrenzung der Rationale von Polizeiarbeit schlecht verträgt: Palantiri – das sind in J.R.R. Tolkiens Jahrhundertroman *The Lord of the Rings* sehende Steine, die den wenigen Herrschern, die sie besitzen, die Macht in Vergangenheit und Zukunft zu blicken verleihen. Im heroischen Kampf gegen eine entfesselte Herrschaft des Bösen – einschließlich gewisser Tücken der sehenden Steine selbst – besteht bekanntlich der Plot des Romans. Der Produktname Gotham legt ebenfalls ein manichäisches Weltbild des Kampfes der Guten gegen die Bösen nahe: Es handelt sich um den Namen der Stadt, in welcher der Comic- und Film-Held Batman sich im Namen ausgleichender Gerechtigkeit mit mächtigen Bösewichten anlegt, wobei nicht zuletzt das Sujet der massenhaften Überwachung von Bürgerinnen und Bürgern eine Rolle spielt.<sup>12</sup> Dies mag ein Werbe-Gag bleiben. Um den Subtext, mittels der Software gelte es, Allmacht zu erlangen, kommt man jeweils aber

---

<sup>12</sup> Christian Geminn verdanke ich den Hinweis auf diesen Überwachungsaspekt, u.a. in Christopher Nolans Nutzung des Batman-Stoffes in dem Kinofilm *The Dark Knight*.

nicht herum – und die zahlreichen, unverblümt antidemokratischen Statements des Palantir-Firmengründers Peter Thiel machen die Sache nicht besser.<sup>13</sup> Im datenschutzrechtlichen sowie demokratiebezogenen Kontext muss es daher eine Provokation bleiben, dass ausgerechnet diese Software genutzt werden soll und nun streitgegenständlich ist.

Das Gericht geht darauf nur andeutungsweise ein. Es macht lediglich klar, kommerzielle Software funktioniere in der Regel intransparent, und erinnert: »Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht [...] eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte« (Rn. 100).

Die Intransparenz der mit hessenDATA zum Einsatz kommenden Technik bleibt allerdings auch in der sprachlichen Fassung bestehen, die das Gericht ihr gibt. Fast möchte man von einer zweiten, einer begrifflichen Black Box sprechen. Technische Spezifikationen werden gezielt vermieden. Stattdessen ist die Rede in vielfacher Hinsicht von »automatisiert« bzw. »Automatisierung«, von »Anwendung« (was sehr generisch bleibt), von »Analyseplattform« (was die Funktionen variabler Verknüpfung unterstreicht), von »Software«, »die komplexere Formen des Abgleichs von Daten erlaubt« (Rn. 109), und im Gegenzug auch von einer »besonderen Technizität« der Regelungen, die zwecks Verfassungskonformität erforderlich seien (vgl. Rn. 112).

Laut Sachverhaltsbeschreibung setzt hessenDATA auf drei sehr unterschiedlich strukturierten (älteren) Datenbanken auf und erlaubt hier verknüpfte Abfragen, ist aber weder direkt mit dem Internet oder dem Hersteller verbunden noch kommen ML- oder KI- (im Sinne von: selbstlernenden) Verfahren zum Einsatz. Die spezifische Leistung der Software scheint eher in der Überwindung der Heterogenität der Datensätze zu liegen als in einer Adaptivität z.B. an die Erfordernisse eines Einzelfalls. Auch generalisierbare Typisierungsleistungen, »Profiling« oder dergleichen scheint hessenDATA nicht zu erbringen. Ebenso scheint die Software nicht auf den drei Datenbanken, auf die sie zugreift, zwecks Entwicklung eines maßgeschneiderten Graphen »trainiert« worden zu sein. Solche – gewiss immer noch anbieterneutralen – Aussagen zur Präzisierung des Leistungsspektrums der streitgegenständlichen Softwarelösung bleiben jedoch Mutmaßungen. Das Gericht trifft sie nicht.

---

13 Zum Unternehmen vgl. den Beitrag von Brenneis/Denker/Gehring in diesem Band. – Die Figur Thiel beschäftigt auch die Medien, vgl. Kaube 2025; der sechsteilige Deutschlandfunk-Podcast »Die Peter Thiel Story« von Mai bis Juli 2025 wurde mehrere Millionen Male abgerufen. <https://www.deutschlandfunk.de/die-peter-thiel-story-100.html> (01.10.2025); einen europäischen »Konkurrenten« zu Palantir, »vergleichbar dem Flugzeughersteller Airbus«, hat ein Leitartikel aber auch ganz abseits der ideologischen Verstrickungen aus rein ökonomischen Gründen gefordert, vgl. Knop 2025.

Man kann hier spekulieren: Soll zwar die Software den Unterschied machen, dennoch aber der Unterschied, den sie ausmacht, softwareübergreifend formuliert sein? Oder soll die Diagnose der Neuheit eben doch relativiert werden, womit die Justiz vom Bild einer disruptiven Technologie ein Stück weit abrückt? Oder geht es – trotz anerkannter Neuheit dessen, was die Technik kann – um eine Art Option fürs inkrementelle Bewerten?<sup>14</sup>

Alles in allem fällt auf, dass das Palantir-Urteil sich ungewöhnlich weit nicht nur auf Methodenfragen einlässt, sondern ebenso auf die Funktionsweisen der Technologie selbst. Allerdings kreierte es einen ganz eigenen Weg zu deren Konkretisierung – wobei es die automatisierte Datenanalyse teils als disruptiv, teils als doch irgendwie lediglich eine Etappe einer Entwicklung hinstellt, die vielleicht sogar einer schiefen Ebene gleicht: vom Händischen und einfach Automatischen zur komplexen Automatisierung. Und weitere Neuerungen zeichnen sich gleichsam am Horizont ab, denn das Gericht spricht sie auch bereits an. Technisch steht die sogenannte Künstliche Intelligenz im Raum, operativ-praktisch die Nutzung digitaler Werkzeuge zu Zwecken der Prädiktion.

### 2.3 »KI« und Predictive Policing

Dass die Palantir-Entscheidung nicht nur auf die Formulierungen in den hessischen und hamburgischen Landesgesetzen abhebt, sondern scharf – und vielleicht sogar in der Hauptsache – an technisch eröffneten Möglichkeitsräumen interessiert ist, zeigen sowohl die vielen im Grunde vorbeugenden Äußerungen zu »KI« (als technischer Option) als auch der Raum, der das Thema Predictive Policing (also einer möglichen künftigen Methodik) einnimmt. Beide Themen werden in der BVerfG-Entscheidung unter dem Gliederungspunkt »Kriterien für die Bestimmung des Eingriffsgewichts« abgehandelt, und dies wiederum unter dem Rubrum »Methoden«.

Man sollte es sicher zunächst vermerken, dass das Gericht Möglichkeiten ausführlich kommentiert, die weder in Hessen praktiziert werden noch in Hamburg geplant sind, sodass man vor allem fragen muss, ob die jeweiligen Landesgesetze diese denn zulassen *würden*. Das Gericht behauptet dies freilich nicht einmal, sondern äußert sich zu beiden Punkten im Grunde ungefragt.<sup>15</sup> Zum Thema »KI« – verstanden als Lernfähigkeit von Systemen – lauten die Ausführungen so:

---

<sup>14</sup> Dies ist eine Vermutung von Andreas Brenneis, dem ich für den Austausch zur Sache danke.

<sup>15</sup> Vgl. Rn. 48, wo das Gericht recht klar die Frage der Zulässigkeit des Einsatzes von »KI« sogar aus dem Gegenstandsbereich des Urteils ausklammert.

»e) Besonderes Eingriffsgewicht kann je nach Einsatzart die Verwendung lernfähiger Systeme, also Künstlicher Intelligenz (KI), haben. Deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden.« (Rn. 100).

Das bedenkliche Eingriffsgewicht von KI-Einsatz, so wohl die Botschaft, wäre demnach (wenn es denn dazu käme) gewiss sehr hoch. Und hinsichtlich eines Predictive Policing stellt das Gericht in einem ähnlichen Eventualmodus gleichsam ein Stoppschild auf:

»Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines ›predictive policing‹ getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein (vgl. EuGH, Urteil vom 21. Juni 2021, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491, Rn. 195).« (Rn. 100).

Ein solches Predictive Policing wird zunächst als »eingriffsintensivierend« bezeichnet (vgl. RN 98), dann aber mit einem Gesetzesvorbehalt belegt:

»Sollen etwa maschinelle Sachverhaltsbewertungen ausgeschlossen werden, die über die Anzeige von Übereinstimmungen zwischen Suchkriterium und durchsuchten Datenbeständen hinausgehen, sollen insbesondere maschinelle Gefährlichkeitsaussagen über Personen im Sinne eines ›predictive policing‹ ausgeschlossen oder die Datenanalyse oder -auswertung von vornherein nur auf die Erkennung gefährlicher oder gefährdeter Orte gerichtet werden, ist das Eingriffsgewicht nur dann verringert, wenn der Gesetzgeber dies selbst vorgibt.« (Rn. 121).

Über diesen Punkt freilich – dass Personen keine vorab gefassten Profile, z. B. keine Gefährlichkeitsstufen zugeschrieben werden sollten – scheint gar keine Uneinigkeit zwischen dem Gericht und den Ländergesetzgebern zu bestehen. So dokumentiert der Entscheid die Aussage des Landes Hessen, »[e]s gehe nicht um umfassende Persönlichkeitsbilder und Sozialprofile, sondern allein um die Effektivierung und Beschleunigung der Datenverarbeitung innerhalb eines klar definierten Datenbestands« (RN 25). Zu jenem *Neuen*, das die Landesgesetze oder auch die auf diesen (und der neuen Software) beruhenden digitalen Ermittlungsrealitäten mit sich bringen, gehört also die prädiktive Arbeit im Sinne eines Predictive Policing (oder gar eines individualisierenden, konkrete Verdächtige ausmachenden Profilings) unmittelbar nicht hinzu.

Das Gericht scheint hier alles in allem eher eine Zukunftsperspektive zu kommentieren, eine (sei es in der Software, sei es in der mit ihr eröffneten Ermitt-

lungspraxis angelegte) schiefe Ebene zu befürchten. Um dann die Gelegenheit zu nutzen. Es werden nämlich schon einmal ganz abseits der Konstellation rund um die beanstandeten Gesetze so etwas wie rote Linien fixiert – und zwar seitens des Gerichts nun ebenfalls prospektiv.

### 3. Schwellenwerte plausibilisieren? Zwischen Technik, Polizeipraxis und Rechtspolitik

Die Perspektive des Entscheids ist ganz auf das Konstrukt des »Eingriffsgewichts« zugeschnitten, von welchem man – darauf läuft die Argumentation des Gerichts jeweils zu – letztlich nur sagen können muss, ob es sinkt oder steigt. Es geht um Tendenzen, denen dann mittels Hürden entgegenzuwirken ist (etwa das Vorliegen der »konkreten« Gefahr, deren hinreichend »konkrete« Bestimmung im Fall der einzelnen Ermittlung, aber auch die hinreichend engen gesetzlichen Voraussetzungen zum Einsatz jener ein »Eigengewicht« besitzenden Technologie). Die Grundrechtsdogmatik hat sich dank einer kleinteiligen Abwägungsjudikatur zu einer Art gigantischer Hydraulik entwickelt, deren miteinander korrespondierende Mehrs und Wenigers in ein Sprachspiel hineinführen, das außer Spezialisten kaum jemand kompetent nutzen kann. Letztlich muss man zudem die Spruchgewalt besitzen, den Vorrang des einen übers andere oder auch die omnipräsenten »Schwellenwerte« zu postulieren.

Auch das Palantir-Urteil bietet hier zwar einiges an. Es fordert von den Ländern, die »automatisierte Analysen« komplexen Typs zulassen wollen, im Gesetzestext selbst »normenklare« und »hinreichend bestimmte« Regelungen zu treffen, und zwar nicht nur zu Datenart und Datenmenge, sondern auch »zur Beschränkung der Datenverarbeitungsmethoden« (Zusammenfassung). Solche Regelungen sollen »in der Sache so eng begrenzt« sein, »dass das Eingriffsgewicht der Maßnahmen erheblich gemindert ist« (ebd.). Die Empfehlungsprosa des Gerichts hebt hierzu gleichsam aufs Herauf- und Herunterdrehen von Stellschrauben ab. So heißt es zu dem, was das Palantir-Urteil ja neu ins Spiel bringen will, nämlich zu den Anforderungen an die zu neuem Wissen führende »Methode«:

»Die mit einer offenen Suche verbundenen Gefahren werden durch eine anspruchsvoll ausgestaltete Eingriffsschwelle verringert (Rn. 104 ff.), können aber auch schon durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden, wenn der Suchvorgang eingrenzend so geregelt ist, dass er einen Bezug zu einem konkreteren Suchanlass voraussetzt. Je geringere Anforderungen der Gesetzgeber an den Anlass einer Datenanalyse oder -auswertung stellt, umso genauer und enger muss er die Methode der Suche regeln.« (Rn. 95).

Mit solchen Darlegungen bleibt die Entscheidung jedoch einigermaßen labyrinthisch. Anhaltspunkte für jene operative Grenze, welche mit der digitalen Auswertungsplattform in der Polizeipraxis in *methodischer* oder *technischer* (oder eben wirklich: primär *politischer*) Hinsicht überschritten ist, sind selbst weder eindeutig methodischer noch eindeutig technischer Art noch auch festgemacht an einem übergeordneten praktisch-politischen Sinn der Norm. Sorgen andere Verfahrensweisen oder verursacht die Kapazität einer Software oder schafft eine Art schiefe Ebene, eine Entwicklung im Rücken von beidem das Problem? Und geht es wirklich um eine real gegebene Alternative zwischen Status quo (der »klassischen« Ermittlungstätigkeit, die jederzeit beizubehalten wäre) und einer neuen, durch »komplexe« Technologien geprägten Normalität, der es, weil die Polizeiarbeit hieran allenfalls in gedrosselter Form teilhaben sollte, ex ante einen Riegel vorzuschieben gilt?

Rein sprachlich scheint die Semantik von Suche und Abgleich im Grunde offen zu lassen, ob hier die intellektuell gesteuerte Recherche klickbasiert plötzlich derart gut unterstützt wird, dass der Polizeiarbeit gleichsam ein unzulässiges digitales Enhancement zuteil wird, welches die informationellen Grundrechte der Bürgerinnen und Bürger gefährdet – oder aber ob es da im Inneren der Maschine, also auf Seiten der Funktionsweise des Softwaresystems, etwas gibt, das in bedenklicher Weise »neues Wissen« produziert.

#### 4. Fazit

Will das Gericht die Polizei auf »klassische Polizeimethoden« beschränken oder will es bestimmte Formen der »komplexen« automatisierten Datenverarbeitung unter ein gesondertes Kontrollregime bringen? In beiden Hinsichten liefert das Urteil zwar Argumente. Es sind aber im Grunde jeweils nur Argumente halber Art, das wollte dieser Beitrag zeigen.

Das Gericht legt sich in der Frage der Neuheit (und damit der Schwellenwerte, die die gesetzlich für zulässig erklärten Softwarelösungen überschreiten) schlicht nicht fest. Man könnte auch sagen, dass es Unschärfen produziert oder auch die Festlegung scheut. Zugleich bringt es mit »KI« und Predictive Policing auf eine eher assoziative Weise Zusatzthemen ins Spiel, angesichts derer man sich wiederum fragen kann: Sind dies Gefahren für die rechtsstaatlich geforderten Methoden, fehlt es an *Umgangskompetenzen* mit neuen technischen Möglichkeiten, oder ist man schlicht mit einer übermächtigen Technologie konfrontiert, die »automatisch« Formen des Wissens produziert, was die Grenzen dessen kompromittiert, was Sicherheitsbehörden überhaupt *können sollten*? Oder, noch kürzer: Geht es um Compliance oder schreibt man den Faktor Mensch von vornherein ab?

Dass sich das Gericht zwischen diesen beiden Lesarten des Einsatzes der umstrittenen Auswertungsplattform nicht entscheidet, ja dass es nicht einmal klar machen möchte, wo genau es eigentlich das Neue jenes durch die Kläger beanstandeten Technologieeinsatzes angesiedelt sieht – in dem neuen Wissen, das ein Nutzender sich erarbeiten kann (man könnte sagen: Neuheit als Verfahren) oder aber in einer komplexen Automatisierungsleistung, die als solche das Neue bereits erbringt (man könnte sagen: Neuheit im Ergebnis) –, bleibt ein irritierender Befund. Letztlich erspart es sich das Gericht, zu sagen, wem es denn nun eigentlich wirklich misstraut: einer nicht mehr »klassisch« arbeitenden Polizei, einer nicht mehr »einfach« funktionierenden digitalen Datenbanknutzung, einem Landesgesetzgeber, der allzu forsch die Verknüpfbarkeit der Bestände seiner Datenbanken ertüchtigt, – oder vielleicht doch einem Softwarehersteller, von dem anzunehmen ist, dass er bereit ist, den Landesbehörden künftig auch »KI«-Verfahren sowie Profiling-Modelle und damit Verfahren des Predictive Policing zu liefern.

Rechtspolitisch wird das Urteil – vielleicht eben aufgrund dieser Unbestimmtheit – aber auch wenig Folgen haben. Weder bekennt sich das Gericht zu dem (im Grunde ja kühnen) Motiv, nur einer zu »klassischen« Verfahren der Datenbanknutzung gezwungenen Polizeiarbeit sei im Digitalzeitalter zu trauen – welche komplexen Analysewerkzeuge auch immer es draußen auf dem Markt gibt. Noch skandalisiert das Urteil wirklich die (stattdessen recht hilflos als »komplexer Abgleich« umschriebene) vollautomatische Verknüpfbarkeit forensisch für relevant gehaltener Daten – und damit bestimmte Typen von Software. Und selbst die Zusammenarbeit mit einem dubiosen außereuropäischen Anbieter, also digitale Souveränität im Bereich deutscher und europäischer Sicherheitsbehörden (durchaus ja ein mögliches Thema), lässt es im Grunde außen vor.

Im Ergebnis zeigt die eigenwillige sprachliche Beschaffenheit der Entscheidung damit nicht nur ihren dogmatischen Sitz im Datenschutzrecht an. In ihr bekundet sich auch nicht allein der Versuch, hinreichend technologieneutral sowie einigermaßen praxisnah zu beschreiben, worum es im Fall Palantir-Gotham oder auch hessenDATA aus verfassungsrechtlicher Sicht geht.

Mit dem durch das Gericht geschaffenen begrifflichen Mehr-Eck von »Neuheit«, »Erkenntnis« und »Automatisierung«, einer als komplexes Abgleichen rekonstruierten »Analyse«, wird vielmehr eine Art Zwischenreich eröffnet, das Schnittstellen und Verantwortlichkeiten scheinbar verschwinden lässt angesichts von im Grunde als übermächtig erscheinenden Technologien. Die Sprache des Gerichts dämonisiert die Technik auf diese Weise vielleicht sogar – und diese kleinteilige Technikfixierung verengt den Blick. Weil die Betrachtung sich auf eine popularisierende Feinbestimmung der neuartigen Funktionsweise der von Palantir vertriebenen Software einlässt, ist von übergeordneten Gesichtspunkten

immer weniger die Rede: Wie stehen die Sicherheitsbelange des Staates zur bedenkenlosen Technikentwicklung auf dem allgemeinen Markt? Sollten neben Datenschutzproblemen womöglich noch ganz andere Machtverschiebungen im Umfeld der Strafverfolgung unsere Besorgnis erregen? Und: warum hat die Polizei eigentlich so veraltete und so schlecht integrierte IT-Systeme, dass allein ein dubioser US-amerikanischer Anbieter hier noch zu helfen können scheint? Auch mit seinen Ausblicken auf die bedenklichen Zukunftsoptionen »KI« und polizeiliche Prädiktion verzichtet das Gericht auf jegliche Kontextualisierung oder Hinterfragung der Entstehung oder Beschaffenheit neuer Technologien.

Im Ergebnis erscheint es immer schwerer, menschliche Aufgabenstellungen und Pflichten in der Polizeiarbeit angesichts einer äußerst leistungsfähigen Software klar zu adressieren. Über den Verfassungsauftrag von Sicherheitsbehörden oder auch über den digitalen Wandel der Gesellschaft als solchen zu sprechen, erscheint sogar gar nicht mehr nötig. Lieber werden neue Beurteilungs- und Kontrollkriterien für eine externe Limitierung des methodisch Zulässigen installiert, die einseitig dem Staat vorwerfen, ihm wüchse durch den digitalen Wandel Macht zu. Man will die Technik bannen. Denen, die mit ihr arbeiten, traut man dies – einen Beitrag zur Aufrechterhaltung rechtsstaatlicher Vorgehensweisen zu leisten – nicht zu.

Vor allem aber, das sollte in der Hauptsache gezeigt werden, verliert das Gericht mit all den vielen, immer kleinteiligeren Schritten zur vermeintlichen Konkretisierung dessen, was angesichts einer bloß technologisch bestimmten Neuheit im Einzelfall abzuwägen sein soll sowie zu tun und zu unterlassen ist, den Sinn der Norm wie auch die Frage nach dem Umgang mit der Macht neuer Technologien aus dem Blick. Der Technikfokus sorgt für eine Art Blow-up-Effekt: Man glaubt, mehr zu sehen und (mittels Grundrechtssemantik) zu kontrollieren. Übergeordnete politische Zielsetzungen aber gehen verloren.

## Quellen und Literatur

- Hessische Landtagsfraktionen CDU und BÜNDNIS 90/DIE GRÜNEN: Änderungsantrag zu dem Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen, Drucksache 19/5412, in: HessLTDrucks 19/6502. <https://starweb.hessen.de/cache/DRS/19/2/06502.pdf> (01.10.2025).
- Kaube, Jürgen: Citizen Thiel, in: *Frankfurter Allgemeine Sonntagszeitung*, 06.07.2025, S. 41 f.
- Knop, Carsten, »Europas digitale Existenzfrage«, in: *Frankfurter Allgemeine Zeitung (FAZ)*, 15.03.2025.

Ders., »Unsere digitale Existenzfrage«, in: *faz-online*, 15.03.2025. <https://www.faz.net/aktuell/politik/inland/europas-digitale-souveraenitaet-digitale-existenzfrage-110357356.html> (01.10.2025).

Popitz, Heinrich, »Über die Präventivwirkung des Nichtwissens«, in: Pohlmann, Friedrich/Eßbach, Wolfgang (Hg.): *Soziale Normen*, Frankfurt am Main 2006, S. 158–174.

# Neue Informationen, neue Erkenntnisse, alte Daten

*Kai Denker*

Im sog. »Palantir-Urteil« des BVerfG zur automatisierten Datenanalyse<sup>1</sup> changieren Begriffe wie Daten, Information, Wissen und Erkenntnisse auf einem Spektrum: Daten erscheinen als ein Rohmaterial, aus dem – durch Verarbeitung – bestehende oder neue Informationen gewonnen, freigelegt oder erzeugt werden können, was dann zu (neuem) Wissen führe – bzw. im polizeirechtlichen Kontext zu (neuen) Erkenntnissen. Unklar bleibt, inwieweit Informationen in Daten stecken, ob Informationen ihrerseits Daten sind, wie sich dies zum Begriff des Wissens – Wissen muss schließlich gewusst werden – und sodann zu dem der Erkenntnisse verhält. Insoweit das Urteil gerade dort die Einsatzmöglichkeiten von (neuen) informationstechnischen Mitteln durch Polizeibehörden einschränkt bzw. dem jeweiligen Gesetzgeber Vorgaben für deren Regulierung macht, da diese neues Wissen oder neue Erkenntnisse ermöglichen, führt die Unklarheit direkt an den Kern des Problems: Es gilt zwischen einer informationstechnisch informierten und über bloßen Datenschutz hinausgehenden Abwägung einerseits und der Praxis der Polizeiarbeit beim Gewinnen von Erkenntnissen andererseits zu vermitteln. In diesem Beitrag soll die Verwendung der Begriffe »Daten«, »Information«, »Wissen« und »Erkenntnisse« in der BVerfGE »definitionsarchäologisch« untersucht werden: Auf welche Definitionen, sofern überhaupt, baut das Urteil auf? Lassen sich die Begriffe systematisch abgrenzen oder bleibt es bei einer changierenden Bewegung zunehmender Verfeinerung? Und wo genau kommt das »Neue« ins Spiel?

Es fällt auf: Definitionen finden sich im Urteil kaum – auch nicht zum Datenbegriff. Auch in Urteilen, auf die verwiesen wird, finden sich keine Definitionen – fast als ob »jedermann weiß«, was Daten, was Informationen und was Wissen sind. Dies stimmt schon für das Urteil des BVerfG zur Volkszählung von

---

<sup>1</sup> BVerfG, Urt. v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, BVerfGE 165, 363 – 442. – Nachfolgend wird aus dem Urteil (unter Nachweis der Randnummern) im Fließtext zitiert.

1983:<sup>2</sup> Bereits hier ist klar, dass Daten das sind, was »[u]nter den Bedingungen der modernen Datenverarbeitung« eben verarbeitet wird. Sucht man nach Legaldefinitionen von »Daten«, wird man meist auf die Regelungen zum Datenschutz verwiesen. Diese Regelungen beziehen sich jedoch auf »personenbezogene Daten«, etwa in Art. 4 DSGVO: Der Ausdruck »personenbezogene Daten« [bezeichnet] alle Informationen, die sich auf eine identifizierte oder identifizierbare Person [...] beziehen«. Weitere Arten von Daten wie »genetische Daten« oder »biometrische Daten« werden aus der Definition der personenbezogenen Daten abgeleitet.<sup>3</sup> Wer nach einer Legaldefinition von »Daten« im Allgemeinen sucht, wird weder hier noch im StGB fündig: Zwar pönalisiert § 202a StGB seit 1986 das Ausspähen von Daten. Es schränkt aber in Abs. 2 ein, nur solche Daten seien gemeint, »die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.« Auch andere Normen wie § 303a verweisen lediglich auf § 202a Abs. 2. Auch die StPO schweigt sich in dieser Weise aus und setzt »Daten« als bekannt voraus. Vielleicht könnte man auf technische Normen zurückgreifen. So lässt etwa die das IT-Vokabular standardisierende Norm ISO/IEC 2382:2015 wissen, dass Daten eine »neu interpretierbare Darstellung von Information in formalisierter Weise, geeignet zur Kommunikation, Interpretation oder Verarbeitung« seien. Daten sind dann stets eine Darstellung von etwas – nämlich von einer Information, d.h. die Information steckt irgendwie »in« den Daten. Daten müssen formalisiert sein, um maschinell prozessierbar zu sein. Nach ISO/IEC 2382:2015 sind Daten dann eine Repräsentation einer Information, die ihrerseits gerade die Bedeutung hat, die ein interpretierendes System diesen Daten zuweist. Wissen wäre, so die Norm weiter, dann eine kontextualisierte, bewertete Information. Daten sind strukturiert, zeichenhaft, können Informationen zum Inhalt haben (müssen aber nicht) und sind jedenfalls das, was am Anfang einer Verarbeitung steht. Sie sind gleichermaßen Rohmaterial wie Schutzobjekt (etwa in der IT-Sicherheit). Und schließlich stehen Daten wieder am Ende einer Verarbeitung: Das, was aus einer informationstechnischen Datenverarbeitung herauskommt, sind selbst wieder Daten.

---

2 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, BVerfGE 65, 1 – 71. Auch das Volkszählungsurteil enthält sich einer systematischen Abgrenzung von »Daten« und »Information«, obzwar beide Begriffe umfassend zur Sprache kommen. Anders als im »Palantir-Urteil« ist hier aber auch keine changierende Begriffsverwendung erkennbar. Anders sieht es im Rasterfahndungs-Beschluss aus (BVerfG, Urt. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 – 381), das »Daten« und »Information« über weite Strecken miteinander zu identifizieren scheint, etwa indem es »persönlichkeitsbezogene Informationen« neben »personenbezogene Daten« setzt (z.B. Rn. 94).

3 Auch das alte Bundesdatenschutzgesetz hilft hier nicht weiter.

Kompatibel zu dieser technischen Auffassung bleibt jedenfalls der europäische Gesetzgeber. Sowohl im *Data Act* (DA) als auch im *Data Governance Act* (DGA) hat dieser den Begriff der Daten wortgleich wie folgt bestimmt:

»Daten« jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material; [...]«<sup>4</sup>

Hier wird zwischen der DSGVO und dem DGA bzw. dem DA ein subtiler Unterschied deutlich: In der DSGVO bezeichnet der Ausdruck »personenbezogene Daten« eine bestimmte Art von Informationen, nämlich solche, »die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen«,<sup>5</sup> im DGA bzw. DA aber sind Daten eine Darstellung von Informationen, also eine Repräsentation. DSGVO, DGA und DA definieren Daten unter Rückgriff auf einen Informationsbegriff, ohne dass dieser selbst wieder Gegenstand einer Definition würde – die Definition ist uneinheitlich und grundsätzlich gilt, dass es keine einheitliche Definition gibt – weder rechtlich noch technisch. Die Definitionen changieren – und das ist auch im »Palantir-Urteil« der Fall. Auch für Informationen und Wissen ergibt sich ein Fehlbefund: Mehr noch als für Daten wird offenbar für Informationen angenommen, dass jedermann wisse, was gemeint sei. Greift man zum Duden, so erfährt man immerhin, dass Information u.a. der Gehalt einer zeichencodierten Nachricht sei. Diese kybernetische Definition passt zu einigen der oben herausgearbeiteten Definitionen von »Daten«, insofern dort Informationen als etwas bezeichnet werden, was in Daten repräsentiert sei. Wir werden aber sehen, dass im vorliegenden Urteil die Verhältnisse deutlich komplizierter liegen, da »Information« dort zwischen zwei Polen changiert und sie an »Wissen« und »Erkenntnisse« herangerückt wird.

Im Folgenden werden die zueinander changierenden Verwendungen von »Daten«, »Informationen«, »Wissen« und »Erkenntnisse« im Urteil rekonstruiert. Es zeigt sich dabei, dass von »Informationen« einmal in einer objektiven Rolle mit starkem Bezug auf Daten und einmal in einer subjektiven Rolle mit klarem Bezug auf Wissen und Erkenntnisse die Rede ist. Dies erlaubt es – so meine These –, eine datenorientierte Rechtsprechung mit der Polizeigesetzgebung zu vermitteln. Zugleich scheint sich das Gericht hier einen Weg zu öffnen, nicht nur die Herkunft von Daten und deren Verarbeitungszwecke zum Entscheidungsgegenstand zu machen, sondern auch die bei der (datenschutzrechtlich gesprochen) »Datenverarbeitung« eingesetzten informationstechnischen Mittel

---

4 Art. 2 Data Act; sowie wortgleich Art. 2 Data Governance Act.

5 Art. 4 Nr. 1 DSGVO.

selbst noch einmal gesondert zu charakterisieren. Diese sind es dann, die eine neue Eingriffstiefe hervorbringen.

## 1. Daten

Im Urteil findet sich die Zeichenketten »Daten« ganze 620-mal, oft in Komposita wie »Datenverarbeitung«, »Datenanalyse« oder »Datenbestände«. Beschränken wir uns auf ganze Wörter, also das alleinige Vorkommen der Zeichenkette, findet sie sich immerhin noch knapp 246-mal. Übergeht man die Darstellung des Parteivortrags (Rn. 20 ff) und konzentriert sich auf die ausführlichen Entscheidungsgründe des Gerichts (ab Rn. 50 ff), sind davon noch immer die meisten Fundstellen »qualifiziert«, etwa als »personenbezogene Daten« (z.B. Rn. 55, 65, 69, 70), »staatlich erhobene Daten« (Rn. 55), »über den konkreten Anlass und rechtfertigenden Grund [...] hinaus« oder »im Rahmen der für die Datenerhebung maßgeblichen Zwecke« genutzte Daten (Rn. 55), Daten, die einer Behörde gehören (Rn. 58), »Daten aus Wohnraumüberwachungen und Online-Durchsuchung« (Rn. 59) oder »Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen« (Rn. 62). Überhaupt geht es oft um die Herkunft von Daten (Rn. 65), teils »näher eingegrenzter Herkunft« (Rn. 72), teils »bereits erhobene« (Rn. 70) oder ganz allgemein »gewonnene Daten« (Rn. 59) – Daten, die jedenfalls nicht nur eine Herkunft, sondern auch einen Ort haben, etwa in einer »Datei der hessischen Polizei« (Rn. 65), also »Daten, die zwar gegenwärtig in den eigenen Datenbeständen der Behörde gespeichert sind, die aber ursprünglich von einer anderen Stelle erhoben und an sie weitergegeben wurden« (Rn. 65), also sämtliche »einmal erhobenen und gespeicherten Daten« (Rn. 67, 79). Kurz: Daten haben einen Ort und eine Provenienz, etwa wenn sie aus dem Kontext der Terrorbekämpfung stammen (Rn. 81, 82). Unausgesprochen bleibt, was genau mit »Daten« gemeint ist, da es ohnehin klar ist: Es sind eben die (teils personenbezogenen) Daten behördlicher Datenbestände – und um was anderes soll es sich handeln als um Zeichenketten, die irgendwie in elektronischer, magnetischer oder optischer Form gespeichert und für die maschinelle Verarbeitung geeignet sind. Würde es dabei bleiben, wäre die informationstechnisch informierte Auswertung des Urteils damit erledigt. Daten werden aber nicht einfach nur erhoben und in Beständen abgelegt und sind vielleicht gekennzeichnet, sondern sie sind insbesondere auch mit Metadaten gekennzeichnet (Rn. 65). Mehr noch: Einschlägig sind Fragen des Datenschutzes und damit sind rechtliche, nicht technische Eigenschaften von Daten Thema und das ist insbesondere ihr Zweck (Rn. 56). Wenig trivial ist die Frage der »Zweckänderung von Daten« (Rn. 63), besonders die »zweckändernde Weiternutzung der Daten« (Rn. 60), d.h. es geht

um die »Nutzung der Daten zu neuen Zwecken« (Rn. 60), also zu Zwecken, die bei ihrer ursprünglichen Erhebung vielleicht nicht absehbar waren, jedenfalls nicht intendiert wurden. Kriterium hier ist dann »nach verfassungsrechtlichen Maßstäben auch für den geänderten Zweck« die fiktive Neuerhebung der Daten (Rn. 62).

Dass Daten irgendwie genutzt (Rn. 58, 59, 60) werden können, ist wenig überraschend und die Techniker:in mag rechtliche Fragen gerne den Jurist:innen überlassen, etwa wann eine »weitere« (Rn. 62) oder eine »neue Nutzung der Daten« (Rn 62, 64) vorliegt. Schließlich formuliert etwa die DSGVO technologieneutral: Dort ist nämlich die Verarbeitung von Daten – nicht anderes ist die Nutzung von Daten in technischer Hinsicht – jeder »mit oder ohne Hilfe automatisierter Verfahren ausgeführte[r] Vorgang«,<sup>6</sup> also letztlich die Aneinanderreihung informationstechnischer Verfahrensschritte. Das gilt in technischer Hinsicht auch für die »Verknüpfung von Daten« (Rn. 67), wozu sich etwa in der DSGVO nur wenig findet: Die Verknüpfung von (personenbezogenen) Daten wird als möglicher eigenständiger Verfahrensschritt behandelt, der dann nur unter Beachtung der Zweckbindung<sup>7</sup> erlaubt und oft folgenabschätzungspflichtig<sup>8</sup> ist, zumal wenn die (weiteren) »Zwecke der Verarbeitung ein voraussichtlich hohes Risiko [...] zur Folge haben«, etwa im Fall von Profiling.<sup>9</sup> Nun beschränkt sich das Urteil nicht darauf, datenschutzrechtliche Fragen für den Einsatz neuer informationstechnischer Mittel durch die Polizeibehörden in Hamburg und Hessen durchzudeklinieren und deren jeweilige Anwendbarkeit zu bestimmen, sondern fokussiert die »zusammenführend[e] Verwendung vormals getrennter Daten« (Rn. 50), die auch als »verknüpfende Auswertung vorhandener Daten« (Rn. 69) weitergehend sei: Diese können »über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen[de]« »spezifische Belastungseffekte haben« (Rn. 67), etwa indem die im Verfahren angegriffenen Regelungen in § 25a HSOG und § 49 HmbPolDVG darauf ausgerichtet seien, »neues Wissen zu erzeugen«(!, Rn. 67) – ein Begriff, den die DSGVO beispielsweise nicht kennt. Dies kann im Besonderen erfolgen durch »die statistische Auswertung der gespeicherten Daten« (Rn. 67), in den angegriffenen Regelungen aber im Allgemeinen »praktisch alle informationstechnisch mögliche Methoden«, mit denen dann »weitreichende Erkenntnisse« und »neue Zusammenhänge« erschlossen werden könnten (Rn. 67). Auch wenn die Nutzung »einmal gewonnene[r] Erkenntnisse« durch die Polizei »als Spuren- oder Ermittlungsansätze allein oder in Verknüpfung mit

---

6 Art. 4 Nr. 2 DSGVO.

7 Vgl. Art. 5 und Art. 6 Abs. 4 DSGVO.

8 Vgl. Art. 35 DSGVO.

9 Vgl. ebd.

anderen ihr zur Verfügung stehenden Informationen[!–KD] als Ausgangspunkt weiterer Ermittlungen« »für sich genommen nicht ungewöhnlich« sei (Rn. 68), gehe die »automatisierte Analyse oder Auswertung nach § 25a HSOG und § 49 HmbPolDVG [...] schon deshalb weiter, weil sie die Verarbeitung großer und komplexer Informationsbestände ermöglicht« (Rn. 69).<sup>10</sup> Unklar bleibt, was genau mit »groß« und »komplex« an dieser Stelle gemeint ist – und inwieweit hier mehr als eine bloße Steigerungslogik vorliegt. Jedenfalls geht es, da es um automatisierte Verarbeitung geht, sicher über die manuelle Auswertung hinaus, der praktische Grenzen gesetzt sind (Rn. 52, 70).<sup>11</sup> Der Punkt, den das Gericht hier setzt und der unter dem Problem der Neuheit verhandelt wird, ist bemerkenswert, da er stark auf die praktischen Eigenschaften informationstechnischer Mittel zur schnellen Verarbeitung abstellt, dies aber eben unter dem diskreten Prädikat »Neuheit« verhandelt: »Je nach der eingesetzten Analyseverfahren können zudem durch verknüpfende Auswertung vorhandener Daten neue persönlichkeitsrelevante Informationen gewonnen werden, die ansonsten so nicht zugänglich wären« (Rn. 69). Hier deutet sich bereits der eingeschlagene Weg an: Es geht offenbar um die Zugänglichkeit einer Information, die zwar schon in den Daten steckt, aber in der Praxis ohne die neuen Mittel gewissermaßen »noch nicht« zugänglich wäre.

Es fällt auf: In dem Moment, an dem das Gericht über die bloße datenschutzrechtliche Erwägung der Herkunft, Zweckbindung, Verarbeitung, Weitergabe oder Löschung von Daten hinausgeht, bedient es sich der Begriffe Information und Wissen, oft mit dem Prädikat »neu« versehen – gelegentlich spricht es auch von »Erkenntnissen«, wobei es, wie wir noch sehen werden, eine Brücke zum Begriffssystem der Polizei schlägt. Vorerst ist festzuhalten: Das Gericht führt die bekannte Rede über einen technisch nicht klar bestimmten Datenbegriff rechtlich fort, so dass man mit einer um rechtliche Fragestellungen (Herkunft, Zweck, Kennzeichnung) erweiterten, technischen Definition von Daten zwar keine wesentlichen Erkenntnisse gewinnt, aber auch nicht auf Widersprüche

<sup>10</sup> Das Urteil verwendet durchgehend die Wendung »Datenanalyse oder -auswertung« und nimmt damit die Formulierungen der beiden angegriffenen Regelungen aus dem HSOG und dem HmbPolDVG auf. Das Gericht hält aber fest: »Ein maßgeblicher Unterschied zwischen den Wörtern Datenanalyse und Datenauswertung ist nicht zu erkennen.« (Rn. 148).

<sup>11</sup> Insoweit die Hamburger Behörde für Justiz und Verbraucherschutz vorgetragen hat, dass der »automatisierte Zugriff [...] sich nicht vom gezielten Blick eines Beamten in eine Akte oder ein Dateisystem im Sinne einer manuellen Auswertung« unterscheide (Rn. 34), ist sicher einzuräumen, dass sich jedes noch so komplexe informationstechnische System manuell, d.h. von Hand mit ausreichend Papier, Bleistift, Zeit und Personal ohne Einsatz maschineller informationstechnischer Mittel simulieren lässt, jedoch liegt auf der Hand, dass diesem theoretischen Szenario in der Praxis jederzeit enge Grenzen gesetzt sind.

stößt. Überraschend wird es dort, wo (neue) Informationen und (neues) Wissen begrifflich auftauchen.

## 2. Information

Die Zeichenketten »Information« findet sich weit seltener als »Daten« im Urteil: 78-mal, wobei viele Fälle in »informationeller Selbstbestimmung« und »Informationsfreiheit« (aus der Amtsbezeichnung der Datenschutzbeauftragten) bestehen. Einige wenige Fälle sind metaphorische Bildungen wie der »Informationsfluss« aus einem Parteivortrag (Rn. 8). Beschränkt man sich auf ganze Wörter, findet sich »Information« (im Singular) gar nicht, im Plural findet sich »Informationen« 32-mal. Ähnlich wie Daten erscheinen Informationen als etwas, was im weitesten Sinne handhabbar ist, etwa wenn »so viele Informationen wie möglich zu einem Sachverhalt zusammen[ge]tragen« werden sollen, um »daraus Schlüsse zu ziehen« (Rn. 13). Oft werden Informationen mit »Erkenntnissen« konjugiert, so etwa bereits in den angegriffenen Regelungen: »unbedeutende Informationen und Erkenntnisse«, die auszuschließen seien (Rn. 4, 5). Insbesondere ließen sich, so im Vortrag der Beschwerdeführer, Informationen erzeugen: »Aufgrund der technischen Entwicklung ergäben sich neue, eingriffsintensivere Möglichkeiten der Herstellung von Verknüpfungen und der Erzeugung neuer Informationen, wobei auch der Einsatz komplexer Algorithmen und lernfähiger Systeme in Betracht komme« (Rn. 19). Informationen sind aber auch enthalten, und zwar in Datenbeständen: »Die dazu in den polizeilichen Datenbeständen enthaltenen Informationen könnten gerade unter Zeitdruck kaum manuell gewonnen werden; eine automatisierte Datenanalyse sei daher von großer Bedeutung für erfolgreiches polizeiliches Handeln.« (Rn. 52). Informationen werden zudem »gewonnen«, nämlich auf Grundlage einer Datenerhebung (Rn. 57), oder »erlangt«, etwa durch »besonders eingriffsintensive Maßnahmen« (Rn. 61). Damit spielt auch für Informationen die Provenienz eine entscheidende Rolle (Rn. 64). Überhaupt ist nicht nur von Datenbeständen die Rede, sondern auch von »Informationsbestände[n]«, die ebenfalls groß und komplex sein können (Rn. 69). Schließlich können Informationen unterschiedlich gut zur Verfügung stehen (Rn. 68), oder aber auch gar nicht »zugänglich« sein (Rn. 69).

Das Verhältnis von Daten und Informationen zueinander changiert: Mal sind Daten und Informationen im Text anscheinend fast dasselbe:

»Der Gesetzgeber kann danach – bezogen auf die Datennutzung von Sicherheitsbehörden – eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewich-

tigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist.« (Rn. 63 – meine Hervorhebung, KD)

Die Ersetzungsprobe zeigt, dass der Begriff »Information« problemlos durch »Daten« ersetzt werden könnte. Gleichzeitig sind Informationen und Daten gerade nicht dasselbe: Informationen sind in Daten enthalten (Rn. 69, 118). Sie werden erzeugt, wenn bereits vorhandene Daten analysiert oder ausgewertet werden – bzw. es wird Zugriff auf sie hergestellt (beide Wendungen: Rn. 147). Der Informationsbegriff im Urteil changiert: Informationen sind Daten, Informationen sind nicht einfach Daten, aber sie sind bereits da, es muss nur Zugriff erzeugt werden oder aber Informationen werden neu erzeugt.<sup>12</sup>

Wenngleich die fehlende technische Präzision nicht ganz von der Hand zu weisen ist, würde man es sich zu einfach machen, hier bloß eine begriffliche Fortsetzung der Rechtsprechung (vgl. »informationelle Selbstbestimmung« und »Datenschutz«) zu sehen, die auf rechtliche, nicht technische Fragen abstellt. Das Changieren scheint eine bestimmte Funktion im Urteil zu erfüllen, die die Verbindung von bestehenden Daten zu neuem Wissen und neuen Erkenntnissen vermittelt. Technisch ist einzuräumen, dass sich die Begriffe »Daten« und »Informationen« präziser trennen lassen, als es das Urteil an einigen Stellen unternimmt: Informationen sind nicht einfach Daten, sondern Daten repräsentieren Informationen, d.h. insoweit Informationen einen semantischen Gehalt aufweisen, sind Daten ihre syntaktische Repräsentation in Form von Zeichenketten. Anders gesagt: Daten weisen einen Informationsgehalt auf, der sich insbesondere quantifizieren lässt. Informationstheoretisch bieten sich zwei Denkschulen an, die man grob mit den Namen Claude E. Shannon und Andrei Nikolajewitsch Kolmogorow bezeichnen könnte. Bei Shannon handelt es sich bei Information um ein Maß für die Unsicherheit über den Wert einer Zufallsvariable. Je mehr Informationen zur Verfügung stehen, desto sicherer kann ich den Wert einer Zufallsvariable bestimmen. Andersherum: Je weniger Informationen ich über eine Zufallsvariable habe, desto mehr kann ich von ihrem Wert überrascht werden.<sup>13</sup> In einem der primitivsten denkbaren Modelle könnte man sich vorstellen, die Bevölkerung eines Landes durchnummerieren und darauf zu zielen, eine bestimmte Person zu identifizieren. Mit jedem Bit Information, das über diese Menge Personen gewonnen wird, halbiert sich die Menge, in der die zu identifizierende Person zu finden wäre und die Chance, sie zufällig zu finden, verdoppelt sich. Insoweit ist die Rede-

---

<sup>12</sup> Die Vorstellung »neuer Informationen«, die sich aus der Zusammenführung von Daten gewinnen ließen, findet sich bereits im Urteil zur Rasterfahndung – allerdings nur einmal, vgl. BVerfG, Urt. v. 04.04.2006 – 1 BvR 518/02, BVerfGE 115, 320 – 381, Rn. 101.

<sup>13</sup> Informationstheoretiker:innen mögen mir diese weitgehende Vereinfachung verzeihen.

weise, dass Informationen aus Daten gewonnen werden, um nach und nach Erkenntnisse zu verdichten, sicher völlig richtig. Entscheidend ist, dass hierbei Informationen nicht an sich erzeugt werden, sondern sie werden den Datenbeständen, in denen Informationen über die zu identifizierende Person enthalten sind, entnommen, d.h. sie müssen durch ein Analyseverfahren extrahiert werden. In informationstheoretischer Sicht können die Redeweisen des Urteils, dass neue Informationen erzeugt würden, nur subjektiv gedeutet werden: Die Informationen sind in den Daten vorhanden und sie werden »für uns« zugänglich gemacht – und tatsächlich finden wir auch diese Redeweisen im Urteil. Entscheidend ist dabei eben der Punkt, dass durch deterministische Informationsverarbeitung der Informationsgehalt einer Datenmenge zwar reduziert, aber nicht erhöht werden kann. Während Shannon mit Blick auf Rauschen hier aber nicht von völlig deterministischen Verfahren spricht, weist Kolmogorow im Modell der algorithmischen Informationstheorie, die auf die Komplexität algorithmischer Verfahren abstellt, umso eindringlicher auf diesen Umstand hin: Objektiv lassen sich keine Informationen erzeugen. Sie werden uns aber subjektiv zugänglich, indem Daten durch die Datenverarbeitung in Daten überführt werden, die übersichtlicher sind, d.h. indem Daten am Ende einer Datenverarbeitung stehen, in denen Informationen zugänglich sind, da sie überblickt werden können – und zwar gerade deshalb, da andere Informationen in der Verarbeitung verloren gehen. Damit wird die Behauptung der Hamburger Justizbehörde, es handele sich dem Prinzip nach um nichts anderes als den *gezielten* Blick eines Beamten in die Akte verätherisch: Der Blick ist eben nur dann gezielt, wenn er bereits entsprechend *informiert* erfolgt. Festzuhalten bleibt: Auch das komplexeste deterministische informationstechnische Verfahren fügt dem Informationsgehalt bestehender Daten nichts hinzu,<sup>14</sup> sondern im Gegenteil: Es reduziert den Informationsgehalt dahingehend, dass eine übersichtliche, d.h. für uns zugängliche Darstellung erreicht wird. Mit anderen Worten: Die Leistung informationstechnischer Systeme in etwa polizeilicher Ermittlungsarbeit besteht nicht in der Erzeugung neuer objektiver Information im Sinne des Informationsgehalts bestehender Datensätze, sondern in der Reduktion manuell zu verarbeitender Daten bei der polizeilichen Erkenntnisgewinnung, was dann aber seinerseits mehr subjektive Information ermöglicht, da gerade nicht erst alle bestehenden Datensätze manuell ausgewertet werden müssen – das ist freilich auch dem Gericht klar, wenn

---

14 Mit Blick auf den algorithmischen Informationsbegriff nach Kolmogorow ist gleichwohl zu präzisieren, dass ein algorithmisches Verfahren selbst einen Informationsgehalt aufweist, der die Verarbeitung »informiert«. Der Informationsgehalt eines algorithmischen Verfahrens ist, von großen Sprachmodellen abgesehen, aber in der Praxis stets deutlich geringer als der Informationsgehalt der zu verarbeitenden Daten.

es festhält, dass überhaupt erst durch den Einsatz informationstechnischer Systeme große und komplexe Mengen an Datenbeständen praktisch zusammengeführt und ausgewertet werden können, nämlich »vor dem Hintergrund informationstechnischer Entwicklung die Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten zu steigern, indem Anhaltspunkte für bevorstehende schwere Straftaten gewonnen werden, die im Datenbestand der Polizei ansonsten unerkannt blieben«, schließlich könnten die »dazu in den polizeilichen Datenbeständen enthaltenen Informationen [...] gerade unter Zeitdruck kaum manuell gewonnen werden« (Rn. 52). Präzise, aber vielleicht kontraintuitiv besteht die Leistung derartiger Systeme also darin, die relevante, d.h. zu sichtende Datenmenge zu reduzieren, dabei die gesuchte Information zu erhalten und andere Informationen aus den Daten zu entfernen, um das Ergebnis dann in eine übersichtliche Form zu überführen.

Die Lösung scheint also naheliegend: Dort, wo Informationen mit Daten identifiziert werden, lieber von Daten sprechen; dort, wo Informationen in Daten enthalten sind, lieber von Informationsgehalt sprechen; und dort, wo Informationen »neu« sind, auf einen subjektiven Informationsbegriff abstellen. Tatsächlich unternimmt das Gericht dies dort, wo es von »(neuem) Wissen« spricht. Das Changieren des Informationsbegriffs erfüllt aber noch eine weitere Funktion bei der Charakterisierung informationstechnischer Mittel. Im Folgenden soll zunächst über den Begriff des Wissens gesprochen werden, anschließend über die Erwägungen des Gerichts zu dem Einsatz neuer informationstechnischer Mittel – denn das bisher Gesagte lässt sich auch mit altbekannten maschinellen informationstechnischen Mitteln denken.

### 3. Wissen und Erkenntnisse

»Wissen« taucht im Urteil nur an sechs Stellen auf, dort aber umso eindrücklicher: »Die automatisierte Datenanalyse oder -auswertung nach § 25a HSOG und § 49 HmbPolDVG ist darauf gerichtet, neues Wissen zu erzeugen« (Rn. 67), gemeint ist die »Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die automatisierte Datenanalyse oder -auswertung geschaffen werden kann (vgl. BVerfGE 156, 11 <39 f. Rn. 73 f.>; näher unten Rn. 67 ff.)« (Rn. 50)<sup>15</sup>

---

<sup>15</sup> Das BVerfG verweist hier auf sein Urteil zum Antiterrordateigesetz (BVerfG, Urt. v. 10.11.2020 – 1 BvR 3214/15, BVerfGE 156, 11 – 63.), in dem die Bildung »neues Wissen« (in Anführungszeichen erstmalig zu finden ist: Zitiert wird durch das Gericht dort eine Antwort der Bundesregierung auf eine Kleine Anfrage der Linken, wo es heißt, dass nach Definition der Bundesregierung »Data-Mining« dann vorliege, wenn mit mittels informationstechnischer Verfahren »bereits vorhandene große Datenbestände, zumeist auf

Auch an anderer Stelle zielt das Gericht auf das Potenzial ab, nämlich auf die »potenzielle Weite erzielbaren neuen Wissens« (Rn. 147) oder auf die Frage, »welcher Art das neue Wissen sein kann, das durch diese Maßnahmen erzeugt wird, insbesondere davon, ob und wie viel persönlichkeitsrelevantes Wissen so geschaffen wird« (Rn. 77). Das Gericht stellt im »neuen Wissen« also klar auf eine Möglichkeit ab: Es *kann* durch die in den angegriffenen Regelungen beschriebenen Maßnahmen erlangt (Rn. 99), erzielt, erzeugt oder geschaffen werden. Anders als Informationen ist das Wissen offenkundig nicht schon vorhanden, sondern es ist stets neu – eine Wendung, die sich problemlos mit den Überlegungen zum subjektiven Informationsbegriff versöhnen lässt: Wissen ist stets subjektiv, da es gewusst werden muss. Oder anders formuliert: Dem klassischen Wissensbegriff nach ist Wissen die wahre, gerechtfertigte Meinung (*pace* Gettier). Das Gericht nennt so eine Definition nicht, kennt sie aber wenigstens indirekt, da es sich durchaus mit dem Problem der Wahrheit als Problem der Datenqualität (Rn. 95), Verarbeitungsfehlern (Rn. 90, 102, 109) und der Begründetheit durch die fehlende Nachvollziehbarkeit informationstechnischer Verarbeitungen (Rn. 43, 90, 100; siehe unten) beschäftigt. Daneben findet sich wenig, was eine weitere Bestimmung des Wissensbegriffs zu erlauben scheint. Lediglich an einer Stelle findet sich noch eine Äquivokation von »neuem Wissen« mit »neuer Information«:

»Das Gewicht des in der Erlangung neuen Wissens durch eine automatisierte Datenanalyse liegenden eigenen Eingriffs in die informationelle Selbstbestimmung kann sich aber dadurch verringern, dass die Verwendung dieser neuen Informationen an spezifische Voraussetzungen geknüpft wird.« (Rn. 99)

Der Informationsbegriff reicht also von den Datenbeständen hin zum neuen Wissen, ohne allerdings konkret zu werden. Das mag für die Diagnose, dass der Informationsbegriff im Urteil zwischen zwei Polen changiert, ausreichen, bleibt aber für sich genommen unbefriedigend. Neues verspricht der Erkenntnisbegriff, obgleich die angegriffenen Normen hier zunächst beide sprachlich nicht unterscheiden: Es geht um »Informationen und Erkenntnisse«,<sup>16</sup> offenbar um eine Brücke vom eher datenrechtlichen (objektiven) Informationsbegriff zum polizeirechtlichen Erkenntnisbegriff sprachlich zu vermitteln. Das Gericht folgt dieser Ineinssetzung nicht, sondern verhandelt das Problem (polizeilicher) Erkenntnisse mit einer gewissen Distanz zum Informationsbegriff, wenngleich

---

statistisch-mathematischen Verfahren basierend, selbständig auf Zusammenhänge analysiert werden, um auf diesem Wege »neues Wissen« zu generieren.« (BTDrucks 17/11582, S. 3) Für die Bundesregierung scheint es sich hier noch um uneigentliche Redeweise zu handeln, während das BVerfG im vorliegenden Urteil an Rn. 50 das »neue Wissen« zur eigentlichen Redeweise adelt.

<sup>16</sup> Diese Formulierung findet sich – wenngleich negativ – bereits in den angegriffenen Normen, da »unbedeutende Informationen und Erkenntnisse ausgeschlossen« würden, vgl. § 25a Abs. 2 HSOG a. F.

hier sofort vieles bekannt vorkommt: Auch Erkenntnisse können »neu« sein, was allerdings vom vorhandenen Datenbestand abhängt (Rn. 35). Die Verarbeitung von Daten »verschaffe der Polizei neue Erkenntnisse und Zusammenhänge« (Rn. 39). Erkenntnisse würden »abgeschöpft« (Rn. 67), was die Vorstellung enthält, die Erkenntnisse seien bereits in »den zur Verfügung stehenden Daten« vorhanden und müssten nur eingesammelt oder aufgelesen werden. Alltäglich jedenfalls ist die »Zusammenstellung und Bewertung von aus unterschiedlichen Quellen erlangten Informationen«, woraus die »polizeiliche Erkenntnisgewinnung [...] Ergebnis« sei (Rn. 68). Gemeint ist zudem ein »Modell abgestufter Erkenntnisverdichtung« als Basis für »Ermittlungstätigkeit« (Rn. 69). Dies mag auf eine graduelle Unterscheidung hinweisen, etwa auf die Vorstellung gesicherten Wissens gegenüber sich erst verdichtenden, noch indiziellen, vielleicht fragmentarischen Erkenntnissen, die vielleicht noch keine gerichtsfesten Beweise darstellen, aber in der Polizeiarbeit dennoch hinreichend konkretisiert sein mögen, um behördliches Handeln zu rechtfertigen – eine derartige, systematische Unterscheidung ist im Urteil aber m.E. nicht erkennbar, sondern eine Ersetzungsprobe legt nahe, dass auf den Begriff des Wissens zugunsten des Erkenntnisbegriffs verzichtet werden könnte.

Hinzu kommt jedenfalls noch das Problem »praktischer Erkenntnisgrenzen«, die durch die »Befugnis zur automatisierten Datenanalyse oder -auswertung« überwunden werden solle, um »verfassungsrechtlich legitim« auf die »Effektuierung der Gefahrenbekämpfung« zu zielen (Rn. 70). Die Folge ist nicht nur eine »entscheidend[e]« Änderung der »Arbeitsweise und Erkenntnismöglichkeiten der Polizei«, sondern auch eine »bedeutend[e]« Erhöhung des »Gewicht[s] der individuellen Beeinträchtigung« (Rn. 70). Kurz: Erkenntnisse können »weitreichende[r]«, »breiter[]« und »tiefer[]« sein (Rn. 90), sind also tatsächlich eher graduell einzuschätzen als der härtere Wissensbegriff, aber werden ebenso wie dieser im Potenzial verhandelt: Es sind Erkenntnisse, die »erlangt werden können« (Rn. 90). Ob das Verfassungsgericht eine solche systematische Unterscheidung von Wissen und Erkenntnissen im Sinn hatte, muss offenbleiben. Deutlich wird, dass anders als beispielsweise im Urteil zum Antiterrordateigesetz vom 10. November 2020 das »neue Wissen« hier zu eigentlichen Redeweise geworden ist, die als Resultat einer automatisierten Datenanalyse oder -auswertung im Sinne des Data-Minings erscheint. Mit der Betonung der Rolle von Erkenntnissen hingegen organisiert das Urteil einen Bezug zum Polizeirecht und zu polizeilichen Praxis. Unterbelichtet bleiben aber noch die spezifischen Effekte des Data-Minings oder ähnlicher avancierter Methoden der Datenanalyse oder -auswertung: Die bisher erarbeitete Charakterisierung von »neuem Wissen« und »neuen Erkenntnissen« als subjektive neue Information aus bestehenden Daten lässt sich auch mit klassischen informationstechnischen Mitteln fassen. Zu denken wäre etwa an klassi-

sche Suchfunktionen, die ebenfalls dabei helfen, sich große Datenmengen mittels geschickter, aber manueller Stichwortsuche zu erschließen.

#### 4. Maßnahmen der Datenanalyse oder -auswertung

Soweit ließ sich wenig spezifisches für die in § 25a HSOG und § 49 HmbPolDVG geregelten Maßnahmen feststellen: Die Rekonstruktion der Begriffsverwendung von »Daten«, »Information«, »Wissen« und »Erkenntnis« zeigte zwar, wie eine gewisse Mehrdeutigkeit des Informationsbegriffs zwischen den technisch und rechtlich charakterisierten Daten einerseits und den polizeilich relevanten Erkenntnissen andererseits vermittelt, indem der Informationsbegriff von der objektiven Seite von Informationen an sich, die nicht »neu« sein können, auf die subjektive Seite, auf der Informationen »für uns« neu, da überraschend oder erstmals zugänglich sein können, wechselt. Allerdings zielen die angegriffenen Regelungen und entsprechend das Urteil darüber hinaus auf eine neue Art der polizeilichen Erkenntnisgewinnung, denn:

»Die Maßnahme erschließt die in den Daten enthaltenen Informationen damit intensiver als zuvor. Sie bringt nicht nur in den Daten angelegte, aber zunächst mangels Verknüpfung verborgene Erkenntnisse über Personen hervor, sondern kann sich bei entsprechendem Einsatz einem »Profiling« [...] annähern. Denn es können sich softwaregestützt neue Möglichkeiten einer Vervollständigung des Bildes von einer Person ergeben, wenn Daten und algorithmisch errechnete Annahmen über Beziehungen und Zusammenhänge aus dem Umfeld der Betroffenen einbezogen werden. Insoweit kann auch die Kombination personenbezogener und nicht personenbezogener Daten und gegebenenfalls die algorithmentypische Berücksichtigung bloßer Korrelationen neue, sonst nicht sicht- oder ermittelbare persönlichkeitsrelevante Aufschlüsse geben. Ein herkömmliches Verfahren, die nach dem Modell abgestufter Erkenntnisverdichtung erfolgende Ermittlungstätigkeit, wird hierdurch mit einer viel größeren Durchschlagskraft versehen [...]« (Rn. 69)

Wir stoßen also abermals auf graduierende Überlegungen: »intensiver«, »annähern« und eine »viel größere Durchschlagskraft«. In einem letzten Schritt soll daher untersucht werden, wie das Urteil auf die eingesetzten informationstechnischen Mittel reflektiert. Es fällt auf: Die Entscheidung hangelt sich an zwei grundlegenden Modellen der technischen Informationsverarbeitung entlang, die sich oft eher implizit als explizit auch in anderen Entscheidungen und Regelungen zum Umgang mit Daten finden lassen: einem Datenlebenszyklus und dem EVA-Prinzip, also dem grundsätzlichen Modell informationstechnischer Mittel bestehend aus Eingabe, Verarbeitung und Ausgabe, wobei es in der Literatur unterschiedlich gehandhabt wird, ob die Speicherung Teil der Verarbeitung ist oder – wie in der vorliegenden Entscheidung – als zusätzliches Element hinzukommt.

In einem einfachen Modell des Datenlebenszyklus ist dieser in fünf Phasen unterteilt: Erhebung, Speicherung, Nutzung (durch Verarbeitung), Weitergabe und Löschung. Das Gericht arbeitet hier entsprechend der Logik des Datenschutzes und diskutiert insbesondere Herkunft und Zweckbestimmung von Daten. Über Fragen des Datenschutzes im engeren Sinne geht das Gericht aber dort hinaus, wo es sich ausführlich mit der Verarbeitung von Daten beschäftigt. Dies kommt zwar etwa auch in der DSGVO vor, insoweit diese von automatisierten Verfahren der Verarbeitung spricht, wozu neben dem Erheben und Erfassen auch das Organisieren, Ordnen, Anpassen, Verändern, Auslesen, Abgleichen oder Verknüpfen gehört, aber ohne dabei auf die konkreten informationstechnischen Methoden einzugehen. Infrage steht nun aber in einem engeren Sinne der Mittelcharakter, womit das Gericht augenscheinlich einem Trend folgt, neben den Daten wieder auch verstärkt informationstechnische Mittel selbst zum Gegenstand rechtlicher Regulation zu machen – gegenwärtig am deutlichsten wohl im AI Act der EU zu beobachten.

Auch wenn das Gericht darauf abstellt, dass das Gewicht eines Eingriffs nach den rechtlich geschaffenen Eingriffsmöglichkeiten zu beurteilen ist und nicht etwa nach den gegenwärtigen technischen Möglichkeiten (Rn. 149), sind die Erwägungen zu bereits bestehenden Möglichkeiten des informationstechnischen Mitteleinsatzes im Urteil aufschlussreich: So ist allein die Menge der eingesetzten Daten vermutlich kein geeignetes Kriterium (vgl. Rn. 142), um das Eingriffsgewicht zu bestimmen bzw. zu senken,<sup>17</sup> sondern neben den umfangreichen Erwägungen zur zweckändernden Datennutzung oder zur Beschränkung der Nutzung von »neuen Informationen« durch spezifische Voraussetzungen (Rn. 99), die ich an dieser Stelle übergehe, thematisiert das Gericht die informationstechnischen Mittel selbst, wobei es überraschenderweise zwischen »lernenden« und »deterministischen« Systemen unterscheidet: Unter deterministischen Systemen versteht man in der Informationstechnik Systeme, die bei gleicher Eingabe stets die gleiche Ausgabe liefern. Dem stehen nicht-deterministische oder probabilistische Systeme gegenüber. Die aufteilende Unterscheidung in »lernend« und »deterministisch« ist daher schief. Zwar ist richtig, dass in avancierten KI-Systemen auch Zufallsquellen eingesetzt werden, um in heuristischen Verfahren technische Optimierungen zu erreichen, jedoch sind auch KI-Systeme von diesen Zufallsquellen abgesehen deterministische Systeme und »Lernfähigkeit« lässt sich auch ohne sie erreichen. Hinzu kommt: Bei vielen praktischen

---

<sup>17</sup> In Rn. 142 nennt das Gericht eine überraschende Quantifizierung: »[...] eine Lieferung [enthalte] ungefähr 100.000 Daten.« Ohne Angabe darüber, was ein Datum, also ein einzelner Datenpunkt, ist, ist diese Angabe uneindeutig. Möglicherweise ist in dem Kontext mit Datum ein komplexer Eintrag in einer Datenbank gemeint. Technisch könnte dies aber genauso gut ein einzelnes Zeichen bedeuten.

KI-Systemen ist zwischen dem Modelltraining und der Inferenz klar zu trennen. Beim Modelltraining wird aus einem Trainingsdatensatz ein Modell errechnet, welches als dann feste Parametrisierung für die Inferenzalgorithmen dient, die kurz gesagt ›das Gelernte‹ auf konkrete Fälle anwenden. Insofern mit ›lernenden Systemen‹ also gemeint ist, dass sich diese KI-Systeme während ihres Einsatzes anpassen und verändern, ist damit nur ein bestimmter Typus nicht notwendigerweise nicht-deterministischer KI-Systeme gemeint. Das BVerfG bedient sich hier einer technisch fragwürdigen Abgrenzung und bemerkt schließlich:

»Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein[.]« (Rn. 100).

Es scheint, dass das Urteil hier zwei Aspekte miteinander vermischt: die etwaige Lernfähigkeit bestimmter KI-Systeme auch im Einsatz und die oft als ›Blackbox‹ charakterisierte, fehlende Nachvollzieh- oder Erklärbarkeit der Ausgaben hinreichend komplexer IT-Systeme – nicht nur von KI-Systemen im Besonderen. Jedenfalls ist dies auch die Stoßrichtung des EuGH-Urteils vom 21. Juni 2021, das das Gericht in Rn. 100 zitiert und das das Problem präziser fasst:

»Darüber hinaus brächte der Rückgriff auf solche Technologien die Gefahr mit sich, dass der nach den Bestimmungen der PNR-Richtlinie erforderlichen individuellen Überprüfung der Treffer und der Rechtmäßigkeitsprüfung die praktische Wirksamkeit genommen wird. Wie der Generalanwalt in Nr. 228 seiner Schlussanträge im Wesentlichen ausgeführt hat, kann es sich nämlich angesichts der für die Funktionsweise von Technologien der künstlichen Intelligenz kennzeichnenden mangelnden Nachvollziehbarkeit als unmöglich erweisen, den Grund zu erkennen, aus dem ein bestimmtes Programm einen Treffer erzielt hat. Unter diesen Umständen könnte die Nutzung solcher Technologien den Betroffenen auch ihr in Art. 47 der Charta verankertes Recht auf einen wirksamen gerichtlichen Rechtsbehelf nehmen, das nach dem 28. Erwägungsgrund der PNR-Richtlinie auf hohem Schutzniveau gewährleistet werden soll, damit insbesondere gerügt werden kann, dass die erzielten Ergebnisse nicht frei von Diskriminierung seien.«<sup>18</sup>

Dass auch »deterministische Systeme« nicht notwendigerweise nachvollziehbar sind, bemerkt das Gericht so dann allerdings selbst: »Aber auch die Auswertungsvorgänge deterministischer Systeme, deren Analysefunktion sich also nicht eigenständig verändern kann, sondern in der Software unveränderlich vorprogrammiert ist, können komplex und für die Anwendenden und Betroffenen schwer nachvollziehbar sein.« (Rn. 101).

---

18 EuGH, Urt. v. 21.06.2021, C-817/19, *Ligue des droits humains gegen Conseil des ministres*, ECLI:EU:C:2022:491, Rn. 195.

Das Gericht möchte die Bewertung der Eingriffsintensität weder allein zweckbezogen von dem erwartbaren Wissen (vgl. Rn. 77) noch allein mittelbezogen vom Einsatz von KI-Technologien abhängig machen – zumal hierfür weder eine allgemein akzeptierte Legaldefinition vorliegt noch es überhaupt klar ist, in welchem Umfang die in Frage stehende Palantir-Software Gotham überhaupt KI-Technologien einsetzt.<sup>19</sup> Stattdessen stellt es zum einen auf unterschiedlich intensive Typen der Datenverarbeitung ab, an deren einem Ende »sehr schlichte[n] Formen des Abgleichs einer überschaubaren Zahl von Daten näher eingegrenzter Herkunft« (Rn. 72) stehen,<sup>20</sup> über gewissermaßen auf einem Kontinuum der Eingriffsintensität weitergehende »Möglichkeiten der automatisierten Weiterverarbeitung von Daten« (Rn. 72) bis hin zu komplexen Analysewerkzeugen, etwa der Künstlichen Intelligenz (Rn. 100), die selbst Analyseentscheidungen treffen und zuvor freigelegte Erkenntnisse selbst wieder zur Eingabe für weitere, mehrstufige Analyseverfahren haben (Rn. 93). Kurz: nicht alle Verarbeitungsmöglichkeiten von Daten sind gleich und abgestellt wird offenbar insbesondere auf die Komplexität der Auswertung, d.h. sowohl der Verarbeitung wie auch des erwartbaren Ergebnisses. Je einfacher nämlich die Verknüpfungen und Verfahren sind, desto geringer sei auch der Eingriff in die informationelle Selbstbestimmung. Problematisch bleibt aus informationstechnischer Sicht die Bewertung der Komplexität von Verfahren und erwartbarem Ergebnis. Der algorithmische Informationsbegriff nach Kolmogorov gibt hier zwar in der Theorie Hinweise, ist aber praktisch nicht berechenbar.<sup>21</sup> Zudem betrifft das Problem der Komplexität die möglichen Freiheitsgrade einer Auswertung: So ist zu unterscheiden, ob vorgegebene Auswertungsschemata nur in engen vordefinierten Grenzen parametrisiert und damit auch im Vorhinein einer Kontrolle unterworfen werden können oder ob die Analysesoftware den Charakter einer Programmierplattform hat, auf der komplexe Analysefunktionen

<sup>19</sup> Die demokratische Kontrolle einer Software wie Gotham durch Journalismus und Zivilgesellschaft scheitert regelmäßig daran, dass sie nicht öffentlich verfügbar ist und etwa mit synthetischen Daten durch unabhängige Expert:innen ausprobiert und diskutiert werden kann.

<sup>20</sup> Am unteren Ende des Spektrums sieht das Gericht Methoden eines »einfachen Datenabgleich[s]«, worunter es einen »suchende[n] Vergleich von Daten zur Feststellung von Übereinstimmung«, also eine Stichwortsuche versteht (Rn. 91).

<sup>21</sup> Art. 51 Abs. 2 AI Act definiert auf EU-Ebene hingegen eine klare Schwelle von 10 Quadrillionen FLOPs, also der Zahl der für die Erstellung eines KI-Modells aufgewendeten Gleitkommaoperationen. Ist eine solche Schwelle erreicht, dann wird für ein KI-Modell mit allgemeinem Verwendungszweck angenommen, dass es über Fähigkeiten mit hohem Wirkungsgrad verfügt, so dass es die Einstufung »mit systemischem Risiko« erhält. Eine solche Schwelle funktioniert nur unter zusätzlichen ökonomischen Annahmen, etwa zu unternehmerischen Zielen wie Kostensenkung und Effizienzsteigerung. Inwieweit sich eine quantifizierbare Schwelle für polizeiliche Data-Mining-Praktiken finden ließen, kann hier nicht beantwortet werden.

frei miteinander arrangiert und verknüpft werden können. In diesem Fall sind die Möglichkeiten der Datenanalyse oder -auswertung bereits aus theoretischen Gründen vorab nicht zu beschränken. Auch juristisch scheint die Sache vertrackt: Für den Fall der Daten lassen sich Abwägungen auf Ebene von »Art, Umfang und denkbare[r] Verwendung der Daten sowie [der] Gefahr ihres Missbrauchs«, der »Zahl der Betroffenen« und der »Intensität der individuellen Beeinträchtigung im Übrigen« (Rn. 76) ausmachen. Schwierig bleibt die Frage der Methode der Datenanalyse:

»Daneben beeinflusst die zugelassene Methode der Datenanalyse oder -auswertung die Eingriffsintensität. Besonderes Eingriffsgewicht kann der Einsatz komplexer Formen des Datenabgleichs haben. Wenn die Polizei aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen kann, daraus neue Zusammenhänge erschließen, aus mehrstufigen Analysen neue Verdachtsmomente erzeugen und hier weitere Analyseschritte oder operative Maßnahmen anschließen kann, [...]. Bei komplexen Formen des Datenabgleichs besteht zudem mit Blick auf individuellen Rechtsschutz und aufsichtliche Kontrolle und die dafür unerlässliche Möglichkeit, Fehler zu erkennen und zu korrigieren, die Schwierigkeit der Nachvollziehbarkeit der eingesetzten Algorithmen (vgl. BVerfGE 154, 152 <259f Rn. 192>). Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können.« (Rn. 90).<sup>22</sup>

Die Komplexität steige, so das Urteil, insbesondere durch zwei Faktoren: Erstens kann auch der suchende Vergleich »durch eine höhere Zahl an Abgleichschritten und Verknüpfungen« (Rn. 92) ein höheres Eingriffsgewicht entfalten, insoweit »die Zahl der vorprogrammierten Abgleichschritte, die sich ohne weiteren, im Einzelfall menschlich veranlassten Anstoß vollziehen können, [nicht] von vornherein begrenzt« (Rn. 92) ist und die »Verknüpfungsmöglichkeiten« hierdurch reduziert sind. Offen bleibt freilich, wie eine solche Zahl definiert werden könnte, zumal sie bereits von der Komplexität primitiver Verarbeitungsoperationen auf einer Plattform abhängt. Anders formuliert: Auch eine große Zahl an für sich genommen einfachen Abgleichschritten kann eine geringere Eingriffstiefe darstellen als eine kleinere Zahl, komplexer, nicht notwendig KI-basierter Verar-

---

22 Das Gericht verweist hier auf sein BND-Urteil (BVerfG, Urt. v. 19.05.2020 – 1 BvR 2835/17, BVerfGE 154, 152–312), in dem es unter der genannten Rn. 192 festhält, dass »gegebenenfalls auch der Einsatz von Algorithmen, insbesondere die Sicherstellung ihrer grundsätzlichen Nachvollziehbarkeit in Blick auf eine unabhängige Kontrolle« zu regeln sei. Inwieweit dies bei einer Software wie Gotham von Palantir, deren genaue Verfahren als Geschäftsgeheimnisse geschützt werden, überhaupt möglich sein soll, ist dem Verfasser unklar. Sollte das Gericht mit der Forderung nach unabhängiger Kontrolle algorithmischer Verfahren in etwaigen weiteren Verfahren ernst machen, ließe sich der Einsatz von Gotham hiernach kaum rechtfertigen.

beitungsschritte. Umgekehrt kann die freie Verknüpfbarkeit für sich genommen einfacher Verarbeitungsschritte den Charakter einer völlig flexiblen, *Turing-mächtigen* Programmierplattform entfalten und damit eine höhere Eingriffstiefe zur Folge haben als eine Menge komplexer Verarbeitungsschritte, die sich nicht flexibel miteinander verknüpfen lassen. Eine Bewertung in Abhängigkeit von der Zahl an Verarbeitungsschritten setzt daher stets eine Bestimmung dessen voraus, was ein einzelner Verarbeitungsschritt umfassen kann und wie diese überhaupt miteinander verknüpft werden können. Das Gericht hat dieses Problem offenbar wenigstens zum Teil gesehen und ergänzt daher zweitens Überlegungen zur Offenheit der Methode, kommt hier aber wieder auf Aspekte des unüberwachten Lernens, also des automatischen Findens von (statistischen) Auffälligkeiten zurück:

»Das Eingriffsgewicht ist dagegen umso höher, je offener die Methode des Suchvorgangs gestaltet ist und je weniger die automatisierte Datenanalyse oder -auswertung durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster gesteuert wird. Denn je offener ein automatisierter Suchvorgang zur vorbeugenden Bekämpfung von Straftaten im Vorfeld konkreter Gefahren ausgestaltet ist, je weniger Sachverhaltsbezug die Suche also hat, umso eher werden durch die Suche überhaupt erst Anhaltspunkte für eine Gefahr generiert. [...] Das Eingriffsgewicht erhöht sich insbesondere, wenn die Datenanalyse oder -auswertung nicht auf einem Suchbegriff, jedenfalls nicht auf einem auf den bislang erkennbaren Sachverhalt bezogenen Suchbegriff gründet, sondern darauf zielt, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, die darüber hinaus (automatisiert) in weiteren Abgleichsschritten mit bestimmten Datenbeständen verknüpft werden und so zu weiteren Informationen führen können, nach denen zu suchen die Polizei zuvor keinen Anlass hatte.« (Rn. 93).

Das durch die Verdoppelung des Informationsbegriffs eröffnete Feld, die Methoden der Verarbeitung, also die Methoden der Gewinnung »neuer Erkenntnisse«, in den Blick zu nehmen erweist sich damit als zweischneidig: Einerseits wird die Diskussion überhaupt erst möglich, ja nötig, andererseits wird deutlich, dass es hierzu noch an einem geeigneten Vokabular fehlt: Es fehlt an – auch rechtlich belastbarer – Sprache, um die Komplexität von Verfahren ohne ständigen Rückgriff auf die beiden Seiten des Informationsbegriffs, also möglicher Daten und möglicher Erkenntnisse, zu charakterisieren. Es ist zwar völlig richtig, dass Offenheit und Zahl der Verarbeitungsschritte – sowie in Ergänzung zum Urteil: die Flexibilität ihrer Verknüpfbarkeit – die Komplexität eines informationstechnischen Verfahrens zu charakterisieren erlauben, aber begründete, »anspruchsvoll ausgestaltete Eingriffsschwellen« (Rn. 95) hierzu lassen sich jenseits des Ausschlusses bestimmter Datenverarbeitungsmethoden weder rechtlich noch politisch bestimmen.

## 5. Fazit

Trotz oder gerade dank changierender Sprache öffnet das Gericht die Möglichkeit, über die Eingriffsintensität automatisierter Datenanalyse oder -auswertung weitgehend innerhalb des etablierten datenschutzrechtlichen und polizeirechtlichen Vokabulars zu sprechen: Durch die semantische Verdoppelung von Informationen zwischen objektiver ›bestehender‹ Informationen ›an sich‹ auf Seite der Daten und der subjektiven ›neuen‹ Information ›für uns‹ wird nah an der Data-Mining-Metapher das Herauslocken, Gewinnen, Freilegen von ›neuen‹ Informationen und damit ›neuen‹ Erkenntnissen formulierbar. Zwischen beiden befinden sich informationstechnische Mittel, die regelmäßig kaum nachzuvollziehen sind, mächtige Such-, Verknüpfungs- und Auswertungsfunktionen zur Verfügung stellen und dies auch ohne Einsatz künstlicher Intelligenz im engeren Sinne. Auch wenn sich das Gericht der aktuellen Sorge um die neuen KI-Technologien nicht ganz entziehen kann, gewinnt es einen im Weiteren noch zu präzisierenden Blick auf die Rolle informationstechnischer Mittel selbst. Zugleich legt es den Finger in die Wunde: Auch ›vor KI‹ war es kaum möglich zu überblicken, welche ›neuen Informationen‹ und ›Erkenntnisse‹ sich aus bestehenden Daten gewinnen ließen. Dass es überhaupt denkmöglich ist, dass aus bestehenden Daten ›neue‹ Informationen gewonnen werden können, verweist auf den ständigen Überschuss unserer Datenspuren, die durch die technologische Entwicklung beständig mit neuen Mitteln ausgewertet werden können, um ›Geheimnisse‹ aufzudecken, die wir teils nicht über uns preisgeben wollen, teils nicht einmal selbst über uns wissen.<sup>23</sup>

---

<sup>23</sup> Vgl. den Beitrag von Brenneis/Denker/Gehring in diesem Band.



# Risikoabwägungen und Abwägungsrisiken – Zur Einordnung automatisierter Datenanalysen durch das Bundesverfassungsgericht anhand von Risikokalkulationen und damit einhergehenden Risiken selektiver Bewertung

*Andreas Brenneis*

## 1. Einleitung: Risikoabwägungen und Abwägungsrisiken

Der Beitrag erörtert die Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 als »automatisierte Datenanalyse« bezeichnete Methode.<sup>1</sup> Der Fokus liegt auf der Konzeption von »Risiken«, die das Gericht bei seiner Bewertung der automatisierten Datenverarbeitung im Rahmen der Polizeiarbeit explizit wie implizit berücksichtigt. Dabei geht es zum einen darum, welche Risikobetrachtungen in die Urteilsprechung eingeflossen sind und wie diese formuliert werden. Daneben soll aber auch in den Blick genommen werden, welche Risiken im Urteil keine – oder jedenfalls keine explizite – Rolle spielen.

Recht klar ist, dass das ›Palantir-Urteil‹ versucht, zwei Risiken zu bestimmen, abzuwägen und auszutarieren: Das Risiko einer übermäßigen Beschränkung der Arbeit von Sicherheitsbehörden und damit ggf. einhergehend sogar öffentliche Sicherheitsrisiken zum einen, und Risiken bezüglich nicht hinnehmbarer Verletzungen des Rechts auf informationelle Selbstbestimmung zum anderen. Die kleinteiligen, auf zahlreiche Präzedenzen aufsetzenden Ausführungen des Gerichts belegen: Der Abwägungsvorgang ist geprägt durch grundrechtsdogmatische Routinen.

Die nachfolgenden Überlegungen zielen darauf ab, dass eine echte Risikoabwägung auf diese Weise womöglich gerade nicht erfolgt. Meine Vermutung lautet, dass durch die Komplexität der Risikosemantik, die das Gericht in Anschlag bringt, zentrale Aspekte der automatisierten Datenanalyse unter einer Menge an

---

<sup>1</sup> BVerfG, Urt. v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 – Automatisierte Datenanalyse. Nachfolgend wird aus dem Urteil (unter Nachweis der Randnummern) im Fließtext zitiert.

Stellschrauben und Parametern verdeckt werden, die für eine Bewertung einer im Wesentlichen *technischen* Neuerung selbst aber von zentraler Bedeutung gewesen wären. Das Gericht vermengt zudem Risiken einer Normverletzung mit Risiken auf der Ebene von (kausalen) Folgen des Einsatzes entsprechender Softwaresysteme selbst. Zugleich wird in der Abwägungslogik das Verfahren der automatisierten Datenanalyse verkürzend primär als technisches Mittel und nicht hinreichend als soziotechnisches System begriffen. Die »klassische« Polizeirecherche wird der Recherche unter Einbeziehung von Systemen wie hessenDATA letztlich disjunkt gegenübergestellt. Variable Nutzungsmöglichkeiten der Technik – etwa durch eigens qualifiziertes Polizeipersonal – werden durch den Fokus auf wiederum technische Parameter zur Senkung des Eingriffsgewichts der Maßnahme selbst verschlossen. Faktoren wie eine stärkere Berücksichtigung der menschlichen Aufsicht könnten aber beispielsweise zu einer situativ passenderen Ausgestaltung der automatisierten Datenanalyse führen. Der geschulte Umgang mit dem infrage stehenden System könnte aber sowohl das Grundrecht auf informationelle Selbstbestimmung schützen wie auch eine effektive und effiziente Polizeiarbeit erlauben.

Die These dieses Beitrags lautet folglich, dass mit der im Urteil angelegten Abwägung von Risiken über die Parameter zur Steigerung oder Senkung des Eingriffsgewichts einer automatisierten Datenverarbeitung selbst Risiken einhergehen. Diese sehe ich in folgenden Punkten:

- Eine grundrechtsdogmatische Abwägung, die die Gefahr einer (aus einer Technik resultierenden) Normverletzung als Risiko modelliert, wird analytisch wie auch in ihren Botschaften unklar, wenn sie zugleich im engeren Sinne technische Risiken diskutiert und in die Abwägung einfließen lässt.
- Durch den Fokus auf die technische Seite der automatisierten Datenanalyse kommt aus dem Blick, dass jedes technische System notwendig in funktionale Arrangements innerhalb von Institutionen eingebunden ist. Auch die automatisierte Datenverarbeitung ist ein soziotechnisches System. Durch die Verkürzung auf ein technisches System werden Ansatzpunkte für eine mögliche Regulierung und Einhegung der Grundrechtseingriffe ausgeblendet.
- Durch die restriktive Regulierung der automatisierten Datenanalyse, die aus den komplexen Risiko-Abwägungen primär auf Seiten der Technik verortete Optionen einer Risikominimierung ableitet, werden der Polizei Möglichkeiten verwehrt, die diese sinnvoll für ihre Arbeit einsetzen könnte.

Der Begriff des Risikos wird in diesem Beitrag genutzt, um juristische und technikphilosophische Perspektiven aufeinander zu beziehen. In technikphilosophischer Hinsicht wird »Risiko« üblicherweise als ein Zustand oder Ereignis definiert, bei dem es möglich ist, dass unerwünschte und schädliche Konse-

quenzen eintreten, ohne dass dies jedoch sicher vorhergesagt werden kann.<sup>2</sup> Risiken zeichnen sich dabei durch zwei zentrale Merkmale aus: die Wahrscheinlichkeit ihres Eintretens und das Ausmaß potenzieller Schäden, beides pflegen Technikfolgenabschätzungen detailliert zu beschreiben und zu quantifizieren.<sup>3</sup> Technische Systeme bergen dabei nicht nur unmittelbar erkennbare Risiken, sondern auch epistemische Unsicherheiten und Nebenwirkungen, die oftmals erst im Verlauf ihrer Nutzung deutlich werden.

In der juristischen Perspektive, insbesondere in der Abwägungslogik des Rechts, werden Risiken häufig als kollidierende Interessen verstanden, bei denen Nutzen und Schaden unterschiedlicher Handlungsoptionen systematisch gegeneinander gewichtet werden.<sup>4</sup> Juristische Abwägungen beruhen hierbei auf einer rationalisierten Entscheidungsstruktur, die im Sinne der Verhältnismäßigkeitsprüfung versucht, Risiken möglichst transparent und nachvollziehbar gegeneinander auszubalancieren. Auch vom Risiko einer Normverletzung kann in diesem Zusammenhang die Rede sein. Eine technikphilosophische Kritik an dieser juristischen Logik hebt hervor, dass solche Risikoabwägungen tendenziell technische Unsicherheiten und gesellschaftliche Implikationen unterschätzen oder gar übersehen, weil sie komplexe soziotechnische Zusammenhänge auf scheinbar objektiv messbare Größen reduzieren.<sup>5</sup>

Dem Urteil des Bundesverfassungsgerichts liegt eine allenfalls teilweise explizit gemachte Risikokalkulation zugrunde. Ebenso werden Risiken unter Inkaufnahme eines Ebenenwechsels miteinander verrechnet: Mittels des eingeschätzten Ausmaßes potentieller Verletzungen des Grundrechts auf informationelle Selbstbestimmung von potentiell betroffenen Rechtssubjekten wird das Risiko automatisierter Datenverarbeitung kalkuliert. Der Faktor der Eintrittswahrscheinlichkeit findet dabei ebenso wenig hinreichende Berücksichtigung wie die Risiken, die mit einem qualitativ oder quantitativ eingeschränkten Einsatz von Formen automatisierter Datenanalyse einhergehen.

## 2. Der grundlegende Zielkonflikt: Effektive Polizeiarbeit vs. informationelle Selbstbestimmung

Der Rahmen, innerhalb dessen das Gericht seine Gründe und Abwägungen darlegt, ist durch zwei Werte gekennzeichnet, die zueinander im Widerspruch ste-

---

2 Beck 1986.

3 Hubig 2007; Grunwald 2019.

4 Rückert 2011.

5 Jasanoff 1999.

hen und Abwägung fordern. Auf der einen Seite haben Sicherheitsbehörden das Anliegen, von technischen Möglichkeiten der Digitalisierung Gebrauch zu machen – die damit einhergehenden Verbesserungen in der Aufgabenerfüllung, also in den Prozessen und der Zielerreichung der Polizeiarbeit, sind gesellschaftlich und verfassungsrechtlich gewünscht. Dem stehen allerdings Einschränkungen des Rechts auf informationelle Selbstbestimmung von Bürgerinnen und Bürgern gegenüber, deren Daten im Zuge polizeilicher Recherchen verarbeitet werden. Nachfolgend werden die beiden Werte nicht rechtswissenschaftlich, sondern mit Blick auf einige praktische Implikationen knapp skizziert.<sup>6</sup>

## 2.1 Legitimer Zweck – erfolgreiches polizeiliches Handeln

Ausgangspunkt des Urteils zu automatisierter Datenanalyse sind Verfassungsbeschwerden gegen Ermächtigungen der beiden Bundesländer Hamburg und Hessen, mit denen die Polizeien jeweils die Befugnis erhalten haben, automatisierte Verfahren der Datenauswertung einzusetzen. Das Urteil referiert die Gründe für die Ermächtigungen in Hamburg und Hessen wie folgt: Die Regelungen der Länder »schaffen vor dem Hintergrund erweiterter technischer Möglichkeiten, Informationstechnologie auch in der polizeilichen Arbeit zu nutzen, eine spezielle Rechtsgrundlage dafür, bisher unverbundene, automatisierte Dateien und Datenquellen in Analyseplattformen zu vernetzen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen, um die polizeiliche Aufgabenerfüllung auf diese Weise zu erleichtern und zu verbessern« (Rn. 2). Dadurch sollen »insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, [...] eingehende [...] Erkenntnisse bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden« können (Rn. 3).

Etwas detaillierter verweist die Begründung des hessischen Gesetzentwurfs zu § 25a HSOG darauf, »dass ohne den Rückgriff auf derartige automatisierte Anwendungen wegen eines unverbundenen Nebeneinanders zahlreicher automatisierter Verfahren, Daten und Informationssysteme mit unterschiedlichen Zweckbindungen, Nutzerkreisen, Datenarten und Betroffenenkreisen wesentliche Anhaltspunkte für Gefahren und bevorstehende Straftaten in der aktuellen ›IT-Struktur‹ der Polizei verborgen blieben [...]«. (Rn. 8). Demge-

---

<sup>6</sup> Für eine juristische Einordnung zentraler Entscheidungen des Bundesverfassungsgerichts im Bereich der inneren Sicherheit (Rasterfahndung, Online-Durchsuchung, Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung und Antiterrordatei) vgl. Bull 2025.

genüber könne ein automatisiertes Analysetool eine »umfassende Analyse der verfügbaren Daten« ermöglichen; die Polizei werde dadurch in die Lage versetzt »über die bisherigen Erkenntnismöglichkeiten hinaus Zusammenhänge sowie Handlungsmuster und damit auch künftiges strafbares oder gefährliches Verhalten von Personen erkennen und geeignete präventive Maßnahmen treffen« zu können (ebd.).

Seitens der Gesetzgeber sollen also die Polizeibehörden in die Lage versetzt werden, technisch auf der Höhe der Zeit zu arbeiten. Denn offenbar – Stichwort »aktuelle IT-Infrastruktur« – können Polizeidienststellen das Potential ihrer Kompetenzen derzeit aufgrund technischer Restriktionen nicht immer ausschöpfen. Die IT ist veraltet. Das betrifft zweierlei: erstens die Analyse der verfügbaren Daten. Man scheint eine Datenanalyse in der gleichen Weise vornehmen zu wollen, wie zuvor auch, nur dass durch die Unterstützung der Maschine der Durchsatz höher sein würde, wodurch mehr Daten oder – als ideale Grenze – alle relevanten Daten in der Analyse berücksichtigt werden können. Zweitens halten Beschwerdeführer und Gericht aber durch die Software auch eine Verarbeitung der Daten für möglich, welche »über die bisherigen Erkenntnismöglichkeiten hinaus« führt.

Das Gericht sieht auch in einer entsprechenden Steigerung der Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten einen legitimen Zweck. Es weist auf die Möglichkeit hin, Anhaltspunkte aus dem Datenbestand der Polizei zu gewinnen, die ohne eine automatisierte Datenanalyse unerkannt blieben und somit unter aktuellen Bedingungen nicht zur Verfügung stünden: »Die angegriffenen Regelungen dienen dem legitimen Zweck, vor dem Hintergrund informationstechnischer Entwicklung die Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten zu steigern, indem Anhaltspunkte für bevorstehende Straftaten gewonnen werden, die im Datenbestand der Polizei ansonsten unerkannt blieben.« (Rn. 52) Nicht ganz klar wird, ob hier der Gewinn weiterer Anhaltspunkte selbst noch Teil des Zwecks ist oder als ein Mittel gedacht wird, wie dieser Zweck erreicht werden könnte. Diese Frage ist relevant, weil einer der Hauptkritikpunkte an den mit den Ermächtigungen legitimierten Softwarelösungen gerade das Erzeugen neuen Wissens ist. Es ist also zu klären, wie sich die Gewinnung von sonst unerkannt bleibenden Anhaltspunkten zu der Generierung neuen Wissens verhält.

In der Urteilsbegründung folgt auf die Darlegung der grundsätzlichen Legitimität automatisierter Datenanalysen eine Rekapitulation der Argumentation der hessischen Landesregierung. Diese begründet die Notwendigkeit der fraglichen Analysen mit den veränderten Rahmenbedingungen der polizeilichen Ermittlungsarbeit, insbesondere mit der zunehmenden Heterogenität und Komplexität der anfallenden Daten. Demnach entstehen ständig neue Herausforde-

rungen dadurch, dass immer vielfältigere Prozesse, Interaktionen und Praktiken digitale Spuren hinterlassen, deren Auswertung die polizeilichen Ressourcen übersteigt.<sup>7</sup> Vor diesem Hintergrund rechtfertigt der hessische Gesetzgeber den Einsatz automatisierter Datenanalysen pragmatisch mit dem Ziel, trotz des stark gestiegenen Datenvolumens und der wachsenden Komplexität der Daten relevante Informationen zügig zu identifizieren und nutzbar zu machen. Diese pragmatische Begründung macht sich auch das Gericht zu eigen, wenn es eine Notwendigkeit für Ermächtigungen für die automatisierte Datenanalyse zugesteht, weil durch diese »für die Verhütung von Straftaten relevante Erkenntnisse erschlossen werden können, die auf andere, grundrechtsschonendere Weise nicht gleichermaßen zu gewinnen wären« (Rn. 53). Beide Charakterisierungen – das Gewinnen von sonst unerkannt bleibenden Anhaltspunkten bzw. das Erschließen von auf grundrechtsschonendere Weise nicht zu gewinnenden Erkenntnissen – changieren allerdings zwischen quantitativen und qualitativen Gesichtspunkten: Der Gewinn von Anhaltspunkten oder Erkenntnissen kann bedeuten, dass man mit der neuen Software einfach mehr erhält als ohne automatisierte Datenverarbeitung. Oder aber der Gewinn besteht darin, auch qualitativ neuartige Erkenntnisse zu erlangen.

Im Sinn einer reinen Effizienzsteigerung hat die zuständige Behörde für Justiz und Verbraucherschutz der Freien und Hansestadt Hamburg für die mit der Ermächtigung avisierte Softwarenutzung argumentiert: Der fragliche § 49 HmbPolDVG sei nur die »Ermächtigung für eine technische Hilfestellung [...] von allenfalls moderater Eingriffsqualität«, denn der »automatisierte Zugriff unterscheide sich nicht vom gezielten Blick eines Beamten in eine Akte oder ein Dateisystem im Sinne einer manuellen Auswertung« – es werde somit »lediglich ergänzend eine technische Alternative bereitgestellt« (Rn. 34). Im Einklang mit dieser Argumentationslinie liegt auch die Auffassung, dass tatsächlich qualitativ neue Erkenntnisse durch die Software nicht möglich seien, da die »Möglichkeiten einer Gewinnung neuer Erkenntnisse [...] durch den vorhandenen Datenbestand eingeschränkt seien« (Rn. 35). Die Datenverarbeitung erlaube gleichwohl dennoch, dass sich neue Verdachtsmomente ergeben könnten und in der Folge auch sich an diese anschließende operative Maßnahmen, was jedoch bei der Verarbeitung von in polizeilichen Dateisystemen gespeicherten Daten

---

7 »Die hessische Landesregierung hat in diesem Verfahren dargelegt, die Polizeibehörden seien infolge der insbesondere in den Bereichen terroristischer und extremistischer Gewalt sowie der organisierten und schweren Kriminalität zunehmenden Nutzung digitaler Medien und Kommunikationsmittel mit einem ständig anwachsenden und nach Qualität und Format zunehmend heterogenen Datenaufkommen konfrontiert. Die dazu in den polizeilichen Datenbeständen enthaltenen Informationen könnten gerade unter Zeitdruck kaum manuell gewonnen werden; eine automatisierte Datenanalyse sei daher von großer Bedeutung für ein erfolgreiches polizeiliches Handeln.« (Rn. 52).

»nichts Ungewöhnliches« (Rn. 35) sei. Es dürfte keine sonderlich gewagte Vermutung sein, zu sagen, dass genau das der Sinn einer Datenanalyse sein sollte – sei sie nun automatisiert oder händisch: In den Daten Indizien aufzufinden, die als Hinweise die Möglichkeit eines bestimmten Sachverhalts untermauern und dadurch Thesen belegen, erhärten, abschwächen oder widerlegen. Der Geschwindigkeitszuwachs macht auch einen qualitativen Unterschied, die Güte des Leistbaren steigt.

Zusammenfassend lässt sich zur Motivation für den Einsatz automatisierter Datenanalyse in der Polizeiarbeit festhalten: Das Gericht sieht es als legitim an, mithilfe von automatisierten Datenanalysen Anhaltspunkte zu erschließen und Erkenntnisse zu gewinnen. Aufgeworfen ist die Frage nach der Grenze zwischen der als legitim erachteten Gewinnung neuer Anhaltspunkte bzw. Erkenntnisse und dem Recht auf informationelle Selbstbestimmung, durch das die Datenanalyse zu begrenzen ist. Zu klären ist die Frage, inwiefern die Gewinnung neuer Anhaltspunkte (welche ja als legitimer Zweck anerkannt wird, vgl. Rn. 52) der Ebene der »zusammenführenden Verwendung vormals getrennter Daten« zuzuordnen ist oder der Ebene der »Erlangung besonders grundrechtsrelevanten neuen Wissens« (Rn. 50). Wie also hängt das Gewinnen von Anhaltspunkten zusammen mit dem Gewinnen von »in polizeilichen Datenbeständen enthaltenen Informationen« und der Möglichkeit, dass »relevante Erkenntnisse erschlossen werden« (Rn. 53)?

Das Problem der Qualitätsverbesserung (oder auch des Mehr an Effizienz), das mit der Automatisierung der Datenbankzugriffe einhergeht, kulminiert im für das Urteil zentralen Begriff des »neuen Wissens«, dessen Grundrechtsrelevanz auf das Recht auf informationelle Selbstbestimmung bezogen werden soll.

## 2.2 Hintergrund der informationellen Selbstbestimmung: das Volkszählungs-Urteil von 1983

Der argumentative Ausgangspunkt der Entscheidung zur automatisierten Datenanalyse ist das Recht auf informationelle Selbstbestimmung, da das Gericht alle anderen Punkte der Klageschrift abweist. Das Recht auf informationelle Selbstbestimmung geht auf das Volkszählungs-Urteil von 1983 zurück, dessen zentrales Argument für die Grundrechtsrelevanz von Datenerhebung und Datennutzung sogenannte »chilling effects« sind, also wahrscheinliche Verhaltensänderungen, weil Betroffene befürchten, abweichende Verhaltensweisen würden registriert und brächten früher oder später nachteilige Folgen mit sich. Es wird also die Gefahr gesehen, dass Personen eingeschüchtert werden und sich quasi in vorausseilendem Gehorsam zu Verhaltensanpassungen veranlasst sehen, auf

Selbstbestimmung unter Umständen letztlich sogar zu verzichten drohen. Im Urteil von 1983 wird dazu – unter Verwendung der Kategorie des Risikos – notiert:

»Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.«<sup>8</sup>

Man könnte resümieren: Das Urteil reagiert auf das empirisch vorhandene Risiko, dass Personen durch das Speichern von Daten für sich selbst Risiken sehen – was wiederum ein Risiko für das Gemeinwohl enthält. Zum Schutz der individuellen Persönlichkeitsentfaltung und davon abgeleitet auch des freiheitlich demokratischen Gemeinwesens sieht das Urteil von 1983 »unter den modernen Bedingungen der Datenverarbeitung« entsprechende Schutzrechte bezüglich der persönlichen Daten vor – gefasst eben als Recht auf informationelle Selbstbestimmung bzw. die persönliche Befugnis, selbst über eigene Daten zu bestimmen.

Aber auch schon im Volkszählungs-Urteil wird ausgeführt, diese Befugnis sei gegen ein »Allgemeininteresse« der Gemeinschaft abzuwägen und könne so mitunter eingeschränkt werden:

»Dieses Recht auf ›informationelle Selbstbestimmung‹ ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ›seine‹ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden [...]. Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.«<sup>9</sup>

Bemerkenswert ist hier eine doppelte Begründungsfigur, die auch für das Urteil zu automatisierter Datenanalyse wichtig ist. Das Gebot, die Spannung von Individuum und Gemeinschaft gegebenenfalls zugunsten der Gemeinschaftsgebundenheit aufzulösen ist, kann als die normative Dimension der Begründung aufgefasst werden, sie bildet einen substanziellen Teil des verfassungsrechtlichen

<sup>8</sup> BVerfGE 65, 1 (43).

<sup>9</sup> BVerfGE 65, 1 (43 f.).

Rahmens der Bundesrepublik Deutschland. Daneben hat die Einschränkungsbegründung aber auch eine epistemische Dimension, nämlich in Bezug auf den Status von Information. Information – und man darf wohl ergänzen: auch die der Information zugrundeliegende Sammlung bzw. Zusammenstellung an Daten – »stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann« – und das auch bei personenbezogener Information. Das Gericht erkennt also an, dass realer Informationen (und Daten) im sozialen Gewebe des menschlichen Miteinanders existieren, indem sie dort zirkulieren. Man könnte sagen, dass auch mit dieser Perspektive eine Grundsatzentscheidung getroffen ist: Wenn Information primär ein »Abbild sozialer Realität« ist, dann erhält auch jedes individuelle Datum seine Bedeutung erst vor dem Hintergrund einer sozialen Ontologie. Der logische Ausgangspunkt für die vom Bundesverfassungsgericht artikulierte Auffassung von Information ist kein Individualismus (und übrigens auch nicht »Privatheit«), sondern die soziale Realität. Innerhalb des hier anzutreffenden informationellen Gewebes wird dann den Individuen hinsichtlich ihrer Daten ein Schutzbereich eingeräumt – zunächst ohne weitere Definition. Klar ist allerdings, wogegen sich der Grundrechtsschutz richtet: Informationelle Selbstbestimmung dient dem »Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten« – so der erste Leitsatz zum Urteil.

Näherhin schützt die Verfassung Daten und Informationen »unter den modernen Bedingungen der Datenverarbeitung« bezüglich »Preisgabe und Verwendung«. Die Preisgabe und Verwendung von Daten werden hierbei von vornherein im Lichte technischer Möglichkeiten in Augenschein genommen.

### 2.3 Die Argumente der Beschwerdeführenden

In den Beschwerden gegen die Polizeigesetze von Hessen und Hamburg geschieht das auch: das Softwaresystem, das auf zuvor nur getrennt abfragbare Datenbanken durchgängigen Zugriff erlaubt, ändere die Polizeipraxis. Die Beschwerdeführenden leiten hieraus nicht eine neue Grundrechtsverletzung, sondern eine veränderte »Eingriffstiefe« einer an sich bereits zuvor gegebenen (allerdings unter den Bedingungen der »aktuellen IT« noch hinnehmbaren) Grundrechtsverletzung ab. Angriffspunkt der Beschwerden ist damit die (die bisherige polizeilich Datenbankpraxis legitimierende) höchstrichterliche Abwägung selbst bzw. eine überkommene Risikoeinschätzung, die angesichts der effizienteren digitalen Lösung nun nicht mehr akzeptabel ist: »Aufgrund der technischen Entwicklung ergäben sich neue, eingriffsintensivere Möglichkeiten der Herstellung von Verknüpfungen und der Erzeugung neuer Informationen«

(R. 19) – nicht zuletzt auch durch den möglichen Einsatz komplexer Algorithmen sowie lernfähiger Systeme. Zum einen geht es dabei um die Qualität der neuen Informationen, insofern die »hinsichtlich der eingesetzten Methode offene Ermächtigung zur verdeckten Datenverarbeitung [...] die Erstellung von Persönlichkeits- und Sozialprofilen« (ebd.) erlaube. Einen diese Qualität mitbedingenden quantitativen Aspekt führen die Beschwerdeführenden gesondert an – im Urteil explizit in der Kategorie des Risikos formuliert: »Weil von der Datenanalyse oder -auswertung in großer Zahl Menschen erfasst seien, die hierfür keinen Anlass gegeben hätten, könnten die Maßnahmen enorme Streubreite haben. Ein besonderes Risiko ergebe sich insoweit aus dem Zugriff auf Daten aus polizeilichen Vorgangsverwaltungsdatenbanken.« (ebd.) Weil sich automatisiert also mehr Daten analysieren lassen, ergeben sich besondere Formen der Eingriffsintensität, die wiederum besondere Rechtfertigungsanforderungen bedingen.

Diese Anforderungen fokussieren die Eingriffsschwelle automatisierter Datenanalyse als Maßstab zur Abwägung gegenüber dem Recht auf informationelle Selbstbestimmung. Andere Argumente der Beschwerdeführenden hat das Bundesverfassungsgericht als unzulässig zurückgewiesen.<sup>10</sup>

## 2.4 Technische Potentiale und normative Vermittlung

Das Urteil zu automatisierter Datenverarbeitung wägt zwei (oder eigentlich sogar drei) heterogene Normordnungen gegeneinander ab – auf der einen Seite Anforderungen der Sicherheitsbehörden an möglichst gute Arbeitsbedingungen, auf der anderen Seite mögliche Eingriffe in persönliche Grundrechte (und als drittes kommt so etwas wie der technische Status quo, demgemäß das »Aktuelle« und das »Neue« einander gegenüberstehen, in normativer Hinsicht ins Spiel). Vonseiten der Effizienz polizeilicher Arbeit stellt sich die Frage, ob die Polizei mit den eingesetzten Mitteln ihre bestehenden Ziele ausreichend gut erreicht oder ob Effizienzgewinne anzustreben und zu erzielen sind. Solange sich weder an den Zielen noch an den Mitteln grundsätzlich etwas ändert, bleibt dies ein rein technisches Problem. Nach Auffassung des Gerichts ist aber genau dies nicht der Fall: Die automatisierte Datenanalyse führt potenziell zu einer qualitativen Veränderung der Datenverarbeitung selbst. Diese qualitative Veränderung, die sich

---

<sup>10</sup> Angeführt wurde etwa noch als rechtsstaatliche Herausforderung, dass effektiver Rechtsschutz im Rahmen automatisierter Datenanalyse nur durch eine unabhängige Instanz zu gewährleisten sei (Rn. 22) und dass jedenfalls die Regelungen ohne ausreichende Verfahrenssicherungen hinsichtlich Transparenz, Rechtsschutz und Kontrolle seien (Rn. 21).

in der Möglichkeit der Gewinnung »neuen Wissens« zeigt, bildet den Kern der Argumentation im Urteil, in Abschnitt 3 komme ich darauf zu sprechen.

Zuvor gilt es hinsichtlich dieser potenziellen qualitativen Änderung wiederum verschiedene Ebenen zu unterscheiden: Zum einen lässt sich auf der Ebene des technisch Möglichen danach fragen, wie weit Softwarelösungen die Bedarfe der Polizeiarbeit bedienen können und inwiefern das, was im Urteil als automatisierte Datenanalyse bezeichnet wird, zu einer effizienten Polizeiarbeit beitragen kann. Hierbei lässt sich auseinanderhalten, was heute möglich ist (sei es quasi out-of-the-box bei einem Softwareanbieter erhältlich oder erst zu entwickeln) und was vielleicht zukünftig möglich sein könnte. Bei Letzterem handelt es sich um ein erkennbar spekulatives Thema, dessen Bedeutung allerdings, angesichts sprunghafter Entwicklungen im Bereich digitaler Produkte, nicht unterschätzt werden darf.

Von der Ebene der technischen Möglichkeit lässt sich diejenige der Bedarfe und Ansprüche – man könnte auch sagen: der Wünsche – absetzen. Hier spielen die Erwägungsgründe des Urteils eine Rolle, die zwei verschiedene Extreme (einschließlich denkbarer Zwischenpositionen) berücksichtigen: Auf der einen Seite sind da die Wünsche der Polizei, der zuständigen Behörden und der politischen Verantwortungsträger. Diese mögen verschieden motiviert sein und im Detail auch unterschiedliche Herangehensweisen favorisieren, lassen sich aber zusammenfassen unter dem Stichwort der »bestmöglichen polizeilichen Aufgabenerfüllung«. Im Zweifelsfall läuft diese Position auf eine umfassende Nutzung vorhandener Daten hinaus, auf die Verarbeitung mit allen zur Verfügung stehenden Methoden und mit einer Offenheit gegenüber technischen Neuerungen, wo diese dem Ziel dienlich sind – oder sein könnten.<sup>11</sup> Das andere Ende des Spektrums markieren die Anliegen der Beschwerdeführenden als Repräsentanten derjenigen, die ihre persönlichen Daten möglichst umfassend geschützt vor staatlichen Eingriffen wissen wollen. Das Wünschbare könnten diese unter dem Stichwort der »informationellen Selbstbestimmung« zusammengefasst verstehen, wobei damit gemeint ist, dass keine staatlichen Stellen Daten von Personen verarbeiten und Informationen über Personen nutzen, wo dies in die Privatsphäre der Personen eingreift. Die Maximalforderung lautete hier, staatliche Stellen sollten personenbezogene Daten und Informationen gar nicht nutzen.

---

<sup>11</sup> Auch eine Offenheit gegenüber eher experimentellen Formen der Softwarenutzung geht mit dieser Position einher: Polizeiarbeit würde demnach einem Forschungsprozess gleichen, wo sich mitunter ja auch die Forschungsmethode im Verlauf der Forschung oder durch die Qualität der Ergebnisse rechtfertigen lässt.

Die Abwägungslogik des Urteils geht auf die beiden genannten Ebenen ein, trennt diese aber nicht voneinander. Vielmehr zielt das Urteil darauf ab, die beiden Positionen auf den jeweiligen Ebenen innerhalb des Rahmens der Verfassung miteinander zu vermitteln und so selbst wiederum einen Rahmen für die rechtmäßige Nutzung einer automatisierten Datenanalyse zu erstellen.

### 3. »Automatisierte Datenanalyse« und »Neues Wissen«

Die grundrechtsrelevante Qualität einer automatisierten Datenanalyse – in der Sprache des Gerichts das zu prüfende Eingriffsgewicht –, lässt sich analytisch als Ergebnis des Zusammenspiels mehrerer Schritte darstellen.<sup>12</sup> In einem ersten Schritt werden Daten erhoben und zur Verfügung gestellt, dann werden sie verarbeitet, dann resultieren daraus Ergebnisse. Der Dreischritt aus Sammeln, Verarbeiten und Darstellen ist zwar in mehrfacher Hinsicht unterkomplex (u. a. werden Schritte in digitalen Prozessen typischerweise iterativ wiederholt, und auch das Erheben von Daten und deren Einspeisung in ein Verarbeitungssystem können zwei verschiedene Schritte sein), er ist aber für ein Verständnis der Vorgänge der Datenverarbeitung hilfreich und strukturiert auch die Argumentation des Gerichts. Bei allen drei Schritten sieht das Gericht Möglichkeiten für Risikoabwägungen und -anpassungen, was sich detailliert nachzeichnen lässt.<sup>13</sup> Im Folgenden geht es jedoch lediglich um die Logik dieser Abwägung insgesamt.

Bei der automatisierten Datenanalyse ist die Frage der Datensammlung dem eigentlichen Kernstück der Analyse vorgelagert; und auch die Präsentation von Ergebnissen behandelt das Gericht weniger intensiv als die algorithmische Verarbeitung der Daten einschließlich deren Aufbereitung für die Polizeiarbeit.<sup>14</sup> Neben der Art und dem Umfang der verarbeitbaren Daten konstatiert das Gericht auch für die zugelassene Methode der Datenanalyse einen Einfluss auf die Eingriffsintensität. Das wird insbesondere in Randnummer 90 ausgeführt:

»Besonderes Eingriffsgewicht kann der Einsatz komplexer Formen des Datenabgleichs haben. Wenn die Polizei aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen, daraus neue Zusammenhänge erschließen, aus mehrstufigen Analysen neue Verdachtsmomente erzeugen und hieran

---

<sup>12</sup> Vgl. den Beitrag von Andreas Brenneis und Bettina Schöndorf-Haubold in diesem Band.

<sup>13</sup> Vgl. die Beiträge von Lea Rabe sowie von Christopher Giogios in diesem Band.

<sup>14</sup> Dabei bettet das Urteil den Dreischritt noch einmal ein in die (das Feld begrenzende) Frage nach dem Anlass, der eine automatisierte Datenanalyse überhaupt rechtfertigt. Hierbei lässt sich hier die repräsentative Strafverfolgung von der präventiven Gefahrenabwehr unterscheiden. Für beide Felder werden dann wiederum anlassbezogene Eingriffsschwellen definiert. Konkret beschränkt sich das Urteil auf die Frage der Gestaltung der Eingriffsschwelle in der vorbeugenden Bekämpfung von Straftaten (vgl. Rn. 47).

weitere Analyseschritte oder operative Maßnahmen anschließen kann, können die Nachteile aufgrund einer automatisierten Datenanalyse oder -auswertung für die Betroffenen erheblich sein und das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen [...].« (Rn. 90)

Hieraus ergibt sich eine idealtypische Prozesskette, bei der verschiedene Prozessschritte technisch aufeinander folgen, wobei mit jedem weiteren Schritt die möglichen Nachteile für Rechtssubjekte, und damit die normativen Gewichtungen zunehmen. Die Schritte sind folgende:

1. Abschöpfen von Erkenntnissen aus Daten,
2. Erschließung neuer Zusammenhänge,
3. Erzeugung neuer Verdachtsmomente und schließlich
4. weitere Analyseschritte oder sogar
5. operative Maßnahmen.

Dabei erscheinen insbesondere die Schritte 1 bis 3 für eine automatisierte Datenverarbeitung spezifisch zu prüfen.<sup>15</sup>

### 3.1 Data Mining und »Neues Wissen«

Wie passt das in den Rahmen der Vorstellung, es würden Daten »automatisch verarbeitet«? Nachfolgend stelle ich die grundlegenden Prozessschritte des sogenannten Data Mining vor und lege dar, dass bei entsprechenden Ansätzen informatisches Können und domänenspezifisches Wissen zusammenarbeiten müssen. Für den Kernprozess des Data Mining, die Konfiguration von algorithmischen Verfahren zum Zweck der Identifikation von Mustern in Daten, die sogenannte Parametrisierung, ist eine passgenaue Anpassung auf die konkrete Problemstellung erforderlich. Aber auch schon die vorgelagerte Auswahl von Aufgaben sowie von Verfahrensoptionen für das Data Mining kann ohne Domänenwissen nicht hinreichend zielgenau die Anforderungen eines Feldes – wie z.B. der Polizeiarbeit – berücksichtigen. Wenn es, nach der Argumentation des Gerichts, also legitim (oder sogar geboten) ist, mithilfe automatisierter Datenanalysen Anhaltspunkte zu gewinnen und Erkenntnisse zu erschließen, aber bei der Erzeugung neuen Wissens Vorsicht walten soll und die Analyse von dieser Seite her be-

---

<sup>15</sup> Denn die Rede von weiteren Analyseschritten (4) ist so abstrakt, dass es inhaltsleer ist – und zudem können sich an jeder Stelle in einem kriminalistischen Prozess weitere Analyseschritte anschließen. Ähnliches gilt für die operativen Maßnahmen: Diese kommen nicht durch die Automatisierung der Datenanalyse zusätzlich zu der Polizeiarbeit dazu, sondern sind mit oder ohne Automatisierung essenzieller Bestandteil derselben.

grenzt werden muss, dann stehen die Gesetzgeber wie auch die Softwareanbieter vor der Herausforderung, diese Begrenzung innerhalb der Datenverarbeitung tatsächlich zu realisieren.

Data Mining zielt auf in großen Datenmengen identifizierbare Muster, Zusammenhänge oder Trends – gerade auch solche, die aufgrund des Aufwandes händisch nicht zu ermitteln wären, also bis dato unbekannt sind. Algorithmen und statistische Verfahren extrahieren dabei aus Rohdaten für die jeweiligen Zwecke potenziell wertvolle Informationen. Data Mining ist Teil des Forschungs- und Arbeitsfeldes der Big Data Analytics und unterscheidet sich von klassischer Datenanalyse insofern, dass hier – und darin liegt die Stärke des Ansatzes – die eingesetzten Algorithmen auch zuvor unstrukturierte (oder unspezifisch strukturierte) Daten verarbeiten und dabei Muster automatisch identifizieren.

Mitunter wird der Terminus Data Mining für den gesamten Prozess des »Knowledge Discovery in Databases« (KDD) genutzt, der auch Schritte wie die Vorverarbeitung und Auswertung beinhaltet, während Data Mining im engeren Sinne nur den eigentlichen Verarbeitungsschritt des Knowledge Discovery-Prozesses bezeichnet, also die Entdeckung von Wissen. Dabei geht es entgegen der metaphorischen Bezeichnung (»Entdecken«) um die Gewinnung von Wissen aus bereits vorhandenen Daten. Die Mustererkennung ist hierfür streng genommen eine Vorstufe, auf die die Extraktion eines Wissens folgt, das »gültig (im statistischen Sinne), bisher unbekannt und potentiell nützlich« ist.<sup>16</sup> Alle drei Kriterien – und insbesondere die Nützlichkeit – fordern ein menschliches Urteil. Die vielgenutzte Definition von Fayyad stellt die Wissensextraktion mittels Knowledge Discovery gleichwohl als Resultat der Anwendung von Algorithmen zur Auflistung von Mustern oder Modellen heraus: »Data mining is a step in the KDD process that consists of applying data analysis and discovery algorithms that, under acceptable computational efficiency limitations, produce a particular enumeration of patterns (or models) over the data.«<sup>17</sup> Diesen vierten von insgesamt fünf Schritten des Fayyad-Modells, bei dem es letztlich um die Konfiguration spezifischer Data Mining-Verfahren geht, beschreiben Cleve und Lämmel in ihrer Darstellung des Gebiets der Analyse von Massendaten als Kombination von Parametrisierung und Modellbildung:

»Liegen geeignete Datenbestände in akzeptabler Qualität vor, können die Analysen durchgeführt werden. In dieser Phase erfolgt die Verfahrensauswahl und deren Einsatz zur Identifikation von Mustern im vorbereiteten Datenbestand. In einem ersten Schritt wird zunächst entschieden, welche grundlegende Data-Mining-Aufgabe (beispielsweise Klassifizierung oder Cluster-Bildung) vorliegt. Daran schließt sich die Auswahl eines geeigneten Data-Mining-Ver-

---

<sup>16</sup> Vgl. Ester/Sander 2000, S. 1.

<sup>17</sup> Fayyad et al. 1996, S. 41.

fahrens an. Nach der Auswahl eines für die konkrete Problemstellung geeigneten Verfahrens wird dieses konfiguriert. Diese Parametrisierung bezieht sich auf die Vorgabe bestimmter methodenspezifischer Werte, wie zum Beispiel die Festlegung minimaler relativer Häufigkeiten für einen Interessantheitsfilter, die Auswahl der bei der Musterbildung oder -beschreibung zu berücksichtigenden Attribute oder die Einstellung von Gewichtungsfaktoren für einzelne Eingabevariablen. Wenn eine zufriedenstellende Konfiguration gefunden wurde, kann mit der Suche nach interessanten Mustern in den Daten begonnen werden. Die Analyse-Verfahren erzeugen ein Modell, welches dann als Grundlage für die Bewertung dieser oder anderer Daten dient.«<sup>18</sup>

Ein entscheidender Faktor ist bei der Konfiguration von Data Mining-Verfahren, dass die Datenbestände zunächst einmal als statisch aufzufassen sind und nicht als dynamisch: die Menge der für die Mustererkennung relevanten Daten ist eine geschlossene. »Neues« kommt gerade nicht hinzu. Allerdings werden nun auf dieser Basis die Parametrisierung und die Modell-Erzeugung vorgenommen, was dann Muster in den Daten (»neu«) anschaulich macht. Modelle können in einem weiteren Schritt dann selbstverständlich auch auf zusätzliche Daten angewandt werden. Die Folge ist allerdings, dass die Konfiguration der Data Mining-Algorithmen nicht mehr den initial gesetzten Anforderungen entspricht, die ursprüngliche Modellkonfiguration büßt an Leistungsfähigkeit ein. Dieses Phänomen ist als »Concept Drift« bekannt und kann in verschiedenen Varianten auftreten.<sup>19</sup> Gegebenenfalls ist es daher nötig, das Modell kontinuierlich anzupassen.

Aufgrund des Phänomens der Concept Drift muss man bei der algorithmischen Auswertung dynamischer Daten immer wieder die Konfiguration der Data Mining-Algorithmen prüfen. Auch hierfür ist es nötig, Domänenwissen und domänenspezifische Anforderungen an Analyseergebnisse mittels menschlicher Urteilskraft mit den Algorithmen zur Mustererkennung zu vermitteln. Man muss die Drift erkennen und auch verstehen. Ebenso müssen in der an das eigentliche Data Mining anschließenden Phase – Evaluation und Interpretation der Ergebnisse – informatische und domänenspezifische Expertise aufeinander bezogen bleiben. Das Ziel eines Data Mining-Prozesses ist die Ausbildung neuen und sinnvoll interpretierbaren Wissens. Die Maschine gibt dieses Wissen aber nicht einfach aus. Cleve und Lämmel beschreiben den finalen Schritt im Prozess des Knowledge Discovery in Databases wie folgt:

»In dieser Phase des KDD-Prozesses werden die entdeckten Muster und Beziehungen bewertet und interpretiert. Diese Muster sollen den Anforderungen der Gültigkeit, Neuartigkeit, Nützlichkeit und Verständlichkeit genügen, um neues Wissen zu repräsentieren und einer Inter-

---

<sup>18</sup> Cleve/Lämmel 2020, S. 10.

<sup>19</sup> Vgl. Webb et al. 2016.

pretation zugänglich zu sein. Letztere ist Voraussetzung für die Umsetzung der gewonnenen Erkenntnisse im Rahmen konkreter Handlungsmaßnahmen. Bei weitem nicht alle der aufgedeckten Muster erfüllen diese Kriterien. Die Analyseverfahren fördern häufig viele Regelmäßigkeiten zutage, die irrelevant, trivial, bedeutungslos oder bereits bekannt waren, aus denen [...] folglich kein Nutzen erwachsen kann, oder die nicht nachvollziehbar sind.«<sup>20</sup>

Zentral ist, dass »neues« Wissen letztlich Interpretationswissen ist und dass die richtige Interpretation des algorithmisch gewonnenen und übermittelten Musters ein hohes Maß an Domänenkenntnissen erfordert. Die Autoren kennzeichnen die Auswertung von Ergebnissen aus Data Mining-Prozessen als »Interpretation«. Die Ergebnisse werden dabei interessanterweise als so vorläufig beschrieben, dass aus Sicht des Lehrbuchs bei dem Versuch, Ergebnisse zu interpretieren, typischerweise ein wiederholter »Rücksprung« in eine vorige Phase und eine Wiederholung der Prozessschritte angeraten erscheint.<sup>21</sup> Gesichertes, nämlich tatsächlich brauchbares neues Wissen erfordert also eine Art Basteln.

Gleicht man dies mit Wahrheitstheorien aus dem Bestand der philosophischen Tradition ab, dann wäre Data Mining ein technisches Mittel, das Heuristiken unterstützt, die sich der Wahrheit annähern. Dem entspricht eine Approximationstheorie, die Wahrheit als einen nicht wirklich beendbaren iterativen Prozess versteht. Nach der Korrespondenztheorie bzw. eben spezifisch der Abbildungstheorie der Wahrheit erbringt ein Data Mining-Modell dann wahre Ergebnisse, wenn es die realen Zusammenhänge in den Daten korrekt widerspiegelt, wenn also der Objektbereich hinsichtlich seiner relevanten Eigenschaften richtig abgebildet wird. Ein Modell zur Vorhersage von Kreditrisiken wäre beispielsweise dann »wahr«, wenn seine Prognosen exakt mit den tatsächlichen Zahlungsausfällen übereinstimmen. Data Science-Ansätze kombinieren oft beide Perspektiven: Modelle streben eine möglichst genaue Annäherung an reale Muster an und werden an ihrer Übereinstimmung mit empirischen Daten gemessen.

Methoden des Data Mining erschaffen, so ließe sich resümieren, eine auf Daten aufliegende Oberfläche, welche eine strukturierte Zusammenschau von Daten erlaubt, die zuvor nicht unbedingt aufeinander bezogen waren. Data Mining leistet so die Herstellung und Darstellung eines Bezugs zwischen Daten. Die entsprechenden Methoden zielen darauf ab, unkenntliche Strukturen in großen Datenvolumina als Oberflächensignatur zu modellieren. »Wissen« erschaffen sie jedoch nicht aus sich heraus.

<sup>20</sup> Cleve/Lämmel 2020, S. 10.

<sup>21</sup> Vgl. Cleve/Lämmel 2020, S. 11.

### 3.2 Automatisierte Datenanalyse – Aufdecken und Generieren von Anhaltspunkten

Gewinnt die Polizei mittels Musterbildung Erkenntnisse, die einzelne Personen betreffen, dann führen Zusammenhänge und Verdachtsmomente zu einer erhöhten Eingriffsintensität. Das Urteil fasst die diesbezüglichen Faktoren konzise zusammen:

»Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffssensitiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können«. (Rn. 90)

In dieser Beurteilung gibt es zwei voneinander getrennte Aspekte, die das Gericht zurecht mit Aufmerksamkeit bedenkt. Zunächst wird als Möglichkeit einer Datenanalyse vermerkt, »breitere und tiefere Erkenntnisse über Personen« erlangen zu können. Dies kann als der epistemische Aspekt der automatisierten Datenanalyse charakterisiert werden, es geht hier um Erkenntnisse, die man aus den Daten und Informationen gewinnt. Diese Erkenntnisse sind es auch, die das Gericht als »neues Wissen« beschreibt, durch dessen Herstellung sich eine automatisierte von einer nicht-automatisierten Datenanalyse unterscheidet und somit das Recht auf informationelle Selbstbestimmung tangieren könnte. Neben dem epistemischen gibt es aber auch einen rein technischen Aspekt, nämlich die Frage nach der Nachvollziehbarkeit der durch die Software erstellten Verknüpfungen.

»Bei komplexen Formen des Datenabgleichs besteht zudem mit Blick auf individuellen Rechtsschutz und aufsichtliche Kontrolle und die dafür unerlässliche Möglichkeit, Fehler zu erkennen und zu korrigieren, die Schwierigkeit der Nachvollziehbarkeit der eingesetzten Algorithmen.« (Rn. 90)

Technisch gesehen zählt hier allein der Prozess der Verknüpfung selbst. Die tatsächliche Bewertung, ob eine Verknüpfung sinnvoll ist oder nicht, lässt sich auch wieder nur mittels einer auf den Sachverhalt gerichteten Überprüfung evaluieren. Die Fehler- und Diskriminierungsanfälligkeit der Methode insgesamt basiert auf der inhärenten Verbindung des technischen Aspekts der Methode mit dem epistemischen. Denn Diskriminierungen können durch die Methode sowohl erzeugt wie auch perpetuiert werden und sind anders als die Verknüpfungen ohne Basis in der Realität.<sup>22</sup>

---

22 Wo Verknüpfungen in den Daten, sofern es eben korrekte, angemessene, richtige Verknüpfungen sind, auf Verknüpfungen in der Realität verweisen bzw. diese abbilden, liegt die Sache bei Diskriminierungen und anderen Fehlern anders: Hierbei sind die Daten nicht einfach mehr oder weniger nahe an der Realität und bilden diese mehr oder weniger angemessen ab, sondern diese Fehler in der Datenana-

Die epistemische und die technische Dimension von (automatisierter) Datenanalyse können aus Sicht des Gerichts verschieden stark gewichtet sein. Der – ebenfalls durch das Gericht so definierte – »einfache« Datenabgleich wird als der wenig eingriffsintensive Pol des Kontinuums definiert, innerhalb dessen die Methode der automatischen Datenanalyse verortet wird. Das Urteil erläutert die charakteristischen Merkmale:

»Beim einfachen Abgleich erfolgt die Suche nach einem vorhandenen Datenbestand etwa über eine Person, indem im jeweiligen System die eingegebenen Daten des Betroffenen an den gespeicherten Daten vorbeigeführt werden; als automatisches Datenverarbeitungsverfahren führt der Dateienabgleich insoweit regelmäßig Datenbestände zusammen, um Übereinstimmungen der Daten festzustellen oder Daten des einen Bestands in den anderen zu überführen [...]. Der einfache Abgleich ist also ein suchender Vergleich von Daten zur Feststellung von Übereinstimmungen.« (Rn. 91)

Ein Datenabgleich besteht in der Überprüfung, ob und inwieweit Daten übereinstimmen, die ggf. in verschiedenen Systemen genutzt werden. Eine Automatisierung könnte hier die umfassende Integration verschiedener Datenbankabfragen bedeuten, was die Interoperabilität derselben und entsprechend gestaltete Schnittstellen und Interfaces voraussetzt.<sup>23</sup>

Vom einfachen Abgleich ausgehend ist die Steuerung durch polizeiliche Suchmuster für das Gericht zentral, wobei der Suchvorgang durch Formen automatisierter Datenanalyse verändert wird: Das Gericht stellt in seinem Urteil heraus, dass das Eingriffsgewicht umso höher ist, »je offener die Methode des Suchvorgangs gestaltet ist und je weniger die automatisierte Datenanalyse oder -auswertung durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster gesteuert wird« (Rn. 93). Aufschlussreich ist hierzu die qualifizierende Erläuterung, da eine Datenanalyse nicht wesentlich durch konkrete polizeiliche Suchmuster angeleitet sei, würden Anhaltspunkte für eine Gefahr überhaupt erst generiert: »[J]e offener ein automatisierter Suchvorgang zur vorbeugenden Bekämpfung von Straftaten im Vorfeld konkreter Gefahren ausgestaltet ist, je weniger Sachverhaltsbezug die Suche also hat, umso eher werden durch die Suche überhaupt erst Anhaltspunkte für eine Gefahr generiert« (Rn. 93).

---

lyse sind Nichtübereinstimmungen mit den etablierten Kategorien zur Beschreibung der Realität und wirken sich als Fehlklassifikationen aus.

<sup>23</sup> Vgl. für diesen einfachen Abgleich auch die Definition von Borsdorf 2006, S. 52: »Unter »Datenabgleich« wird der Abgleich erhobener personenbezogener Daten durch den Polizeivollzugsdienst mit dem Inhalt polizeilicher Dateien verstanden. Zum Zweck der Aufklärung einer Straftat, der Aufenthaltsermittlung sowie der Gefahrenabwehr können die personenbezogenen Daten mit dem Fahndungsbestand abgeglichen werden.«

In Abschnitt 2.1 wurde dargelegt, dass es einen legitimen Zweck darstellt, ansonsten nur aus Aufwandsgründen unerkannte Anhaltspunkte zu generieren. Die Unterscheidung zwischen »Generieren« oder »Aufdecken« von Anhaltspunkten stellt von daher ein Gelenkstück der höchstrichterlichen Argumentation dar. Zumindest bedenkenswert scheint es, zu fragen, ob es nicht sinnvoll ist, wenn im Zuge der vorbeugenden Bekämpfung von Straftaten auch (neue) Anhaltspunkte für Gefahren ausgemacht werden. Bezeichnet man solche Anhaltspunkte als »generiert«, scheint dies zu bedeuten, dass sie gleichsam (allein) aus der Verknüpfung der Daten heraus entstehen und somit zunächst auch nur in der Sphäre der Daten ihren Bestand haben.

Ein davon analytisch zu trennender Schritt bliebe so die Überprüfung, ob derartige allein aus den Daten generierte Anhaltspunkte auch in der Realität tatsächliche Anhaltspunkte sind. Diese Frage wirkt auf diejenige nach der Qualität der Daten sowie der Qualität der Datenverarbeitungsmethode (hier also: der automatisierten Datenanalyse) zurück. Der sogenannte »Sachverhaltsbezug« ist sowohl eine logische wie auch eine temporale Kategorie. Denn erst mit Bestehen eines Sachverhalts in der polizeilichen Arbeit und dazugehörigen polizeilichen Suchmustern können Daten in einer zu Recherchezwecken angedachten Weise zugeordnet werden. Deutlich wird dies im Vergleich zwischen der offenen Suche und der Analyse statistischer Auffälligkeiten:

»Das Eingriffsgewicht erhöht sich insbesondere, wenn die Datenanalyse oder -auswertung nicht auf einem Suchbegriff, jedenfalls nicht auf einem auf den bislang erkennbaren Sachverhalt bezogenen Suchbegriff gründet, sondern darauf zielt, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, die darüber hinaus (automatisiert) in weiteren Abgleichsschritten mit bestimmten Datenbeständen verknüpft werden und so zu weiteren Informationen führen können, nach denen zu suchen die Polizei vorher keinen Anlass hatte.« (Rn. 93)

Auch hier stellt sich wieder die Frage, ob nicht diese weiteren Informationen für die Polizeiarbeit hilfreich sind, ganz gleich, ob die Polizei bis dato einen Anlass hatte nach ihnen zu suchen oder nicht. Das Generieren von Anhaltspunkten speist sich aus statistischen Auffälligkeiten in den Daten und weist durch weniger Sachverhaltsbezug als das Abgleichen von Daten ein höheres Eingriffsgewicht auf. Und auch hier scheint eine Regelung über die Quantität der Daten im Hintergrund der Überlegungen und Abwägungen zu stehen, wo eigentlich ein qualitativer Maßstab angemessen zu sein scheint. Es geht nach dem Urteil um Informationen, nach denen die Polizei in gewisser Weise sowieso schon Ausschau gehalten hat und die einem schon eröffneten »Fall« zugeordnet werden können. Sollte es aber stattdessen nicht um eine bestmögliche Auswertung der legitim verfügbaren Daten gehen, um so die für die Polizeiarbeit relevantesten, wichtigsten, zielführendsten Informationen zu erhalten?

Ohne Sachverhaltsbezug kann nichts als Anhaltspunkt gelten. Ein den Sachverhaltsbezug besonders griffig ausbuchstabierender Faktor ist die tatsachengestützte Verbindung zu einer konkret verantwortlichen Person. Personen, die keinen »zurechenbaren Anlass gegeben haben«, sollen auch nicht in polizeiliche Maßnahmen einbezogen werden.<sup>24</sup> Der Personenbezug von Datensätzen schafft hier insofern tatsächlich das Risiko der Diskriminierung, als sich in den statistischen Mustern immer auch Vor- und Fehlurteile abbilden. Die Frage ist aber, ob das Thema der Diskriminierung eigentlich ein technisches Problem ist – also eines der algorithmischen und automatisierten Analyse von Daten – oder nicht vielmehr eines von schlecht geordneten, also in den erhobenen Merkmalen bereits potenziell diskriminierenden Daten. Möglicherweise wird durch die Einschränkung der Datenverarbeitungsmethoden etwas der ausführenden Technologie zu Last gelegt, was eigentlich als eine Frage der Datenqualität diskutiert werden sollte.

Die Technik kann als soziotechnisches System nicht an sich neutral sein, aber der reine Vorgang der Verarbeitung von Daten ist es schon. Ob Datenverarbeitungen dabei »in Sekundenschnelle durchgeführt« (Rn. 86) oder ob Abfragen zu Betroffenen nur mal eben »an den gespeicherten Daten vorbeigeführt werden« (Rn. 91) – das sollte dabei keine relevante Frage sein. Das Gericht regelt eine datenintensive Technologie im Wege des Blicks auf die Verarbeitung der Daten – Methode, Umfang und Art –, wobei aus dieser Aufzählung allein die Art der Daten (nicht aber die Beschaffenheit der Datensätze im Detail) eine Rolle für die Qualität der Daten zu spielen scheint. Erstaunlicherweise wird das Stichwort »Qualität« auch gar nicht aufgerufen. Augenscheinlich meint das Gericht von der realen Datenqualität absehen zu können, weil diese wohl (an anderer Stelle) stets hinreichend klar reguliert wäre und demnach gewissen Qualitätsstandards genügen sollte. Wäre aber die Qualität der Daten tatsächlich hinreichend gut, müsste man auch deren Umfang nicht begrenzen und die Methode zu deren Verarbeitung nicht aufgrund von Diskriminierungsrisiken einschränken.

Im Rahmen der Sachverhaltsbewertungen führt das Urteil gesondert die Möglichkeit der Verwendung lernfähiger algorithmischer Systeme an – solcher Systeme also, die man als »Künstliche Intelligenz« (KI) bezeichnet. Als eine janusköpfige Leistung solcher KI-Systeme – nämlich potenziellen Mehrwert und po-

---

<sup>24</sup> Vgl. hierzu Rn. 94: »Der Grundrechtseingriff gewinnt auch an Gewicht, wenn Suchvorgänge nicht auf näher umschreibbare Personen ausgerichtet sind und keine sachliche Verbindung zwischen dem gefährdeten Rechtsgut und den von der automatisierten Anwendung Betroffenen vorausgesetzt wird. Es fehlt dann jede tatsachengestützte Verbindung zu einer konkret verantwortlichen Person. Ein solcher Bezug wird dann überhaupt erst durch die Maßnahme hergestellt, und es steigt das Risiko, dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben.«

tenzielle Gefahr – beurteilt das Gericht, »dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden« (Rn. 100).

Und auch hier springt ins Auge, dass das Gericht an eine Technik ohne diese steuernde Nutzende zu denken scheint. »Automatisierung« scheint demnach ein Szenario auszuschließen, in welchem sich Fragen folgender Art stellen: Wären bestimmte Verknüpfungen nicht in einem ersten Schritt interessant, um sie aber notwendig in einem zweiten Schritt von qualifizierten und befugten Polizist:innen zu überprüfen? Und wenn man eine Vermutung hegt – sollte man nicht die Möglichkeiten der Technik nutzen, um diese gegenzuprüfen – selbstredend ohne blind auf Korrektheit eines digitalen Rechercheergebnisses zu vertrauen? Höherstufig ließe sich fragen: Sollte man nicht zumindest ausprobieren, ob im Einsatz selbstlernender Systeme Effizienzgewinne liegen oder sogar Chancen für eine erfolgreichere Polizeiarbeit? Wie in anderen Bereichen des Einsatzes von KI auch, so könnte auch hier die Maßgabe sein, dass Vorschläge der Maschine akzeptiert und ernstgenommen werden, aber nicht als blind zu befolgen gelten. Dass automatisiert produzierte Vorschläge nicht unreflektiert angenommen und eventuelle Konsequenzen daraus unhinterfragt in die Tat umgesetzt werden sollten, wäre eine geradezu klassische Antwort der Technikfolgenforschung auf die Betrachtung der Schnittstelle zwischen bei der Polizei arbeitenden Personen und dem diesen assistierenden System. Als »Methode« könnte man auf dieser Linie einen klar gesteuerten Einsatz von KI hinsichtlich der Erfolgs- oder ggf. Misserfolgsbilanz relativ klar beurteilen – so wie andere Methoden oder Verfahren auch.<sup>25</sup>

Die automatisierte Ausgestaltung von Mustern (durch Weiter- oder sogar durch Neuentwicklung) sieht das Gericht auch insofern als riskant an, wenn möglicherweise »selbstständig [...] Aussagen im Sinne eine ›predictive policing‹ getroffen werden« (Rn. 100), wobei die hierbei zu treffenden prädiktiven Aussagen abgegrenzt werden von solchen, die lediglich dem »Ausweis von Beziehungen oder Zusammenhängen« dienen. Diese Entgegensetzung lässt sich durchaus kritisch hinterfragen, insofern Konsequenzen auch schon diesseits prädiktiver Absichten eine Rolle spielen. Die Risiken bezüglich der Nachvollziehbarkeit bzw. Überprüfbarkeit maschinell generierter Aussagen – und zwar sowohl bei deterministischen (Rn. 101) wie besonders bei selbstlernenden (Rn. 100) Systemen –

---

25 Zum Vergleich: Es werden auch nicht alle Polizist:innen bei der »Verdichtung« gleichermaßen erfolgreich sein und es wird entsprechend verschiedene Herangehensweisen geben. Manche nach Lehrbuch, manche idiosynkratisch, manche spontan. In genau dieser Hinsicht könnte auch der Einsatz automatisierter Datenanalyse bewertet und ggf. »befördert« werden.

steigen jedenfalls, sollten die Algorithmen sich selbst im Zuge der Datenverarbeitung adaptieren können. Selbstlernende Systeme stellen also (auch hinsichtlich des »neuen Wissens«, das sie generieren) ein besonderes Problem dar:

»So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe algorithmische Systeme können sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein [...]. Dann droht zugleich die staatliche Kontrolle über diese Anwendung verloren zu gehen.« (Rn. 100)

Obleich die Beurteilung berechtigt ist, wirkt sie wie eine etwas dramatische Warnung gegenüber den Möglichkeiten. Wird hier vor einer General Artificial Intelligence gewarnt? Was soll es konkret heißen, dass der Staat die Kontrolle über die Anwendung verliert? Daneben hebt das Gericht das generelle Risiko der Fehleranfälligkeit von Softwarelösungen (Rn. 102) sowie die wachsende Bedeutung von Maßnahmen der Qualitätssicherung hervor. Als weitere Risiken werden benannt: Der unbemerkte Zugriff auf oder sogar die Manipulation von Daten durch Unbefugte (Rn. 100) sowie die Fehleranfälligkeit von Softwarelösungen generell (Rn. 102).

Dies alles sind Kriterien, um die Schwere eines Eingriffs in die informationelle Selbstbestimmung von Betroffenen zu beurteilen (Rn. 104). Wenn ein entsprechend dieser Kriterien schwerwiegender Eingriff durch eine automatisierte Datenanalyse ermöglicht wird, dann ist dies nur unter denselben Voraussetzungen zulässig, wie sie auch für eingriffsintensive heimliche Überwachungsmaßnahmen gelten (Rn. 104) – also sowohl hohe Anforderungen an das zu schützende Rechtsgut wie auch wie auch an den Eingriffsanlass. Bei weniger eingriffsintensiven Maßnahmen – also wenn Art und Umfang der Daten respektive die Methode zu deren Verarbeitung eingeschränkt sind – ist es demgegenüber ausreichend, wenn die Ermächtigungsnorm eine konkretisierte Gefahr als Anlass oder den Schutz besonders gewichtiger Rechtsgüter voraussetzt (Rn. 107). Und wenn die Daten nach Art und Umfang sowie die Methode zu deren Analyse schon im Vorfeld gesetzlich so eingeschränkt sind, dass eine automatisierte Datenanalyse »nicht zu tieferen Einsichten in die persönliche Lebensgestaltung der Betroffenen führt als sie die Behörde, wenngleich aufwändiger und langsamer, auch ohne automatisierte Anwendung realistisch erlangen könnte«, oder wenn die Befugnis von vornherein nur darauf zielt, »gefährliche oder gefährdete Orte zu identifizieren, ohne dabei personenbezogene Informationen zu generieren«, dann vermag schon die Einhaltung des Grundsatzes der Zweckbindung eine entsprechende Maßnahme zu rechtfertigen, weil somit sichergestellt ist, dass es einen Eingriffsanlass gibt (Rn. 108).

Daraus ergibt sich ein Stufenmodell der im Urteil insgesamt zu würdigenden Risiken:

- *Stufe 1:* Hohes Risiko der Datenanalyse – Ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung. Daher hohe Anforderungen an Rechtsgut und Anlass als Voraussetzung.
- *Stufe 2:* Mäßiges Risiko der Datenanalyse – Weniger eingriffsintensive Maßnahme durch Einschränkung von Datenart, Datenumfang oder Verarbeitungsmethode. Abzuwägen gegenüber einer konkreten Gefahr als Anlass oder zum Schutz eines besonders gewichtigen Rechtsguts.
- *Stufe 3:* Niedriges Risiko der Datenanalyse – Wenig intensive Maßnahme durch Einhaltung des Grundsatzes der Zweckbindung sowie gleichzeitige Einschränkung von Datenart, Datenumfang oder Verarbeitungsmethode, so dass keine tieferen Einsichten möglich sind.

### 3.3 Ein spezielles mögliches Ergebnis der Risikobewertung: »Predictive Policing«

Die Ergebnisse einer automatisierten Datenanalyse können prädiktiven Charakter haben – ohne dabei auf Personen bezogen zu sein. Dies ist etwa der Fall, wenn sie auf die »Erkennung gefährlicher oder gefährdeter Orte« zielen (R. 97). Da sich polizeiliche Daten nach den Kategorien Raum und Zeit ordnen lassen, sind Analysen auch dieses Zuschnitts möglich. In der Palantir-Entscheidung stellt das *Predictive Policing* eine (nicht entscheidungserhebliche, sondern lediglich erwähnte) Steigerungsform der mittels Systemen vom Typ hessenDATA künftig möglichen Datenanalyse dar. Die Spielräume einer nicht personenbezogenen (sondern etwa auf Orte oder Fallgestaltungen wie Automaten Sprengung oder Wohnungseinbruch eingeschränkten) Prädiktion erörtert das Urteil nicht. Entsprechend geschulte Data Scientists könnten gleichwohl überlegen, welche Erkenntnisse sich aus den vorhandenen Daten ohne jeglichen Personenbezug gewinnen lassen würden, um damit die Arbeit der Polizei zu verbessern.

Aber auch in der Gruppe der personenbezogenen Verhältnisse sind freilich Unterscheidungen denkbar. Auf der einen Seite wären solche Ergebnisse vermutlich legitim nutzbar, die nicht mehr als eine »bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten« ergeben (Rn. 98). Hingegen erscheinen »maschinelle Sachverhaltsbewertungen« dann, »wenn im Sinne eines ›predictive policing‹ maschinell Gefährlichkeitsaussagen über Personen getroffen werden«, offenkundig als besonders eingriffsintensiv (Rn. 98).

#### 4. Fazit: Zum Risiko der Abwägungslogik im Urteil

Wenn gespeicherte Datenbestände mittels einer automatisierten Datenanalyse verarbeitet werden, dann greift dies in die informationelle Selbstbestimmung von allen Personen ein, deren Daten bei diesem Vorgang personenbezogenen Verwendung finden (Rn. 50). Demnach greift eine automatisierte Datenanalyse in das Grundrecht auf informationelle Selbstbestimmung eines potenziell großen Kreises an Personen ein.

Das Gericht unterscheidet zwei Ebenen, die sich in der personenbezogenen Verwendung von Daten unterscheiden lassen. Der Argumentation nach, »liegt ein Grundrechtseingriff hier nicht nur in der weiteren, zusammenführenden Verwendung vormals getrennter Daten, sondern *darüber hinaus* in der Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die automatisierte Datenanalyse oder -auswertung geschaffen werden kann« (Rn. 50, Hervorh. d. Verf.). Diese beiden Ebenen – faktische Zusammenführung und methodisch typischerweise erlangte Neuheit des durch die Datenbanknutzung erlangten Wissens – lassen sich wiederum auf die Frage nach der Effizienzsteigerung der Polizeiarbeit und auf das Maß der qualitativ grundlegenden Neuausrichtung derselben beziehen. Wird hier nur das typischerweise aus Recherchen gewonnene Potenzial an Einsichten effizienter gewonnen, oder findet quasi eine Transformation des Wissenserwerbs statt, mit diskontinuierlichen Sprüngen und daraus möglicherweise folgenden emergenten Eigenschaften des gewonnenen Wissens? Das »darüber hinaus« stellt in dieser Hinsicht in der oben zitierten Passage die argumentative Gelenkstelle des Urteils dar. Auf der ersten Ebene werden Daten nur zusammengestellt oder verknüpft bzw. integriert. Davon ist eine zweite Ebene zu unterscheiden, auf der neues Wissen erlangt oder geschaffen wird.

Das Urteil des Bundesverfassungsgerichts zur automatisierten Datenanalyse zielt darauf ab, an der Grenze dieses »darüber hinaus« zwischen dem Schutz der informationellen Selbstbestimmung und den Interessen effektiver Gefahrenabwehr einen Ausgleich herzustellen. Dabei wird mit großer Sorgfalt bestimmt, unter welchen Voraussetzungen automatisierte Analysen zulässig sind und wann sie zu tiefgreifenden Eingriffen führen. Doch gerade diese differenzierende Abwägung bringt eine systematische Schieflage mit sich: Sie operiert weitgehend entlang quasi quantitativer Metriken – Art und Umfang der Daten, Anzahl der Analyseoperationen, Tiefe der Verknüpfungen – ohne zugleich eine kohärente qualitative Bewertung dessen zu leisten, was an neuem Wissen, an Handlungsmacht, aber auch an epistemischer Unsicherheit entsteht.

Die verfassungsrechtliche Bewertung konzentriert sich dabei auf die Eintrittswahrscheinlichkeit negativer Folgen für Betroffene – ein legitimes Anliegen, das jedoch in einer methodischen Einseitigkeit resultiert: Risiken werden

formalisiert und quantifiziert, qualitative Nutzenaspekte bleiben demgegenüber skizzenhaft auf wenige programmatische Sätze beschränkt. Für den Gesetzgeber entsteht so das Bild einer Technik, deren Gefahren feinjustiert geregelt werden müssen – aber eben auch können, deren Vorteile jedoch scheinbar naturwüchsig sind und jedenfalls keiner näheren Begründung bedürfen. Dadurch geraten potenzielle Vorteile wie etwa schnellere Hypothesenbildung, Frühwarnindikatoren oder ressourcenschonende Gefahrenprävention aus dem Blick, weil auch ihr Nutzen zunächst einmal nur qualitativ evaluiert werden kann.

Ich habe in diesem Beitrag versucht zu zeigen, dass diese einseitige Fokussierung Ausdruck der tieferliegenden Abwägungslogik ist: Dass sich Technik automatisierter Datenanalyse über eine Justierung von Eingriffsschwellen, Datenarten und Steuerungsformen hinreichend kontrollieren lässt. Doch zugleich muss die epistemische und institutionelle Struktur der Technik selbst begriffen und in die Regulierung integriert werden. Für einen regulatorischen Zugriff, der auch qualitative Differenzierungen erlaubt.

## Quellen und Literatur

- Beck, Ulrich, Risikogesellschaft. Auf dem Weg in eine andere Moderne, Frankfurt am Main 1986.
- Borsdorf, Anke, »Datenabgleich«, in: Lange, Hans-Jürgen/Gasch, Matthias (Hg.), *Wörterbuch zur Inneren Sicherheit*, Wiesbaden 2006, S. 52–54.
- Bull, Hans Peter, »Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit. Rasterfahndung, Online-Durchsuchung, Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung und Antiterrordatei in der Rechtsprechung des Bundesverfassungsgerichts«, in: van Ooyen, Robert Chr./Möllers, Martin H. W. (Hg.): *Handbuch Bundesverfassungsgericht im politischen System*, 3. Auflage, Wiesbaden 2025, S. 1275–1312.
- Cleve, Jürgen/Lämmel, Uwe, *Data Mining*, 3. Auflage, Berlin/Boston 2020.
- Ester, Martin/Sander, Jörg, *Knowledge Discovery in Databases. Techniken und Anwendungen*, Berlin/Heidelberg 2000.
- Fayyad, Usama/Piatetsky-Shapiro, Gregory/Smyth, Padhraic, »From Data Mining to Knowledge Discovery in Databases«, in: *AI Magazine*, Volume 17, Number 3, 1996, S. 37–54.
- Grunwald, Armin, *Technology Assessment in Practice and Theory*, London 2019.
- Hubig, Christoph, *Die Kunst des Möglichen II. Ethik der Technik als provisorische Moral*, Bielefeld 2007.
- Jasanoff, Sheila, »The Songlines of Risk«, in: *Environmental Values*, Jg. 8, H. 2, 1999, S. 135–152.
- Rückert, Joachim, »Abwägung – die juristische Karriere eines unjuristischen Begriffs oder: Normenstrenge und Abwägung im Funktionswandel«, in: *Juristen Zeitung (JZ)* 2011, S. 913–923.
- Webb, Geoffrey I./Hyde, Roy/Cao, Hong/Nguyen, Hai Long/Petitjean, Francois, »Characterizing concept drift«, in: *Data Mining and Knowledge Discovery*, Volume 30, 2016, S. 964–994.



# Automatisierte Datenverarbeitung und Individualisierung

*Andreas Brenneis, Bettina Schöndorf-Haubold*

## 1. Einleitung: Technikpotenziale und Grundrechtsschutz in der polizeilichen Datenanalyse

In seiner Entscheidung zum Einsatz der Software hessenDATA<sup>1</sup> des Unternehmens Palantir vom 16. Februar 2023<sup>2</sup> zieht das Bundesverfassungsgericht die verfassungsrechtlichen Grenzen für die automatisierte polizeiliche Datenanalyse und unterwirft auch die Verwendung künstlicher Intelligenz strengen Voraussetzungen, die einer Nutzung einiger ihrer spezifischen Potentiale im Bereich der Gefahrenabwehr kategorial entgegenstehen könnten. Unter Berücksichtigung des operativen Mehrwerts und der gesteigerten Komplexität KI-basierter Datenverarbeitungsmethoden attestiert das Gericht diesen ein besonders hohes Eingriffsgewicht, das in konsequenter Fortsetzung seiner sicherheitsverfassungsrechtlichen Rechtsprechung nur jenseits der Eingriffsschwellen der konkreten oder zumindest konkretisierten Gefahr verfassungsrechtlich hingenommen werden könne und in deren zeitlichem (bzw. normativem) Vorfeld durch den Gesetzgeber ausgeschlossen werden müsse.<sup>3</sup>

---

<sup>1</sup> Es handelt sich um die politisch umstrittene Software Gotham, die unter unterschiedlichen Bezeichnungen wie hessenDATA, VeRA (Verfahrensübergreifende Recherche- und Analyseplattform) oder Bundes-VeRA auf der Basis eines Rahmenvertrags des Freistaats Bayern mit dem Unternehmen Palantir in verschiedenen deutschen Bundesländern bereits genutzt wird oder – unter Einschluss der Bundesebene – ggf. genutzt werden soll. Zu den Diskussionen in einzelnen Bundesländern (zuletzt in Baden-Württemberg) sowie auf Bundesebene vgl. Giogios, in diesem Band, insbes. S. 64 ff.; im Bundesrat konnten sich die Länder aus Sorge vor dem Verlust der Datensouveränität jedenfalls nicht auf eine langfristige Nutzung des Produkts verständigen (vgl. die EntschlieÙung vom 21.3.2025, BR Drs. 58/25 (Beschluss)). Kurzfristig scheint allerdings weder weltweit noch auf dem deutschen oder europäischen Markt ein alternatives Produkt zur Verfügung zu stehen, so dass auch die produkt- und technikneutrale rechtliche Diskussion nicht ohne die Bezugnahme auf das konkrete Produkt geführt werden kann.

<sup>2</sup> BVerfGE 165, 363 (Automatisierte Datenanalyse).

<sup>3</sup> BVerfGE 165, 363 (insb. Rn. 100 und 120 f.): »Der Einsatz selbstlernender Systeme muss dafür [= für eine Reduktion der Eingriffsintensität im Vorfeld einer konkretisierten Gefahr] im Gesetz ausdrücklich ausgeschlossen sein.«.

Im Folgenden soll die Frage aufgeworfen werden, ob die technischen Möglichkeiten im Bereich der automatisierten Datenverarbeitung – insbesondere im polizeilichen Kontext – tatsächlich bereits im (alltagssprachlichen wie rechtsdogmatischen) Vorfeld so stark eingeschränkt werden müssen, wie es das Urteil naheulegen scheint, oder ob sich nicht alternative Wege denken lassen, die eine differenziertere Abwägung zwischen gesteigerter technischer Effektivität und dem Schutz des Grundrechts auf informationelle Selbstbestimmung ermöglichen.<sup>4</sup> Die Entscheidung liefert Anhaltspunkte für eine techniksensiblere rechtliche Bewertung der spezifischen Grundrechtsrelevanz, ohne dabei mit den Grundlinien der informationsverfassungsrechtlichen Rechtsprechung zu brechen.<sup>5</sup>

Das Grundrecht auf informationelle Selbstbestimmung schützt in der Formulierung des Bundesverfassungsgerichts im Volkszählungsurteil von 1983 die »Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«.<sup>6</sup> Vor dem Hintergrund zunehmend datenbasierter Formen von Verwaltung und Gefahrenabwehr stellt sich heute nicht nur die Frage, wie dieses Grundrecht wirksam geschützt werden kann, sondern auch, wie dieser Schutz unter Bedingungen ubiquitärer automatisierter Datenverarbeitung und algorithmischer Mustererkennung angemessen zu operationalisieren ist.

Die entscheidenden Aussagen zur Zulässigkeit der automatisierten Datenverarbeitung entwickelt das Gericht im Rahmen der Verhältnismäßigkeitsprüfung zur Rechtfertigung der mit der Datenverarbeitung einhergehenden Grundrechtseingriffe (Rn. 51–122 des Urteils). Es nimmt dabei keine quantitative Bewertung der Eingriffe vor, wohl aber eine qualitative Kumulation über die Begriffsfigur der »Schwere«, die sich über die Zweckbindung auf die Eingabe, mit der Methode auf die Verarbeitung und in den potentiellen Wirkungen auf die Ausgabe und damit Verwendung der Daten bezieht.<sup>7</sup> Bemerkenswert ist, dass dieser Gewichtung auf Seiten der Grundrechtseingriffe nicht systematisch jene Effizienzgewinne gegenüber gestellt werden, die sich durch Datenintegration, Automatisierung und ge-

---

4 Vgl. allgemein zur Technikfolgenabschätzung vor dem Hintergrund der Digitalisierung Schrape 2021, zur Herausforderung informationeller Selbstbestimmung durch die Entwicklung datengetriebener Technologien und Ebers/Sein 2024, Datenethikkommission 2019.

5 Der Beitrag nimmt damit eine vermittelnde Position zwischen der klassischen Grundrechtsdogmatik und informationsrechtlichen Reformüberlegungen zu einer Neuorientierung der rechtlichen Regulierung algorithmenbasierter Wissensgenerierung ein; zu letzterem Broemel/Trute 2016 m.w.N.

6 BVerfGE 65, 1 (Volkszählung). Zur konzeptionellen Kritik an der auf der Entscheidung aufbauenden eigentumsähnlichen Konstruktion informationeller Selbstbestimmung s. schon Britz 2010 m.w.N.

7 Zu diesem informationstechnischen EVA-Prinzip Denker, in diesem Band, S. 129.

gebenenfalls auch den Einsatz von Künstlicher Intelligenz in der Polizeiarbeit erzielen lassen (vgl. hierzu den Beitrag von *Brenneis* im vorliegenden Band).<sup>8</sup>

Ziel des vorliegenden Beitrags ist es, aus technikphilosophischer sowie rechtlicher Perspektive auszuloten, ob und inwiefern eine noch stärker ausdifferenzierte Bewertung und Gestaltung der Schritte und Schwellen in der Datenverarbeitung – insbesondere bei Initiierung und Einsatz der Datenverarbeitung sowie beim Übergang der Analyseergebnisse in die polizeiliche Verwertung – dazu beitragen können, Technikpotenziale auszunutzen, ohne den Schutz der informationellen Selbstbestimmung zu unterlaufen. Der Fokus liegt dabei auf der Struktur automatisierter Analyseprozesse sowie auf den möglichen institutionellen und normativen Arrangements, mit denen sich diese begrenzen und absichern lassen.

## 2. Verhältnismäßigkeit und die Logik der Grundrechtseingriffe im Urteil des BVerfG

Das Urteil des Bundesverfassungsgerichts zur automatisierten Datenanalyse basiert auf der verfassungsrechtlichen Leitlinie der Verhältnismäßigkeit staatlicher Grundrechtseingriffe. Diese verlangt, dass jeder Eingriff einen legitimen Zweck verfolgt und dafür geeignet, erforderlich sowie im engeren Sinne angemessen ist. Zwar nimmt das Gericht (bislang)<sup>9</sup> keine formale Quantifizierung der Eingriffstiefe vor, doch greift es auf die metaphorische Kategorie der »Schwere« zurück, um eine kumulative Betrachtung der grundrechtlichen Belastung zu ermöglichen (vgl. die Beiträge von *Giogios* und *Rabe* im vorliegenden Band).

Wie schon angedeutet ist dabei bemerkenswert, dass sich diese Bewertung einseitig auf die Eingriffsseite konzentriert. Die potenziellen Effizienzgewinne, die sich aus automatisierter Datenverarbeitung ergeben – etwa durch Integration

---

8 Für wichtige Diskussionsbeiträge im Diskurs zu Digitalisierung als Effizienzsteigerung vgl. u. a. Zuffo 1988, Floridi 2014, Morozov 2013, als Überblicksdarstellungen mit dezidiertem Blick auf staatliche Aktivitäten z. B. OECD 2019 sowie Parycek/Siegel 2024 und für einen Überblick zu ethischen Ansätzen der Beurteilung von KI-Systemen Ayling/Chapman 2022; kritisch gegenüber einer zu geringen Gewichtung von Strafverfolgung und Gefahrenabwehr schon in der bisherigen sicherheitsverfassungsrechtlichen Rechtsprechung des BVerfG Bull 2023, S. 23 ff. mit Verweis auf das Sondervotum von Schluckebier in BVerfGE 125, 260 (322); übergreifend zu den Risiken einer generellen Technikkritik ders. 2019.

9 Zu Ansätzen zu einer übergreifenden Quantifizierung von sicherheitsrechtlichen Eingriffen in das Recht auf informationelle Selbstbestimmung mittels einer doppelten Verhältnismäßigkeitsprüfung im Rahmen einer sog. Überwachungsgesamtrechnung bereits Roßnagel 2010, S. 1238 ff.; jetzt Poscher/Kilchling/Landerer 2021, S. 225 ff.; dazu Löffelmann 2024, 18 S. ff.; Geminn 2022, S. 789 ff.; insgesamt kritisch Lindner/Unterreitmeier 2022, S. 915 ff.

heterogener Datenquellen, durch Automatisierung von Abgleichprozessen oder durch den Einsatz von KI zur Mustererkennung – werden nicht systematisch in die Abwägung einbezogen. Insbesondere fehlt es an einer konkreten Bezugnahme auf spezifische Ermittlungspotentiale. Dies führt zu einer Asymmetrie: Der möglichen Gefahr durch Technik wird ein hohes Gewicht beigemessen, während ihr möglicher Nutzen für eine effektivere Gefahrenabwehr nicht als eigenständiger Faktor explizit in die juristische Bewertung eingeht.<sup>10</sup>

Diese Asymmetrie wirft die Frage auf, ob das Verhältnis von Grundrechtsschutz und Sicherheitstechnik nicht differenzierter gedacht werden kann und auch gedacht werden muss – insbesondere dann, wenn die Technik nicht auf die Herstellung personenbezogener Ergebnisse zielt, sondern vorrangig auf strukturierte Erkenntnisse, die zunächst ohne Individualisierung auskommen, wenn also das im Urteil zentrale »neue Wissen« nur der Möglichkeit nach, aber nicht faktisch Bezüge zu Personen aufweist. Was als »neues Wissen« im Urteil verhandelt wird, lässt sich weiter differenzieren und bestimmen. An dieser Stelle setzt der vorliegende Beitrag an: Es geht darum, die normativen Kriterien für die Bewertung der Eingriffstiefe(n) (v.a. also in Bezug auf das Recht auf informationelle Selbstbestimmung) präziser mit der technischen Struktur automatisierter Analyseverfahren (und dabei insbesondere mit der tatsächlichen Zuordnung von Analyseergebnissen zu Individuen) zu verschränken und so ergänzende Bewertungsmaßstäbe zu identifizieren, die sowohl dem Grundrechtsschutz als auch der Funktionslogik der Technik gerecht werden. Individualisierung im Sinne der Herstellung von Personenbezug kann im Zuge automatisierter Datenverarbeitung eine wesentliche Rolle spielen. Aber es lassen sich verschiedene Momente dafür ausmachen, die sich im Rahmen einer Prozesslogik von Erhebung, Verarbeitung und Verwertung von Daten verorten lassen.

### 3. Drei Schritte automatisierter Datenverarbeitung: Erhebung, Verarbeitung, Verwertung

Das für das Urteil titelgebende Stichwort von der »automatisierten Datenanalyse« lässt sich analytisch zunächst in das klassische Modell des Umgangs mit Daten auf drei aufeinander aufbauenden Stufen einordnen: (1) die Datenerhebung, (2) die Datenverarbeitung im engeren Sinne sowie (3) die Auswertung und Verwertung der daraus gewonnenen Erkenntnisse.<sup>11</sup> Zwischen diesen Schritten las-

---

<sup>10</sup> In diese Richtung auch Bull 2019; Volkman 2025.

<sup>11</sup> Zu informationstechnischen Modellen des Umgangs mit Daten s. Denker, in diesem Band, S. 129 ff.

sen sich zwei Schwellen identifizieren, die für die verfassungsrechtliche wie auch die technikethische Bewertung besonders relevant sind: zum einen die Schwelle zwischen der Erhebung und der Verarbeitung, zum anderen jene zwischen der Verarbeitung und der Verwertung.<sup>12</sup> Dadurch lässt sich spezifischer fragen, wo neues Wissen entsteht und wo es wirksam wird.

Während die erste Schwelle – also der Übergang von der Datenerhebung zur algorithmischen Verarbeitung – rechtlich gut konturiert ist und eine zentrale Rolle in der bisherigen Grundrechtsdogmatik spielt, etwa über Zweckbindungen, Speicherbegrenzungen, richterliche Genehmigungsvorbehalte und vor allem über die Anforderungen an einen rechtfertigenden Verarbeitungsanlass, ist die zweite Schwelle weniger deutlich reguliert und scheint in den Erwägungen zudem eine untergeordnete Rolle zu spielen. Gerade an diesem Übergang von der rein technischen Analyse zur konkreten polizeilichen Verwertung stellt sich jedoch die Frage nach dem eigentlichen Ort des Grundrechtseingriffs mit besonderer Schärfe. Bemerkenswert ist außerdem, dass der automatisierte Verarbeitungsvorgang selbst zwar für die Bewertung des Eingriffsgewichts auf der ersten Stufe mit Blick auf Transparenz und Determination vor allem eingriffssteigernde Bedeutung hat, dann aber nicht seinerseits systematisch weiter ausdifferenziert und einer eigenständigen grundrechtsspezifischen Bewertung unterzogen wird. Technikphilosophisch wie grundrechtsdogmatisch stellt sich die Frage, ob und inwieweit es geboten ist, neben der Ersterhebungsschwelle (die eine Voraussetzung für die rechtmäßige Existenz polizeilicher Datenbestände darstellt) allein den Zugriff auf die Daten im Rahmen einer komplexen automatisierten Verarbeitung zum in- und exkludierenden Nadelöhr der verfassungsrechtlichen Beurteilung zu machen.<sup>13</sup>

Im weiteren Verlauf sollen deshalb insbesondere diese zweite Schwelle und ihr vorgelagert der automatisierte Verarbeitungsvorgang selbst näher betrachtet werden. Der Fokus liegt dabei auf der Frage, ob – und unter welchen Bedingungen – technische Verfahren zur automatisierten Datenverarbeitung genutzt werden können, ohne dass damit bereits schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung verbunden sind. Zentral kommt es hierfür auf die tatsächliche und potentielle Individualisierung als Bezugspunkt für eine mögliche Grundrechtsverletzung an. Es ist fraglich, ob das bloß technische Individualisierungspotential, das den besonders grundrechtsrelevanten personenbezoge-

---

12 So wird auch der Verarbeitungsvorgang als solcher über die bloße Speicherung bzw. Löschung der Daten hinaus grund- und datenschutzrechtlich analysiert.

13 Kritisch auch Kuhlmann/Trute 2021, S. 110 f.: »Der input-orientierte Ansatz des Datenschutzes lässt im Grunde die Technologie (Software) und das Modell der Verarbeitung außer Betracht [...]. Daten, Modellierung und Software generieren aber die Ergebnisse in ihrem Zusammenspiel.«.

nen Daten qua definitionem inhärent ist, im Sinne der Volkszählungsentscheidung tatsächlich jeden Verarbeitungsvorgang bereits dem Verdikt der gesteigerten Eingriffsrechtfertigung unterwirft.

Auch die Entscheidung des Bundesverfassungsgerichts bietet Anhaltspunkte für eine differenziertere Betrachtung, die den Menschen (und nicht allein die Technik) zum Urheber (und Adressaten) einer Individualisierung macht. Anders gewendet stellt sich die Frage, ob eine rechtlich relevante Individualisierung (jenseits der menschlichen Initiierung eines Datenverarbeitungsvorgangs) neben der bloß technischen Möglichkeit nicht auch eine zu dieser hinzutretende, tatsächliche oder potenzielle, menschliche Wahrnehmung des Individualisierungsvorgangs voraussetzt und ob und in welchem Kontext das durch eine Datenanalyse gewonnene neue Wissen tatsächlich personenbezogen relevant ist. Automatisierte Datenanalyse wäre demnach als Teil eines soziotechnischen Systems zu verstehen, dessen technische Vorgänge immer auch in menschliche Entscheidungskontexte eingebunden sind.<sup>14</sup> Das Urteil deutet dies an, wenn es das Eingriffsgewicht in Abhängigkeit einerseits von technischen und andererseits von rechtlichen Begrenzungen einer Individualisierung sowohl der Dateneingabe als (insbesondere) auch der Datenausgabe abhängig macht. Eingriffsmindernd wirkt es sich aus, wenn »die Betroffenen als Personen anonym bleiben« (Rn. 76), wenn »der Datenabgleich [...] in Sekundenschnelle durchgeführt wird und die erfassten Daten im Nichttrefferfall keine weitere polizeiliche Tätigkeit veranlassen« (Rn. 86), insofern Abfragen zu Betroffenen (also z. B. Verdächtigen) nur »an den gespeicherten Daten vorbeigeführt werden« (Rn. 91), »wenn die Datenanalyse nicht auf personenbezogene Erkenntnisse, sondern etwa auf die Erkennung gefährlicher oder gefährdeter Orte zielt« (Rn. 97) und die entsprechende Befugnis von vornherein nur darauf und nicht auf die Generierung personenbezogener Informationen gerichtet ist (Rn. 108).

Das Ziel und die Methode des Verarbeitungsvorgangs, die Qualität des Verarbeitungsergebnisses wie auch die Bedingungen und Folgen einer weiteren Verwendung untersucht das Gericht demgegenüber nicht isoliert auf ihre verfassungsrechtliche Zulässigkeit als Einzelschritte, sondern fügt sie im Rahmen der Prüfung der Verhältnismäßigkeit im engeren Sinne in eine umfassende Gesamtbetrachtung des Eingriffsgewichts eines gesamten Datenlebens von der Ersterhebung über die automatisierte Verarbeitung zu möglichen Folgemaßnahmen ein. Das Ziel dieser Gesamtbetrachtung ist es, in Abhängigkeit von dieser (über-)differenzierten Beurteilung des Eingriffsgewichts die Schwelle der Initiierung des Datenverarbeitungsvorgangs (als zentralem Schritt in diesem Da-

---

<sup>14</sup> In diese Richtung übergreifend auch Wischmeyer 2018, S. 14 ff.; zu Regelungsstrukturen für KI-Assistenzsysteme als sozio-technische Systeme Pilniok 2022.

tenleben) zu bestimmen. Folgeschritte wie etwa die Generierung nur bestimmter Ergebnisse, ihre weitere Verwendung im Allgemeinen sowie für besondere Folgemaßnahmen bilden jedenfalls keinen selbständigen Anknüpfungspunkt für verfassungsrechtliche Überlegungen an dieser Stelle.

Es ließe sich aber mit dem Stichwort der Blackbox argumentieren, dass die eigentliche Verarbeitung der Daten (über Teilprozesse wie Klassifikation, Transformation, Standardisierung, Aggregation, Screening, Selektion, Extraktion, Integration, Modellierung) noch in der Blackbox stattfindet und daher in diesem Schritt akzeptable – ausschließlich technische – »Eingriffe« in die informationelle Selbstbestimmung stattfinden, so dass zwischen der (noch) nicht individualisierten technischen Generierung potenziell relevanter Muster und ihrer Überführung in individualisierte Maßnahmen im Rahmen polizeilicher Arbeit zu unterscheiden wäre.<sup>15</sup> Entscheidend wäre die tatsächliche Individualisierung bzw. deren Ermöglichung in rechtlicher, aber auch in tatsächlicher, d.h. technischer Hinsicht. Wenn das Urteil in diesem Zusammenhang davon spricht, dass eine Abfrage, die an »gespeicherten Daten vorbeigeführt« wird, oder ein Abgleich »in Sekundenschnelle« ein geringeres Eingriffsgewicht haben, entspricht es genau dieser Intuition, den Knackpunkt von Eingriffen in das Grundrecht auf informationelle Selbstbestimmung am Übergang der zweiten Schwelle auszumachen, wo die idealerweise neutrale wie qualitätsgesicherte Datenverarbeitung Ergebnisse zeitigt, die Auswirkungen außerhalb der Welt der Datenverarbeitung mit sich bringen – beispielsweise durch die Identifikation von Tatverdächtigen oder polizeilichen Störern im Zuge der Zusammenführung von Datensätzen. Hierbei ist demnach nicht die Initiierung einer Datenanalyse ausschlaggebend, sondern die Datenverarbeitung selbst und die Verwertung ihrer Ergebnisse in der polizeilichen Ermittlungsarbeit stehen im Fokus.

#### 4. Im Innern der Datenverarbeitung

Das Bundesverfassungsgericht misst gerade der zunehmenden Komplexität und Intransparenz automatisierter Datenverarbeitung bereits unabhängig von der Frage von KI eingriffserhöhende Bedeutung zu mit der Konsequenz, den Einsatz

---

<sup>15</sup> Die Blackbox automatisierter Datenverarbeitung kann demnach ein Vorzug sein. Im Zuge der Forschungen zu Explainable AI werden in erster Linie Möglichkeiten diskutiert, wie sich der Blackbox-Charakter überwinden lässt (vgl. Guidotti et al. 2018, Rudresh et al. 2023, von Eschenbach 2021, Zednik 2021), es gibt aber auch Ansätze, welche die – v.a. technischen – Vorteile hervorheben: Loyola-González 2019, Ananny/Crawford 2018.

der Methode selbst nur unter hohen Voraussetzungen an Anlass und Schutzgut zuzulassen. Leitsatz 4 der Entscheidung zu hessenDATA fasst dies so zusammen:

»Ermöglicht die automatisierte Datenanalyse oder -auswertung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten, also nur zum Schutz besonders gewichtiger Rechtsgüter sofern für diese eine zumindest hinreichend konkretisierte Gefahr besteht.«<sup>16</sup>

Das besondere Potenzial einer Analyse-Software nach dem Vorbild von hessenDATA liegt darin begründet, dass Daten aus verschiedenen Quellsystemen übergreifend in einem einheitlichen Datenformat analysefähig zusammengeführt werden können, ohne zuvor physisch verknüpft und standardisiert werden zu müssen. Gerade die Beherrschung großer und undifferenzierter Datenmengen (*Big Data*) macht die besondere Leistungsstärke der entsprechenden Programme aus, für die auch eine Einbeziehung von Social Media und des Internets technisch grundsätzlich nicht ausgeschlossen wäre, so dass die Software bereits unabhängig von zuschaltbaren KI-Elementen weitreichende Datenanalysemöglichkeiten in Orwell'scher Dimension eröffnet.<sup>17</sup>

Unabhängig von der exakten Reproduzierbarkeit der Ergebnisse lassen sich die bei der Suche vorgenommenen Rechenoperation nicht nur im Hinblick auf selbstlernende KI-Systeme, sondern auch für anspruchsvolle deterministische, auf machine learning beruhende Modelle der Datenverarbeitung regelmäßig nicht (ohne sehr spezifische technische Sachkenntnisse) präzise vorhersehen bzw. algorithmisch nachverfolgen. Im Bereich der – noch wenig entwickelten – starken, aber auch bei der bereits im Einsatz befindlichen sog. schwachen KI spricht man deshalb von Blackboxes. Auch hiermit verbindet das Bundesverfassungsgericht eine Steigerung der Eingriffsintensität (Rn. 100 f.). Ähnlich verhält es sich mit der zwangsläufigen Einbeziehung der Daten Unbeteiligter, die zudem auch in keinerlei Bezug zu konkreten, gefahrasierten Abfragen stehen (Rn. 77).

Es stellt sich also die Frage, wie sich die bestehende umfassende Überwachungspotenzialität einer Software, deren technische Möglichkeiten sich exponentiell rasant weiterentwickeln werden, in der grundrechtlichen Bewertung eines konkreten Einsatzes abbilden lässt. Nachvollziehbar und verfassungsgerechtlich abgesichert ist es, den Einsatz normativ an das Vorliegen einer konkretisierten Gefahr zu binden.<sup>18</sup> Denkbar wäre es darüberhinausgehend aber auch,

---

16 BVerfGE 165, 363 (Automatisierte Datenanalyse – Leitsatz 4).

17 Vgl. zur Diskussion von Big Data in der Polizeiarbeit z.B. Kusche/Stefanopoulou 2024, Brayne 2021, Egbert 2020, Wörner 2024, Ruppert 2023, Stock 2023.

18 Verkürzt ist dies die grundsätzliche verfassungsrechtliche Lösung des Bundesverfassungsgerichts (vgl. insb. Leitsätze 3 und 4 der Entscheidung). Eine Konsequenz ist allerdings, dass wesentliche Funktionen

überall dort anzuknüpfen, wo die Einsatzmodalitäten von Menschen bestimmt werden: Dies beginnt bei dem Design und den Suchoptionen einer Software, den verknüpften Datenbeständen und der Öffnung bzw. Schließung gegenüber dem Internet. Initiiert wird eine Datenanalyse in der Regel im Rahmen eines Anfangsverdachts oder einer Gefahrenprognose: Polizeibeamte entscheiden auf der jeweiligen gesetzlichen Grundlage über den konkreten Einsatz eines Analysetools – in Anwendung der durch das Gericht als für den Grundrechtseingriff relevant identifizierten Schwellen. Suchrichtung, -Umfang und -Ergebnis hängen dann aber maßgeblich von der dokumentierbaren konkreten Eingabe ab. Diese kann mit oder ohne Personenbezug erfolgen, wie es auch vorstellbar erscheint, dass die Suche sich auf anonymisierte, nicht personenbezogene und lediglich nachträglich individualisierbare Ergebnisse beschränkt, eine Einschränkung, welche strukturell über die Programmierung (by design) oder alternativ im Zuge der konkreten Nutzung (über entsprechende Prompts) zu gewährleisten wäre. Ebenfalls durch Design oder im Wege der konkreten Abfrage sind besonders sensible und insofern kennzeichnungsbedürftige personenbezogene Daten aus Wohnraum- und Online-Durchsuchungen nachvollziehbar gänzlich oder im hier vorgeschlagenen Modell von einer späteren Individualisierung auszuschließen.<sup>19</sup>

Wäre es möglich, eine Individualisierung zunächst – dokumentierbar – auszuschließen und von weiteren menschlichen Bewertungen und Interventionen abhängig zu machen, scheint es nicht ausgeschlossen, auch im Vorfeld konkretisierter Gefahren mit Bezug auf bestimmte schwerwiegende Straftaten und zum Schutz besonders hochwertiger Rechtsgüter eine softwaregestützte entpersonalisierte Muster-Suche zuzulassen, wenn und solange hiermit keine umfassende gezielte Überwachung von Personen im Sinne eines Predictive Policing ins Blaue hinein ohne eine zumindest konkretisierte Gefahr verbunden wäre.<sup>20</sup> Lassen die

---

nicht genutzt werden können, so dass die Entscheidung sich in Richtung Verbot und Verzicht auswirken müsste; hiergegen abstrakt und ohne Ansehung der Entscheidung Bull 2019, insb. S. 61 und S. 87. Kritisch gegenüber einer möglichen Kapitulation vor der Technik auch Wischmeyer 2020, S. 86.

<sup>19</sup> Vgl. Rn. 59, 64, 81 und 118 der Entscheidung zu den Anforderungen an eine Einbeziehung solcher, besonders schutzwürdiger Daten: »Eine Nutzung der Erkenntnisse als bloßer Spuren- oder Ermittlungsansatz unabhängig von einer dringenden oder im Einzelfall hinreichend konkretisierten Gefahr kommt hier nicht in Betracht.« (Rn. 59).

<sup>20</sup> Weitergehend zum Topos der »Fruchtbarkeit der ungewissen Verwendung« als einem Kernproblem von Big Data und zum »Defizit einer fehlenden Reflexion der Ungewissheit« Broemel/Trute 2016, S. 52 f.: »Ein Teil der besonderen Bedeutung dieser Wissenstechnologie liegt eben gerade darin, dass Daten zu noch unbekanntem Zwecken genutzt werden können und diese eben nicht vorab bekannt sind oder sein müssen«, da andernfalls die »letztlich auf die Generierung bisher unbekannter Zusammenhänge« ausgerichtete Big-Data-Technologie insgesamt entwertet würde; s. schon Trute 2020, S. 116 zu Predictive Policing »als Verdachtsgenerierungstechnologie«, der »es nicht um die Schaffung mystifizierter Persönlichkeitsprofile, nicht um die Ermittlung ins Blaue hinein, nicht um die Einbeziehung einer Unzahl von

hierbei gefundenen Erkenntnisse den Schluss auf das Vorliegen einer konkretisierten Gefahr zu, könnten sie allerdings die Grundlage für weitere polizeiliche Ermittlungen und ggf. einen erneuten Einsatz digitaler Datenanalyse bilden, in deren Zusammenhang auch der gezielte Zugriff auf personenbezogene Daten und damit eine Individualisierung nicht mehr ausgeschlossen wären.

## 5. Die Technik als neutrales Werkzeug? Überlegungen zur Rolle der Datenverarbeitung

Ein zentrales Argument im Urteil des Bundesverfassungsgerichts in der Konsequenz der Volkszählungsentscheidung besteht in der Annahme, dass jede Form und auch jedes Element einer automatisierten Datenverarbeitung bereits als solche(s) grundrechtsrelevant ist – unabhängig davon, ob sie in konkrete polizeiliche Maßnahmen mündet. Diese Grundannahme wirft die Frage auf, inwiefern die technische Verarbeitung von Daten notwendig als »aktive« Handlung des Staates zu bewerten ist oder ob sie nicht auch als vor- bzw. zwischengeschaltete, vor- bzw. aufbereitende und möglicherweise »neutrale« Operation verstanden werden kann.<sup>21</sup> Ein Gedankenexperiment aus der Domäne der Archivwissenschaft mag dies illustrieren: Müsste es bereits als begrifflich für das Wissen relevanter Eingriff verstanden werden, ein Archiv neu zu sortieren, Archivalien zu klassifizieren und sie so für vielfältige Verknüpfungen zugänglich zu machen? Wie wäre es, wenn sich das Archiv nach vorgegebenen Kriterien selbst sortieren würde? Liefse sich der Vorgang unabhängig von dem erzielten Ergebnis bewerten?

Könnten die Verfahren der automatisierten Datenverarbeitung nicht auch als technische Werkzeuge verstanden werden, die sowohl gezielt und individualisiert als auch neutral und ohne Anschauung konkreter Personen eingesetzt werden können, um Datenbestände zu ordnen und dadurch neue Wissenspotentiale zu generieren, denen in der zweiten Variante erst und aufgrund eines gezielten Abrufs auch eine gesteigerte grundrechtliche Bedeutung zukäme? Auch diese als neutral beschriebene Nutzung digitaler Techniken kann in der Fortführung der Rechtsprechung zum Recht auf informationelle Selbstbestimmung

---

Personen« geht, »sondern darum, anhand von Mustern Gefährdungen der Rechtsordnung zu erkennen und wo möglich zu verhindern.«.

21 Mit dem Stichwort der Neutralität soll nicht dafür argumentiert werden, dass Technik an sich tatsächlich neutral ist; klarerweise basieren Gestaltung und Nutzung von Technik (und eben auch Informationstechnik) immer auf Werten und sind damit zumindest potenziell umstritten. Neutralität meint demgegenüber im vorliegenden Kontext Neutralität gegenüber einzelnen Individuen. Der letzte Abschnitt des vorliegenden Textes geht darauf noch einmal detaillierter ein.

nicht als wertfrei und grundrechtsirrelevant verstanden werden, da auch jede Entscheidung, ein Datum zu sammeln und zu klassifizieren, es in einer Analyse zu nutzen etc. mit grundrechtsrelevanten Wertentscheidungen einhergeht. Dennoch lässt sich fragen: Ist es angesichts des in Bezug auf Personal, Raum und Zeit scheinbar unbegrenzten Potenzials der Techniken zwingend, bereits ihrer Aktivierung stets und unausweichlich den Charakter erheblicher Grundrechtseingriffe (oder -gefährdungen) zuzuschreiben oder ließe sich nicht auch die Perspektive einnehmen, dass die potenziellen Risiken etwa technischer Diskriminierung durch fehlerhafte Algorithmen, Verzerrungen in Trainingsdaten oder mangelhafte Modellierung qualitativ prinzipiell vergleichbar sind mit solchen Risiken, die auch bei manuellen (also: händischen) Formen der Datenbearbeitung durch Menschen auftreten?<sup>22</sup>

In dieser Perspektive wäre die Datenverarbeitung stärker als Vorgang in den Blick zu nehmen, so dass nicht die Initiierung, sondern Durchführung und Steuerung und damit die Art und Weise der Kontrolle und Qualitätssicherung – ebenso wie für die »althergebrachten« menschlichen Pendanten – die normative Leitlinie darstellen müssten. Im Zentrum steht dann nicht notwendig die vorgängige Begrenzung technischer Möglichkeiten, sondern die institutionelle und methodische Sicherung der Bedingungen ihrer rechtmäßigen Nutzung. Mit einem Wort: Es geht dann um die menschliche Qualitätssicherung automatisierter Datenverarbeitung, die gerade auch technisch bedingte Phänomene beschränkter Transparenz und Determination (Stichwort: »Blackbox«) in die Kontrolle einbeziehen muss.<sup>23</sup> Denn die Charakterisierung der Datenverarbeitung als Blackbox muss und darf gerade nicht bedeuten, dass die Ergebnisse der (automatisierten) Datenverarbeitung nicht evaluiert und validiert werden könnten.<sup>24</sup>

Diese Verschiebung des Fokus hin zur Qualitätssicherung des Vorgangs der Datenverarbeitung eröffnet neue Perspektiven für die normative Bewertung automatisierter Verfahren. Sie erlaubt es, die Technik nicht notwendig und unausweichlich als eigenständige Bedrohung der Grundrechte zu betrachten, sondern als gestaltbares Element staatlicher Infrastruktur – mit entsprechenden Anforderungen an Dokumentation, Nachvollziehbarkeit und Verantwortlichkeit.

---

22 Vgl. zu Verzerrungen von Daten und Algorithmen in der Polizeiarbeit Egbert 2024.

23 Für eine in diesem Sinne objektivierte Regulierung sprechen sich auch Broemel/Trute 2016, S. 61 f., aus; übergreifend für eine Optimierung der Systeme auch unter Transparenzgesichtspunkten Wischmeyer 2018, S. 42 ff.

24 Ähnlich in Bezug auf Begründungsgebote Ibold 2024. Für eine neue Begründungsarchitektur Wischmeyer 2020, S. 73 ff.

## 6. Die zweite Schwelle: Individualisierung als entscheidendes Kriterium und Personenbezug als rechtlicher Maßstab

Für die Frage, ob und in welchem Umfang durch automatisierte Datenverarbeitung in das Recht auf informationelle Selbstbestimmung eingegriffen wird, gewinnt damit wie geschildert auch die zweite Schwelle – der Übergang von der rein technischen Verarbeitung zur polizeilichen Verwertung – eine zentrale Bedeutung. Denn während jede Verarbeitung personenbezogener Daten grundsätzlich grundrechtsrelevant ist, variiert die Schwere des Eingriffs erheblich in Abhängigkeit vom Grad der Individualisierung der daraus gewonnenen Ergebnisse. Diese rechtstheoretische und rechtsdogmatische Prämisse kann für eine Analyse der technischen Abläufe automatisierter Datenanalyse fruchtbar gemacht werden. Es lässt sich argumentieren, dass die wesentlichen Potenziale technischer Systeme – insbesondere ihre Fähigkeit zur Verarbeitung großer, heterogener und unstrukturierter Datenmengen, zur Automatisierung von Auswertungsprozessen und zur Erkennung komplexer Muster – ohne schwerwiegende Grundrechtseingriffe genutzt werden können, solange die Ergebnisse nicht auf identifizierbare Einzelpersonen bezogen werden. Der für die Bewertung der Grundrechtsrelevanz kritische Punkt ist dann der Übergang von der allgemeinen Mustererkennung zu individualisierten Aussagen. Evident ist dies etwa bei der Markierung oder Bewertung bestimmter Personen als potenziell verdächtig oder anderweitig relevant. Ausreichend wäre aber beispielsweise auch jede Ausgabe individualisierter Ergebnisse ohne polizeiliche Wertungen.

Für eine Bewertung von Systemen wie hessenDATA ist es sinnvoll, deren technische Potenziale möglichst differenziert und kleinteilig zu betrachten. Die Leistungsfähigkeit automatisierter Datenanalyse liegt wesentlich in der Fähigkeit, strukturierte Zusammenhänge aus zuvor unverbundenen oder unübersichtlichen Datenbeständen zu generieren. Dies umfasst zum einen den automatisierten Abgleich großer Datenmengen, zum anderen – insbesondere im Fall lernender Systeme – die algorithmische Identifikation komplexer Muster, die menschlicher Analyse nicht oder nur mit erheblichem Aufwand zugänglich wären. Für die grundrechtliche Bewertung solcher Analyseprozesse ist entscheidend, welche Art von Ergebnissen sie generieren. Zwei Idealtypen lassen sich dabei unterscheiden:

1. Nicht-individualisierte Musterergebnisse: Hierbei handelt es sich um Datenkonstellationen oder Muster, die keine konkreten Personen identifizieren oder diesen zugeordnet werden. Zwar werden zur Generierung solcher Muster personenbezogene Daten verarbeitet, doch verbleiben die Ergebnisse auf einer aggregierten oder anonymisierten Ebene. In diesem Fall ist ein Eingriff

in das Recht auf informationelle Selbstbestimmung zwar nicht ausgeschlossen, seine Schwere aber geringer zu veranschlagen. Solche Verfahren können etwa zur Strukturierung von Lagebildern, zur Erkennung übergeordneter Trends oder zur Entwicklung allgemeiner Hypothesen genutzt werden, ohne dass sie Rückschlüsse auf konkrete Personen zulassen oder unmittelbar polizeiliche Maßnahmen gegenüber Einzelpersonen auslösen. Sie liegen logisch und zeitlich vor der Ausgabe individualisierter Ergebnisse.<sup>25</sup>

2. Individualisierte oder individualisierbare Musterergebnisse: In dieser Kategorie werden durch die Analyse explizit bestimmte Personen als relevant oder verdächtig markiert – sei es durch die Zuschreibung bestimmter Merkmale, durch die Platzierung auf Priorisierungslisten oder durch Hinweise auf zu verfolgende Spuren. Hier tritt der Personenbezug deutlich zutage, und mit der Individualisierung bzw. auch schon der bloßen Individualisierbarkeit konkreter Personen steigt die Eingriffsintensität erheblich, da das Analyseergebnis zur Grundlage staatlicher Maßnahmen gegenüber diesen konkret identifizierbaren Personen werden kann.

Diese Differenzierung ermöglicht es, technische Verfahren nicht pauschal zu bewerten, sondern ihre rechtliche Relevanz gestuft entlang des Grades der Individualisierung zu analysieren. Zugleich eröffnet sie die Möglichkeit, technische Potenziale in einem gestuften System zu nutzen, das zwischen vorbereitender Analyse, individualisierender Ausgabe und eingriffsrelevanter Verwertung unterscheidet. Individualisierung wird damit hier in einem spezifischen eingeschränkten Sinn verstanden: Sie meint nicht bereits die formale Möglichkeit der Zuordnung eines in einen Datenverarbeitungsvorgang einbezogenen Datums zu einer Person ohne Berücksichtigung ihrer Relevanz für ein Verarbeitungsergebnis und damit auch ungeachtet ihrer tatsächlichen oder auch nur potenziellen Wahrnehmbarkeit im Rahmen weiterer menschlicher Ermittlungen und Entscheidungen. Erst mit der vor allem praxisrelevanten operativen Verwendung der individualisierten oder individualisierbaren Ergebnisse eines Datenverarbeitungsvorgangs im Kontext polizeilicher Maßnahmen, erst durch diese Kontextualisierung von im Zuge automatisierter Datenanalyse erkannter Muster realisiert sich das eingriffsrelevante Gewicht der Verarbeitung. Solange die Analyseergebnisse anonym bleiben oder lediglich aggregierte Muster darstellen, ist das Recht auf informationelle Selbstbestimmung zwar berührt und ggf. auch

---

<sup>25</sup> Das Urteil nennt hier z.B. die »Erkennung gefährlicher oder gefährdeter Orte« als eine Art von Wissen, das in diese Kategorie gehören würde (Rn. 97).

gefährdet, doch ist ein solcher Eingriff in seiner Schwere deutlich geringer zu bewerten als im Fall der konkreten Identifizierung.

Mit der Unterscheidung zwischen nicht-individualisierten und individualisierten Eingaben und Ergebnissen ist es möglich, den Ort des eigentlichen Grundrechtseingriffs präziser zu bestimmen. Daraus ergibt sich zugleich ein normativer Spielraum für eine differenziertere Gestaltung technischer Verfahren: Nicht jede Nutzung automatisierter Datenanalyse muss per se als intensiver Eingriff bewertet werden. Entscheidend ist vielmehr, ob – und unter welchen Bedingungen – ein Personenbezug entweder bei der Eingabe und Initiierung einer Abfrage oder erst im Zusammenhang mit der Ausgabe und Verwertung hergestellt wird. Eindeutig bleiben zielgerichtete und von vornherein individualisierte Zugriffe, für die das Gericht die Eingriffsschwellen präzise bestimmt hat. Gleiches muss für individualisierte Ergebnisse gelten, wenn und solange nicht der Vorgang selbst technisch und/oder normativ beschränkt werden kann. Findet eine Individualisierung aber erst in einem sich anschließenden Vorgehen statt, können auch an dieser Stelle Eingriffe grundrechtsverträglich begrenzt werden. Kann eine auch spätere Individualisierung entweder ganz ausgeschlossen oder von weiteren Voraussetzungen abhängig gemacht werden, muss der Zugriff auf die Technik als solcher bei Nichterreichung der vom Gericht formulierten Schwellen nicht gänzlich ausgeschlossen werden, sondern es können Freiräume für ihre Nutzung gewährt werden.

## 7. Normative Ausgestaltung der Schwelle zwischen Analyse und Verwertung

Gerade die zweite Schwelle – der Übergang von der Analyse zur Verwertung der Ergebnisse – bietet einen zentralen Ansatzpunkt für eine differenzierte Regulierung automatisierter Datenverarbeitung im Sinne eines balancierten Verhältnisses zwischen Techniknutzung und Grundrechtsschutz. Denn die Individualisierung der Ergebnisse markiert nicht nur den juristisch relevanten Wendepunkt, sondern auch einen technisch wie organisatorisch normativ gestaltbaren Übergang. Ein denkbare Modell wäre, technische Systeme »by design« so zu konfigurieren, dass sie zwar in der Lage sind, auch personenbezogene oder potenziell individualisierbare Ergebnisse zu generieren, diese Ausgabe der Ergebnisse jedoch von einer klaren menschlichen Entscheidung im Rahmen der Eingabe (unter Einhaltung der hohen Eingriffsschwellen) oder im Rahmen der Ausgabe (ebenfalls unter Einhaltung spezifisch zu gestaltender Eingriffsschwellen) abhängig zu ma-

chen und insbesondere nicht automatisch in polizeiliche Maßnahmen münden lassen.<sup>26</sup>

Stattdessen könnte ein System automatisierter Datenanalyse darauf ausgerichtet und technisch entsprechend programmiert sein, lediglich Vorschläge, Hinweise oder Muster zu liefern, die durch weitere Prüfprozesse validiert werden müssen und gerade eine weitere Individualisierung an spezifische Voraussetzungen knüpfen. Dies würde nicht nur der Idee des menschlichen Kontrollvorbehalts Rechnung tragen (Stichwort: »human oversight«), sondern ließe sich auch mit gestuften Schwellenwerten verbinden, ab denen eine Weiterverfolgung zulässig ist. Solche Schwellenwerte könnten beispielsweise an das Vorliegen einer konkreten oder konkretisierten Gefahr gekoppelt werden, an die Qualität und Plausibilität der algorithmisch generierten Hinweise, an die Zusammensetzung und Konsistenz der zugrundeliegenden Daten oder auch an zusätzliche Kontextinformationen wie etwa die Vorgeschichte einer Person – wobei Letzteres mit Blick auf mögliche Diskriminierungseffekte besonders sensibel zu handhaben wäre. Hier gibt es jedenfalls im Prozess der Datenverarbeitung zahlreiche Stellschrauben, mit denen das Zusammenspiel von Daten, Algorithmik und polizeilicher bzw. kriminalistischer Kontextualisierung austariert werden kann – im Prinzip sogar situativ je nach den Anforderungen eines einzelnen Falls. Diese Logik wäre eine andere als die des Bundesverfassungsgerichts in seiner Entscheidung zur automatisierten Datenanalyse, die es primär und praktisch ausschließlich der ersten Schwelle überantwortet, das Eingriffsgewicht des Zugriffs auf personenbezogene Daten im Wege der automatisierten Datenanalyse zu begrenzen. Statt einer vorgängigen pauschalierenden Einschränkung automatisierter Datenanalyse ließe sich ein effektiver Grundrechtsschutz bei nicht individualisierten Abfragen auch auf der nachgelagerten Stufe der Datenausgabe und der Ergebnisverwendung erreichen.

Wichtig ist dabei, dass die Technik nicht nur durch normative Regeln im Sinne polizeilicher Ermächtigungen begrenzt wird, sondern dass bereits ihre architektonische Gestaltung so erfolgt, dass sie auf eine kontrollierte und kontrollierbare Ausgabe der (nicht vollständig kontrollierbar generierten) Ergebnisse ausgerichtet ist. Die Schwelle zur individualisierten Datenauswertung muss also modelliert sein; und zwar einerseits flexibel genug, um situativ Entscheidungspfade wählen zu können, und andererseits auf der Basis einer gewachsenen und empirisch validierten Historie kriminalistischer Erfahrung mit dem Übergang von der automatisierten Datenanalyse zur weiteren Auswertung ihrer Ergebnisse. Eine solche Modellierung betrifft etwa die Möglichkeit, algorithmische Vorschläge mit Ein-

---

<sup>26</sup> Für stichwortgebende Ansätze des Privacy-by-Design und weitere Privacy-Enhancing-Technologies vgl. Liedtke 2022.

schätzungen über ihre statistische Belastbarkeit zu versehen oder sie mit einem Hinweis zu kennzeichnen, ob (und unter welchen Annahmen) eine Individualisierung technisch möglich ist. So könnte eine Architektur entstehen, die nicht auf unmittelbare Eingriffsentscheidungen zielt, sondern auf strukturierte Entscheidungsunterstützung – mit klar definierten Übergängen, Verantwortlichkeiten und Kontrollmechanismen, etwa durch die Einführung einer Rollentrennung innerhalb des Prozesses der Datenanalyse.

## 8. Organisatorische Trennung von Rollen: Analyse- und Bewertungseinheit versus Ermittlungseinheit

Neben der informationstechnischen Architektur des Vorgangs automatisierter Datenanalyse (inklusive Schutzmechanismen) kann auch die organisatorische Ausgestaltung der Datenverarbeitung wesentlich dazu beitragen, automatisierte Analyseverfahren grundrechtskonform in die polizeiliche Praxis zu integrieren. Denn Verfahren automatisierter Datenanalyse sind Teil eines soziotechnischen Arrangements und laufen nicht im luftleeren Raum ab. Ein besonders wirkungsvoller Ansatz organisatorischer Beschränkung könnte in einer institutionellen Trennung von Rollen liegen – konkret: in der Unterscheidung zwischen der technischen Analyse und Bewertung algorithmisch generierter Ergebnisse einerseits und deren operativer Verwertung im Rahmen der Ermittlungsarbeit andererseits. Dies stellt auch in der Bewertung des Bundesverfassungsgerichts zur ersten Schwelle eine valide Methode zur Sicherung der Grundrechtskompatibilität dar und müsste auch in Bezug auf die zweite Stelle bereits durch den Gesetzgeber angeordnet werden.<sup>27</sup>

Die Aufgabe der Analyse- und Bewertungseinheit (bzw. der »technischen Prüfstelle«) könnte in erster Annäherung darin bestehen, algorithmisch erzeugte Muster oder Hinweise mit Blick auf ihre methodische Belastbarkeit, Aussagekraft und potenzielle Risiken zu bewerten. Diese Einheiten müssten mit spezifischer Expertise ausgestattet sein – sowohl hinsichtlich der Funktionsweise der eingesetzten Systeme als auch in Bezug auf deren Fehleranfälligkeit, mögliche Verzerrungen oder Grenzen der Aussagekraft. Die Aufgabe polizeilich und kriminalistisch versierter Data Scientists wäre es, die Analyseergebnisse

---

<sup>27</sup> Zu gestaffelten Zugriffsrechten im Rahmen sog. Rechte- und Rollenkonzepte vgl. Rn. 140 der Entscheidung. Ansätze eines Rollenkonzepts zeigt die Neufassung von § 25a HSOG, der allerdings lediglich eine generalisierte Zugriffskontrolle über eine bereichsspezifische Rechtevergabe einführt, um insbesondere eine missbräuchliche Verwendung auszuschließen; dazu Bäuerle, in: Möstl/Bäuerle 2025, § 25a HSOG Rn. 108 ff.

einzuordnen, gegebenenfalls zurückzuweisen oder mit qualifizierten Kommentaren zu versehen – etwa zu Wahrscheinlichkeiten, Unsicherheiten oder Voraussetzungen möglicher Auslegungen. Entsprechende Einschränkungen zu Qualität und Validität von Datenanalysen wären eine entscheidende Schwelle vor der Individualisierung von Ergebnissen und ihrer Weitergabe an die jeweils zuständigen operativen Ermittlungseinheiten.

Die operative Ermittlungseinheit würde demgegenüber erst dann aktiv, wenn ein Analyseergebnis durch die vorgelagerte Prüfung freigegeben wurde – sei es zur Weiterverfolgung, zur Kontextualisierung im Ermittlungszusammenhang oder zur kombinierten Bewertung mit weiteren Informationsquellen. Auf diese Weise würde nicht nur ein Reflexionspuffer zwischen automatisierter Analyse und polizeilicher Maßnahme eingezogen, sondern zugleich ein institutioneller Schutzmechanismus gegen die unkritische Übernahme algorithmischer Vorschläge etabliert (Stichwort: »automation bias«).

Eine solche Rollentrennung verfolgt mehrere Ziele: Sie dient der Qualitätssicherung, verhindert eine Vorverlagerung von Entscheidungsmacht auf technische Systeme und schafft zugleich klare Verantwortlichkeiten. Durch die dokumentierte Übergabe zwischen Bewertung und Verwertung kann jederzeit nachvollzogen werden, wer welche Entscheidung auf welcher Grundlage getroffen hat.<sup>28</sup> Gerade im Zusammenspiel mit transparenten Prüfverfahren, standardisierten Protokollen und regelmäßiger Evaluation kann eine solche Trennung eine tragende Säule systematischer Qualitätssicherung bilden. Sie erlaubt nicht nur die Kontrolle über technische Verfahren, sondern ermöglicht auch institutionelle Bedingungen für deren kritische Reflexion und kontinuierliche Verbesserung.

## 9. Qualitätssicherung, Schwellenwerte und die Bedeutung technischer Expertise

Die Nutzung automatisierter Datenanalyse in sicherheitsbehördlichen Kontexten setzt nicht nur klare rechtliche Rahmenbedingungen voraus, sondern bedarf auch einer kontinuierlichen, systematischen Qualitätssicherung. Diese ist unverzichtbar, um sowohl die funktionale Zuverlässigkeit der eingesetzten Systeme als auch deren normgerechte Anwendung im Alltag sicherzustellen. Und sie ist an-

---

<sup>28</sup> Auch das Urteil fordert angesichts der Tatsache, dass Betroffene nicht über eine automatisierte Auswertung ihrer persönlichen Daten informiert werden und daher keine verwaltungsgerichtliche Kontrolle einfordern können, Dokumentationspflichten als Ausgleich (Rn. 113). Übergreifend zur Frage der notwendig menschlichen Verantwortung für den Rückgriff auf KI Rademacher 2020, S. 45 ff.

gebracht, um auf der Basis von Erfahrungen zu validieren, inwiefern Systeme automatisierter Datenanalyse die Qualität der Arbeit von Sicherheitsbehörden verbessern. Qualitätssicherung in diesem Sinne ist also nicht als einmalige Zertifizierung zu verstehen, sondern als fortlaufender, empirisch fundierter Prüfprozess – eingebettet in institutionelle Verfahren und getragen von fachlicher Expertise.<sup>29</sup> Im Zentrum könnten dabei – wiederum in erster Annäherung – Schwellenwerte, Erfolgsquoten und Fehleranfälligkeiten der Analyseverfahren selbst stehen. Diese Parameter müssen regelmäßig überprüft und validiert werden – nicht nur im technischen Sinne, etwa durch Systemtests oder Red Teaming<sup>30</sup>, sondern auch im Hinblick auf die praktischen Konsequenzen, die sich aus fehlerhaften oder irreführenden Analysen ergeben können. Die Frage, bei welchem Schwellenwert ein Hinweis als hinreichend valide gilt, um weiterverfolgt zu werden, ist dabei nicht allein informationstechnisch zu beantworten, sondern bedarf interdisziplinärer Aushandlung – unter Einbeziehung juristischer, kriminalistischer und ggf. auch ethischer Perspektiven. Hier (und nicht bereits vor der Initiierung) könnten auch die vom Gericht entwickelten Schwellen für den Einsatz der Technik zum Zuge kommen. Ebenso wichtig ist die Evaluierung derjenigen institutionellen Verfahren, in denen die Technik automatisierter Datenanalyse eingebettet ist: Wer hat Zugang zu welchen Systemfunktionen? Welche Dokumentationspflichten bestehen? In welcher Form werden Rückmeldungen über falsche Befunde (false positive wie false negative) oder unbeabsichtigte Auswirkungen systematisch erfasst und in die Weiterentwicklung eingespeist? Nur wenn solche prozeduralen Fragen mitbedacht und aktiv gestaltet werden, kann das Ideal einer kontrollierten, verantwortbaren Technikverwendung realisiert werden.<sup>31</sup>

Darüber hinaus sollte sich Qualitätssicherung nicht auf die technische Funktionsweise oder formale Verfahrensregeln beschränken, sondern auch die Effektivität und Treffsicherheit automatisierter Datenanalysen empirisch erfassen und systematisch evaluieren. Es reicht natürlich nicht aus, die generelle Leistungsfähigkeit des Systems zu beschreiben – vielmehr müssen die konkreten polizeilichen und kriminalistischen Ergebnisse in den Blick genommen werden: In welchen Fällen trug die Datenanalyse tatsächlich zur Aufklärung bei? Welche Merkmale, Parameter oder Kombinationen erwiesen sich als besonders aussagekräftig – und welche nicht? Welche Muster führten wiederholt zu Fehl-

---

29 Zu Qualitätsmanagement als Aspekt des Selbstverständnisses lernender Organisationen vgl. Helmold 2023.

30 D.h. die Simulation realitätsnaher Cyberangriffe auf die IT-Infrastruktur einer Organisation, um deren Sicherheitsmaßnahmen zu testen und Schwachstellen aufzudecken.

31 Vgl. zu Ansätzen und Bedarfen einer organisationalen Veränderung der Fehlerkultur innerhalb der Polizei Mahnken/Egbert 2025; übergreifend für eine arbeitsteilige Kontrollinfrastruktur für intelligente Systeme Wischmeyer 2018, S. 61 ff.

einschätzungen? Diese Evaluation sollte nicht nur systembezogen, sondern auch userbezogen erfolgen. Denn der polizeiliche und kriminalistische Mehrwert automatisierter Analyse hängt wesentlich von der Art und Weise ab, wie Polizistinnen und Polizisten mit den generierten Informationen umgehen. Die Nutzung durch einzelne Anwenderinnen und Anwender – etwa welche Hinweise weiterverfolgt, welche verworfen oder welche falsch interpretiert wurden – ist selbst Teil der Effektivitätsbewertung. Daraus ergibt sich eine doppelte Anforderung: Zum einen müssen Analysewerkzeuge so gestaltet sein, dass sie differenzierte Rückmeldungen ermöglichen; zum anderen braucht es auf Seiten der User (und zwar sowohl diesseits wie jenseits der Schwelle) spezifische Kompetenzen, um den Informationsgehalt algorithmischer Ergebnisse überhaupt sachgerecht beurteilen zu können. Ohne diese Fähigkeit zur kritischen Interpretation bleibt die Technik entweder ineffektiv oder birgt das Risiko fehlgeleiteter Maßnahmen – ganz unabhängig von ihrer inhärenten Leistungsfähigkeit.

Zentral für all diese Prozesse ist daher die Verfügbarkeit technischer und methodischer Expertise – nicht nur auf Seiten der Entwicklerinnen und Entwickler, sondern auch innerhalb der Behörden selbst.<sup>32</sup> Eine effektive Qualitätssicherung setzt voraus, dass diejenigen, die mit den Systemen arbeiten, auch befähigt sind, deren Funktionsweise kritisch zu hinterfragen, Grenzfälle zu erkennen und die Aussagekraft von Ergebnissen realistisch einzuschätzen. Das erfordert gezielte Fortbildungen, aber auch neue institutionelle Rollenprofile, in denen Technik-, Rechts- und Anwendungskompetenz systematisch zusammengeführt werden.

## 10. Technische Neutralität, Transparenz und institutionelle Kontrollfähigkeit

Die normative Bewertung automatisierter Datenanalysesysteme darf sich nicht allein auf ihre funktionale Leistungsfähigkeit konzentrieren. Vielmehr stellt sich die grundlegende Frage, unter welchen Bedingungen solche Systeme mit den Anforderungen eines demokratischen Rechtsstaats vereinbar sind. Im Zentrum steht dabei das Prinzip der technischen Neutralität – verstanden nicht im Sinne abstrakter Wertfreiheit, sondern als Gestaltungsprinzip: Technik muss so entworfen, implementiert und institutionell eingebettet sein, dass sie überprüfbar, kontrollierbar und politisch unabhängig bleibt. Diese Aspekte sind erforderliche Bestandteile einer Qualitätssicherung, durch die ein sowohl grundrechtsscho-

---

<sup>32</sup> Vgl. aber zu den Herausforderungen einer entsprechenden Personalgewinnung Schäberle 2023.

nender wie auch möglichst zielführender Einsatz automatisierter Datenanalyse überhaupt erst zu legitimieren ist.

Die dafür notwendige Neutralität ist auf mehreren Ebenen zu gewährleisten. Erstens auf der Ebene der technischen Struktur: Automatisierte Systeme müssen so gestaltet sein, dass ihre Funktionsweise offengelegt, dokumentiert und unabhängig überprüft werden kann. Dies gilt insbesondere für selbstlernende Systeme, bei denen die Auswahl und Gewichtung von Trainingsdaten nicht nur technische, sondern zutiefst normative Entscheidungen implizieren. Verzerrungen, Ausschlüsse oder ideologische Vorprägungen in den Trainingsdaten können sich unmittelbar auf die generierten Muster auswirken – und damit auf die polizeilichen Hinweise, die das System produziert. Zweitens betrifft die Neutralität die Auswahl konkreter technischer Produkte. Kommerzielle Anbieter, die ihre Produkte nicht unabhängig auditieren lassen oder deren unternehmerische Praxis mit politischen Interessen verflochten ist, stellen hier ein Risiko dar. Insbesondere Systeme, die auf proprietären Komponenten beruhen und keinen Zugang zu Quellcode oder Datengrundlagen gewähren, entziehen sich wirksamer Kontrolle. Das zentrale Beispiel für anhaltende Kritik hinsichtlich dieser Anforderungen an Neutralität ist *Palantir Gotham*, das zwar funktional leistungsfähig ist, jedoch weder strukturell transparent noch ideologisch unbedenklich erscheint. Hinterfragt werden müssen in solchen Fällen nicht nur die technische Qualität und die der Resultate, sondern auch die politische und wirtschaftliche Rahmung des Produkts.<sup>33</sup>

Transparenz bildet die zentrale Voraussetzung für jede ernstzunehmende Kontrolle solcher Systeme – nicht nur im Hinblick auf den Code, sondern auch auf Trainingsdaten, Systemparameter und Gewichtungen. Diese Transparenz muss normativ eingefordert und institutionell durchgesetzt werden. Ohne sie bleibt jede Qualitätskontrolle selektiv, zufällig oder bloß deklaratorisch.<sup>34</sup>

Ein weiterer zentraler Aspekt technischer Neutralität liegt in der institutionellen Kontrollfähigkeit – also der Möglichkeit, Systeme im Zweifel zurückzunehmen, auszutauschen oder außer Betrieb zu setzen. Abschaltbarkeit ist kein technisches Detail, sondern eine politische Sicherheitsgarantie. Technik, die sich nicht abschalten lässt (Stichwort: »vendor lock-in«) – sei es wegen technischer Abhängigkeiten, vertraglicher Bindungen oder administrativer Intransparenz –,

---

<sup>33</sup> Vgl. hierzu den Beitrag von Brenneis/Denker/Gehring in diesem Band sowie beispielhaft auch Molnar 2024, die neben Palantir zahlreiche weitere Firmen in dem Bereich Sicherheit und Überwachung vor dem Hintergrund eines sich entwickelnden »Border Industrial Complex« in den Blick nimmt, die mit technischen Mitteln und damit Produkten für die Überwachung von Grenzen (als staatlicher Aufgabe) maximalen ökonomischen Profit erzielen.

<sup>34</sup> Zu so verstandener Transparenz als Herausforderung beim Einsatz intelligenter Systeme Wischmeyer 2018, S. 42 ff; ders. 2020, S. 73 ff.

widerspricht dem Prinzip demokratischer Steuerbarkeit und Verantwortung. In Zeiten politischer Kontingenz, auch in Demokratien, kann der Zugriff auf Daten in wenigen Tagen neu geregelt werden – ohne dass sich formale Datenschutzregelungen ändern müssten. Gerade deshalb ist es essenziell, dass datenverarbeitende Systeme nicht nur jetzt, sondern auch unter veränderten politischen Bedingungen überprüfbar und deaktivierbar bleiben. Ganz generell muss gerade im Umgang mit polizeilichen und damit sensiblen personenbezogenen Daten mit erheblicher Grundrechtsrelevanz die staatliche Datensouveränität von der Erhebung über die Verarbeitung zur Verwertung zu jedem Moment sichergestellt sein. Dies kann es erforderlich machen, eigene Lösungen in Deutschland oder innerhalb der bestehenden Datenverbände der Europäischen Sicherheitsunion zu entwickeln. Nicht allein die Gewährleistungen des Grundgesetzes, sondern auch äquivalente datenschutzrechtliche Verbürgungen in der Europäischen Union stellen – auch in Anwendung eines grundsätzlich technikkompatibleren Ansatzes – hohe Anforderungen gerade an riskante auswärtige Produkte und Anbieter.

Zusammenfassend gilt: Nur wenn Systeme oder Plattformen für die automatisierte Datenanalyse auf strukturell neutrale, transparent überprüfbare und institutionell reversible Weise in den Polizeibetrieb eingebunden werden, lassen sich ihre technischen Potenziale mit dem Schutz der Grundrechte und den Anforderungen demokratischer Kontrolle in Einklang bringen. Die Technik einer automatisierten Datenanalyse darf nicht zur Black Box der Sicherheitsarchitektur werden – sie muss, im Gegenteil, als gestaltbares Element staatlicher Infrastruktur der Öffentlichkeit rechenschaftspflichtig bleiben. Die technischen und rechtlichen Möglichkeiten scheinen hier noch nicht ausgeschöpft zu sein. Es ist das Anliegen dieses Beitrags, mit dem Blick auf die Individualisierung als entscheidendem Akt der Grundrechtsbeschränkung im Dreischritt von Erhebung, Verarbeitung und Auswertung die Datenverarbeitung selbst in Anerkennung ihrer spezifischen Charakteristika in die Gestaltung einzubeziehen und von den nachfolgenden Operationen der Auswertung technisch sowie institutionell abzugrenzen.

## Quellen und Literatur

Ananny, Mike/Crawford, Kate, »Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability«, in: *New Media & Society* 20 (3), 2018, S. 973–989.

Ayling, Jacqui/Chapman, Adriane, »Putting AI ethics to work: are the tools fit for purpose?«, in: *AI and Ethics* (2) 2022, S. 405–429.

- Brayne, Sarah, »Überwachung durch Big Data – Das Beispiel der Polizei«, in: *Kölner Zeitschrift für Soziologie und Sozialpsychologie* (KZfSS) 2021, S. 359–395.
- Britz, Gabriele, »Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts«, in: Hoffmann-Riem, Wolfgang (Hg.), *Offene Rechtswissenschaft*, Tübingen 2010, S. 561–596.
- Broemel, Roland/Trute, Hans-Heinrich, »Alles nur Datenschutz? – Zur rechtlichen Regulierung algorithmenbasierter Wissensgenerierung«, in: *Berliner Debatte Initial* 2016, S. 4–65.
- Bull, Hans Peter, »Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit«, in: van Ooyen, Robert/Möllers, Martin (Hg.): *Handbuch Bundesverfassungsgericht im politischen System*, 3. Aufl., Wiesbaden 2025, S. 1275–1312.
- Bull, Hans Peter, »Über die rechtliche Einbindung der Technik. Juristische Antworten auf Fragen der Technikentwicklung«, in: *Der Staat* 2019, S. 57–100.
- Bundesrat, »Priorisierung, auskömmliche Finanzierung und rechtssichere Implementierung eines gemeinsamen Datenhauses für die Informationsverarbeitung der Polizeien des Bundes und der Länder – Neuausrichtung polizeilicher IT (P20) sowie interimweise zeitnahe Bereitstellung einer gemeinsam betriebenen automatisierten Datenanalyseplattform«, Entschließung vom 21.3.2025, *Bundesrat Drs. 58/25* (Beschluss).
- Datenethikkommission der Bundesregierung, *Gutachten der Datenethikkommission*, Berlin 2019.
- Ebers, Martin/Sein, Karin, »Data-driven Technologies. Challenges for Privacy and EU Data Protection Law«, in: Ebers, Martin/Sein, Karin (Hg.): *Privacy, Data Protection and Data-driven Technologies*, London 2024, S. 3–37.
- Egbert, Simon, »Datafizierte Polizeiarbeit – (Wissens-)Praktische Implikationen und rechtliche Herausforderungen«, in: Hunold, Daniela/Ruch, Andreas (Hg.): *Polizeiarbeit zwischen Praxis-handeln und Rechtsordnung*, Wiesbaden 2020, S. 77–100.
- Egbert, Simon, »Diverse Daten, nicht-diskriminierende Algorithmen: Die Relevanz von Diversität im Rahmen der Datafizierung der Polizei«, in: Staller, Mario/Koerner, Swen (Hg.): *Diversität und Polizei*, Wiesbaden 2024, S. 281–303.
- von Eschenbach, Warren, »Transparency and the Black Box Problem: Why We Do Not Trust AI«, in: *Philosophy & Technology* 34 (2021), S. 1607–1622.
- Floridi, Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford 2014.
- Geminn, Christian, »Zur Institutionalisierung einer Überwachungsgesamtrechnung«, in: *Die Öffentliche Verwaltung* (DÖV), 2022, S. 789–795.
- Guidotti, Riccardo et al., »A Survey of Methods for Explaining Black Box Models«, in: *ACM Computing Surveys*, Vol. 51, No. 5, Article 93, 2018.
- Helmold, Marc, »Qualitätsmanagement, Organisationsentwicklung und die lernende Organisation«, in: Helmold, Marc/Laub, Torsten/Flashar, Bernd/Fritz, Jürgen/Dathe, Tracy (Hg.): *Qualität neu denken*, Wiesbaden 2023, S. 169–175.
- Ibold, Victoria, »Künstliche Intelligenz im Sicherheitsrecht – Begründungsgebot quo vadis?«, in: *Zeitschrift für das Gesamte Sicherheitsrecht* (GSZ) 2024, S. 10–18.
- Kuhlmann, Simone/Trute, Hans-Heinrich, »Predictive Policing als Formen polizeilicher Wissensgenerierung«, in: *Zeitschrift für das Gesamte Sicherheitsrecht* (GSZ) 2021, S. 103–111.
- Kusche, Carsten/Stefanopoulou, Georgia (Hg.), *Digitalisierung als total social fact der Kriminalwissenschaften*, Baden-Baden 2024.
- Liedtke, Thomas, *Informationssicherheit – Möglichkeiten und Grenzen*, Berlin 2022.

- Lindner, Josef Franz/Unterreitmeier, Johannes, »Überwachungsgesamtrechnung: Karlsruhe calculat?«, in: *Juristen Zeitung (JZ)* 2022, S. 915–923.
- Lipton, Zachary, »The mythos of model interpretability«, in: *Communications of the ACM*, 61 (10), 2018, S. 36–43.
- Löffelmann, Markus, »Die Überwachungsgesamtrechnung«, in: *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)* 2024, S. 18–22.
- Loyola-González, Octavio, »Black-Box vs. White-Box: Understanding Their Advantages and Weaknesses From a Practical Point of View«, in: *IEEE Access* 7, 2019, S. 154096–154113.
- Mahnken, Julia Katherina/Egbert, Simon, »Update für die polizeiliche Fehlerkultur? Organisationale Implikationen der Datafizierung«, in: Seidensticker, Kai (Hg.): *Fehlerkultur in der Polizei*, Wiesbaden 2025, S. 183–209.
- Molnar, Petra, *The Walls Have Eyes – Surviving Migration in the Age of Artificial Intelligence*, New York 2024.
- Morozov, Evgeny, *To Save Everything, Click Here: The Folly of Technological Solutionism*, New York 2013.
- Möstl, Markus/Bäuerle, Michael (Hg.), *BeckOK Polizei- und Ordnungsrecht Hessen*, 34. Ed. 2025.
- OECD, *The Path to Becoming a Data-Driven Public Sector*, OECD Digital Government Studies, Paris 2019.
- Parycek, Peter/Siegel, Thorsten, *Von der Digitalisierung zur Automatisierung des Verfahrens*, Kompetenzzentrum Öffentliche IT, Berlin 2024.
- Pilniok, Arne, »Administratives Entscheiden mit Künstlicher Intelligenz: Anwendungsfelder, Rechtsfragen und Regelungsbedarfe«, in: *Die öffentliche Verwaltung (DÖV)* 2022, S. 1021–1031.
- Poscher, Ralf/Kilchling, Michael/Landerer Lukas, »Ein Überwachungsbarometer für Deutschland. Entwicklung eines Konzeptes zur periodischen Erfassung staatlicher Überwachungsmaßnahmen«, in: *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)* 2021, S. 225–232.
- Rademacher, Timo, »Künstliche Intelligenz und neue Verantwortungsarchitektur«, in: Eifert, Martin (Hg.), *Digitale Disruption und Recht*, Baden-Baden 2020, S. 45–72.
- Roßnagel, Alexander, »Überwachungs-Gesamtrechnung – Das BVerfG und die Vorratsdatenspeicherung«, in: *Neue Juristische Wochenschrift (NJW)* 2010, S. 1238–1242.
- Rudresh, Dwivedi et al., »Explainable AI (XAI): Core Ideas, Techniques, and Solutions«, in: *ACM Computing Surveys*, 55 (9), Article 194, 2023.
- Ruppert, Felix, »Big Data und Algorithmen im Rahmen der Kriminalitätsbegegnung«, in: Rüdiger, Thomas-Gabriel/Bayerl, Petra Saskia (Hg.), *Handbuch Cyberkriminalologie*, Wiesbaden 2023, S. 317–346.
- Schäberle, Jürgen, »IT-Projekte in der Polizei – Herausforderungen besonderer Art«, in: Wehe, Dieter/Siller, Helmut (Hg.): *Handbuch Polizeimanagement*. Wiesbaden 2023, S. 1471–1486.
- Schrape, Jan-Felix, »Digitalisierung und Technikfolgenabschätzung«, in: Böschen, Stefan/Grunwald, Armin/Krings, Bettina-Johanna/Rösch, Christine (Hg.): *Technikfolgenabschätzung: Handbuch für Wissenschaft und Praxis*, Baden-Baden 2021, S. 83–96.
- Singelstein, Tobias, »Big Data und Strafverfolgung«, in: Hoffmann-Riem, Wolfgang (Hg.): *Big Data – Regulative Herausforderungen*, Baden-Baden 2018, S. 179–185.
- Stock, Oliver, »Datafizierung, Cloudifizierung, Virtualisierung und KI: das polizeiliche Auftragsverständnis zur Verteidigung der Freiheit im digitalen Zeitalter«, in: Wehe, Dieter/Siller, Helmut (Hg.): *Handbuch Polizeimanagement*, Wiesbaden 2023, S. 1445–1470.

- Trute, Hans-Heinrich, »Zur Entwicklung des Polizei- und Ordnungsrechts 2013 – 2019«, in: *Die Verwaltung (DV)* 2020, S. 99–117.
- Volkmann, Uwe, »Gefahrenerkennung durch Data-Mining«, in: *Hessische Verwaltungsblätter (HeVBl)* 2025, S. 101–108.
- Wischmeyer, Thomas, »Regulierung intelligenter Systeme«, in: *Archiv des öffentlichen Rechts (AÖR)* 2018, S. 1–66.
- Wischmeyer, Thomas, »Künstliche Intelligenz und neue Begründungsarchitektur«, in: Eifert, Martin (Hg.), *Digitale Disruption und Recht*, Baden-Baden 2020, S. 73–92.
- Wörner, Liane, »Weg von den Hürden, hin zu den Möglichkeiten: KI in Polizei und Straftatverfolgung«, in: *Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)* 2024, S. 616–641.
- Zednik, Carlos, »Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence«, in: *Philosophy & Technology* 2021, S. 265–288.
- Zuboff, Shoshana, *In the Age of the Smart Machine: The Future of Work and Power*, New York 1988.

Teil 2:  
Sicherheit vor KI und Sicherheit durch KI



# Sicherheit durch KI oder Sicherheit vor KI – Regelungsstrategien für den polizeilichen Einsatz künstlicher Intelligenz

*Bettina Schöndorf-Haubold<sup>1</sup>*

Der Einsatz automatisierter Datenverarbeitungsmethoden, von machine learning und künstlicher Intelligenz in der und durch die Polizei wirft eine Vielzahl rechtlicher Fragen auf, die mit unterschiedlichen Regelungsansätzen in die Zuständigkeit unterschiedlicher legislativer, exekutiver und judikativer Akteure im unionalen Mehrebenensystem fallen. Noch vor der Frage der verfassungsrechtlichen Zulässigkeit stellt sich die Frage nach der föderalen Zuständigkeit zunächst im deutschen Bundesstaat und darüber hinaus in der Europäischen Union, die ergänzende und zum Teil verdrängende Produktsicherheits- und Datenschutzstandards auch und gerade im Bereich der Sicherheitsgewährleistung erlassen hat. Die Regelungsansätze auf den unterschiedlichen Ebenen variieren zwischen der Effektivierung der Sicherheitsgewährleistung durch KI und dem Grundrechts- und Datenschutz vor KI, zu denen sich auch der risikobasierte produktsicherheitsrechtliche Ansatz des EU-Rechts nicht eindeutig verhält.

## 1. Einleitung: Verschränkungen im Sicherheitsrecht des deutschen Bundesstaats und im europäischen Mehrebenensystem

Die Entscheidung des Bundesverfassungsgerichts zur automatisierten Datenverarbeitung und hessenDATA<sup>2</sup> identifiziert die verfassungsrechtlichen Kernfragen, formuliert die Anforderungen für die automatisierte Datenanalyse und deutet hohe verfassungsrechtliche Hürden für den Einsatz künstlicher Intelligenz in der polizeilichen Gefahrenabwehr an.<sup>3</sup> Gegenstand der Entscheidung sind entsprechende Ermächtigungsnormen aus dem hessischen und dem hamburgischen Polizeirecht. Aktuell wird sowohl für die Ebene des Bundes und

---

<sup>1</sup> Herrn Burak Türkmén danke ich sehr herzlich für seine tatkräftige Mitarbeit im Projekt in vielfältigen Recherchen, Diskussionen und Beiträgen.

<sup>2</sup> BVerfGE 165, 363 (Automatisierte Datenanalyse).

<sup>3</sup> Siehe dazu die Beiträge von Rabe und Giogios in diesem Band.

die Tätigkeit der Bundespolizeien als auch in weiteren Bundesländern über den Einsatz speziell der Software Palantir, deren rechtliche Voraussetzungen und tatsächliche Beschaffung diskutiert.<sup>4</sup> Neben den grundsätzlich reaktiv im Kontext konkreter Normenkontroll- oder Verfassungsbeschwerdeverfahren zu klärenden Verfassungsfragen sind damit die operativen Ebenen vor allem der Länder und im Rahmen spezifischer Zuständigkeiten auch des Bundes aufgerufen, deren jeweilige Gesetzgeber den rechtlichen Rahmen für eine polizeiliche Nutzung setzen.<sup>5</sup>

Flankiert werden diese operativen, verfassungsrechtlich konturierten nationalen Regelungsszenarien durch die jüngst in Kraft getretene europäische KI-Verordnung<sup>6</sup>, den sog. AI-Act, die aus einer dritten Perspektive auf der übergreifenden Ebene der Europäischen Union ebenfalls Anforderungen an den Einsatz künstlicher Intelligenz durch die Sicherheitsbehörden der EU-Mitgliedstaaten stellt und dabei einen produkt- und datenschutzrechtlichen Regelungsansatz verfolgt.<sup>7</sup>

Die jeweiligen Regelungsanliegen sind ungeachtet der gegenständlichen Überschneidungen grundsätzlich verschieden. Verklammert werden sie normhierarchisch formal durch den Anwendungsvorrang des Unionsrechts und den Geltungsvorrang des Verfassungsrechts sowie materiell durch die ebenenübergreifenden Verfassungsgebote des Schutzes individueller Freiheit.

Das Bundesverfassungsgericht steckt mit seiner Entscheidung zu hessen-DATA den Rahmen für weitergehende konkretisierende Überlegungen zur Zulässigkeit des KI-Einsatzes in der Polizei, ohne bereits an dieser Stelle abschließend darüber entschieden zu haben. Ungeachtet ihrer auf Deutschland begrenzten Bindungswirkung hat die Entscheidung das Potential, auch im unionalen Kontext Vorbildwirkung in einem Bereich zu entfalten, in dem die Regelungsansprüche des Unions- und des nationalen Rechts konkurrieren und nicht eindeutig voneinander zu trennen sind.<sup>8</sup>

---

4 Vgl. insb. zur Diskussion im Bundesrat die Entschließung des Bundesrates vom 21.03.2025, BR Drs. 58/25 (Beschluss).

5 S. hierzu den instruktiven föderalen Vergleich von Giogios, in diesem Band.

6 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.06.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, ABl. EU Nr. L 2024/1689 v. 12.07.2024. Zu den Vorgaben der KI-Verordnung, dem Zusammenspiel mit weiteren datenschutzrechtlichen Texten, den Anforderungen an die Nutzung wie auch das Training automatisierter Datenanalysen und den datenschutzrechtlichen Implikationen s. auch den Beitrag von Rabe/Geminn/Johannes, in diesem Band.

7 S. dazu schon Schöndorf-Haubold/Giogios 2024.

8 Eine ähnliche Vorbildwirkung hatte bereits die Entscheidung des BVerfG zur Vorratsdatenspeicherung (BVerfGE 125, 260 (Vorratsdatenspeicherung)) auf die erste Entscheidung des EuGH zur entsprechenden Richtlinie (EuGH, Urt. v. 08.04.2014, C-293/12 u. C-594/12, Digital Rights, ECLI:EU:C:2014:238, in der Kompetenzerwägungen keine Rolle spielten und der EuGH Anforderungen an die nationale Ge-

## 2. Einsatzfelder des polizeilichen KI-Einsatzes

Als mögliche Einsatzfelder für Systeme Künstlicher Intelligenz im Rahmen der Sicherheitsgewährleistung kommen insbesondere die intelligente Videoüberwachung mit Mitteln der biometrischen Fernidentifizierung unter Rückgriff auf face-recognition-Mechanismen,<sup>9</sup> Techniken des sog. personen-, zeit- oder raumbezogenen Predictive Policing<sup>10</sup> und vor allem die KI-gestützte Auswertung großer eigener polizeilicher wie auch öffentlich zugänglicher Datenbestände<sup>11</sup> bis zum Rückgriff auf das Internet (Stichwort Big Data und Data Mining) in Betracht, die gerade als Technik für vorhersagende Polizeiarbeit, zur Erkennung bestimmter Gefahren- oder Kriminalitätsmuster oder zum gezielten und weitreichenden personenbezogenen Profiling genutzt werden kann.<sup>12</sup>

In diesem Kontext dient auch der Einsatz des Systems Gotham von Palantir bzw. hessenDATA – bislang wohl ohne Rückgriff auf bzw. unter Ausschaltung der KI-Funktionen – zur automatisierten Datenanalyse und damit zur zielgerichteten Bewältigung großer Datenmengen im Rahmen der Abwehr terroristischer Gefahren und zur Bekämpfung der organisierten Kriminalität.<sup>13</sup>

---

setzung ausschließlich aus grundrechtlichen Erwägungen abgeleitet hat. Eine Präzisierung der strengen grundrechtlichen Kontrolle deutet sich mit der Entscheidung des EuGH, Urt. v. 30.04.2024, C-470/21, *La Quadrature du Net*, ECLI:EU:C:2024:370, EuZW 2024, S. 657 ff. (m. Anm. Roßnagel), hinsichtlich der Vorratsdatenspeicherung von IP-Adressen zur Verfolgung von Straftaten an, die für die Eingriffsschwere zwischen strikt zu trennenden Kategorien auf Vorrat gespeicherter Daten differenziert (Rn. 79, 84 ff.). Ob hieran unter den Bedingungen automatisierter Datenverarbeitung über operative Systeme wie Gotham festgehalten werden kann, deren besondere Leistungsfähigkeit gerade in der Verknüpfung informationell getrennter Systeme begründet ist, erscheint fraglich. Zu den umstrittenen Kompetenzfragen im Bereich des Sicherheitsrechts vgl. Peuker 2023a, S. 384 ff.; ders. 2023b, S. 535 ff.; Pilniok, in: Dietrich/Pilniok 2024, § 4 Rn. 19; eingehend auch Buchheim, in: Dietrich/Pilniok 2024, § 9. 9 Vgl. die Pressemitteilung des BMI vom 11.10.2018 »Projekt zur Gesichtserkennung erfolgreich« zur Erprobung am Berliner Bahnhof Südkreuz, [www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html](http://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2018/10/gesichtserkennung-suedkreuz.html) (01.10.2025); s. zum Projekt auch die Antworten der Bundesregierung auf zwei Kleine Anfragen BT Drs. 19/6076 und Drs. 19/11771, in denen jeweils auf den Abschlussbericht verwiesen wird, der allerdings nicht mehr online zugänglich zu sein scheint.

10 S. dazu nur Rademacher 2017, S. 366 ff.; Kuhlmann/Trute 2021, S. 103 ff.; aus kriminalwissenschaftlicher Sicht Seidensticker, in: Diebel-Fischer/Hellmig/Tischler 2022, S. 193 ff.

11 Vgl. Kugelmann/Buchmann 2024, S. 1 ff.; zum Begriff des »Data-Mining« BVerfGE 156, 11 (40).

12 Beispiele für den polizeilichen KI-Einsatz bei Rademacher, in: Wischmeyer/Rademacher 2020, S. 227 ff.; Seckelmann 2024, Kap. 21 Rn. 30 ff.; dystopische social scoring-Mechanismen werden für die Polizeiarbeit nicht ernsthaft in Erwägung gezogen.

13 Auch Bayern und NRW nutzen ähnliche Systeme von Palantir unter anderen Bezeichnungen: In Bayern heißt das System VerA (= Verfahrensübergreifende Recherche und Analyse – seit 2024, vorher Erprobung), in NRW Datenbankübergreifende Recherche und Analyse (DAR, seit 2022).

Das Programm greift dazu auf existierende polizeiinterne Datenbestände (POLAS<sup>14</sup>, ComVor<sup>15</sup> und CRIME-ST<sup>16</sup>) sowie ggf. auf weitere erhobene Datenquellen etwa aus Telekommunikationsüberwachungsmaßnahmen<sup>17</sup>, auf forensische Extrakte wie z. B. beschlagnahmte Mobiltelefone oder auf Datenbanken anderer Länder und Sicherheitsbehörden zurück, nicht aber auf allgemein zugängliche Daten aus dem Internet. Der von jedem Polizeiarbeitsplatz mögliche Zugriff ist besonders geschulten Personen vorbehalten. Pro Jahr wird die Plattform in etwa 14 000 Verfahren zur Gefahrenabwehr bzw. zur vorbeugenden Verbrechensbekämpfung eingesetzt.<sup>18</sup> Die konkrete Nutzung und Oberfläche von hessenDATA ist nicht öffentlich zugänglich; auch entsprechende Nachfragen innerhalb der Polizei im Rahmen des Forschungsprojekts wurden aufgrund der nach wie vor bestehenden rechtlichen Unsicherheiten nur sehr zurückhaltend beantwortet. In der Sache dürfte es sich derzeit um eine komplexe Suchmaschine zur gezielten Rückverfolgung insbesondere orts- oder personenbezogener Verdachtsmomente handeln.

Der besondere Nutzen der Analysesoftware besteht darin, Daten aus verschiedenen Quellen in kürzester Zeit verknüpft zu analysieren, ohne sie zuvor vereinheitlichen und physisch zusammenführen zu müssen. Eine Neuerhebung von Daten findet dabei nicht statt.<sup>19</sup> Die Algorithmen- bzw. KI-gestützte Ermittlungsarbeit führt zu Vereinfachung, Beschleunigung und Zentralisierung der Datenanalyse. Sie effektiviert die individuelle Polizeiarbeit und verbessert insbesondere auch die Kooperation der Sicherheitsbehörden untereinander.

### 3. Regulatorische Ausgangslage

Das deutsche Recht wie auch die gewachsene deutsche Sicherheitsarchitektur tun sich – aus unterschiedlichen Gründen – schwer mit einer sich exponentiell entwi-

14 POLizeiAuskunftsSystem für repressive Daten.

15 Computergestütztes Vorgangsbearbeitungssystem für sämtliche Verfahren.

16 Fallbearbeitungssystem zur Speicherung präventiver Daten für künftige Ermittlungsverfahren; vgl. BVerfGE 165, 363 (371 f.).

17 Vgl. § 25a II 4 HSOG n.F.: Im Rahmen der vorbeugenden Straftatenbekämpfung sind Verkehrs- sowie Telekommunikationsdaten von der Datenanalyse allerdings in Hessen auszuschließen.

18 So die Angaben im Verfahren vor dem Bundesverfassungsgericht, vgl. BVerfGE 165, 363 (»Automatisierte Datenanalyse«, 373).

19 Auch die KI-gestützte Analyse ohne Datenneuerhebung muss sich nach BVerfG allerdings an den klassischen Grundsätzen der Zweckbindung bzw. der hypothetischen Datenneuerhebung bei Zweckänderung messen lassen; vgl. BVerfGE 141, 220 (BKAG I, 326 ff. Rn. 284 ff.); s. auch BVerfGE 165, 363 (»Automatisierte Datenanalyse«, 392 ff. Rn. 60 ff.); BVerfGE 169, 332 (BKAG II, Rn. 137 ff.).

ckelnden neuen Technik, deren Beschreibung und erst recht deren Beherrschung an Grenzen stoßen und uneinholbar in der Zukunft zu liegen scheinen:

Dies hängt zum einen mit der grundgesetzlichen Kompetenzverteilung im Bereich der öffentlichen Sicherheit zusammen, die dem Bund lediglich die Rechtsetzungskompetenz im Bereich der repressiven Strafverfolgung sowie für die Bundespolizei als ehemaligen Grenzschutz und das BKA als Zentralstelle für den Informationsaustausch zuweist. Das Gefahrenabwehrrecht gehört demgegenüber zu den klassischen Domänen der Landeszuständigkeit.<sup>20</sup> Es obliegt daher den Landesregierungen und mit Blick auf die Grundrechtssensibilität vor allem den Landesgesetzgebern, die rechtlichen Voraussetzungen für die Verwendung künstlicher Intelligenz in der Polizeiarbeit zu schaffen.

Institutionell trifft die Thematik darüber hinaus auf ein noch immer sehr heterogen ausdifferenziertes polizeiliches Informationswesen im deutschen Bundesstaat. Unter den Stichwörtern Datensouveränität und Verwaltungsautonomie fallen die Zuständigkeit für die Erhebung und den Umgang mit polizeilichen Daten ebenso wie die Gefahrenabwehr selbst in die Kompetenz der einzelnen Bundesländer. Diese grundsätzliche Zuständigkeit der Länder im Bereich der Gefahrenabwehr führt dazu, dass diese das Polizeireicht mit den jeweiligen polizeilichen Befugnisnormen je eigenständig regeln und sie auch die informationsrechtlichen Entscheidungen über die Datenverarbeitungssysteme, die Dateninfrastruktur, die Datenbestände sowie etwa die Entscheidung über den Einsatz automatisierter Verarbeitungstechniken auf der Landesebene treffen.

Die Folge ist eine plural ausdifferenzierte und in erheblichem Maße heterogene Polizeiinformationslandschaft mit hohen technischen und organisatorischen Hürden für den Informationsaustausch. Am 30. November 2016 hatten sich daher die Innenminister von Bund und Ländern bei einem Treffen der Innenministerkonferenz im Rahmen der sog. Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der inneren Sicherheit auf eine Strategie verständigt, um die über Jahre in jedem Land wie auch beim Bund gewachsene Informationsarchitektur und –infrastruktur an die Erfordernisse einer übergreifenden vernetzten Zusammenarbeit und den ständigen unmittelbaren und aktuellen Informationsaustausch zwischen den nationalen, supra- und internationalen Polizeien anzupassen. Spätestens seit der Saarbrücker Agenda verfolgen die Länder und der Bund einen noch mühsamen Weg zur Schaffung einer gemeinsamen, modernen und einheitlichen Informationsarchitektur – ungeachtet der verfassungsrecht-

---

<sup>20</sup> Dies führt noch immer zu der Vermutung, dass die existierenden landesrechtlichen Befugnisse in Ermangelung entsprechender bundesrechtlicher Ermächtigungen in der StPO auch zum polizeilichen Einsatz von KI im Rahmen der (vorbeugenden) Strafverfolgung genutzt werden.

lich klar getrennten Kompetenzverteilung und unter Bezugnahme auf den 2009 mit der Föderalismusreform II eingefügten Art. 91c GG, der die Zusammenarbeit von Bund und Ländern im Bereich der Digitalisierung und bei der Errichtung und dem Betrieb informationstechnischer Systeme ausdrücklich vorsieht.

Die Agenda bildet den Rahmen und das Ziel für sich anschließende Projekte über den Polizei-IT-Fonds<sup>21</sup>, Polizei 2020 und schließlich P20<sup>22</sup>, mit denen ein fachlich, technisch und organisatorisches Gesamtsystem für die insg. 20 Polizeien in Bund und Ländern geschaffen werden soll<sup>23</sup>. Ziel ist die Schaffung eines sog. Datenhauses der Polizei bis 2030, um die Verfügbarkeit der Daten, Datenschutz durch Technik und Effizienzgewinne für die Polizei in einer einheitlichen übergreifenden Dateninfrastruktur sicherzustellen.

Bisher scheint dieser Weg im Bereich des Polizeiinformatikrechts allerdings noch nicht annähernd abgeschlossen.<sup>24</sup> Die Infrastruktur wie auch die Datenlandschaft bleiben heterogen, ein gemeinsames Datenhaus konnte noch nicht realisiert werden. Die Saarbrücker Agenda bleibt daher Ziel weiterer Bemühungen um eine Konsolidierung der polizeilichen Informationslandschaft.<sup>25</sup>

Gerade in der behaupteten jedenfalls kurz- und mittelfristigen Überwindung der rechtlichen, kompetenziellen und finanziellen Hürden einer Harmonisierung der disparaten Dateninfrastrukturen scheint auch der besondere Reiz und Nutzen eines Rückgriffs auf die von Palantir angebotenen Systeme zu liegen. Dies zeigt sich nicht zuletzt klar in der Entschließung des Bundesrates vom 21. März 2025 zur »Priorisierung, auskömmlichen Finanzierung und rechtssicheren Implementierung eines gemeinsamen Datenhauses für die Informationsverarbeitung der Polizeien des Bundes und der Länder – Neuausrichtung polizeilicher IT (P20) sowie interimswise zeitnahe Bereitstellung einer gemeinsam betriebenen automatisierten Datenanalyseplattform«,<sup>26</sup> in der der Bundesrat als Reaktion auf jüngere Anschläge unter Bezugnahme auf die Saarbrücker Agenda bis zum Auf-

21 Verwaltungsvereinbarung über die Errichtung eines Polizei-IT-Fonds und über die Grundlagen der Zusammenarbeit bei der Modernisierung des polizeilichen Informationswesens von Bund und Ländern – Vereinbarung zur Ausführung von Art. 91c I und II 1 und 4 GG v. 06.12.2019.

22 Aus dem Jahr 2023; vgl. [www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI23004.html](http://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI23004.html) (01.10.2025).

23 Neben den Polizeien der 16 Länder gehören hierzu die Bundespolizei, das BKA, das ZKA und die Bundestags-Polizei.

24 Dazu BR Drs. 58/25 (Beschluss).

25 Ironischerweise bezieht sich selbst Palantir auf die Saarbrücker Agenda, um mit dem eigenen Angebot gerade die Defizite und den schleppenden Fortgang des Vereinheitlichungsprozesses zu kompensieren, vgl. Wojtas/Cipierre, »Wie Palantir die Digitalisierung deutscher Polizeien unterstützt«, in: Palantir Blog, 03.03.2023. <https://blog.palantir.com/wie-palantir-die-digitalisierung-deutscher-polizeien-unterst%C3%BCtzt-3791d65bccb6> (01.10.2025).

26 BR Drs. 58/25 (Beschluss).

bau und zur noch gänzlich ungewissen Einweihung des gemeinsamen polizeilichen Datenhausökosystems die Öffnung des Bundes für die Beschaffung einer gemeinsamen Datenanalyseplattform einfordert, die Nancy Faser als zuständige Innenministerin im Sommer 2023 mit Blick auf Palantir noch dezidiert ausgeschlossen hatte. Palantir selbst wird in dem Beschluss nicht genannt, scheint aber in Ermangelung von Alternativen jedenfalls die von einer Reihe von Bundesländern favorisierte Plattform zu sein.<sup>27</sup>

#### 4. Regulierungsstrategien, Akteure und Dilemmata

Das eigentliche Dilemma des KI-Einsatzes durch die Polizei bildet sich in den beiden Perspektiven »Sicherheit durch KI« versus »Sicherheit vor KI« ab, die die unterschiedlichen Blickwinkel einerseits effizienterer polizeilicher Aufgabenerfüllung und andererseits verfassungs- und datenschutzrechtlicher Abwehrrechte akzentuieren. Das EU-Recht fügt dem einen produktbezogenen Ansatz hinzu, indem es besonders riskante KI-Verwendungen auch und gerade im Bereich der Sicherheitsgewährleistungen entsprechend kennzeichnet, partielle Verbote ausspricht und auf diese Weise erst die Voraussetzungen für entsprechende Produktentwicklungen und -nutzungen schafft.

Auf einer ersten Stufe agieren die Exekutiven und Parlamente der Länder, treffen die Entscheidungen für einen entsprechenden Einsatz künstlicher Intelligenz durch die Polizei, beschaffen Produkte und erlassen die erforderlichen Rechtsgrundlagen. Vorrangiges Regelungsanliegen ist die Effektivierung der Polizeiarbeit durch Nutzung moderner Techniken (Sicherheit durch KI). Im Rahmen der Bindung an Recht und Gesetz nach Art. 1 Abs. 3, 20 Abs. 3 GG sind auch alle Landesorgane und -behörden stets zur Einhaltung der Grundrechte und zur Beachtung eines verhältnismäßigen Grundrechtsschutzes verpflichtet. Im Zweifelsfall wird diese Verfassungsbindung im Wege der Verfassungsbeschwerde oder Normenkontrolle durch das Bundesverfassungsgericht präzisiert und durchgesetzt. Insofern lässt sich von einer Priorisierung des Freiheitsschutzes durch das BVerfG gegenüber den polizeilichen Effektivierungsanliegen sprechen (Sicherheit vor KI).

Das techniksensible unionale Produktrecht steht zwischen diesen Polen. Es nimmt insb. Datenschutzrisiken in den Blick, operiert aber weitgehend nicht

---

<sup>27</sup> Baden-Württemberg steht vor der Einführung des Systems; das Saarland hat sich einer Nutzung bislang mit guten Gründen verschlossen; neben Hessen nutzen auch Bayern und Nordrhein-Westfalen mit unterschiedlichen Bezeichnungen Anwendungen von Palantir im Bereich der Gefahrenabwehr. Siehe hierzu Giogios, in diesem Band, xxx.

mit Verboten, sondern mit Ausnahmen und Vorgaben, die einen Einsatz von KI-basierten Produkten durch die Sicherheitsbehörden vorrangig ermöglichen und nicht ausschließen (Sicherheit mittels KI).

In der rechtswissenschaftlichen Diskussion lässt sich nicht zuletzt in der Folge der Entscheidung des BVerfG zur automatisierten Datenverarbeitung ganz eindeutig eine Priorisierung des Individualrechtsschutzes beobachten, die allerdings als solche nicht ungewöhnlich ist, verdankt doch das Verwaltungsrecht selbst seine Existenz der Notwendigkeit einer rechtsstaatlichen Disziplinierung der Verwaltung und insbesondere der Polizei. Tatsächlich spielt die Frage des – schwer messbaren – positiven Beitrags des KI-Einsatzes zur Sicherheitsgewährleistung jedenfalls in den wissenschaftlichen Auseinandersetzungen eine deutlich geringere Rolle, während die umgekehrte Frage nach den rechtlichen Risiken, allen voran den Grundrechtsgefährdungen durch KI bis zur Frage der übergreifenden Bilanzierung staatlicher Überwachungsmaßnahmen,<sup>28</sup> die Gerichte und die Wissenschaft beschäftigt.<sup>29</sup> Die reale Wirkweise, das Halluzinationspotential und die Blackboxphänomene von künstlicher Intelligenz verschärfen das rechtliche Besorgnispotential einer hochdynamischen Technik, deren besondere Eigenart auch in ihrer nur begrenzten technischen Beherrschbarkeit zu liegen scheint und deren Kompatibilität mit den klassischen verfassungsrechtlichen Anforderungen erst noch herausgearbeitet werden muss.<sup>30</sup>

Es kommt hinzu, dass sich verfassungsrechtlich die Sorge vor der Möglichkeit einer umfassenden staatlichen Überwachung im Kontext einer KI-unterstützten Polizeiarbeit unmittelbar aufdrängt und damit verbunden die Frage nach den rechtsstaatlichen Grenzen bis hin zu einem vollständigen Ausschluss eines KI-Einsatzes durch die Polizei. Dies richtet sich zum einen gegen jede vollständige Automatisierung polizeilicher Prognosen und Entscheidungen durch eine Künstliche Intelligenz und damit gegen eine Ersetzung menschlicher Entscheidung durch eine maschinelle, die sich zudem gerade dadurch auszeichnet, dass sie sich nicht (mehr) vollständig algorithmisch determinieren lässt und dass weder ihre Funktionsweise noch die von ihr produzierten Ergebnisse sich in all

---

28 Zur sog. Überwachungsgesamtrechnung im Kontext der Vorratsdatenspeicherung bereits Roßnagel 2010, S. 1238 ff.; jetzt Poscher/Kilchling/Landerer 2021, S. 225 ff.; dazu Geminn 2022, S. 789 ff.; Löffelmann 2024, S. 18 ff.; kritisch Lindner/Unterreitmeier 2022, S. 915 ff.

29 Hierauf weist insb. auch Bull 2025, S. 23 ff. mwN. hin; zu den Risiken einer generellen Technikkritik ders. 2019, über die rechtliche Einbindung der Technik.

30 Überlegungen zu einer techniksensibleren Stufung der Verhältnismäßigkeitsprüfung bei Brenneis/Schöndorf-Haubold, in diesem Band.

ihren Einzelschritten und Bestandteilen identifizieren, beschreiben und damit auch nachvollziehen und überprüfen lassen.<sup>31</sup>

Es ist wichtig, darauf hinzuweisen, dass es weder technisch noch auf der Basis des geltenden Datenschutzrechtes um eine solche Ersetzung menschlicher Entscheidung durch die KI geht, sondern allein um ihren unterstützenden Einsatz zur Vorbereitung menschlicher Entscheidungen, zur Ermöglichung, Erleichterung und vor allem auch Bestätigung polizeipraktischer Arbeit.<sup>32</sup> Auch jenseits der Dystopie stellen sich hier vielfältige rechtspraktische und rechtsdogmatische Fragen, die auch mit dem AI-Act oder der Rechtsprechung des BVerfG bislang noch unzureichend gelöst sind.

Hinzu kommen praktische Probleme: So hängt die Qualität der mit einer KI erzeugten Ergebnisse von der Qualität der Ausgangsdaten einschließlich der Trainingsdaten zur Entwicklung der KI selbst ab. Die bislang nicht im Einzelnen rekonstruierbare Fehlerquote bleibt relevant und zugleich unkalkulierbar.<sup>33</sup> Das grundsätzlich produktive Halluzinationspotential einer KI scheint nicht einmal mit den Mitteln künstlicher Intelligenz erfassbar zu sein.

Gerade die vielen Unwägbarkeiten wirken auch auf den rechtlichen Zugriff zurück und zeigen die praktischen Grenzen der präzisen rechtlichen Erfassung von KI auf, die sich in offenen Rechtsgrundlagen niederschlagen. Hinreichende Bestimmtheit wäre aber wiederum eine zentrale Voraussetzung für die verfassungsrechtliche Akzeptanz dieser dynamischen und vielfältigen Technologie. Auch hiermit hängt zusammen, dass Sicherheit durch KI sich aus der Perspektive des Rechts weitgehend in Sicherheit vor KI verwandelt.

Im Unterschied zu den Gesetzgebungsorganen auf Landes- Bundes- und Unionsebene verfolgt das Bundesverfassungsgericht allerdings keine »Regulierungsstrategie« im eigentlichen Sinne. Es ist als Gericht, das nur verfahrensbezogen auf Antrag tätig wird, auch nicht zur gestaltenden Regulierung politischer Sachverhalte aufgerufen. Mit seiner detaillierten Verhältnismäßigkeitsrechtsprechung und den strikten Vorgaben im Hinblick auf die rechtsstaatliche geforderte Bestimmtheit steckt es allerdings den Rahmen der nationalen Gesetzgebung in den grundrechtsrelevanten Bereichen sehr präzise ab und gibt

---

31 Zu den Herausforderungen, die sich hieraus ergeben Wischmeyer 2020.

32 So auch Golla 2021, S. 672 Fn. 53 mit Verweis auf Art. 11 JI-RL, § 54 BDSG und das entspr. Landesrecht. Zu den sich gleichwohl auch hieraus ergebenden Herausforderungen für die Verantwortungsarchitektur Rademacher 2020, S. 45 ff.

33 Zu Berichten über Techniken der Iris-Erkennung s. Spehr, Gesichtserkennung statt Geheimzahl, in: Frankfurter Allgemeine Zeitung (FAZ), 08.11.2024. <https://www.faz.net/aktuell/technik-motor/digital/gesichtserkennung-statt-geheimzahl-110086874.html> (01.10.2025); Kugelmann/Buchmann 2024, S. 1 mwN.

damit dem Gesetzgeber in vielen Bereichen eine grundrechtsgebundene und freiheitssichernde Regulierungsstrategie vor.

In diesem Sinne soll der in der Tendenz »prohibitive« Ansatz des Bundesverfassungsgerichts,<sup>34</sup> der sich bereits in der Entscheidung zu hessenDATA abzeichnet und ausdrücklich als Teil einer konsequenten sicherheitsverfassungsrechtlichen Rechtsprechungslinie angesehen wird, als Ausdruck einer verfassungsgebundenen restriktiven Regelungsstrategie verstanden werden, deren Ziel der möglichst weitgehende Schutz des Rechts auf informationelle Selbstbestimmung ist.<sup>35</sup>

Während das deutsche Verfassungsrecht den Einsatz von KI in der Polizei hohen Rechtfertigungslasten unterwirft, scheint das produktbezogene EU-Recht zwar ebenfalls die Gefährlichkeit der Technik in den Vordergrund zu stellen, begründet mit den ausdrücklichen Ausnahmen und Regelungen für die Sicherheitsbehörden allerdings im Regelfall die Zulässigkeit einer entsprechenden Verwendung künstlicher Intelligenz und folgt so einem wenn nicht gegenläufigen, zumindest aber unterschiedlichen Ansatz.

Mit der Bindung an die Grundrechte der EU-Grundrechtecharta und eine in diesem Kontext noch wenig ausgeprägte Grundrechtsrechtsprechung des EuGH bleibt aber auch das EU-Recht offen für eine engere Auslegung und höhere Bindungen. Auch in diesem EU-rechtlichen Regulierungsrahmen bleiben die gesetzliche Ermächtigung zu einem Einsatz von KI ebenso wie ihre polizeiliche Nutzung vorrangig die Aufgabe der mitgliedstaatlichen (und das heißt für Deutschland Landes-)Gesetzgeber und der Sicherheitsbehörden auf der Landesebene.

Jede Regulierung wird durch die Tatsache erschwert, dass Erfahrungen zum polizeilichen KI-Einsatz in der Praxis wie auch schon in der Entwicklung fehlen<sup>36</sup> – oder jedenfalls empirisch schwer zu ermitteln sind, da den Polizeibehörden auf unsicherer Rechtsgrundlage ein Einsatz von KI kaum möglich ist und auch Auskünfte außerhalb bekannter Projekte jedenfalls selbst zu Forschungszwecken kaum erteilt werden. Empirische Studien zum Einsatz von KI in Deutschland beschränken sich notwendig auf den Rahmen dessen, was bislang erlaubt und möglich ist und betreffen folglich eher unproblematische Felder wie etwa der raum- und zeitbezogenen Kriminalitätsvorhersage.<sup>37</sup> Angesichts der Bedeutung

34 Zu einer möglichen Entwertung der Big-Data-Technologie Broemel/Trute 2016, S. 52 f.; ferner bereits Trute 2019 zu Predictive Policing.

35 Zur verfassungsrechtlichen Konzeption informationeller Selbstbestimmung s. nur Britz 2010.

36 Auch die Entwicklung und das Training an Echt Daten setzen eine belastbare Rechtsgrundlage, qualitativ akzeptable Daten und geschlossene Datenräume voraus. Es ist fraglich, ob US- und chinesische Systeme auf den sich kulturell und rechtlich signifikant unterscheidenden Rechtsraum übertragen werden können.

37 In diese Richtung schon Broemel/Trute 2016, S. 50 ff.

und auch rasanten Weiterentwicklung von KI stellt sich umso drängender die Frage, ob es unabhängig von den notwendig zu beantwortenden rechtlichen Herausforderungen denkbar, praktisch möglich und politisch wünschenswert ist, angesichts der Unzulänglichkeiten, Fehler und Risiken von KI den Sicherheitsbehörden den (notwendig verantwortungsvollen und rechtlich disziplinierten) Rückgriff auf diese omnipräsente Zukunftstechnik im Umgang mit digitalen Daten über hohe Verwendungshürden praktisch zu verwehren.<sup>38</sup>

## 5. Sicherheit durch KI als Anliegen operativer Sicherheitsgesetzgebung

Im Unterschied zum Verfassungsrecht, das vor allem Grenzen setzt, bezweckt das Fachrecht in erster Linie die Ermöglichung des KI-Einsatzes. Da nach der Volkszählungsentscheidung des BVerfG kein personenbezogenes Datum belanglos ist, bedarf jedenfalls der Zugriff auf personenbezogene Daten stets einer einfachrechtlichen gesetzlichen Ermächtigungsgrundlage.<sup>39</sup>

Neben Hessen, NRW und Bayern verfügen noch Sachsen-Anhalt und seit diesem Jahr auch Rheinland-Pfalz über eine Ermächtigung zur automatisierten Datenanalyse. Auch Baden-Württemberg hat sich jüngst für die Einführung einer entsprechenden Regelung entschieden. Die Hamburgische Ermächtigungsgrundlage wurde mit der hessischen – noch bevor sie überhaupt angewendet worden war – verworfen, die hessische allerdings im Anschluss an die Entscheidung des Gerichts geändert neu erlassen.<sup>40</sup>

Für den Bund sah ein der Diskontinuität zum Opfer gefallener Entwurf aus dem Januar 2025 entsprechende Änderungen des BPolG, des BKAG und auch der StPO zur Einführung der automatisierten Datenanalyse sowie einer Ermächtigung zum nachträglichen biometrischen Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet vor. Angesichts der Tatsache, dass Bayern bereits seit einigen Jahren mit Palantir in der Erprobung und nun seit Dezember 2024 auch offiziell arbeitet und darüber hinaus einen Rahmenvertrag für den Bund und alle Bundesländer mit dem Unternehmen abgeschlossen hat, der ohne

---

38 Alternative Überlegungen bei Brenneis/Schöndorf-Haubold, in diesem Band; kritisch auch Volkman 2025.

39 BVerfGE 65, 1 (Volkszählung).

40 § 25a Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung der Bekanntmachung vom 14.01.2005, zuletzt geändert durch Gesetz vom 13.12.2024, GVBl. 2024 Nr. 83; auch gegen den neuen § 25a HSOG wurde bereits Verfassungsbeschwerden erhoben, s. Giogios, in diesem Band.

weitere Ausschreibung den Abschluss weiterer Verträge ermöglicht, ist damit zu rechnen, dass der neue Bundesinnenminister das bayerische Projekt einer Bundes-VeRA wieder aufgreift, dem die frühere Innenministerin eine Absage erteilt hatte.

In grundsätzlicher Anerkennung der Effektivitätsgewinne beim Einsatz automatisierter Datenverarbeitungsmethoden bei der vorbeugenden Bekämpfung schwerer Straftaten hat das BVerfG die zugrundeliegenden Rechtsgrundlagen in Hessen und in Hamburg gleichwohl für verfassungswidrig erklärt und seine Rechtsprechung zu den Voraussetzungen und Anforderungen an den automatisierten Umgang mit personenbezogenen Daten im Bereich des Sicherheitsrechts konsequent weiter konkretisiert.

## 6. Sicherheit vor KI als verfassungsrechtliche Schranke operativer Sicherheitsgesetzgebung

In der Sache ging es in der Entscheidung vom 16. Februar 2023 zu hessenDATA, um eine bzw. mehrere Verfassungsbeschwerden gegen zwei praktisch gleichlautende Normen des hessischen und des hamburgischen Polizeirechts, durch die Polizeibehörden ermächtigt wurden, in Einzelfällen zur vorbeugenden Bekämpfung schwerer Straftaten oder zur Abwehr qualifizierter Gefahren bereits rechtmäßig erhobene personenbezogene Datenbestände mit Hilfe automatisierter Anwendungen weiterzuverarbeiten. Mit Hilfe der Analyseplattform hessenDATA wurden (und werden) bisher unverbundene Datenbestände vernetzt, um Zusammenhänge zwischen Personen, Gruppen oder Institutionen zu identifizieren, die in der händischen Analyse wenn überhaupt nur mit erheblichem Aufwand aufzufinden wären.

Die Entscheidung bietet dem Gericht die Gelegenheit, seine Rechtsprechung zum Recht auf informationelle Selbstbestimmung im Bereich des Polizeiinformationsrechts weiter zu entwickeln und für die algorithmenbasierte automatisierte Datenverarbeitung zu präzisieren. Eine klare Unterscheidung zwischen unterschiedlichen Formen künstlicher Intelligenz wird dabei (noch) nicht getroffen; selbst lernende Systeme finden, ohne Gegenstand der Entscheidung zu sein, in den Ausführungen zur möglichen Eingriffsschwere aber ausdrückliche Erwähnung.<sup>41</sup>

Entscheidend ist für das Gericht das mit einer automatisierten Datenverarbeitung verbundene Eingriffsgewicht, das bei Einsatz künstlicher Intelligenz und

---

<sup>41</sup> Zu den Einzelheiten der Entscheidung s. die Beiträge von Rabe und Giogios, in diesem Band, xxx.

insbesondere selbst lernender Systeme zusätzlich erhöht wird. Der Bestimmung des Eingriffsgewichts kommt die zentrale Bedeutung für die Rechtfertigungshürden einer Maßnahme zu: Je höher das Eingriffsgewicht, desto umfangreicher die Sicherungen und desto höher auch die Eingriffsschwelle – in der polizeirechtlichen Dogmatik also die Anforderungen an den Eingriffsanlass, regelmäßig das Vorliegen einer konkreten Gefahr als hinreichend wahrscheinlicher Schadensrealisierung.

Komplexe Methoden werden per se als eingriffsintensiv bewertet, ein Verzicht auf bestimmte Methoden (in der Prüfung ihrer Zulässigkeit zirkulär) als eingriffsmindernd. Die Eingriffsintensität einer automatisierten Datenanalyse hat das Gericht in Abhängigkeit von der Komplexität und den Risiken der Verarbeitungsmethode umso höher bewertet und in dieser Logik der Verwendung lernfähiger KI-Systeme ein besonderes Eingriffsgewicht attestiert. Es hat dabei eine ganze Reihe von Risiken aufgelistet:

»Wenn die Polizei aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen, daraus neue Zusammenhänge erschließen, aus mehrstufigen Analysen neue Verdachtsmomente erzeugen und hieran weitere Analyseschritte oder operative Maßnahmen anschließen kann, können die Nachteile auf Grund einer automatisierten Datenanalyse oder -auswertung für die Betroffenen erheblich sein und das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen. Bei komplexen Formen des Datenabgleichs besteht zudem mit Blick auf individuellen Rechtsschutz und aufsichtliche Kontrolle und die dafür unerlässliche Möglichkeit, Fehler zu erkennen und zu korrigieren, die Schwierigkeit der Nachvollziehbarkeit der eingesetzten Algorithmen. Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffssensitiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können.«<sup>42</sup>

»Besonderes Eingriffsgewicht kann je nach Einsatzart die Verwendung lernfähiger Systeme, also Künstlicher Intelligenz (KI), haben. Deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines ›predictive policing‹ getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen mensch-

---

42 BVerfGE 165, 363 (Automatisierte Datenanalyse, Rn. 90).

lichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein.«<sup>43</sup>

Sinkende staatliche Kontrollmöglichkeiten und die Gefahr eines schwer kontrollierbaren Zugriffs und Einflusses privater Anbieter etwa im Rahmen der Wartung der eingesetzten Systeme verstärken das Eingriffsgewicht weiter.

Die Konsequenz dieser Analyse und der gründlichen Auseinandersetzungen mit den Herausforderungen von KI sind eine deutliche Anhebung der Eingriffsvoraussetzungen und damit zuallererst der Anforderungen an den Gesetzgeber in der Schaffung der für den Einsatz erforderlichen Rechtsgrundlagen sowie in der Sache eine grundsätzliche Beschränkung des Einsatzes von KI auf bestimmte Situationen, in denen der Eingriffsanlass bereits konkretisiert gegeben ist:

»Ermöglicht die automatisierte Datenanalyse oder -auswertung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten, also nur zum Schutz besonders gewichtiger Rechtsgüter, sofern für diese eine zumindest hinreichend konkretisierte Gefahr besteht. Das Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter ist nur dann verfassungsrechtlich verzichtbar, wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten durch Regelungen insbesondere zur Begrenzung von Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahmen erheblich gemindert ist.«<sup>44</sup>

Diese Anforderungen beschränken und reduzieren aus verfassungsrechtlichen Gründen die Einsatzmöglichkeiten einer KI-gestützten Datenauswertung in erheblichem Maße und schließen gerade einen Rückgriff auf das besondere Potential der Generierung neuen Wissens durch KI unabhängig von konkreten Gefahrenverdachtslagen praktisch weitgehend aus.

Auch wenn die Entscheidung und die in ihr weiterentwickelten Anforderungen für das Polizeiinformationsrecht aus der Perspektive des deutschen Rechts auf informationelle Selbstbestimmung gleichwohl folgerichtig erscheinen, ist zweifelhaft, ob sie bei aller Berechtigung der Grundrechtssensibilität des KI-Einsatzes im klassischen verfassungsrechtlichen Zugriff den Besonderheiten und der praktischen Bedeutung der KI im Rahmen der Digitalisierung auch der Polizeiarbeit hinreichend gerecht werden. In der scheinbar mathematischen Addition des Eingriffsgewichts scheinen Effektivitätsgewinne und Gefahrenabwehrerfolge, die im Bereich der Sicherheitsgewährleistung jedenfalls in den Fällen der Terrorismusabwehr und der vorbeugenden Bekämpfung schwerwie-

---

43 BVerfGE 165, 363 (Automatisierte Datenanalyse, Rn. 100).

44 BVerfGE 165, 363 (Automatisierte Datenanalyse, LS 4).

gender Straftaten immer auch Sicherheitsgewinnen entsprechen, nicht ebenso mathematisch eingestellt werden zu können.

Die entscheidende Frage ist, ob den geschilderten Risiken des KI-Einsatzes nicht auch auf der Ebene der Verwendung des KI-generierten Wissens angemessen und grundrechtswahrend begegnet werden kann.<sup>45</sup> Bislang fehlen die rechtlichen Instrumente für eine angemessene Disziplinierung des KI-Einsatzes, die den zu Recht erkannten Grundrechtsrisiken auch ohne einen weitgehenden Verzicht auf den KI-Einsatz begegnen würden. Die klassische Dogmatik erweist sich hier nicht notwendig als einzige und am besten geeignete Antwort auf die Risiken automatisierter Datenverarbeitung und die Herausforderungen ihrer dynamisch rasanten Weiterentwicklung, ohne künstliche Intelligenz als schon heute annähernd unausweichliche neue Technologie für die Sicherheitsgewährleistung übermäßig zu beschränken oder sogar auszuschließen.

Hierzu trägt allerdings auch das EU-Recht nur wenig bei, da der produktspezifische Ansatz kaum materielle Anforderungen an die Grundrechtskompatibilität des KI-Einsatzes bereithält. Das EU-Recht verdrängt trotz des grundsätzlichen Anwendungsvorrangs das nationale Recht auch nicht, sondern lässt ihm im Gegenteil Raum, wenn es – hier speziell auf die Sicherheitsbehörden bezogen – den Einsatz von KI von den jeweiligen nationalen Ermächtigungen abhängig macht und damit gerade die Frage nach Eingriffsschwelle und Eingriffsintensität als den zentralen Parametern einer grundrechtlichen Verhältnismäßigkeitsprüfung dem nationalen Recht überlässt.<sup>46</sup> So behält auch die nationale Verfassungsrechtsprechung ihre Gültigkeit, und das Thema bleibt jedenfalls aus einer Grundrechtsperspektive ein in erster Linie nationalrechtliches.<sup>47</sup>

## 7. Sicherheit mittels KI als Gegenstand produktbezogener unionaler Binnenmarktregulierung

Das EU-Recht geht mit der KI-Verordnung<sup>48</sup> einen anderen Weg, indem es zukünftige KI-Verwendung vorrangig eher ermöglichen, denn begrenzen will und damit eine grundsätzlich andere Perspektive einnimmt. Nicht unumstritten

---

45 Hierzu Brenneis/Schöndorf-Haubold, in diesem Band.

46 So auch Kugelmann/Buchmann 2024, S. 5 ff.

47 Nichtsdestotrotz ist zu erwarten, dass der EuGH wie auch im Falle der Vorratsdatenspeicherungs-RL den grundrechtlichen Rahmen für eine sicherheitsrechtsrelevante EU-Gesetzgebung konkretisieren wird, s. bereits oben in Fn. 472.

48 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.06.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, ABl. EU Nr. L 2024/1689 v. 12.07.2024.

folgt die KI-Verordnung einem traditionellen binnenmarktorientierten Regelungsansatz, der in einer umfassenden produktbezogenen Regulierung auch Behörden und Verwaltung adressiert und auch nationale Reservatskompetenzen wie die Sicherheitsgewährleistung nicht ausnimmt.<sup>49</sup> Stärker zukunftsgerichtet will die Verordnung Entwicklung, Vertrieb und Einsatz von KI folglich umfassend steuern und damit die Voraussetzungen für einen verantwortungsvollen Wettbewerb von KI in der EU schaffen. Die überraschend detaillierten Ver- und Gebote für die mitgliedstaatlichen Polizei- und Sicherheitsbehörden<sup>50</sup> ergänzen die Produktregulierung um Verwendungsregelungen, die stärker im Datenschutz zu verorten sind und auf begründete, insb. kompetenzrechtliche Kritik gestoßen sind.<sup>51</sup> Je detaillierter die Regelungen gerade die Sicherheitsbehörden und nicht allgemeine Produkthanforderungen in den Blick nehmen, umso stärker stellt sich die umstrittene Kompetenzfrage, die in Bezug auf die (insb. operative) Gewährleistung innerer Sicherheit grundsätzlich klar zu Gunsten der Mitgliedstaaten zu beantworten ist.<sup>52</sup>

Auch wenn die EU keine Kompetenz für eine Vereinheitlichung des nationalen Polizei- und Sicherheitsrechts besitzt,<sup>53</sup> ist ihr kompetenzrechtlich gleichwohl nicht jeder Zugriff auf sicherheitsrechtliche Fragen versperrt.<sup>54</sup> Dies folgt zum einen bereits notwendig aus der Anerkennung einer geteilten Zuständigkeit im und für den Raum der Freiheit, der Sicherheit und des Rechts (Art. 4 Abs. 2 j) AEUV). Zum anderen deckt auch die Binnenmarktkompetenz des Art. 114 AEUV jedenfalls den regulierenden produktbezogenen Zugriff auf die Informationstechnologie unabhängig bzw. einschließlich ihrer Verwendung durch die Sicherheitsbehörden ab und wird dabei durch eine robuste Rechtsprechungspraxis des EuGH

---

49 Vgl. hierzu Schöndorf-Haubold/Giorgios 2024; s. auch Meyer 2025, S. 156 ff.; die Verordnung bringt klar zum Ausdruck, dass die Entwicklung, Inbetriebnahme oder Verwendung künstlicher Intelligenz (auch) zu Zwecken der Strafverfolgung oder der öffentlichen Sicherheit ungeachtet nationaler Erstzuständigkeiten in ihren Anwendungsbereich fallen. Mit der »nationalen Sicherheit« wird lediglich der Aufgabenbereich der Geheimdienste in Entsprechung zu Art. 4 Abs. 2 EUV vom Regelungszugriff der KI-Verordnung ausgenommen; zu dessen restriktiver Auslegung vgl. EuGH, Urt. v. 16.01.2024, C-33/22, Österreichische Datenschutzbehörde, ECLI:EU:C:2024:46, Rn. 46 ff.; zu Kompetenzfragen Pilniok, in: Dietrich/Pilniok 2024, § 4 Rn. 19; Buchheim, ebda. § 9.

50 Vgl. insb. Art. 3 Nr. 44 und 45, Art. 5 Abs. 1 lit. d, g, h, Abs. 2–7 KI-VO sowie Anhang II, Art. 6 Abs. 2 und iVm Anhang III Nr. 1, 6 und 7 und Art. 26 Abs. 10 und 11 KI-VO (Fn. 46).

51 S. Peuker 2023a, S. 388 ff.; Valta/Vasel 2021, S. 143; vermittelnd Buchheim, in: Dietrich/Pilniok 2024, § 9 Rn. 49 f.: »sovereigns in sovereignty-respecting chains«.

52 So auch Peuker 2023a, S. 388 ff.; Valta/Vasel 2021, S. 143.

53 Dazu auch Schöndorf-Haubold, in: Ehlers/Fehling/Pünder 2021, § 68 Rn. 17 ff.

54 S. hierzu in Bezug auf den AI-Act Buchheim, in: Dietrich/Pilniok 2024, § 9.

gestärkt,<sup>55</sup> die keine Zweifel an einer Annexkompetenz für mitzuregelnde Fragen nationaler Sicherheitsgewährleistung zulassen will.<sup>56</sup>

Darüber hinaus begründet auch die sicherheitsinformativrechtliche JI-Richtlinie (EU) 2016/680<sup>57</sup> einen umfassenden Bezug zum EU-Recht ungeachtet der Tatsache, dass auch sie sich dem Vorwurf ausgesetzt sieht, ihren Anwendungsbereich über die Grenzen der unionalen Gesetzgebungskompetenz hinaus in Bereiche rein innerstaatlicher Sicherheitsgewährleistung zu überdehnen.<sup>58</sup> Zusammen mit Art. 16 AEUV und der in Titel V des AEUV vorgesehenen polizeilichen Zusammenarbeit ergibt sich daraus ein umfassender Regelungsanspruch für das Sicherheitsinformativrecht.<sup>59</sup>

Der übergreifende Regelungsansatz der KI-Verordnung knüpft an einen Binnenmarkt- und/oder Datenschutzbezug an, um die Kompetenz des EU-Gesetzgebers zu begründen. Ungeachtet ihrer Rechtsqualität als Verordnung bzw. Gesetz stellt sie keine Vollregelung dar,<sup>60</sup> sondern geht vom Erfordernis nationaler Ermächtigungsnormen für einen KI-Einsatz aus,<sup>61</sup> den das EU-Recht zwar teilweise detailliert reguliert, aber nicht bereits seinerseits auch ermöglicht. Dies eröffnet bzw. belässt Spielräume für die entsprechenden nationalen Regelungen unter Einschluss etwaiger begrenzender grundrechtlicher Standards für den Einsatz und die Verwendung von KI-Systemen, die im Anwendungsbereich der EU-Grundrechtecharta zukünftig auch vom EuGH gesetzt werden könnten.<sup>62</sup>

---

55 S. schon EuGH, Urt. v. 20.05.2003, C-465/00, ORF, ECLI:EU:C:2003:294, Rn. 41 mwN.

56 Vgl. Peuker 2023a, S. 390; Peuker 2023b, S. 540 f.

57 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, ABl. EU 2016 Nr. L 119/89; zum Zusammenspiel s. auch Rabe/Geminn/Johannes, in diesem Band.

58 S. insb. die Subsidiaritätsrüge des Bundesrates, Beschluss v. 30.03.2012, BR-Drs. 51/12.

59 Peuker 2023a, S. 390 ff.; zur – unbegrenzten – Reichweite des unionalen Polizeiiinformativrechts und zum Anspruch des EuGH, damit verbundene Grundrechtseingriffe am Maßstab der EU-Grundrechtecharta zu überprüfen, s. EuGH, Urt. v. 04.10.2024, C-548/21, CG/Bezirkshauptmannschaft Landeck, ECLI:EU:C:2024:830.

60 Zu den unterschiedlichen kompetenziellen Anforderungen an Vollregelungen im Unterschied zu konkretisierungsbedürftigen Mindestanforderungen s. Peuker 2023a, S. 396 f. mwN.; Buchheim, in: Dietrich/Pilniok 2024, § 9.

61 Vgl. z. B. Art. 5 Abs. 5 KI-Verordnung (EU) 2024/1689 (Fn. 46) für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme.

62 Die Entscheidungspraxis zur Vorratsdatenspeicherung stellt einen vergleichbaren Sachverhalt dar; s. EuGH, Urt. v. 30.04.2024, C-470/21, La Quadrature du Net, ECLI:EU:C:2024:370; s. zu grundrechtlichen Anforderungen im Bereich des Polizeiiinformativrechts auch EuGH, Urt. v. 04.10.2024, C-548/21, CG/Bezirkshauptmannschaft Landeck, ECLI:EU:C:2024:830 zum polizeilichen Zugriff auf die Daten auf einem sichergestellten Mobiltelefon.

In der Sache normiert die am 2. August 2024 in Kraft getretene KI-Verordnung<sup>63</sup> eine risikobasierte Systematik mit unterschiedlichen Stufen und unterscheidet – grundsätzlich übergreifend und technologieneutral zwischen vier Risikostufen:<sup>64</sup> Auf der höchsten Risikostufe stehen sog. verbotene Praktiken vor sog. Hochrisiko-KI-Systemen, KI-Systemen mit begrenztem Risiko und solchen mit lediglich geringem oder keinem Risiko. Vor allem für die Hochrisikosysteme sieht die Verordnung umfangreiche Dokumentations-, Informations- und Aufklärungspflichten vor.

Interessant wird es aus der regulierungsrechtlichen Perspektive einerseits in der Kategorie der zulässigen Hochrisikosysteme, der ausdrücklich auch eine Reihe von sicherheitsrechtlichen Einsatzszenarien zugeordnet werden. Hier werden Anbieter, Betreiber und Produkthersteller zum Teil noch ungeklärten Pflichten unterworfen, die jedenfalls bei marktgängigen Produkten eher zu einer Hemmung der Entwicklung solcher Systeme führen könnten.

KI-Systeme für eine sicherheitsbehördliche Verwendung stellen insoweit einen Sonderfall dar, als sie ausdrücklich und in systematischer Abweichung von der produktbezogenen Regulierung in ihrer Verwendung beschränkt werden. Die Verordnung enthält damit Regelungen, die auch, aber nicht in erster Linie die privaten Entwickler der geeigneten KI-Systeme verpflichten und darüber hinaus unmittelbar den KI-Einsatz durch die übergreifend als Strafverfolgungsbehörden bezeichneten Sicherheitsbehörden betreffen:<sup>65</sup>

Auf der höchsten Risikostufe der – eigentlich – verbotenen Praktiken im KI-Bereich ordnet Art. 5 KI-VO eine Reihe von sicherheitsrelevanten und in erheblichem Maße grundrechtssensiblen KI-Verwendungen ein, zu denen etwa Systeme eines automatisierten Profilings zur alleinigen, abschließenden und nicht bloß unterstützenden Risikobewertung der Begehung von Straftaten sowie KI-Systeme, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern, gehören. Insbesondere die in den Gegenausnahmen versteckten positiven Regelungen sind für den Einsatz von KI durch die Si-

---

63 Zur Anwendung kommen die Regelungen allerdings aufgrund der Übergangsbestimmungen in Art. 111 und 113 KI-Verordnung insb. auch für bereits in Betrieb genommene Systeme zum Teil seit dem 2.2.2025 (Art. 1–5), zum Teil seit dem 2.8.2025, zu weiten Teilen aber auch erst ab dem 02.08.2026 bzw. Art. 6 Abs. 1 ab dem 2.8.2027.

64 S. auch Rabe/Geminn/Johannes, in diesem Band. Allgemein zur Regelungssystematik der KI-Verordnung s. nur Krönke 2024, S. 529 ff.; Roth-Isigkeit 2024, S. 15 ff.

65 Bereits in den Begriffsbestimmungen bezieht die KI-Verordnung Strafverfolgungsbehörden mit präventiven wie repressiven Zuständigkeiten in den Anwendungsbereich der Verordnung ein und erhebt damit einen klaren Regelungsanspruch ihnen gegenüber; vgl. Art. 3 Nr. 45 und 46 der KI-VO (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (s. bereits oben in Fn. 53).

cherheitsbehörden relevant – etwa im Rahmen des lediglich unterstützenden *Profiling*s, das sich nach Art. 5 Abs. 1 d) KI-VO »bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen«. Das grundsätzliche Verbot wird hier mit Auflagen für die Sicherheitsbehörden gelockert.

Ähnlich, allerdings noch weit ausführlicher gilt dies für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme<sup>66</sup>, deren grundsätzliches Verbot die Folie für eine ausführliche Regulierung ihres Einsatzes zu Strafverfolgungszwecken zu bilden scheint. So ist eine Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen nach Art. 5 Abs. 1 h) KI-VO ungeachtet des Verbots dann zulässig, wenn sie zur Erreichung bestimmter höherrangiger Ziele unbedingt erforderlich ist, wie etwa zur gezielten Suche nach Opfern schwerer Verbrechen oder Vermissten, zur Abwehr dringender Terrorgefahren oder von akuten Gefahren für Leib und Leben oder zur gezielten Suche nach Strafverdächtigen, die im Verdacht stehen, eine der im Anhang II aufgeführten schweren Straftaten begangen zu haben.

In Anbetracht der besonderen Grundrechtssensibilität der Echtzeit-Fernidentifizierung unterwirft Art. 5 Abs. 2 der KI-VO diesen Ausnahmetatbestand weiter einem konkreten Einzelfallbezug zur Identifizierung einer speziell betroffenen Person sowie einer doppelten Folgenabwägung der Verwendung bzw. Nichtverwendung des Systems. Der Einsatz eines solchen Systems setzt darüber hinaus eine gesetzliche Ermächtigung durch den Mitgliedstaat voraus, die in weiteren Absätzen des Artikels präzisiert werden. Hier verlässt die KI-VO ihren eigenen Regelungsansatz und verfolgt jedenfalls punktuell ein gleichermaßen sicherheitspolitisches wie datenschutzrechtliches Anliegen.

Im Hinblick auf die sog. Hochrisiko-KI-Systeme verweist Art. 6 Abs. 2 KI-Verordnung hinsichtlich der nächsten Risikostufe lediglich auf Anhang III, der in Nr. 6 den sicherheitsbehördlichen KI-Einsatz betrifft: Hier werden u.a. KI-Systeme zur Risikobewertung, als Lügendetektor, zur Erstellung von Personenprofilen oder zur Bewertung von Beweismitteln als Hochrisikosysteme qualifiziert.

Angesichts der zum Teil offenen Verwendungsbeschreibungen einerseits und der zunehmenden Komplexität der Analyse großer Datenmengen andererseits liegt es nahe, sicherheitsbehördliche KI-Systeme sowohl im Bereich der prognostischen Gefahrenabwehr als auch im Rahmen der ermittlungs- und beweisbezogenen Strafverfolgung regelhaft (und auch im Zweifel mindestens) als Hochrisi-

---

66 Kritisch zur Differenzierung zwischen nachträglicher und Echtzeit-Fernidentifizierung Coombe 2024, S. 262 ff.

kosysteme zu behandeln. Ausnahmslos gilt das nach Art. 6 Abs. 3 UAbs. 3 für jede Form des Profilings natürlicher Personen.<sup>67</sup>

Art. 6 Abs. UAbs. 2 der VO scheint aber Ausnahmen zuzulassen für Systeme zur Durchführung »eng gefasster Verfahrensaufgabe[n]« und für Systeme, denen nur (und wohl auch ausschließlich) eine vorbereitende Aufgabe für eine Bewertung im Sinne von Anhang III zukommt. Die Verordnung vermutet in diesen Fällen das Fehlen eines wesentlichen Einflusses auf das Ergebnis der Entscheidungsfindung und schließt damit schon das Risiko einer erheblichen Grundrechtsbeeinträchtigung aus.

Funktionalität wie auch Grundrechtssensibilität komplexer KI-Systeme sprechen demgegenüber für einen sehr begrenzten Anwendungsbereich dieser ohnehin eng auszulegenden Ausnahmebestimmung. Es ist schwer vorstellbar, dass KI-fähige Anwendungen zur automatisierten Datenanalyse wie z.B. hessenDATA, sofern mit ihrer Hilfe (schon aufgrund nationaler Grundrechtsanforderungen ausschließlich vorbereitende) Such- und Musterabfragen vorgenommen werden, als Systeme mit minimalen Risiken unterhalb der Schwelle der Hochrisiko-KI gelten könnten, für die die Verordnung lediglich Rahmenregelungen für Anbieter und Betreiber bereithält. Jedenfalls jeder gezielte relevante Personenbezug dürfte auch jenseits der Gegenausnahme für das Profiling die Einordnung als Hochrisikosysteme rechtfertigen.<sup>68</sup>

Auch die Einstufung als Hochrisikosystem löst aber nicht Mechanismen des Grundrechts- und Datenschutzes, sondern das von der KI-Verordnung normierte produktsicherheitsbezogene Konzept der System-Regulierung aus<sup>69</sup>, so dass zum jetzigen Zeitpunkt Fragen des Grundrechts- und Datenschutzes jenseits der generellen datenschutzrechtlichen Anforderungen der JI-Richtlinie weitgehend den einzelstaatlichen Ermächtigungsgrundlagen und ihrer etwaigen verfassungsrechtlichen Kontrolle durch nationale Verfassungsgerichte überlassen bleiben.

---

67 S. auch insb. Anhang III Nr. 6 der KI-VO (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.

68 Zustimmend Bäuerle 2025, S. 131.

69 Ungeachtet dessen fordert die Art. 5 Abs. 2 S. 2 KI-VO (EU) 2024/1689 eine Grundrechtsfolgenabschätzung als (vorrangig) prozedurale Sicherung; vgl. dazu Hilgendorf/Härtlein 2025, Art. 5 Rn. 64 ff., 95 ff.

## 8. KI im Einsatz der Sicherheitsbehörden zwischen operativer Effektivität, produktspezifischer Qualität und individueller Freiheitssicherung

Gemeinsam ist den so verstandenen Regulierungsstrategien die Entscheidung für eine grundsätzliche Zulassung des KI-Einsatzes sowie ein flankierendes Schutzrecht, das nicht zwangsläufig ausschließlich subjektiv-rechtliche gedacht werden muss. Zu erwarten ist eine weitere Verbreitung und technische Fortentwicklung der Einsatzoptionen künstlicher Intelligenz sowie auch eine (Leit-)Entscheidung des EuGH zu grundrechtlichen Mindeststandards für die entsprechenden Bestimmungen der KI-Verordnung.

Die Beobachtung eines prioritären Interesses an der Disziplinierung des KI-Einsatzes bzw. der KI hat ungeachtet ihrer unzweifelhaften Berechtigung zirkuläre Konsequenzen und Rückwirkungen auf den gesetzgeberischen Umgang mit KI. Führt die gesteigerte Komplexität der Technik zu einem erhöhten Eingriffsgewicht, dem wiederum (nur) mit einer Verschärfung der Eingriffsschwelle begegnet werden soll, werden Formen der anlassunabhängigen, musterbasierten Wissensgenerierung mithilfe von KI jedenfalls in der Konsequenz der klassischen sicherheitsverfassungsrechtlichen Rechtsprechungslinie des Bundesverfassungsgerichts praktisch ausgeschlossen. Verfassungsrechtlich unausweichlich ist dies angesichts der vielfältigen unterschiedlichen Parameter, die in die Bewertung der Eingriffsschwere einerseits und der Rechtfertigungsregimes andererseits einfließen, nicht.

Die eigentliche zentrale Herausforderung stellt ein sowohl produktbezogenes als auch grundrechtssensibles Regulierungs-Modell für den sicherheitsbehördlichen KI-Einsatz dar, das zum einen Innovation und Entwicklung ermöglicht und die Verwendung intelligenter Systeme auch nicht grundsätzlich ausschließt oder auf traditionelle Funktionen begrenzt, das aber andererseits auch die Risiken der fehlenden Nachvollziehbarkeit, der Fehleranfälligkeit, der möglichen und systembedingten Verzerrungen, der Abhängigkeit von Datenmaterial, Datenqualität und Trainingserfolgen, der kaum vorhersehbar beschleunigten Dynamik, der Manipulationsgefahr etc. weder ausblendet, noch unterschätzt, sondern hierfür verfassungsrechtlich hinreichende Antworten findet; ein Regulierungsmodell also, das im Wege einer progressiven Steuerung verbunden mit einer konservativen Disziplinierung der Schlüssel für eine gleich effektiv wie verantwortungsvolle Sicherheitsgewährleistung durch KI ist.<sup>70</sup>

---

<sup>70</sup> Zu übergreifenden Vorschlägen für Regelungsstrukturen und Regulierungsansätze s. Pilniok 2022, S. 1021 ff.; Wischmeyer 2023, S. 1 ff.; für einen verantwortlichen Umgang mit Technikkritik Bull 2019,

Anknüpfungspunkte finden sich bereits in der KI-Verordnung: So können die Einrichtung von Reallaboren und die Erprobung von KI-Systemen in abgegrenzten Sandboxes auch im Bereich der Sicherheitsgewährleistung nach Art. 59 Abs. 1 und 2 KI-VO genutzt werden. Rechtsdogmatische Ansätze für eine grundrechts- und innovationskompatible Lösung könnten alternative Grundrechtssicherungen sein: In Betracht kämen beispielsweise eine Neubewertung der Eingriffsintensität einzelner KI-gestützter Verarbeitungsvorgänge, die Aufgabe der dogmatisch ohnehin begründungsbedürftigen Überwachungsgesamtrechnung, ein Ausgleich durch strengere Prüfung und Anforderungen der Verwendung der KI-generierten Ergebnisse, eine strikte Diskriminierungskontrolle, Bestimmtheitsanforderungen an den Gesetzgeber im Rahmen des technisch Möglichen, Transparenz und Datenschutzkontrolle oder ggf. Verbandsklagen durch Computerverbände, um Wissens-Asymmetrien und Kontrolldefizite auszugleichen. Hier ist die weitere Rechtsentwicklung auch auf das intra- und interdisziplinäre Gespräch und das Verstehen der ethischen und technischen Hintergründe angewiesen.<sup>71</sup>

Es bleibt die Aufgabe der nationalen Gesetzgeber auf Bundes- und Landesebene, für die Verwendung künstlicher Intelligenz durch die Polizei(en) einen objektivrechtlichen qualitätssichernden Ansatz zu wählen, der insbesondere Datenqualität und Datensicherheit gewährleistet, Rechte- und Rollenkonzepte einrichtet und Datenschutz by design einfordert, um opake Techniken der Wissensgenerierung trotz der bekannten (und unbekanntenen) blackbox-Phänomene im Rahmen des Möglichen transparent und kontrollierbar zu machen und verfassungsrechtliche Rechtfertigungslasten aufzuerlegen, ohne den Einsatz von KI in der Polizei und durch die Polizei zwangsläufig weitgehend auszuschließen.

## Quellen und Literatur

- Bäuerle, Michael, »Automatisierte und KI-gesteuerte Datenverarbeitung und -analyse bei den Sicherheitsbehörden«, in: *Zeitschrift für Datenschutz (ZD)* 2025, S. 128–132.
- Britz, Gabriele, »Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts«, in: Hoffmann-Riem, Wolfgang (Hg.), *Offene Rechtswissenschaft*, Tübingen 2010, S. 561–596.
- Broemel, Roland/Trute, Hans-Heinrich, »Alles nur Datenschutz? Zur rechtlichen Regulierung algorithmenbasierter Wissensgenerierung«, in: *Berliner Debatte Initial* 2016, S. 4–65.

---

S. 57 ff.; vgl. auch den an der individualrechtlichen Linie des BVerfG orientierten Ansatz von Brenneis/Schöndorf-Haubold, in diesem Band.

<sup>71</sup> Vgl. dazu die Beiträge in diesem Band.

- Buchheim, Johannes, »Sovereigns in chains? Art. 4(2) sent. 3 TEU and EU law constraints on the use of AI in national security contexts«, in: Dietrich, Jan-Hendrik/Pilniok, Arne (Hg.): *European Security Union*, Baden-Baden 2024, § 9.
- Bull, Hans Peter, »Über die rechtliche Einbindung der Technik. Juristische Antworten auf Fragen der Technikentwicklung«, in: *Der Staat* 58 (2019), S. 57–100.
- Bull, Hans Peter, »Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit«, in: van Ooyen, Robert/Möllers, Martin (Hg.): *Handbuch Bundesverfassungsgericht im politischen System*, 3. Auflage, Wiesbaden 2025, S. 1275–11312.
- Bundesrat, »Priorisierung, auskömmliche Finanzierung und rechtssichere Implementierung eines gemeinsamen Datenhauses für die Informationsverarbeitung der Polizeien des Bundes und der Länder – Neuausrichtung polizeilicher IT (P20) sowie interimswise zeitnahe Bereitstellung einer gemeinsam betriebenen automatisierten Datenanalyseplattform«, EntschlieÙung vom 21.3.2025, Bundesrat Drs. 58/25 (Beschluss).
- Coombe, Jason, »Die Fehlbewertung der nachträglichen biometrischen Fernidentifizierung in der KI-VO«, in: *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* 2024, S. 262–266.
- Gemmin, Christian, »Zur Institutionalisierung einer Überwachungsgesamtrechnung«, in: *Die Öffentliche Verwaltung (DÖV)* 2022, S. 789–795.
- Golla, Sebastian, »Algorithmen, die nach Terroristen schürfen – »Data-Mining« zur Gefahrenabwehr und zur Strafverfolgung«, in: *Neue Juristische Wochenschrift (NJW)* 2021, S. 667–672.
- Hilgendorf, Eric/Härtlein, Johannes, *Verordnung über künstliche Intelligenz: KI-VO*, Baden-Baden 2025.
- Krönke, Christoph, »Das europäische KI-Gesetz: Eine Verordnung mit Licht und Schatten«, in: *Neue Zeitschrift für Verwaltungsrecht (NVwZ)* 2024, S. 529–534.
- Kugelman, Dieter/Buchmann, Antonia, »Der Algorithmus und die Künstliche Intelligenz als Ermittler«, in: *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* 2024, S. 1–10.
- Kuhlmann, Simone/Trute, Hans-Heinrich, »Predictive Policing als Formen polizeilicher Wissensgenerierung«, in: *Zeitschrift für das Gesamte Sicherheitsrecht (GSZ)* 2021, S. 103–111.
- Lindner, Josef Franz/Unterreitmeier, Johannes, »Überwachungsgesamtrechnung: Karlsruhe calculat?«, in: *JuristenZeitung (JZ)* 2022, S. 915–923.
- Löffelmann, Markus, »Die Überwachungsgesamtrechnung«, in: *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)* 2024, S. 18–22.
- Meyer, Simon Diethelm, »Der Einsatz künstlicher Intelligenz durch Sicherheitsbehörden«, in: *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)* 2025, S. 156–161.
- Peuker, Enrico, »Datenschutz als Annexkompetenz – Zu Kompetenzgrenzen der europäischen KI-Regulierung im Bereich der Gefahrenabwehr und Strafverfolgung durch die Mitgliedstaaten«, in: *Zeitschrift für Digitalisierung und Recht (ZfDR)* 2023a, S. 384–397.
- Peuker, Enrico, »Unionsrechtliche Regelungskompetenzen im Bereich der nationalen Sicherheit – Zur Auslegung von Art. 4 Abs. 2 S. 3 EUV unter kritischer Würdigung der EuGH-Rechtsprechung«, in: *Europarecht (EuR)* 2023b, S. 535–563.
- Pilniok, Arne, »Administratives Entscheiden mit Künstlicher Intelligenz: Anwendungsfelder, Rechtsfragen und Regelungsbedarfe«, in: *JuristenZeitung (JZ)* 2022, S. 1021–1031.
- Pilniok, Arne, »Governance of the European Security Union«, in: Dietrich, Jan-Hendrik/Pilniok, Arne (Hg.): *European Security Union*, Baden-Baden 2024, § 4.

- Poscher, Ralf/Kilchling, Michael/Landerer Lukas, »Ein Überwachungsbarometer für Deutschland. Entwicklung eines Konzeptes zur periodischen Erfassung staatlicher Überwachungsmaßnahmen«, in: *Zeitschrift für das gesamte Sicherheitsrecht (GSZ)* 2021, S. 225–232.
- Rademacher, Timo, »Predictive Policing im deutschen Polizeirecht«, in: *Archiv des öffentlichen Rechts (AöR)* 2017, S. 366–416.
- Rademacher, Timo, »Artificial Intelligence and Law Enforcement«, in: Wischmeyer, Thomas/Rademacher, Timo (Hg.): *Regulating Artificial Intelligence*, Cham 2020, S. 225–255.
- Rademacher, Timo, »Künstliche Intelligenz und neue Verantwortungsarchitektur«, in: Eifert, Martin (Hg.), *Digitale Disruption und Recht*, Baden-Baden 2020, S. 45–72.
- Roßnagel, Alexander, »Überwachungs-Gesamtrechnung – Das BVerfG und die Vorratsdatenspeicherung«, in: *Neue Juristische Wochenschrift (NJW)* 2010, S. 1238–1242.
- Roth-Isigkeit, David, »Der neue Rechtsrahmen für Künstliche Intelligenz in der Europäischen Union«, in: *Künstliche Intelligenz und Recht (KIR)* 2024, S. 15–20.
- Schöndorf-Haubold, Bettina, »Europäisches Sicherheitsrecht«, in: Ehlers, Dirk/Fehling, Michael/Pünder, Hermann (Hg.): *Besonderes Verwaltungsrecht*, Bd. 3, 4. Aufl., Heidelberg 2021, § 68.
- Schöndorf-Haubold, Bettina/Giogios, Christopher, »KI im Einsatz für die Sicherheit – Innovation und Kontrolle im Spannungsfeld von europäischer Gesetzgebung und nationaler Souveränität«, in: *Verfassungsblog*, 10.12.2024. <https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/> (01.10.2025).
- Seckelmann, Margrit, »Einsatz bei der Polizei: Kommunikation, Online-Streifen, Trojaner, Facebook-Fahndung, Biometriesoftware, (intelligente) Videoüberwachung, Predictive Policing, Body-Cams und Fotodrohnen«, in: dies. (Hg.), *Digitalisierte Verwaltung. Vernetztes E-Government*, 3. Aufl., Berlin 2024, Kap. 21.
- Seidensticker, Kai, »Predictive Policing: Eine problembehaftete Methode der Kriminalprävention«, in: Diebel-Fischer, Hermann/Hellmig, Lutz/Tischler, Maya (Hg.): *Technik und Verantwortung im Zeitalter der Digitalisierung*, Rostock 2022, S. 193–219.
- Spehr, Michael, »Gesichtserkennung statt Geheimzahl«, in: *Frankfurter Allgemeine Zeitung (FAZ)*, 08.11.2024. <https://www.faz.net/aktuell/technik-motor/digital/gesichtserkennung-statt-geheimzahl-110086874.html> (01.10.2025).
- Trute, Hans-Heinrich, »Zur Entwicklung des Polizei- und Ordnungsrechts 2013–2019«, in: *Die Verwaltung* 2020, S. 99–118.
- Valta, Matthias/Johann Justus Vassel, »Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz – Mit viel Bürokratie und wenig Risiko zum KI-Standort?«, in: *Zeitschrift für Rechtspolitik (ZRP)* 2021, S. 142–145.
- Volkmann, Uwe, »Gefahrenerkennung durch Data-Mining«, in: *Hessische Verwaltungsblätter (HeVBl)* 2025, S. 101–108.
- Wischmeyer, Thomas, »Regulierung intelligenter Systeme«, in: *Archiv des öffentlichen Rechts (AöR)* 2018, S. 1–66.
- Wischmeyer, Thomas, »Künstliche Intelligenz und neue Begründungsarchitektur«, in: Eifert, Martin (Hg.), *Digitale Disruption und Recht*, Baden-Baden 2020, S. 73–92.
- Wojtas, Anna/Cipierre, Paula, »Wie Palantir die Digitalisierung deutscher Polizeien unterstützt«, in: *Palantir-Blog*, 03.03.2023. <https://blog.palantir.com/wie-palantir-die-digitalisierung-deutscher-polizeien-unterstutzt-3791d65bccb6> (01.10.2025).

# hessenDATA in rechtssoziologischer Perspektive – Rechtstatsächliche Aspekte der automatisierten Datenanalyse durch die hessischen Polizeibehörden

*Michael Bäuerle*

## 1. Einleitung

Das hessenDATA -Urteil vom Februar 2023<sup>1</sup> steht in einer langen Reihe von »Ja, aber...«-Entscheidungen des Bundesverfassungsgerichts zu informationellen Eingriffsbefugnissen der Sicherheitsbehörden.<sup>2</sup> Aus verfassungsrechtlicher Perspektive stellen insoweit weder seine Existenz, noch sein grundsätzlicher argumentativer Aufbau eine Überraschung dar.

Anknüpfend an die sog. Volkszählungsentscheidung des Bundesverfassungsgerichts<sup>3</sup> betrachtet es die automatisierte Datenanalyse als Eingriff in das Grundrecht auf informationelle Selbstbestimmung und wendete auf die Rechtsgrundlage die aus dem Grundsatz der Verhältnismäßigkeit entwickelten Maßstäbe an.

Die Entscheidung wirft jedoch hinsichtlich ihres Gegenstands – einer bisher in und aus der Polizeipraxis unbekanntenen Informationstechnologie – etliche sowohl verfassungsrechtsdogmatische als auch sprachliche und (technik-)philosophische Fragen auf.<sup>4</sup>

Im Folgenden sollen die Entscheidung und ihr Gegenstand indessen nicht unter diesen Aspekten, sondern unter rechtssoziologischen Gesichtspunkten betrachtet werden. Es soll gezeigt werden, dass die Wechselwirkungen zwischen Recht und sozialer Wirklichkeit im Hinblick auf die automatisierte polizeiliche Datenanalyse mittels des Palantir-Programms, ihrer rechtlichen Regelung und deren verfassungsgerichtlicher Überprüfung keineswegs belanglos waren und sind.

Die Grundlage für die Betrachtung liefert zunächst die Vorgeschichte von hessenDATA, sodann aber allem das Urteil selbst. Dieses hat sich ausweislich

---

1 BVerfGE 165, 363.

2 Dazu näher Bäuerle 2023, S. 9, 88 ff.

3 BVerfGE 65, 1.

4 Vgl. dazu die Beiträge von Rabe, Giogios, Gehring und Denker in diesem Band.

der nicht zu knappen deskriptiven Passagen der Entscheidungsgründe eingehend mit der praktischen Anwendung der Technologie befasst. Es soll versucht werden, diese rechtstatsächlichen Erkenntnisse zumindest näherungsweise den vorhandenen rechtssoziologischen Erkenntnissen zur Praxis der Legislative und der Exekutive – respektive der Polizeibehörden – zuzuordnen.

## 2. Normatives Modell vs. Wirklichkeit

Nach dem normativen Modell der Exekutive erfolgt deren Steuerung bekanntlich durch Bindung an die Parlamentsgesetze, die parlamentarische Verantwortung der Regierung, die ministerielle Aufsicht und eine hierarchische Organisationsstruktur; dieses Modell verleiht ihr zugleich die demokratische Legitimation.<sup>5</sup>

### 2.1 Normalität informeller Praxen

Rechtssoziologisch ist es indessen mittlerweile unbestritten, dass das normative Modell die Verwaltungswirklichkeit zumindest unvollständig beschreibt. Tatsächlich entstehen bzw. existieren innerhalb jeder Verwaltung informelle Beziehungen und Gruppenbildungen, subjektive Präferenzen, fachliche Orientierungen und Rollen sowie Konkurrenzen und Konfliktsituationen, die Hierarchiestränge unterlaufen und praeter- oder paralegale Verhaltensmuster und Problemlösungsstrategien hervorbringen können. Die Existenz und Folgen solcher informalen Phänomene als zwangsläufiger Begleiterscheinung formaler Organisation sind von *Niklas Luhmann* früh entdeckt und als »brauchbare Illegalität« umschrieben worden.<sup>6</sup> Solche Muster sind mittlerweile – wenig überraschend – auch in der deutschen Polizeiforschung recht ausführlich nachgewiesen.<sup>7</sup> Im Hinblick auf das Recht wird etwa der Befund eines »Nicht-Handeln-Dürfens« oder »Nicht-so-Handeln-Dürfens« in der konkreten Einsatzsituation den erfahrungsgestützten Vorstellungen der »Basis« vom »richtigen Polizeihandwerk« gegenübergestellt.<sup>8</sup> Anhand dieser werden die rechtlichen Grenzen auf ihre Praxistauglichkeit geprüft und ggf. relativiert oder verworfen.<sup>9</sup> Im Zweifel

---

<sup>5</sup> Vgl. dazu und zum Folgenden m.w.N. Bäuerle 2012, S. 31 ff.

<sup>6</sup> Luhmann 1964, S. 303 ff.

<sup>7</sup> Vgl. Mensching 2008; Jacobsen 2001; Schöne 2011; Behr 2008.

<sup>8</sup> Vgl. Schöne 2011, S. 231 ff.; Behr 2000, S. 177 ff.; Behrendes 2006, S. 46 ff.

<sup>9</sup> Behrendes 2006, S. 47; das wohl älteste, bekannteste – und wohl inzwischen überholte – Beispiel betrifft mit der Umdefinition von strafrechtlich relevanten Gewalttätigkeiten in häuslichen Gemeinschaften

dominieren polizeikulturell präformierte Gerechtigkeitsvorstellungen, zu denen auch eine kritische Distanz zum Justizsystem gehört,<sup>10</sup> das Handeln.

## 2.2 Informelle Praxen und nachlaufende Gesetzgebung

Bezogen auf die vor dem hessenDATA -Urteil ergangene Reihe der verfassungsgerichtlichen Entscheidungen zum Informationsrecht der Sicherheitsbehörden standen solche informellen polizeilichen Praxen nicht selten ganz am Anfang: Ein nicht unerheblicher Teil der verfassungsgerichtlich überprüften informationellen Eingriffe – wie die Rasterfahndung oder die Quellen-Telekommunikationsüberwachung – entstanden infolge neuer technischer Möglichkeiten in bzw. aus der Polizeipraxis heraus, ohne dass es bereits die erforderliche gesetzliche Ermächtigung hierfür gegeben hätte. Dass die gesetzlichen Generalklauseln für die polizeiliche Gefahrenabwehr und Strafverfolgung hierfür nicht ausreichen, stand seit der Volkszählungsentscheidung des Bundesverfassungsgerichts unverrückbar fest. Sobald eine öffentliche Diskussion über solche Praxen in Gang kam und von Seiten der Polizei die Unverzichtbarkeit des jeweiligen Instrumentariums für die Aufgabenerfüllung betont worden war, fanden die neuen informationellen Eingriffe sodann regelmäßig nicht etwa eine parlamentarische Missbilligung, sondern eine Rechtsgrundlage die im Wege »nachlaufender Gesetzgebung« durch die Parlamente geschaffen wurde.<sup>11</sup>

## 2.3 Ausnahme hessenDATA

Dies gilt für hessenDATA jedoch gerade nicht. Der automatisierten Datenanalyse mit Hilfe des Programms der Firma Palantir stand zum Zeitpunkt seiner Regelung durch den Gesetzgeber keine bereits informell etablierte Polizeipraxis gegenüber, die nachlaufend hätte legalisiert werden sollen. Die hessische Ermächtigungsgrundlage für die automatisierte Datenanalyse wurde vielmehr im Juli 2018 gleichzeitig mit bzw. kurz nach der Inbetriebnahme<sup>12</sup> des Systems geschaffen; die Parallelvorschrift aus Hamburg wurde bereits erlassen, bevor ein solches System

---

zu »privaten Streitigkeiten« einen Fall, in dem umgekehrt die rechtliche Handlungspflicht umgangen wird.

<sup>10</sup> Dessen strafende Praxis als zu weich empfunden wird, vgl. Behr 2008, S. 206.

<sup>11</sup> Vgl. mit weiteren Nachweisen Bäuerle 2012, S. 42 f.

<sup>12</sup> BVerfGE 165, 363 (370); HessLT-Drs. 19/6502, S. 41.

angeschafft war.<sup>13</sup> hessenDATA stellt damit gleichsam eine »von oben« eingeführte polizeiliche Informationstechnologie dar<sup>14</sup> und entspricht insoweit dem normativen Modell (erst das Gesetz, dann die Praxis) geradezu idealtypisch.

#### 2.4 Vorabregulierung digitaltechnischer Eingriffe

Dieser Befund wäre nicht weiter bemerkenswert, würde er es doch dem Gesetzgeber ermöglichen, Grund und Grenzen der avisierten polizeilichen Praxis dem normativen Modell entsprechend vorab in dem für polizeiliche Eingriffe typischen »Wenn-dann«-Schema zu regeln.

Dass dabei mit der automatisierten Datenanalyse ein mittels Digitaltechnik vorzunehmender Informationseingriff erfolgen soll, stellt(e) insoweit keine Besonderheit dar, als die Regulierung solcher Eingriffe – wie etwa die Ermächtigungen zu Funkzellen-Abfragen und dem Einsatz von IMSI-Catchern – längst zur gesetzgeberischen Routine gehören, in deren Rahmen die ggf. bereits bestehende polizeiliche Praxis einzuhegen versucht wurde.

Allerdings zeichnen sich die bisher geregelten Eingriffe dieser Art dadurch aus, dass zwar ihr faktisches Ergebnis (etwa die Erlangung der IMSI und IMEI von Mobilfunkgeräten oder das Mithören verschlüsselter Telekommunikation) vorgegeben war, nicht aber die Technik oder Technologie, mit der es erzielt wird. Diese war jeweils längst vorhanden und über die Frage, ob sie von einem privaten Anbieter bezogen werden muss und ggf. von welchem, wurde mit Blick auf die vorhandenen polizeitechnischen Ressourcen und – soweit erforderlich – nach den Kriterien des Vergaberechts entschieden.

#### 2.5 Regulierung nach Vorgabe privater Programmieretechnik

Erst die Beschaffung des Programms der Firma Palantir stellte den Gesetzgeber<sup>15</sup> vor die Aufgabe, an der Stelle eines technikneutralen und ergebnisorientierten Informationseingriffs die technischen Resultate und die Verwendung der von ei-

---

13 In Bayern wurde eine entsprechende Rechtsgrundlage ebenfalls mit Inbetriebnahme des Systems erlassen und Rheinland-Pfalz hat – wie Hamburg – zwar die Norm, nicht aber das System.

14 Deren Erwerb durch das Land einen Untersuchungsausschuss im Hessischen Landtag zur Folge hatte, der vor allem beschaffungsrechtlichen Fragen zum Gegenstand hatte, vgl. HessLT-Drs. 19/6864 (Teile A und B), dessen Berichte die Vorgänge um den Erwerb der Software ausführlich dokumentieren und (unterschiedliche) bewerten.

15 Also vor allem das Landesinnenministerium als »Vorschriftenwerkstatt«, Begriff von Baer 2023, § 5 Rn. 48 (unter Berufung auf Smeddinck).

nem privaten Anbieter für die Polizei erworbenen Software zu regeln. Nach § 25a Abs. 1 HSOG a. F. durften die Polizeibehörden zu diesem Zweck »gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten.« Während der Begriff der Weiterverarbeitung an die datenschutzrechtliche Terminologie des § 20 HSOG anknüpfte, war mit dem im öffentlichen Recht bis dahin unbekanntem Terminus<sup>16</sup> der »automatisierten Anwendung zur Datenanalyse« der gesetzgeberische Code für das Programm gefunden.

Sodann folgte in § 25a Abs. 2 HSOG a. F. die Wendung: »Im Rahmen der Weiterverarbeitung nach Abs. 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.«<sup>17</sup> Damit beschrieb das Gesetz recht genau das polizeispezifische Potential vom »Gotham«, das dafür geschaffen ist heterogene, inkompatible und getrennte personenbezogene Datenbestände, wie sie die polizeiliche IT aufweist, zusammenzuführen, miteinander kompatibel zu machen und die Ergebnisse in einer unter verschiedensten Aspekten recherchierbaren Form grafisch sichtbar zu machen.

Aus der aus dem normativen Modell folgenden Maxime »erst das Gesetz, dann die Praxis« wurde gleichsam »erst die Software, dann das Gesetz«. Zwar stand und steht die Modernisierung der polizeilichen IT-Systeme in Bund und Ländern schon länger auf der innenpolitischen Agenda. Der Bedarf an einer dergestalt leistungsfähigen Analyseplattform entstand jedoch erst, als man deren Existenz auf dem Markt politisch zur Kenntnis genommen hatte.

Ungewöhnlich ist daran weniger die Tatsache, dass eine informationelle Eingriffsbefugnisse der Polizei infolge des technischen Fortschritts entstand. Auch die Befugnisse zur DNA-Analyse oder zur Quellen-Telekommunikationsüberwachung entstanden erst, als die jeweiligen Techniken zur Verfügung standen.

---

<sup>16</sup> Zwar war die Regelung des Einsatzes von Software dem öffentlichen Recht zum Zeitpunkt der Schaffung des § 25a HSOG a. F. nicht gänzlich unbekannt, das Verwaltungsverfahrensgesetz (VwVfG) spricht an vergleichbarer Stelle in § 35a etwa von »automatischen Einrichtungen« mittels derer unter bestimmten Voraussetzungen Verwaltungsakte erlassen werden dürfen.

<sup>17</sup> Diese Formulierung ist aus der Regelung des § 6a Antiterrordateigesetz übernommen, wonach diese Möglichkeiten für einen sehr viel beschränkteren Datenbestand als »erweiterte projektbezogene Datennutzung« zum Zweck der Terrorabwehr bestehen sollten; dies wurde jedoch mangels einer geeigneten Softwarelösung von 2015 bis heute nie in die Tat umgesetzt (vgl. etwa BT-Drucks. 19/26367, S. 4, zum Umfang des Datenbestands der Antiterrordatei ebendort S. 3); zur Verfassungsmäßigkeit der Regelung BVerfGE 156, 11.

Bisher ging es jedoch dabei stets um gleichsam marktreife Techniken, die nicht dergestalt monopolisiert waren, dass – zumindest nach der im rechtspolitischen Raum verbreiteten Ansicht – nur ein Anbieter zur Verfügung stand und steht.

Nur vor diesem Hintergrund konnte eine somit Ermächtigungsgrundlage nach der Maxime »erst die Software, dann das Gesetz« entstehen. Rechtspolitiker mit Grundkenntnissen der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung wären ohne die Kenntnis von der Existenz der Software vermutlich nicht auf die Idee gekommen, den Polizeibehörden zur vorbeugenden Bekämpfung von Straftaten eine Befugnis an die Hand zu geben, die eigenen umfangreichen »Datentöpfe« mit ganz unterschiedlichen Zweckbestimmungen weitgehend beliebig auf Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen automatisiert durchforsten zu lassen.<sup>18</sup>

Da es dem Gesetzgeber allerdings verfassungsrechtlich unbenommen bleibt, die polizeiliche Praxis nach dieser Maxime zu regulieren, ließ das Bundesverfassungsgericht das Gesetzgebungsverfahren insoweit freilich unbeanstandet. Dass das Gericht den rechtstatsächlichen Hintergrund nicht ganz unkritisch zur Kenntnis genommen und Gefahren erkannt hat, die inzwischen unter dem Stichwort der nationalen Datensouveränität öffentlich diskutiert werden, lässt es jedoch in einer knappen Passage erkennen: »Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte.«<sup>19</sup>

## 2.6 Tatsächlicher Hintergrund

Fragt man nach dem tatsächlichen Hintergrund für den Erwerb und Einsatz der Software der Firma Palantir, über den auch im Internet etwa auf Seiten wie »Police-IT«<sup>20</sup> diskutiert wird, stößt man vor allem auf Defizite bei der Entwicklung der polizeilichen IT-Landschaft durch Bund und Länder in den letzten Jahrzehnten. Entstanden ist dadurch nach weit verbreiteter Ansicht eine zersplitterte, in Teilen veraltete und länderübergreifend wenig kompatible Struktur mit mehr als 60 unterschiedlichen Datenbanksystemen und unzähligen Datenformaten und -typen. Die zweckführende Bedienung dieser Struktur verlangt den Bediensteten – wenn sie möglich ist – nach übereinstimmenden Berichten aus der polizeilichen Praxis jedenfalls einiges ab.

---

18 Vgl. zu dem insoweit sehr viel beschränkteren Ansatz im Rahmen von § 6a ATDG oben 2.4.

19 BVerfGE 165, 363 (408).

20 S. <https://police-it.net/> (01.10.2025).

Für dieses Problem, bot und bietet das Programm der Firma Palantir nun zeitnah eine Lösung, weil es eben gerade dafür konzipiert und darauf ausgerichtet ist, heterogene, inkompatible und getrennte Datenbestände zusammenzuführen, miteinander kompatibel und umfassend recherchierbar zu machen.

Vor diesem Hintergrund hatte sich bislang schon technisch-faktisch keine auf automatisierte Datenanalyse gerichtete informelle Polizeipraxis bilden können, die im Wege der bisher gängigen nachlaufenden Gesetzgebung hätte reguliert werden können. Der entscheidende Regelungsimpuls<sup>21</sup> für die Schaffung der Ermächtigungsrundlage »von oben« war insoweit vielmehr die Erkenntnis der Verfügbarkeit einer Lösung für die festgestellten Defizite. Dementsprechend deutlich wurde und wird Bereitstellung dieser Lösung auch von den Polizeien in Bund und Ländern gefordert, wengleich dabei nunmehr regelmäßig zugleich auf das Erfordernis der Wahrung der verfassungsrechtlichen Vorgaben aus dem hessenDATA -Urteil hingewiesen wird.

### 3. hessenDATA in der polizeilichen Praxis

Wie das Bundesverfassungsgericht darlegt,<sup>22</sup> wird das System in Hessen seit seiner Bereitstellung rege genutzt. Dort hatte das Land angegeben, dass es in 14.000 Fällen pro Jahr genutzt worden sei und das ca. 2100 Personen zugriffsberechtigt seien.

#### 3.1 Geringer Anteil der Nutzungen zur Gefahrenabwehr

Davon entfielen nach Angaben des Landes allerdings nur 2.000 Fälle auf die Anwendung zur Abwehr einer Gefahr, also die Tatbestandsalternative, die das BVerfG als die deutlich unproblematischere angesehen hatte und die von politischer Seite in der öffentlichen Diskussion nicht selten als Hauptzweck der Technologie hervorgehoben wird. 12.000 Fälle entfielen auf die sog. vorbeugende Bekämpfung von Straftaten.

Das bedeutet, dass 86% der Anwendungen in Hessen in Fallgestaltungen erfolgte, in denen sich Straftaten nur mehr oder weniger vage abzeichneten, weshalb hier verfassungsrechtlich höhere Anforderungen gelten. Dabei bilden offensichtlich regelmäßig bereits eingeleitete konkrete Ermittlungen wegen bereits begangener Straftaten den Anlass für diese Anwendungen, da es in Hessen

---

21 Vgl. dazu Baer 2023, § 6 Rn. 18 ff. (36).

22 BVerfGE 165, 363 (373).

vor allem kriminalpolizeiliche Dienststellen sind, die Zugriff auf hessenDATA haben, also diejenigen Einheiten, die eben Ermittlungen nach der Strafprozessordnung (StPO) vorzunehmen haben.

Somit hatte es im Bereich der automatisierten Datenanalyse zwar keine informelle polizeiliche Praxis gegeben, die von einer nachlaufenden Gesetzgebung legalisiert worden wäre; der genannte Befund lässt jedoch darauf schließen, dass sich im Nachgang zur Regulierung »von oben« mittlerweile eine rechtlich nicht ganz unproblematische informelle Praxis gebildet hat. Die Anwendung des Systems anlässlich bereits begangener Straftaten lässt nämlich außer Betracht, dass das System rechtlich ausschließlich zur Gefahrenabwehr und zur vorbeugenden Bekämpfung der Kriminalität eingesetzt werden darf, da dem Land nur für diese polizeilichen Aufgaben eine Gesetzgebungskompetenz zusteht. Der Einsatz zur Strafverfolgung – also der Ermittlung bereits begangener Straftaten – fällt in die Gesetzgebungskompetenz des Bundes, der in der Strafprozessordnung bisher keine entsprechende Befugnisnorm geschaffen hat. Praktisch ist das System jedoch dafür auch und gerade sehr gut geeignet.

### 3.2 Informelle Nutzung zur rechtlich nicht vorgesehenen Strafverfolgung

Legt man zugrunde, dass das die Nutzung des Systems für strafprozessuales Handeln der Polizei – wie auch das BVerfG betont<sup>23</sup> – nicht zugelassen ist, jedoch in Hessen vor allem von der Kriminalpolizei für die vorbeugende Straftatenbekämpfung aus Anlass bereits laufender Ermittlungen genutzt wird, spricht vieles dafür, dass das aus hessenDATA gewonnene »neue Wissen« (wie das Bundesverfassungsgericht die Resultate des Softwareeinsatzes nennt)<sup>24</sup> im Ergebnis auch – wenn nicht gar in erster Linie – dazu verwendet wird, nunmehr die erforderlichen Beweise für das Strafverfahren gegen die (mutmaßlichen) Täter zu sammeln. Oder auch dazu, diese (mutmaßlichen) Täter überhaupt erst ausfindig zu machen.

Die Praxis würde dem Einwand, das System dürfe nur zur Gefahrenabwehr und vorbeugenden Bekämpfung von Straftaten genutzt werden vermutlich damit begegnen, dass die Strafverfolgung etwa von Drogen- oder Waffenhändlern ja auch dazu beitrage, dass zukünftige Straftaten von diesen verhindert oder sie von solchen abgeschreckt würden (in der Praxis wird dieser Effekt auch als »Prävention durch Repression« bezeichnet).

---

23 BVerfGE 165, 363 (433, 439)

24 Als solches beschreibt das Bundesverfassungsgericht das Resultat automatisierter Datenanalysen, vgl. BVerfGE 165, 363 (395 f.).

Rechtsdogmatisch ist dieses Vorgehen indessen mit der derzeitigen Rechtslage nicht kompatibel. Auch das Bundesverfassungsgericht hebt hervor<sup>25</sup>, dass insoweit die im Zusammenhang mit laufenden strafprozessualen Ermittlungen gewonnenen Erkenntnisse ausschließlich für Prognosen verwendet werden dürfen, ob weitere Straftaten drohen, nicht aber, für die Verfolgung dieser Straftaten.

Es erscheint – wie gesagt – sehr fraglich, ob dies in der Anwendungspraxis tatsächlich geschieht. Zwar wird etwa die Herkunft der Erkenntnis, welche Personen zu einer Tätergruppierung gehören oder zum Tatzeitpunkt in die entsprechende Funkzelle eingeloggt waren, vermutlich später nicht als Hinweis auf eine hessenDATA-Recherche in der Akte niedergelegt werden. Das erlangte »neue Wissen« wird aber vermutlich oft die Grundlage dafür (gewesen) sein, klassische Beweismittel, wie Fingerabdrücke oder den Inhalt von Telefonaten oder Chats zu gewinnen. Das oft allein schon deshalb, weil man ohne das Wissen gar nicht auf den oder die Tatverdächtigen gestoßen wäre.

Unter rechtspolitischen Gesichtspunkten ließe sich eine verfassungskonforme Regelung auf der Grundlage des hessenDATA-Urteils auch für die repressive automatisierte Datenanalyse in der StPO sicherlich schaffen und der Bundesrat hat jüngst auch den Erlass einer solchen Norm eingefordert.<sup>26</sup>

Bis diese Regelung kommt, bewegen sich die Polizeibehörden jedoch zumindest in einem »Graubereich«, der dem Phänomen der »brauchbaren Illegalität« im Sinne Luhmanns unterfallen dürfte. Er beschreibt dieses als ein Handeln in Organisationen, das gegen Regeln verstößt, dem Zweck der Organisation aber dienlich ist und deshalb tendenziell toleriert wird. Warum sollte man – dürfte in der polizeilichen Praxis gefragt werden – den mit Hilfe des »neuen Wissens« ermittelten Täter nicht einem Strafverfahren zuführen und damit den eigentlichen Zweck kriminalpolizeilicher Arbeit erfüllen? Dies gilt umso mehr, als die Herkunft der als Voraussetzung für die klassische Beweiserhebung erlangten Erkenntnisse aus hessenDATA von außen kaum jemals belegbar sein wird, also die aus rechtssoziologischer Sicht für die Normeinhaltung sehr relevante Sanktionserwartung für den Fall des Normverstoßes entfällt. Entscheidungen der Instanzgerichte, die die Rechtswidrigkeit der Informationserlangung aus dieser Quelle oder ein darauf bezogenes Beweisverwertungsverbot feststellen, stehen angesichts deren fehlender Belegbarkeit schlicht nicht zu erwarten.

---

25 BVerfGE 165, 363 (433).

26 BR-Drucks. 58/25 S. 6.

### 3.3 Keine extensive Nutzung des Systems durch Hessens Polizei

Was die vom Bundesverfassungsgericht referierten Zahlen und Fakten in Bezug auf die faktische Verwendung des Systems allerdings auch zeigen, ist, dass hessenDATA von der Hessischen Polizei nicht so intensiv genutzt wird wie es auf den ersten Blick erscheinen mag. Von den ca. 15.000 Bediensteten der hessischen Polizei (von denen etwa 3.500 täglich im Einsatz sein dürften) sind mit 2.100 Zugriffsberechtigten nur ca. 14 % ermächtigt, das System zu verwenden. Von diesen nutzen statistisch täglich 33 das System zur vorbeugenden Bekämpfung von Straftaten und 5 zur Gefahrenabwehr. Rechtstatsächlich ist hessenDATA also weit davon entfernt ist, zu einem allgegenwärtigen Alltagsinstrument geworden zu sein, also gleichsam zu einem »Google für Polizisten«.

Wie eine journalistische Recherche ergeben hat<sup>27</sup>, nutzt Bayern im Vergleich die dort im September 2024 unter dem Namen VeRA in Betrieb genommene Software, bisher allerdings noch deutlich seltener (100 Nutzungen zwischen September 2024 und Mai 2025), dafür aber entgegen der gesetzlichen Vorgabe auch in Bezug auf weniger schwerwiegende Kriminalität und – vermutlich – auch für repressive Zwecke.

### 3.4 Zugrundeliegende Informationseingriffe

Wie das Bundesverfassungsgericht hervorgehoben hat, hängt das Eingriffsge-  
wicht dieser Nutzung nicht zuletzt vom Gewicht der Informationseingriffe ab,  
die der Speicherung von Daten in den recherchierbaren Datenbanken vorausge-  
gangen sind. Dass sich unter diesen Daten ein erheblicher Anteil befindet, der  
tatsächlich auf schwerwiegenden Grundrechtseingriffen beruht, lässt auf der  
Grundlage in § 101b StPO vorgesehenen Berichtspflichten veröffentlichten Zah-  
len für den Bereich der Strafverfolgung tatsächlich annehmen. Danach wurden  
alleine in Hessen im Jahr 2023 in 758 Verfahren 2588 Telefonanschlüsse überwacht  
(§ 100a StPO, darunter in 3 Fällen durch sog. Quellentelekommunikationsüber-  
wachung) und in 1015 Fällen Verkehrsdaten erhoben (§ 100g StPO), darunter in  
657 Fällen in Form von Funkzellenabfragen, die besonders umfangreiche Da-  
tenbestände hervorbringen, da stets zahlreiche nur zufällig in der betroffenen  
Funkzelle eingeloggte Personen miterfasst werden. In 65 Fällen würden darüber  
hinaus Nutzungsdaten bei Telemediendiensten erhoben (§ 100k StPO) und in

---

<sup>27</sup> Krempel, »Big Data: Deutsche Polizisten nutzen Palantir auch bei Eigentumsdelikten«, heise.de, 19.06.2025. <https://www.heise.de/news/Palantir-Deutsche-Ermittler-nutzen-Big-Data-auch-bei-kleinerer-Kriminalitaet-10453580.html> (01.10.2025).

einem Fall eine Onlinedurchsuchung durchgeführt (§ 100b StPO).<sup>28</sup> Hinzu kommen die Daten aus entsprechenden Eingriffen zur Gefahrenabwehr (über die in Hessen allerdings keine genauen Daten vorliegen)<sup>29</sup> und die aus anderen Ländern stammenden Daten aus entsprechenden Eingriffen, soweit auf diese wegen länderübergreifender Relevanz im Rahmen des polizeilichen Informationsaustausches in Hessen zugegriffen werden kann. Hierzu können auch Daten aus sog. großen Lauschangriffen zählen, von denen es 2023 zwar zur Strafverfolgung in Hessen keinen gegeben hat, in den anderen Bundesländern jedoch insgesamt zehn. Bei den Daten aus allen diesen Informationseingriffen handelt es also sich um solche, bei denen das Eingriffsgewicht im Sinne des Bundesverfassungsgerichts hoch ist; der analysierte Datenbestand gleichsam mit »empfindlichen« Daten angereichert ist, wodurch die verfassungsrechtliche Forderung nach einer maßvollen Nutzung ihre rechtstatsächliche Grundlage erhält.

#### 4. Fazit

Aus rechtssoziologischer Perspektive erweisen sich hessenDATA und das dazu ergangene Urteil des Bundesverfassungsgerichts somit unter mehreren Gesichtspunkten als Sonderfall. Das Gericht hatte über die Rechtsgrundlage für eine Technologie zu entscheiden, für die rechtspolitisch gleichsam das Angebot die Nachfrage geschaffen hatte. Eine vorausgegangene informelle polizeiliche Praxis des durch die Technologie ermöglichten »Data-Mining« in den polizeilichen Datenbanken hatte es daher nicht gegeben.

Auch wenn die Polizeibehörden diese Technologie seit ihrer Einführung »von oben« quantitativ bisher maßvoll nutzen, können sie materiell den Versuchungen eines nicht zweckkonformen Einsatzes zur Strafverfolgung jedoch offensichtlich nur begrenzt widerstehen. Dem mit der Einführung verbundenen rechtspolitischen Versprechen einer Nutzung vor allem zur Abwehr schwerster Gefahren wird die Praxis in den wenigsten Fällen gerecht, greift aber gleichwohl auf einen Datenbestand zurück, der zu einem nicht unwesentlichen Teil aus Informationseingriffen mit hohem Eingriffsgewicht resultiert.

Das Urteil des Bundesverfassungsgerichts dürfte allerdings die Sensibilität der Praxis für die mit der automatisierten Datenanalyse verbundene rechtsstaatliche und grundrechtliche Problematik gesteigert haben. Das Gericht hat die (fehlende) Sanktionserwartung der Praxis also zu einem gewissen Grad verfassungs-

---

<sup>28</sup> Die folgenden Zahlen sind abrufbar unter [https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken\\_node.html#AnkerDokument226698](https://www.bundesjustizamt.de/DE/Service/Justizstatistiken/Justizstatistiken_node.html#AnkerDokument226698) (01.10.2025).

<sup>29</sup> Vgl. zu der insoweit mit § 17a HSOG nicht vereinbaren Situation Bäuerle 2025, § 17a Rn. 14 ff., Rn. 17.1.

rechtlich kompensiert. Auch die wiederkehrenden Berichte über Verfassungsbeschwerden gegen (neue) Landespolizeirechtsnormen zur automatisierten Datenanalyse<sup>30</sup> dürften in eine ähnliche Richtung wirken.

Rechtspolitisch bleibt zu hoffen, dass vor diesem Hintergrund auch das Bemühen um eine Modernisierung der polizeilichen IT – nunmehr unabhängig von der schnellen Lösung mittels monopolisierter Software eines privaten Anbieters – nicht (länger) nachlässt.

## Quellen und Literatur

- Baer, Susanne, *Rechtssoziologie*, 5. Auflage, Baden-Baden 2023.
- Bäuerle, Michael, »Demokratisierung der Polizei?«, in: Bäuerle, Michael/Dann Philipp, Wallrabenstein, Astrid (Hg.): *Demokratie-Perspektiven, Festschrift für Brun-Otto Bryde, Tübingen 2012*, S. 23 ff.
- Bäuerle, Michael, *Das Informationsrecht der Sicherheitsbehörden zwischen Konstitutionalisierung und Europäisierung*, Frankfurt am Main 2024.
- Behr, Rafael, *Cop Culture. Der Alltag des Gewaltmonopols*, 2. Auflage, Heidelberg 2008.
- Behrendes, Udo, »Zwischen Teamgeist und Korpsgeist«, in: *POLIZEI-heute 2/2006*, S. 46 ff.
- Frischholz, Andreas, »Klage gegen Palantir-Software: Verfassungsbeschwerde gegen automatisierte Datenanalyse in Bayern«, in: *Computer Base*, 24.07.2025. [https://www.computerbase.de/news/netzpolitik/klage-gegen-palantir-software-verfassungsbeschwerde-gegen-automatisierte-datenanalyse-in-bayern.93639/#:~:text=Die%20Gesellschaft%20f%C3%BCr%20Freiheitsrechte%20hat%20gemeinsam%20mit%20dem,erhoben.%20Hintergrund%20ist%20der%20Einsatz%20der%20umstrittenen%20Palantir-Software%20\(01.10.2025\)](https://www.computerbase.de/news/netzpolitik/klage-gegen-palantir-software-verfassungsbeschwerde-gegen-automatisierte-datenanalyse-in-bayern.93639/#:~:text=Die%20Gesellschaft%20f%C3%BCr%20Freiheitsrechte%20hat%20gemeinsam%20mit%20dem,erhoben.%20Hintergrund%20ist%20der%20Einsatz%20der%20umstrittenen%20Palantir-Software%20(01.10.2025))
- Jacobsen Astrid, *Die gesellschaftliche Wirklichkeit der Polizei*, Bielefeld 2001.
- Krempf, Stefan, »Big Data: Deutsche Polizisten nutzen Palantir auch bei Eigentumsdelikten«, in: *heise online*, 19.06.2025. <https://www.heise.de/news/Palantir-Deutsche-Ermittler-nutzen-Big-Data-auch-bei-kleinerer-Kriminalitaet-10453580.html> (01.10.2025).
- Luhmann, Niklas, *Funktion und Folgen formaler Organisation*, 2. Auflage, Berlin 1972 (unveränderte Nachdruck der ersten Auflage 1964), S. 303 ff.
- Mensching, Anja, *Gelebte Hierarchien*, Heidelberg 2008.
- Möstl, Markus/Bäuerle, Michael (Hg.): *BeckOK Polizei und Ordnungsrecht Hessen*, 34. Edition, München 2025.
- Schöne, Marschel, *Pierre Bourdieu und das Feld Polizei*, Frankfurt 2011.

---

<sup>30</sup> Vgl. etwa Frischholz, »Klage gegen Palantir-Software: Verfassungsbeschwerde gegen automatisierte Datenanalyse in Bayern«, in: *Computer Base*, 24.07.2025. [https://www.computerbase.de/news/netzpolitik/klage-gegen-palantir-software-verfassungsbeschwerde-gegen-automatisierte-datenanalyse-in-bayern.93639/#:~:text=Die%20Gesellschaft%20f%C3%BCr%20Freiheitsrechte%20hat%20gemeinsam%20mit%20dem,erhoben.%20Hintergrund%20ist%20der%20Einsatz%20der%20umstrittenen%20Palantir-Software%20\(01.10.2025\)](https://www.computerbase.de/news/netzpolitik/klage-gegen-palantir-software-verfassungsbeschwerde-gegen-automatisierte-datenanalyse-in-bayern.93639/#:~:text=Die%20Gesellschaft%20f%C3%BCr%20Freiheitsrechte%20hat%20gemeinsam%20mit%20dem,erhoben.%20Hintergrund%20ist%20der%20Einsatz%20der%20umstrittenen%20Palantir-Software%20(01.10.2025)).

# Data is Power – Code is Ideology: Selbstmarketing und politische Positionierungen an der Spitze von Palantir

*Andreas Brenneis, Kai Denker, Petra Gehring*

## Einleitung

An der Spitze von Palantir – der Firma hinter der »Sicherheitssoftware« Gotham – stehen zwei Personen, deren Selbstvermarktung maßgeblich zum Ruf ihres Unternehmens beiträgt: Alexander (»Alex«) Karp und Peter Thiel. Beide Akteure positionieren sich im Wege medialer Äußerungen persönlich als avantgardistische, exzentrische Tech-Entrepreneure wie zugleich politisch, teils auch mit (populär)philosophischem Anspruch. Dies strahlt wiederum – sicher nicht unabsichtlich – auf den Nimbus von Palantir als Unternehmen wie auch auf seine Produkte ab.

Wir sehen hier ein Spannungsfeld aus drei, auf den ersten Blick wenig zusammenhängenden Bezügen: Zunächst ist auf Seiten der Protagonisten ein im Laufe der Jahre zunehmend autoritärer anmutender Techno-Libertarismus zu konstatieren, der ein aus liberal-demokratischer Perspektive grotesk übersteigertes Freiheitsverständnis impliziert, dessen Verwirklichung mittels digitaler Mittel angestrebt werden soll. Des Weiteren und damit eng verbunden ist ein Denken in Krisen und disruptiven Entwicklungen: Mit diesen könnten bestehende demokratische Institutionen in naher Zukunft zusammenbrechen, ja: sie würden dies tun. Sofern die Produktpalette von Palantir geeignet scheint, sich zu einem solchen Szenario präventiv zu verhalten (oder mindestens prospektiv Vorkehrungen zu treffen), liegt der Marketingcharakter dieser »Krisen«-Semantik auf der Hand. Schließlich ist paradoxerweise trotz der libertären Botschaften doch auch eine Staatsnähe zu konstatieren, nicht zuletzt gehen Karp und Thiel mit einem gewissen Heroismus von Staatsschutz und Gefahrenabwehr auf typische Palantir-Kunden zu. Diese sind Sicherheitsorgane, Sicherheitsbehörden und auch militärische Akteure.

In unserem Beitrag unternehmen wir den Versuch, diesen Befund zu erläutern sowie im Spannungsfeld von Selbstmarketing und politischer Positionierung zu interpretieren. Vermeintliche Widersprüche zwischen den drei skizzierten ar-

gumentativen Kontexten können, so unsere These, aufgelöst werden, wenn man die libertäre und zugleich autoritäre Rhetorik von Karp und Thiel als Ausdruck eines Ideologiehybrids versteht, der sich aus einer Melange von libertärem Denken und autoritärem Handeln konstituiert – dem libertären Autoritarismus des *neoreactionism* (NRx) bzw. des *dark enlightenment*. Diese Ideologie, die gleichermaßen antimodern wie technologieaffin ist, rekuriert auf Ideen von Nick Land und Curtis Yarvin. Sie verbindet technologische Eliteherrschaft mit autoritärer Ordnungslogik, insbesondere unter dem Druck realer oder antizipierter Krisen – und das alles unter dem Banner einer tiefen Skepsis gegenüber Fortschritt und demokratischen Verhältnissen. Als ein zweiter, die vermeintlichen Widersprüche integrierender Punkt fungieren die marktlichen und *public relations*-Belange des Unternehmens selbst. Palantir vermarktet auf diese Weise einerseits zwar »nur« Software. Andererseits zieht es seine Kunden nahezu zwangsläufig in ein Spiel, das nicht nur eine dystopisch angehauchte Aufwertung des politischen Großthemas »Sicherheit« betreibt, sondern eben auch die durch Karp und Thiel verkörperten Ideologien ins Gespräch bringt und salonfähig macht.<sup>1</sup>

Die für Palantir wesentlichen Verstrickungen von Marketing, Politik und Ideologie erörtern wir in einem ersten Schritt anhand zweier zentraler Texte, mit denen Thiel und Karp ihre eigenen Positionen hinsichtlich Unternehmensgründung und -führung darstellen. Dabei nehmen wir eine möglichst große Zeitspanne in den Blick, um Kontinuitäten in der Selbstdarstellung an der Spitze von Palantir nachzuweisen. Zunächst gehen wir insbesondere auf Peter Thiels (zusammen mit Blake Masters verfasste) Startup-Fibel *From Zero to One – Notes on Startups, or How to Build the Future* von 2014 ein. In zeitliche Nachbarschaft um die Debatten, ob deutsche Sicherheitsbehörden Palantir nutzen sollten, fällt dann das 2025 erschienene Buch *The Technological Republic – Hard Power, Soft Belief and the Future of the West*, in dem Alexander Karp (gemeinsam mit Nicholas Zamiska) Palantir als die Firma präsentiert, welche bei der Lösung der Probleme des Westens stolz vorangeht.

Daran anknüpfend stellen wir einige der zentralen Positionen und Thesen aus dem Bereich des libertären Autoritarismus bzw. auch Cyberlibertarismus, Technolibertarismus oder *Californian Ideology* – die vielen Selbst- und Fremdbezeichnungen zeigen schon die Dringlichkeit an, mit der hier Debatten geführt werden – dar sowie einige der Diskurslinien zu der sogenannten Dark Enlightenment-

---

<sup>1</sup> Mühlhoff 2025 sieht in diesem Denken eine moderne Form des Faschismus. Wir wollen dieser vorschleunigen Identifikation nicht folgen: Zwar gibt es sicher palingenetische Krisenerzählungen, die auf eine Überwindung gegenwärtiger Krisenbehauptungen zielen, jedoch lässt sich das ultranationalistische Moment ebenso wenig erkennen, wie sich der Elitismus dieser Ideologie populistisch deuten lässt. Vgl. Griffin 1993, S. 26.

Bewegung. In einem dritten Schritt ziehen wir einige Verbindungen zwischen den Selbstdarstellungen der starken Männer an der Spitze von Palantir und den u. a. durch Land und Yarvin initiierten Diskursen. Ein letzter Schritt stellt schließlich die Frage, was sich aus den ideologischen Verstrickungen der Führungsriege von Palantir über den Code der Software des Unternehmens ableiten lässt.

## 1. Peter Thiel: Der postlibertäre Technokrat

»Ich glaube nicht mehr, dass Freiheit und Demokratie vereinbar sind.«<sup>2</sup>

Peter Thiel ist Mitgründer und seither Aufsichtsratsvorsitzender von Palantir sowie der größte private Anteilseigner. Zurzeit erfährt er weltweit und auch in Deutschland große Aufmerksamkeit, im Silicon Valley ist sein Einfluss allerdings schon lange bekannt, wie Max Chafkin in seiner Biografie von 2021 herausstellt.<sup>3</sup> Von dort ausstrahlend hat Thiel eine regelrechte Fanbasis aufgebaut – und seine Fans »sehen in Thiel den Vorkämpfer einer so hypermodernen wie reaktionären Kultur; den Vordenker einer postdemokratischen und postliberalen Welt, in der sich genialische Männer gegen störende Beschränkungen, z.B. durch demokratische Prozesse, durchsetzen«.<sup>4</sup> Dabei verdanke Thiel das Merkmal des Intellektuellen und des Vordenkers einer Reihe von Publikationen und Interviews, in denen er als politischer Theoretiker aufträte, als Dozent für politische Theorie in Stanford, als Experte für Politische Theologie und als Geschichtsphilosoph, der sich mit dem byzantinischen Reich ebenso auskenne wie mit der Aufklärung.<sup>5</sup> Zudem legt er auf YouTube Klassiker der reaktionären Moderne aus – Carl Schmitt, Oswald Spengler, Friedrich Nietzsche – und ist so auf ganz verschiedenen diskursiven Ebenen zugleich unterwegs.

Für die Frage nach Marketing und politischer Positionierung wollen wir uns hier auf ein viel besprochenes, aber eher wenig diskutiertes, weil auf den ersten Blick nicht sonderlich kontroverses Werk von Thiel beziehen. In seinem Buch *From Zero to One – Notes on Startups, or How to Build the Future* erklärt er anhand seiner Erfolge, was es brauche, um erfolgreich Unternehmen zu gründen. Sein

---

<sup>2</sup> Zit. n. Doherty 2020.

<sup>3</sup> Vgl. Chafkin 2021.

<sup>4</sup> Zorn 2025.

<sup>5</sup> Vgl. ebd. Kontrovers diskutiert werden zumeist Thiels Buch *The Diversity Myth: Multiculturalism and Political Intolerance on Campus*, das er 1995 mit David O. Sacks veröffentlicht hat, seine *Essays The Straussian Moment* (2007) sowie *The Education of a Libertarian* (2009) und mitunter auch sein Engagement für die an der Stanford University von ihm 1987 gegründete und seither unterstützte Zeitschrift *Stanford Review*, die als eine Institution angesehen wird, über die Interessierte einen ersten Zugang in das Universum von Peter Thiel bekommen können.

argumentativer Ausgangspunkt ist, dass es für den Erfolg der amerikanischen Wirtschaft vor dem Hintergrund einer gigantischen administrativen Bürokratie tatsächlicher Wunder bedürfe – und dass diese Wunder möglich seien in Form von Technik. Technik sei deshalb ein Wunder, weil sie erlaube, mit weniger mehr zu machen – »it allows us to do more with less«. <sup>6</sup> Dabei sei das, was mehr gemacht werde, nicht einfach mehr vom Gleichen, sondern bestehe in substanziellen Veränderungen. Thiel unterscheidet zwei Formen des Fortschritts, die man für die Zukunft anpeilen könne: Während horizontaler Fortschritt schon vorhandene Technik skalieren, beziehe sich vertikaler Fortschritt darauf, tatsächlich disruptives »Neues« zu entwickeln.

Die Frage nach dem Fortschritt und seiner Wertschätzung verortet Thiel im Kontext einer kulturellen Theorie über verschiedene Einstellungen zur Zukunft. In seiner Startup-Fibel verarbeitet Thiel sogar eine kulturelle Verfallstheorie, nach der es gerade die unbestimmten Einstellungen gegenüber der Zukunft sind, welche die dysfunktionalen Zustände in der Welt bedingen. Statt auf der Basis fester Überzeugungen Ziele zu verfolgen, seien in allen gesellschaftlichen Bereichen (wie Bildung, Politik, Philosophie) Werte leitend, die dazu führen, sich Portfolios vielseitiger Optionen zusammenzustellen und dabei nichts mehr als vielgestaltige Mittelmäßigkeit zustande zu bringen. Für die Zeit bis in die 1960er Jahre sieht Thiel demgegenüber für die westliche Welt und insbesondere die USA ein goldenes Zeitalter optimistischer Zukunftsplanung, das auf Basis einer anpackenden Weltsicht zahlreiche Erfolge in allen Bereichen des gesellschaftlichen Lebens zeitigt hätte – wobei Thiel primär anschauliche Beispiele aus den Bereichen der Ingenieurwissenschaften nennt (Empire State Building, Golden Gate Bridge, Interstate Highway System), aber auch das Manhattan Project. Der Geist dieser Zeit und ihrer Projekte ist für Thiel verlorengegangen und muss zum Wohle der amerikanischen Wirtschaft – geradezu palingenetisch – wiedererrungen werden. Wobei Thiel, um den Verfallsformen des zielstrebigem Optimismus entgegenzutreten, eine kulturelle Revolution als notwendig ansieht: »We have to find our way back to a definite future, and the Western world needs nothing short of a cultural revolution to do it.« <sup>7</sup>

Für den Bereich der Unternehmensgründung legt Thiel vor diesem düster gezeichneten Hintergrund dar, dass das Verfolgen von Zielen besonders dann lukrativ sei, wenn es dabei um das Aufdecken von Geheimnissen ginge. Geheimnisse wiederum gebe es in zwei Bereichen: Zum einen gebe es die Geheimnisse der Natur und andererseits die Geheimnisse der Menschen – sowohl Fakten, die sie nicht über sich selbst wissen, als auch Fakten, die sie lieber im Verborgenen halten

---

<sup>6</sup> Thiel 2014, S. 2.

<sup>7</sup> Thiel 2014, S. 81.

wollten.<sup>8</sup> Die Überzeugung, dass der Westen eine kulturelle Revolution<sup>9</sup> brauche, um wieder im Fahrwasser eines definitiv optimistischen Geistes transformative Projekte großen Ausmaßes angehen zu können, ist das Fundament, auf dem die anderen hier zusammengefassten Überlegungen zur Rolle von Technik und von Geheimnissen auch einen Aufschluss über die Position von Palantir in Peter Thiels System von Glaubenssätzen einnimmt. Computer und Software seien das beste Mittel, um erfolgreiche Firmen am Markt zu etablieren, weil sie über den technologischen Ansatz hohe Effizienzgewinne erlaubten und dabei nicht mit den Bedürfnissen von menschlichen Arbeitern einhergingen. Für Computer sind also weniger Ressourcen nötig und sie können zudem spezifische technologische Angebote machen, die vertikalen Fortschritt bedeuten, so dass Unternehmen, die auf der Arbeit von Computern aufbauen, über ihre Technologie – zumindest eine Zeit lang – außerhalb des Wettbewerbs prosperieren können.<sup>10</sup> Dabei ist der Ansatz von Thiel aber einer, der nicht allein auf Software setzt, sondern diese komplementär zu menschlichen Entscheidungen ansieht. Palantir nutzt Software dezidiert dazu, Geheimnisse von Menschen zugänglich zu machen – um Einsichten aus verschiedenen Datenquellen zu extrahieren. Thiel nutzt für seine Beschreibung von Palantir den Vergleich der beiden größten Spionageeinheiten der USA, nämlich CIA und NSA – und siedelt Palantir als eine glorreiche Verbindung beider Ansätze in der Mitte an, wo sich das Beste aus beiden Welten vereint. Wie die NSA kann Palantir riesige Datenmengen durchkämmen, aber durch die Verbindung mit hochspezialisierten Analysten kann Palantir wie die CIA extrem qualifizierte Entscheidungen treffen.<sup>11</sup>

## 2. Alexander Karp: Der libertäre Gouverneur des Sicherheitsapparats

Alex Karp ist Mitgründer, CEO und Großaktionär von Palantir. Er schreibt nicht so viel und beständig wie Peter Thiel, hat aber gerade in letzter Zeit zwei durchaus beachtete Bücher veröffentlicht, die sich beide dezidiert mit Palantir und mit avancierter Software sowie dem Zusammenspiel althergebrachter und computer-

---

8 Als grundlegenden Ratschlag für Entrepreneurre hält Thiel daher fest: »So when thinking about what kind of company to build, there are two distinct questions to ask: What secrets is nature not telling you? What secrets are people not telling you?«, Thiel 2014, S. 103.

9 Der Begriff der »kulturellen Revolution« ist zunehmend von der Neuen Rechten übernommen worden und markiert dort das Programm, die angebliche linke Hegemonie nach 1968 zu brechen.

10 Vgl. Thiel 2014, S. 144.

11 Vgl. Thiel 2014, S. 146–147.

generierter Intelligenz beschäftigen.<sup>12</sup> Da ist zum einen das Buch *Von Artificial zu Augmented Intelligence*, eine Art Interviewband mit programmatischem Vorwort, wobei die Interviews von Paula Cipierre und Paul Hiesserich, beide zum Zeitpunkt des Erscheinens in leitenden Funktionen bei Palantir, geführt wurden.<sup>13</sup> Ganz im Sinne des Geschäftsmodells von Palantir propagiert das Buch ein symbiotisches Verhältnis menschlicher und künstlicher Intelligenz – und die Interviews geben aus unterschiedlichen Perspektiven Einblicke, wie KI kreative Prozesse, persönliche Sichtweisen und etwa auch handwerkliche Leistungen erweitern könnte. Deutlich programmatischer ist Karp's 2025 erschienenes Buch *The Technological Republic*, das er zusammen mit dem Palantir-Rechtsexperten Nicholas Zamiska verfasst hat. Darin zeichnen die Autoren ein düsteres Weltbild und kritisieren u.a. den aktuellen Zustand der westlichen Technologiebranche. Das Buch fordert einen grundlegenden Wandel ihres Zwecks und ihres Verhältnisses zur Regierung, und es versteht sich als Manifest für einen engagierteren und am nationalen Interesse ausgerichteten Technologiesektor, wobei Palantir viele dieser Prinzipien verkörpert und entsprechend als Vorbild dargestellt wird. Das Buch möchte einen Einblick in das größere politische Projekt geben, das Palantir auch ist. Oder sein soll – Karp betont selbst explizit die Vorteile, die das Erzählen von Heldengeschichten mit sich bringt. Es handelt sich dabei also um eine Arbeit, die klar als Teil der Palantir'schen Selbstvermarktung zu werten ist.

Im Kern ist das Buch eine Anklage gegen die angebliche Selbstzufriedenheit oder auch Selbstvergessenheit des Westens, insbesondere im Silicon Valley, wobei die Darstellung an Martin Heideggers Diagnosen zum »Man« erinnern, mit denen dieser eingängig vermeintliche Verfallsformen von Eigentlichkeit beschrieben hat – also dem, was eigentlich wichtig und an der Zeit wäre. Karp und Zamiska argumentieren, dass zögerliche Führung, intellektuelle Schlappeheit und eine anspruchslose Sicht auf das technologische Potenzial die USA und ihre Partner im Westen – die Rede ist oft von »the West« – verwundbar gemacht haben. Sie behaupten, die Tech-Industrie sei von ihrer historischen Rolle abgekommen, sich großen nationalen Herausforderungen zu stellen, und konzentrierte sich stattdessen auf eine oberflächliche und gewinnorientierte Beschäftigung mit konsumorientierten Anwendungen wie Foto-Sharing-Apps und Marketing-Algorithmen. Das Ziel der Zusammenarbeit von Silicon Valley und US-Regierung müsse dagegen darin bestehen, den geopolitischen Vorteil des Westens aufrecht zu erhalten

---

12 Seine Dissertation »Aggression in der Lebenswelt: Die Erweiterung des Parsonsschen Konzepts der Aggression durch die Beschreibung des Zusammenhangs von Jargon, Aggression und Kultur« hat Alexander Karp übrigens 2002 an der Goethe Universität Frankfurt verteidigt.

13 Vgl. Karp/Hiesserich/Cipierre 2023.

und gegenüber den Feinden zu verteidigen, die schon heute deutlich pragmatischer vorgehen.

Das Buch plädiert für eine Rückkehr zu intensiver Zusammenarbeit von Tech-Branche, einer technologisch versierten Regierung und dem Militär und betont die Dringlichkeit sowie die Notwendigkeit einer Befassung mit nationalen und globalen Herausforderungen, insbesondere dem neuen Wettrüsten mit den Mitteln der künstlichen Intelligenz.<sup>14</sup> KI ermögliche es den Gegnern im militärischen Bereich im Vergleich zu den USA aufzuholen und deren Vormacht herauszufordern. Weil aus der Sicht von Karp KI die internationale Politik im 21. Jahrhundert in ähnlicher Weise bestimmen wird, wie Atomwaffen dies ab der Mitte des 20. Jahrhundert getan haben, müsse deutlich mehr in die Entwicklung entsprechender Software investiert werden – er plädiert für die Entfesselung eines Wettrüstens bezüglich der ausgefeiltesten KI-Waffensysteme.<sup>15</sup> Proklamiertes Ziel ist dabei die Stärke der Abschreckung auf der eigenen Seite zu haben: »a new era of deterrence built on AI is set to begin«. <sup>16</sup> Weil letztlich das Überleben der USA und seiner westlichen Partner davon abhängen, müsse hier mehr investiert werden<sup>17</sup> – als Vorbild könnten Programme in der Größenordnung des Apollo-Programms der NASA zählen – und letztlich fordert Karp mit einem noch drastischeren Vergleich ein neues Manhattan-Projekt:

»The United States and its allies abroad should without delay commit to launching a new Manhattan Project in order to retain exclusive control over the most sophisticated forms of AI for the battlefield – the targeting systems and swarms of drones and eventually robots that will become the most powerful weapons of this century.«<sup>18</sup>

Und Palantir steht genau hierfür bereit – auch gegen Widerstände:

»Palantir builds software and artificial intelligence capabilities for defense and intelligence agencies in the United States and its allies across Europe and around the world. Our work has been controversial, and not everyone will agree with our decision to build products that enable offensive weapons systems. But we have made a choice, notwithstanding its costs and complications.«<sup>19</sup>

Die von Palantir vermeintlich schon vorgelebte Entschiedenheit bei der Konzentration auf die Probleme von nationaler Bedeutung vermisst Karp in großen Teilen der Tech-Branche des Silicon Valley. Ihnen sei die Bedeutung und die letztliche Tragweite der Technologieentwicklung nicht klar, wofür er u. a. auch »linke

---

14 Vgl. Karp/Zamiska 2025, S. 12.

15 Vgl. Karp/Zamiska 2025, S. 26.

16 Karp/Zamiska 2025, S. 28.

17 Vgl. Karp/Zamiska 2025, S. 45.

18 Karp/Zamiska 2025, S. 46.

19 Karp/Zamiska 2025, S. 63.

Diskurse« zu Inklusion sowie etwa auch Debattenbeiträge der Postcolonial Studies verantwortlich macht.<sup>20</sup> Dabei kritisiert Karp »die Eliten« für ihren fortwährenden Angriff auf die Religion zugunsten einer »thin and meager ideology that masquerades as thought«.<sup>21</sup> In für Krisenbeschreibungen typischer Manier spitzt Karp die Säkularisierungstendenzen in der zweiten Hälfte des 20. Jahrhunderts stark zu und spricht von der »systematic eradication of religion from public life« sowie einem »assault on religion«, welcher der Nation ihre Seele zu berauben drohe: »The soul of the country was at stake, having been abandoned in the name of inclusivity. The problem is that tolerance of everything often constitutes belief in nothing.«.<sup>22</sup> Das zeigt nochmal deutlich die Kampfzone, in der Karp im eigenen Land Gegner ausmacht, welche die nationale Identität – in einem »intellectual war on the concept of the nation«<sup>23</sup> – und damit auch die Vormacht der USA in der Welt bedrohen. Ihr Fehler liege nach Karp darin, dass sie sich nicht auf eine Diskussion über nationale Ziele einlassen, sie also nicht bereit sind »to venture into a discussion about the good, as opposed to merely the right«<sup>24</sup> – wobei die Diskussionen über das Gute offenbar v.a. aus dem Fundus der Religion gespeist werden können: »If contemporary elite culture continues its assault on organized religion, what will remain to sustain the state?«<sup>25</sup>

Statt einem Pluralismus oder gar einem »frenetic pursuit of a shallow egalitarianism«<sup>26</sup> nachzugehen, gelte es, sich einem Kampf um das Neue anzuschließen.<sup>27</sup> Und in diesem Kampf soll auch ein »sense of belonging and investment in a grand narrative of triumph and defeat«<sup>28</sup> wiederhergestellt werden, das in der amerikanischen Kultur durch den Angriff auf die Religion und die Inthronisierung eines Pluralismus verlorengegangen sei. Und Karp ist optimistisch: »We will find a way to build coalitions and bands of warriors.«<sup>29</sup> Die aufgrund von Diskussionen um Inklusivität, Egalitarismus etc. fehlgeleiteten Personen der Tech-Branche sollten sich nach Karp nun schnellstmöglich dem nationalen – und für das Buch titelgebenden – Projekt einer »Technological Republic« zuwenden. Also Schluss machen mit dem »technological escapism«<sup>30</sup> marktgetriebener Entwick-

---

20 Die Autoren behaupten, dass die diskursive Bewegung »towards the ethereal, the post-national, and the essentially academic has strained the moral capacity of our species.«, Karp/Zamiska 2025, S. 70.

21 Karp/Zamiska 2025, S. 72.

22 Karp/Zamiska 2025, S. 73.

23 Karp/Zamiska 2025, S. 81.

24 Karp/Zamiska 2025, S. 80.

25 Karp/Zamiska 2025, S. 200.

26 Karp/Zamiska 2025, S. 215 f.

27 Vgl. Karp/Zamiska 2025, S. 201 und 204.

28 Karp/Zamiska 2025, S. 192.

29 Karp/Zamiska 2025, S. 192.

30 Karp/Zamiska 2025, S. 172.

lungen (also von Consumer-Apps) und allzu viel Pietät im Umgang mit Transparenz, Grundrechten und dergleichen:

»The risk is that we begin to privilege the seemingly unobjectionable goals of transparency and process over what actually matters – building submarines, developing our most elusive cures, preventing terrorist attacks, and advancing our interests. Such utilitarian calculus is unattractive. But in any struggle, we must sometimes set aside aesthetic distaste. We too often hide behind our piety as a way of avoiding more challenging and indeed uncomfortable questions about outcomes and results.«<sup>31</sup>

Statt allzu sanftmütiger Abwägungen gelte es, die richtigen Bedarfe zuerst einmal wahr und dann auch ernst zu nehmen. Karp vertritt hier einen an Resultaten orientierten Pragmatismus der »voracious« und »ravenous« ist, also einen ausgehungerten, gierigen, unersättlichen Pragmatismus, wie er der Ingenieurskultur und insbesondere den Tech-Entwicklern des Silicon Valley eigen sei.<sup>32</sup> Karp unterstreicht, was er damit meint, mit einem bemerkenswerten Beispiel, nämlich der Rekrutierung von Wissenschaftlern aus Nazi-Deutschland nach dem Ende des Zweiten Weltkrieges. Wenn man erfolgreich sein will, dann heiligt der Zweck auch mal das Mittel, alte Feinde für die eigene Sache einzuspannen – man dürfe hier nicht zu stolz sein.<sup>33</sup>

Es komme im Prinzip und vor allem darauf an, die richtigen Geschichten zu erzählen, auch gerade im Bereich des Nation-Building. Im Abschnitt »The Next 1000 Years« hebt Karp die Bedeutung von Mythologie und geteilten Geschichten für den Aufbau eines tausendjährigen Empires – man ist geneigt zu denken: Reichs – hervor. Und erläutert wiederum, dass Palantir hier mit seiner Anknüpfung an Tolkiens Saga *Herr der Ringe* ein Positivbeispiel sei.<sup>34</sup> Palantir wird als lebendiges Beispiel für die Umsetzung der Kernbotschaften des Buches dargestellt. Der Fokus des Unternehmens auf »harte Probleme« in Bereichen wie Landesverteidigung, Geheimdienst, öffentliche Gesundheit und Katastrophenhilfe stimmt

31 Karp/Zamiska 2025, S. 187.

32 Vgl. Karp/Zamiska 2025, S. 159, 161 und 167.

33 Vgl. Karp/Zamiska 2025, S. 161.

34 Vgl. Kaarp/Zamiska 2025, S. 199.»The necessary task of building the nation, of constructing a collective identity and shared mythology, is at risk of being lost because we grew too fearful of alienating anyone, of depriving anyone of the ability to participate in the common project. It is this disinterest in mythology, in shared narratives, that we have as a culture taken too far. Palantir takes its name from The Lord of the Rings, by J.R.R. Tolkien, and some have suggested that Tolkien references are favorites of the ›far right.‹ The critique is representative of the left's broader error, both substantive and strategic. An interest in rooting the aims of a corporate enterprise in a broader context and mythology should be celebrated, not dismissed. We need more common tomes, more shared stories, not fewer, even if they must be read critically over time.« übrigens ist Palantir nicht die einzige Firma, an der Peter Thiel beteiligt ist und die Gegenstände oder Namen aus Herr der Ringe zitiert: Es gibt auch noch Anduril (autonome militärische Systeme), Arda (Investments), Mithril (Risikokapital) u. a. m.

direkt mit der Forderung des Buches überein, dass Technologie vitalen nationalen Interessen dienen sollte und nicht nur die Launen des Marktes befriedigen soll. Zudem verkörpert Palantir damit ein gemeinsames – und das heißt bei Karp ein national-US-amerikanisches bzw. auch ein westliches Projekt<sup>35</sup> und bedient sich mythologischen und narrativen Elementen.

Karp geht auch auf das Zustandekommen des wahrscheinlich wichtigsten Vertrags in der Geschichte von Palantir ein, nämlich mit dem US-Militär, also der US-Bundesregierung. Dazu beschreibt Karp zunächst die Situation des US-Militärs in Afghanistan im Jahr 2011, wo die Einsatzkräfte vor Ort oft mit Bombenanschlägen auf Verkehrsrouten Probleme und viele Todesfälle zu beklagen hatten. Karp beschreibt die Situation ähnlich wie heute Fachleute in den Sicherheitsbehörden auch die Lage beschreiben: Es sind viele Informationen da, aber sie sind verstreut und sie ergeben kein Gesamtbild, kein einheitliches Lagebild. Palantir konnte schon 2011 die Informationen zusammenbringen.<sup>36</sup> Weil die Vergabe eines Großauftrags an Palantir allerdings nicht zustande gekommen ist, hat die Firma 2016 ein eine Klage beim US Court of Federal Claims eingereicht, mit dem Argument, dass die US Regierung nicht auf die Produkte kommerzieller Anbieter zurückgegriffen habe, wo dies möglich gewesen sei, sondern stattdessen weiter an einer Eigenentwicklung gearbeitet habe.<sup>37</sup> Palantir hat Recht bekommen und ist seit 2017 einer der zentralen Softwareanbieter des US Militärs.

### 3. Der libertäre Autoritarismus des Neoreactionism

Die kalifornische Ideologie des Technolibertarismus setzt für die Herstellung, Erhaltung und Erweiterung individueller und wirtschaftlicher Freiheit und die größtmögliche Selbstbestimmung der beteiligten Akteure auf digitale Technologien.<sup>38</sup> David Golumbia hat in seiner kritischen Auseinandersetzung mit den Ideen und dem Diskurs des Cyberlibertarismus herausgearbeitet, dass es sich nicht um ein kohärentes System handelt, sondern um eine Ansammlung verschiedener und keineswegs immer zueinander passender Vorstellungen.<sup>39</sup> Schon 1997 hat Langdon Winner in dem Artikel »Cyberlibertarian myths and

---

35 »Palantir itself is an attempt – imperfect, evolving, and incomplete – at constructing a collective enterprise, the creative output of which blends theory and action. The company's deployment of its software and its work in the world constitute the action.«, Karp/Zamiska 2025, S. xvi.

36 Vgl. Karp/Zamiska 2025, S. 141.

37 Vgl. Karp/Zamiska 2025, S. 153.

38 Vgl. di Fabio 2022; Rathje 2025.

39 Vgl. Golumbia 2024a; Golumbia 2024b.

the prospects for community«, auf den der Begriff des Cyberliberalismus zurückgeht, als dessen drei Kernelemente einen technologischen Determinismus sowie Forderungen nach radikalem Individualismus und unbeschränktem Kapitalismus definiert.<sup>40</sup> Für Golumbia ist der Kerngedanke die Überzeugung, dass digitale Technologien außerhalb der Kontrolle demokratischer Regierungen stehen sollten, da nur dann die Möglichkeiten einer uneingeschränkten Selbstverwirklichung im größtmöglichen Ausmaß gegeben seien. Zwei für Thiel und Karp einschlägige Stichwortgeber gehen weit über diese Vorstellungen hinaus: Nick Land und Curtis Yarvin.

Nick Land – »Philosoph« des libertären Autoritarismus – etwa dreht das Denken von Gilles Deleuze und Félix Guattari »auf rechts«. Hierzu übernimmt er insbesondere das Denken in Geschwindigkeitsdifferentialen, Gradienten und Zeitlogiken. So sei, so Land, Neoreactionism (NRx) eine spezifische Art den Zeitpfeil im Feld der politischen Philosophie zu entdecken.<sup>41</sup> Land spricht hier gerne von einer »degenerative ratchet«, einem Mechanismus, der sich nur in eine Richtung bewegen kann: nämlich in Richtung von Fortschritt (»progress«), bis der Mechanismus sich nicht mehr fortsetzen kann und anhält. Das nächste gehöre nicht mehr zur Ratsche selbst, sondern komme von außen. Hier tritt der auch als Mencius Moldbug bekannte Blogger und Informatiker Curtis Yarvin auf den Plan: Dieser sei, so Land, der »critical catalyst« für die NRx-Bewegung, etwa wenn er neben das Bild der Ratsche einen »reboot« als disruptives Außen setze.<sup>42</sup> Dabei verbindet Yarvin radikal anti-demokratischen Libertarismus mit einem zutiefst autoritären Elitedenken, dem jede Gleichheitsvorstellung fremd ist. Kurz: Stattdessen soll eine Art technokratischer »Unternehmens-Feudalismus«<sup>43</sup> geschaffen werden.

### 3.1 Nick Land: anti-humanistische Beschleunigung

Nick Land promovierte 1987 an der University of Essex mit einer Arbeit zu Heidegger und lehrte anschließend bis 1998 an der University of Warwick Kontinentalphilosophie. Hier gründete er zusammen mit der britischen Philosophin

40 Vgl. Winner 1997.

41 Vgl. Land: »The Idea of Neoreaction«, 28.06.2013. Lands Beiträge zur Entwicklung des Neoreactionism sind online in Blogs, Postings und Kommentaren verstreut und wurden in teils frei zugänglichen, teils vermarkteten eBooks herausgegeben. Wir zitieren Land hier nach dem durch den rechtsextremen Kleinverlag Passage Publishing veröffentlichten eBook Xenosystems (Land 2024 [2013]), das Beiträge versammelt, die ursprünglich offenbar unter der nun abgeschalteten Domain xenosystems.net veröffentlicht wurden. Lands Beiträge nennen wir unter Angabe des jeweiligen Beitragstitels mit Datum.

42 Land: »The Idea of Neoreaction«, 28.06.2013.

43 Yarvin: »A Positive Vision«, 13.11.2008.

Sadie Plant die informelle Forschungsgruppe Cybernetic Culture Research Unit (CCRU), in der Philosophie, Science-Fiction, Technokultur und Okkultismus zusammenflossen. Die CCRU wurde in popphilosophischen Kreisen in den 1990er Jahren Kult und Land so als charismatischer wie unkonventioneller Redner bekannt. In diese Zeit fällt auch seine Beschäftigung mit Georges Bataille, was Land zu einer nihilistischen und anti-humanistischen Position führte. 1998 verließ Land Warwick, verfiel dem Amphetaminkonsum und verschwand Anfang der 2000er Jahre aus der Öffentlichkeit. Ab Mitte der 2000er Jahre, nun in Shanghai ansässig, trat Land wieder in Erscheinung als Autor im rechten ideologischen Spektrum. Hier wurde er zur Schlüsselfigur der NRx-Bewegung, für die er auch den Begriff »Dark Enlightenment« prägte.

Lands Denken schließt an den französischen Poststrukturalismus an: Inspiriert von Deleuze' und Guattaris Projekt einer »Universalgeschichte der Kontingenzen« entwickelte Land einen extremen Antihumanismus, der den Anspruch erhebt, Deleuze' und Guattaris Analyse der Dynamik von Kapital und Begehren von der Vorstellung von Wunschmaschinen auf ein maschinelles, also gerade nicht menschliches Begehren hin zu radikalieren. Hier bricht sich ein Denken Bahn, laut dem die Bewegungen des Kapitalismus durch Beschleunigung zu intensivieren seien. Land sieht hier aber anders als Deleuze' und Guattari kein »linkes« transformatives Potenzial, sondern das Versprechen, den Kapitalismus, wenngleich auch mit potenziell katastrophischen Effekten, jenseits des Menschen zu entfesseln – Land führt hier eine radikal ins Positive gewendete Marx-Lektüre mit Ideen einer libidinösen Ökonomie, Ideen der Kybernetik und der Memetik zusammen. Land, als prominentester Vertreter des »*accelerationism*«, entwickelt damit die Vision eines autoritären Technokapitalismus, an dessen (vorläufigem) Endpunkt eine technologische Singularität steht. Kurz: Land radikalisiert deleuzo-guattarisches Denken der Deterritorialisierung durch Beschleunigung, d.h. der Auflösung bestehender, etwa gegen das freie Begehren gerichteter Herrschaftsstrukturen, ohne aber deren Warnung vor der lauernden Reterritorialisierung in anderen »despotischen Regimen« ernst zu nehmen. Schon 1992 sah Land in seiner Studie zu Bataille in jeder Politik, die sich gegen derartige Entwicklungen des Kapitalismus richte, »the last great sentimental indulgence of mankind«: »What matters is burning a hole through the wall.«<sup>44</sup> Die radikal beschleunigten Kräfte des Kapitalismus, der endlich vollständig zu entfesseln und für das Chaos zu öffnen sei, umfasst, kurz gesagt, alles: Technik, Märkte, Informationsflüsse, Körper, ... – alles im Namen einer Überwindung des humanistischen Denkens und der menschlichen Organisati-

---

44 Land 1992, S. 140.

on einer Gesellschaft, dieser »detour in the inexorable death-flow«<sup>45</sup>. Um 2010 spaltete sich der *accelerationism* in ein linkes und ein rechtes Projekt. Der linke Akzelerationismus zielt seitdem in einer »gelenkten Beschleunigung« auf die technologische Entfesselung im Namen einer postkapitalistischen Zukunft, blieb aber eine marginale Position. Lands rechtsgerichteter Akzelerationismus, den er zusammen mit Curtis Yarvin zu einem radikal antidemokratischen Projekt entwickelte, sieht dagegen in der Beschleunigung eine destruktive Kraft um ihrer selbst Willen und erinnerte damit wohl nicht zufällig an das futuristische Manifest und ein Revolutionsdenken Sorell'scher Prägung: Es ist die Vision eines intensiven Lebens in der Entfesselung und der Zerstörung ohne Endziel einer neuen Ordnung. Der Rechtsdeleuzianer Land macht die Demokratie dabei als eine Tradition und althergebrachte Lebensweisen zersetzende Kraft aus: »What democracy has not yet ruined, it is ruining«<sup>46</sup>. Demokratie sei nicht nur nicht mit Freiheit (wie Land sie sich vorstellt) vereinbar, sondern sie bewege sich notwendig auf einen Zustand zu, in dem der Staat die öffentliche Meinung manipulierte.<sup>47</sup>

Die Haltung, die diesem Angriff auf jedes liberaldemokratische Denken zugrunde liegt, sei der »Neoreactionism« – Land legt Wert darauf, es ohne Bindestrich zu schreiben, damit es ein besser findbarer Begriff würde. Es sei die Haltung, die das Scheitern der Demokratie als Instrument der Kontrolle des Staates (d.h. auch dessen Beschränkung) konsequent anerkenne und dies auf die Aufklärung zurückführe: Diese habe nicht nur Tradition und Mythos aufgelöst, sondern auch den Menschen, das Denken, die Technik zu einem Gegenstand der Manipulation gemacht, statt diese tatsächlich freizusetzen. Damit sei der Staat übergriffig geworden. NRx sei demgegenüber eine heterogene Familie von Haltungen, die nicht einfach nur die Gegenaufklärung wiederhole. Zwar finden sich auch in NRx religiös-romantische Haltungen, aber eben auch nationalistisch-rassistische und technokratische Positionen, die jenseits ihrer gemeinsamen Diagnose des totalitären Potentials von Demokratie als Meinungsmanipulationsmaschine unvereinbar scheinen. Land versucht hier Gemeinsamkeiten zu kartieren: Kern seiner Überlegungen ist die Zurückweisung von Gleichheit. Diese werde von der De-

45 Land 1992, S. 30.

46 Land: »The Problem of Democracy«, 09.08.2014.

47 In einer quasi-kybernetischen Denkbewegung argumentieren Land (und Yarvin) hier, demokratische Wahlen legten zwar prima facie jenseits bloßer Kontrolle auch auf Gestaltungs- und Optimierungsbewegungen fest. Tatsächlich fungiere das Wahlgesehen aber dann doch nur als eine Maschine, die lediglich auf Wahlerfolge ziele und nicht auf Wohlergehen. Entsprechend bedürfe es eines effektiveren »Feedback-Mechanismus«. Gemeint ist, dass eine neue, technolibertäre Demokratie im Namen der Effizienz das Elektorat radikal reduziert, etwa auf eine kleine Zahl der finanzstärksten Steuerzahler\*innen. Das Parlament gliche damit einem Aufsichtsrat, der den CEO des Staates bestimme und kontrolliere, vgl. Land: »Undiscovered Countries«, 14.02.2014.

mokratie zwar versprochen, könne von dieser aber nur zum Preis eines Verlusts von Freiheit hervorgebracht werden. Gleichheit sei Kern der Aufklärung und werde von der NRx-Bewegung durchgehend und übereinstimmend zurückgewiesen: »People are not equal. They never will be. We reject equality in all its forms.«<sup>48</sup> Ferner stimme man darin überein, dass die (politische) Rechte recht habe, nicht die Linke, und dass Hierarchie grundsätzlich eine gute Idee sei, wie auch traditionelle Geschlechterrollen. Demokratie sei »irredeemably flawed« und sei abzulösen – und »Liberatarianism is retarded«.<sup>49</sup>

Die letztgenannte Positionierung mag vielleicht überraschen, da Libertarismus selbst ebenfalls zu einer rechten Position gezählt werden darf, wenngleich sicher nicht im völkisch-autoritären Sinne. Mit anderen rechten und gar rechts-extremen Positionen teilt das radikal libertäre Denken jedoch klar sozialdarwinistische Vorstellungen, die gegen Gleichheit, Emanzipation oder sozialen Ausgleich gerichtet sind. Auch hinsichtlich der Lösung, die wir genauer im Fall von Curtis Yarvin rekonstruieren werden, hält Land fest, dass, solange noch keine Tyrannei erreicht sei, was für ihn offenbar bedeutet, dass man sich der (staatlich-demokratischen) Manipulation ja noch entziehen könne, alle Formen von Protest und Rebellion »leftist perversions« seien, die keinerlei Schutz oder Anerkennung verdient hätten.<sup>50</sup> Stattdessen seien alle Lösungen, die für NRx in Frage kämen, Formen der Sezession, also der Abspaltung von bestehenden staatlichen Strukturen, wobei Land offen lässt, ob er hier die Gründung eigener (Klein)Staaten oder individuelle Auswanderungsentscheidungen im Sinn hat. Dabei beruft sich Land auf Friedrich von Hayek, der unter dem Stichwort »Katallaxie« eine Depolitisierung, d.h. die gezielte staatliche Manipulation, zugunsten einer Tradition der spontanen Ordnung beschrieben habe.<sup>51</sup> Land sieht hier nicht-menschliche Kräfte am Werk: Märkte, Maschinen, und wohl in Anspielung auf Gramsci: Monster – aber keine Herrscher.<sup>52</sup> Dazu sei nicht einfach eine »drastic regression« erforderlich, sondern NRx ziele – in einer durchaus unklaren Steigerungslogik – auf eine »highly-advanced drastic regression«.<sup>53</sup> Dazu sei hinter die Ursprünge der Aufklärung zurückzugehen: »because Reason has failed the test of history«.<sup>54</sup>

Land sieht in der NRx-Bewegung einen »Burke-on-steroids« am Werk, eine Überdrehung konservativer Ordnungsvorstellungen, in der die Tradition nicht bewahrt, sondern in einer zynischen Bewegung durch techno-darwinistisch, an-

---

48 Land: »Premises of Neoreaction«, 03.02.2014.

49 Ebd.

50 Ebd.

51 Land: »Flavors of Reaction«, 19.02.2013.

52 Ebd.

53 Ebd.

54 Land: »Neoreaction (For Dummies)«, 17.04.2013.

ti-humanistisch, zersetzend und entfesselt durch ihre Mutation ersetzt werden soll. Was dies noch mit dem vergleichsweise gemäßigten, aber von Land ange-rufenen Konservativen Edmund Burke zu tun haben soll, kann offenbleiben und zeigt vielleicht eher etwas über Lands Schreibstil: Bezüge werden, teils explizit, teils implizit, aufgemacht, selten klar eingelöst, aber überall einer Logik der Überwindung durch Intensivierung oder Beschleunigung unterstellt. Das alles in Antagonismus zu etwas, was bei Land und Yarvin »the Cathedral« heißt.

Die Metapher der Kathedrale ist zu einem prominenten Bezugspunkt und Erkennungszeichen rechter Diskurse geworden und wird meistens auf Curtis Yarvin zurückgeführt. Tatsächlich lässt sich die Metapher bereits 1997 bei Eric S. Raymond finden, der etwa in *The Cathedral and the Bazaar* die Kathedrale als das Schema strukturierter, hierarchischer Softwareentwicklung im Gegensatz zum Modell des Bazars beschrieb, der das offene und dezentral koordinierte Modell der Open Source-Entwicklung beschreibe.<sup>55</sup> Die Kathedralenmetapher erfährt bei Land und Yarvin jedoch eine wichtige Verschiebung: Nicht nur verschwindet weitgehend die Rede vom Bazar – vielleicht ist die freie Konkurrenz von auch linken Ideen doch zu emanzipativ: schließlich haben nicht wenige linke oder emanzipative Ideen ja angeblich eine kulturelle Hegemonie erobert – es geht auch nicht mehr um den Bau der Kathedrale, sondern um die bereits gebaute Kathedrale, kurz: Sie wird zu einem Symbol bestehender kirchlicher (und das meint hier: staatlicher) zentraler Macht. Die Rede vom »deep state« lässt grüßen. Dass sich der Informatiker Yarvin und der Philosoph Land dennoch auf Raymond beziehen, lässt sich kaum übersehen, zumal Yarvin 2022 einen mit »The Cathedral or the Bizarre« überschriebenen Meinungsbeitrag mit Verweis auf Raymond eröffnete und feststelle: »Any centralized organization is a cathedral. Any decentralized movement is a bazaar.«<sup>56</sup> Der demokratische Staat im Bild der Kathedrale ist bei Land also eine zentralisierte Machtformation, die auf die Manipulation des von ihr beherrschten Gebiets optimiert, also nicht über funktionierende Feedbackmechanismen verfügt. Die Antwort auf diese Problemdiagnose können wir bei Curtis Yarvin finden.

---

<sup>55</sup> Raymond hat die Metapher in einem Essay 1997 geprägt und 1999 in einer Monographie weiter ausgearbeitet. Vgl. Raymond 1999, 2001 [1999]. Raymond selbst gibt keine Quelle für diese Metapher an, stellt aber klar, dass er sich den Bau einer Kathedrale vorstellt: Eine hocharbeitsteilige, langfristig angelegte, aber zentral organisierte Bauplanung, in der gewissermaßen von Anfang an die wesentlichen Eigenschaften des Bauwerks feststehen und auf Befehl eines Baumeisters ausgeführt werden. Das mag eine naive Vorstellung des Baus von Kathedralen sein, der Kontrast zum Bazar wird jedoch umso klarer: Auf dem Bazar (der freien Softwareentwicklung) reüssiert, was nachgefragt und weiterverwendet wird. Der Bau der Kathedrale aber enthält in Analogie zur durch ein Unternehmen managementförmig gesteuerte Softwareentwicklung nur »von oben« Gewolltes.

<sup>56</sup> Yarvin 2022.

### 3.2 Curtis Yarvin: Neocameralismus, Patchwork und CEO-Souverän

Curtis Yarvin (\*1973) ist ein US-amerikanischer Softwareentwickler und politischer Autor. Er studierte Informatik an der Brown University und nahm später ein Promotionsstudium an der University of California in Berkeley auf, das er jedoch ohne Abschluss verließ. Seine berufliche Laufbahn begann in der Tech-Industrie, wo er in verschiedenen Softwareunternehmen tätig war, insbesondere im Bereich verteilter Systeme und Netzwerkarchitekturen. In den frühen 2000er Jahren gründete er ein eigenes Technologieunternehmen mit dem Ziel, eine alternative digitale Infrastruktur zu entwickeln. Parallel dazu trat er ab 2007 unter dem Pseudonym Mencius Moldbug mit politischen Schriften hervor. Auch wenn oder vielleicht, gerade weil er keine akademische Karriere verfolgte, gilt er in bestimmten Teilen der Tech-Szene, aber auch in rechtsintellektuellen Zirkeln als brillanter, wenn auch exzentrischer Denker. Bewunderung erfährt er dort weniger wegen formaler akademischer Leistungen als aufgrund seines originellen, oft provokativen Schreibstils, in dem er komplexe politische und technische Fragestellungen in eigenständige Theoriegebäude überführt. Hier erfährt er gerade in der »Dark Enlightenment«-Szene eine regelrechte Hochachtung für seine radikal auftretende Systemkritik, die er mehr noch als Land in Form von Blog-Essays ausarbeitet, insbesondere im Blog *Unqualified Reservations*, das er von 2007 bis 2024 pflegte.<sup>57</sup>

Zu den Yarvin beeinflussenden Autoren müssen der die Österreichische Schule der Nationalökonomie vertretende Wirtschaftswissenschaftler Ludwig von Mises (1881–1973), mit dem US-amerikanischen Ökonom und Philosophen Murray Rothbard (1926–1995) zudem der zentrale Stichwortgeber der anarchokapitalistischen Bewegung und insbesondere der ebenfalls der Österreichischen Schule zuzuordnende Ökonom und Vertreter des Anarchokapitalismus Hans-Hermann Hoppe (\*1949) gezählt werden. Hoppe hatte 2001 mit *Democracy. The God That Failed*<sup>58</sup> die liberalen Demokratien als eine Serie von Misserfolgen zu rekonstruieren gesucht, in der insbesondere Arbeitslosigkeit, Staatsverschuldung und Ausweitung des Staatsapparats durch die politische Einflussnahme von Lobbygruppen unausweichlich seien. Hoppe führt dies insbesondere auf die Vorstellung zurück, die Demokratie basiere auf öffentlichem Eigentum ohne entsprechende Verantwortlichkeit und plädiert für eine Regierung des Privateigentums, wie sie allenfalls in der ebenfalls abzulehnenden Monarchie zu finden gewesen sei. Monar-

---

<sup>57</sup> Anders als in *Lands Fall* ist das Blog *Unqualified Reservations* noch online und präsentiert eine Reihe von eBooks als PDF, die Yarvins Beiträge versammeln. Wir zitieren Yarvin nach den Blog-Einträgen auf *Unqualified Reservations*.

<sup>58</sup> Vgl. Hoppe 2003.

chie sei, wenn man schon einen Staat haben müsse, der Demokratie vorzuziehen, so Hoppe, aber beantwortet würde damit nicht, ob man überhaupt einen Staat haben müsse.<sup>59</sup> Stattdessen seien alle staatlichen Aufgaben zu privatisieren und staatliche Herrschaft damit zugunsten eines völlig entfesselten Marktes abzulösen.

Yarvin, der seinerseits Land seltener erwähnt als umgekehrt, schließt an Hoppes Demokratiekritik an, erkennt in Hoppes Vorstellungen von in freier Konkurrenz stehenden, privaten Sicherheitsunternehmen, die offenbar zugleich als Versicherungen fungieren sollen, »unprotected protection agencies«, also kurz, so Yarvin: »gangs«.<sup>60</sup> Die »gang« erscheint bei Yarvin dann in einem aus seiner Sicht positivem Licht, was seine Werthaltungen deutlich macht: Die »gang« neige, so Yarvin, nämlich dazu, sich territorial zu organisieren, zusammenhängende Gebiete (»real-estate«) zu sichern, sich hierbei nicht zu überschneiden und sich schließlich zu einem Land (»country«) zu entwickeln, das seine Verhältnisse zu anderen »gangs« regelt: »Formalization maximizes the gang's profits and greatly improves its clients' quality of life.«<sup>61</sup> Es ist eine typische Geste der Yarvin'schen Gedankengänge, negativ konnotierte Begriffe zu wählen und diese dann in einer Art transgressiven Humor umzudeuten. Yarvin zielt dabei aber nicht nur auf die Beschreibung eines von ihm imaginierten Idealzustands gegenüber einem problematisierten Ist-Zustand, sondern möchte Wege zur Herbeiführung des Idealzustands skizzieren. Auch wenn er dies selbst vielleicht nicht umsetzen könne – so wenig wie er ein Regisseur sei, obzwar er Filme möge –, spekuliert Yarvin über mögliche Wege zur Umsetzung, ohne hier freilich allzu konkret zu werden. Sicher ist nur, dass die Außenpolitik (mit Ausnahme der Sicherheitspolitik) beendet und die US-Regierung, gar der gesamte US-Staatsverbund aufgelöst werden müsse und zwar zugunsten einer Aufteilung in seine »largest 100 or 200 or 500 metropolitan areas«, im Rückgriff auf Tom Hayden: »one, two, three, many Monacos«.<sup>62</sup> Diese Vorstellung einer Auflösung klassischer Nationalstaaten zu einem Netzwerk marktwirtschaftlich konkurrierender Klein- oder Stadtstaaten bezeichnet Yarvin als »Patchwork« – einem »Political System for the 21st Century«, so der Untertitel des unter dem Autorennamen Mencius Moldbug vermarkteten E-Books, das Blogbeiträge sammelt. Das Cover des offenbar im Eigenverlag erschienenen eBooks schmückt

---

59 Vgl. Hoppe zit. n. Yarvin: »From Mises To Carlyle«, 04.02.2010. <https://www.unqualified-reservations.org/2010/02/from-mises-to-carlyle-my-sick-journey/> (01.10.2025).

60 Yarvin: »What is to be done?«, 02.07.2008.

61 Ebd.

62 Ebd. Wo Yarvin 2008 aber noch an die bleibende Bedeutung des US-Dollars zu glauben scheint, verbindet sich spätestens ab Mitte der 2010er Jahre auch die Vorstellung dezentraler Digitalwährungen wie Bitcoin mit neoreaktionären Vorstellungen.

übrigens eine deutschsprachige Karte des alten deutschen Reiches etwa zur Mitte des 18. Jahrhunderts mit seinen unzähligen Klein- und Kleinststaaten.

Es geht Yarvin aber keineswegs um eine Rückkehr zur Verfassung des Heiligen Römischen Reiches Deutscher Nation mit einer möglichst schwachen Reichsebene (wenngleich dies dem heutigen Zustand gegenüber sicher eindeutig vorzuziehen wäre, so Yarvin) und es geht ihm auch nicht um eine Wiedererrichtung eines Netzes von kulturell verbundenen, aber politisch unabhängigen Stadtstaaten des alten Griechenlands, sondern um die Remodellierung der Patchwork-Staaten als private Unternehmen. Diese als Neokameralismus bezeichnete Vorstellung, die sich selbst als durch den preußischen Kameralismus inspiriert betrachtet und dessen Verwaltungslogik neu interpretieren will, ist radikal technokratisch und unternehmerisch: Das Staatsziel wird die Effizienz und Stabilität der »Staatsfirma«, die von einem CEO geführt wird, der aber von einer Souveränität der Shareholder abhängig ist und dessen Legitimation auf Eigentum und Leistung basieren soll. Das Leistungsprinzip gilt auch für die Einwohner\*innen des Patchwork-Staates: Statt zu verwaltende Untertanen oder vielleicht sogar Bürger\*innen sind sie gleichermaßen Kund\*innen und Humankapital, über das rational und im Namen des Privateigentums zu herrschen ist, was – und hier zieht sich die argumentative Schlinge zu – auf eine radikale Reduktion staatlicher Eingriffe hinauslaufen soll: Da die Einwohner\*innen zugleich Kund\*innen sind, können diese jederzeit kündigen und den Staat verlassen, was eine an der Freiheit des Einzelnen ausgerichtete Regierung im Mikrostaat sichern soll.

Nach Yarvins Vorstellung des Neokameralismus sollen dabei Staat und Unternehmen zu »Sovcorps« verschmelzen, einer Verbindung aus »sovereigns« (Staat) und »corporations« (Unternehmen). Entscheidungen zu treffen und durchzusetzen werde dadurch einfacher, schneller, effektiver: Weil Politik und Wirtschaft nicht mehr als getrennt verstanden werden, sondern als Teile einer Organisation. Wirtschaftliche Macht basiere dabei auf dem Streben nach Exportüberschüssen – und Handelsdefizite gelten als Schwäche, die unter anderem durch Zölle oder andere protektionistische Maßnahmen zu beseitigen sei. Schließlich ließen sich nach Yarvin durch einen modernen Staatsfond übergreifende Projekte finanzieren und strategische Reserven bilden – ähnlich der einstigen »Kriegskasse« des preußischen Staates.<sup>63</sup> Der Neokameralismus hat wenig mit seinem angeblichen historischen Vorbild gemein, bedient sich aber dessen Vokabulars – eine weitere für Yarvin typische Denkgeste: Nur mäßig verstandene historische Vorstellungen oder Verhältnisse dienen als Ausgangspunkt für eine Spekulation, die libertär-autoritäre Vorstellungen reaktualisiert, womit das antidemokratische Ergebnis bereits feststeht.

---

63 Vgl. Hübl 2025.

### 3.3 Zusammenfassung

Zusammenfassen lassen sich die vielzähligen Motive, mit denen die angeführten Autoren arbeiten, nur schwer. Klar tritt das negative Freiheitsverständnis hervor, das in staatlichen oder supranationalen Regulierungen nichts anderes erkennen kann als die Einschränkung von Entfaltungsmöglichkeiten. Hinzu kommt ein Akzelerationismus, ein Denken im Stil der Maxime »move fast and break things«. Das Verhältnis libertär-autoritärer Ideen zu Szenarien eines antidemokratischen Umsturzes und zur Gewalt bleibt ambivalent. Einerseits erklärt Curtis Yarvin, jener auch für Thiel einflussreiche Vordenker libertär-autoritären Denkens, sein eigener Ansatz reagiere auf das Scheitern demokratischer und internationaler völkerrechtlicher Ordnungen an der Aufgabe, Gewalt und Kriege ein für alle Mal zu beenden. Ziel sei es, so Yarvin, eine Ideologie zu finden, in der Gewalt – gemeint ist körperliche Gewalt, keine geistige oder strukturelle Gewalt – nicht mehr vorkomme. Andererseits kann ein Szenario, welches das demokratisch legitimierte, staatlich durchgesetzte Gewaltmonopol durch private Sicherheitsfirmen ersetzen will, nicht als gewaltfrei bezeichnet werden. Es richtet sich gegen die Demokratie und enthält auch der Zivilgesellschaft gegenüber eine permanente Drohung mit Gewalt: Eine Privatpolizei nicht länger staatlich eingeehten Typs würde mit Gewalt insbesondere das Eigentumsrecht schützen. Freilich müssten, so Yarvin, auch die – nun notwendig bewaffneten Sicherheitsdienste – daran gehindert werden, die Eigentumsordnung in Frage zu stellen. Er stellt sich hier eine kryptografische Absicherung vor: Die Waffen der Sicherheitsarbeiter seien mit Schlüsseln zu sichern, die die Shareholder, also die besitzende Klasse des zu schützenden Privatstaates, kontrollierten, womit sie den Einsatz der Waffen freigeben und widerrufen könnten. So soll, wohlgemerkt, nicht ein Schutz von Individuen insgesamt organisiert, sondern allein die Durchsetzung des Eigentumsrechts realisiert werden.

Der libertäre Autoritarismus erweist sich damit als ein ideologischer Hybrid. Es geht teils um die Rückkehr zu vorstaatlichen Werten, teils um eine technokratische Zukunftsvision, deren autoritäre Praxis sich zwar oft theorieschwach zeigt, aber nichtsdestoweniger Anleihen aus ganz verschiedenen Quellen aufgreift und vermengt. Die Position Thiels bejaht diese Vermengung, versteht sich aber gerade darin dann doch als »Denken« – und sogar als aufklärerisch. Es lässt sich auf die Dark Enlightenment-Bewegung zurückführen. Geprägt von Nick Land, um sich gegen die Ideale der historischen Aufklärung zu stellen, wurde die »Dunkle Aufklärung« insbesondere mit Curtis Yarvin zur Bewegung. Die »Dunkle Aufklärung« sieht in den als aufklärerisch markierten Werten wie Vernunft, Fortschritt, Gleichheit und Demokratie die Ursache für moralische Schwäche, gesellschaftlichen Verfall und ineffiziente Regierungen, wogegen nur eine Rückkehr zu hierar-

chischen, autoritären Gesellschaftsformen helfen könne. Herbeizuführen ist dies im Einklang mit revolutionären Palingenesevorstellungen durch eine intellektuelle Elite, die zunächst mit liberal-demokratischen Vorstellungen zu brechen habe. Anders aber als die historische Bewegung der Gegenaufklärung des 18. und 19. Jahrhunderts mit ihren religiösen und romantischen Strömungen, positioniert sich die dunkle Aufklärung technokratisch und weit überwiegend säkular. Sie nimmt also Elemente der Gegenaufklärung zweifelsohne auf, argumentiert aber nicht etwa metaphysisch oder allein mit der Natur des Menschen, sondern basiert auf einer Radikalisierung ökonomischer Theorien, die man als solche eher der Moderne zuschlagen wird. Anders als in ultranationalistischen Vorstellungen existiert in der dunklen Aufklärung auch kein organischer, mit der »Schicksalsgemeinschaft Nation« identifizierbarer Volkskörper, sondern eine radikal individualisierte Herrschaft des als Privateigentümer imaginierten, allein seinen Eigeninteressen verpflichteten Subjekts.

#### 4. Karp, Thiel und die »Dunkle Aufklärung«

Die offensiv politischen Botschaften und auch die dubiosen Kontaktnetze von Vertreterinnen und Vertretern des Silicon Valley sind in den letzten Jahren vielfach dargestellt worden. Ob es um die Verbindungen der Chefs der Tech-Konzerne zum Rechtspopulismus geht,<sup>64</sup> um die im Valley geschürten Krisennarrative, die Gefahren heraufbeschwören und dann individualistische Handlungsalternativen gegenüber kollektiven Lösungen induzieren,<sup>65</sup> oder um die Anstrengungen einer digitalen Transformation der Marktwirtschaft<sup>66</sup>: Die »politische Ideologie des Silicon Valley«<sup>67</sup> ist dabei kein kohärentes politisches Programm, aber einige Strömungen gewinnen dennoch immer deutlichere Konturen. Tilman Baumgärtel hat in einer Artikelserie die Einflüsse der »Make America Great Again«-Bewegung zusammengestellt und geht dabei insbesondere auch auf Nick Land und Curtis Yarvin ein, die er als Inspiratoren einer Dark Maga-Bewegung ausmacht.<sup>68</sup> Peter Thiels Einfluss auf die Regierung ist mittlerweile auch nicht mehr beschränkt auf beratende Funktionen wie in Trumps erster Administration (wo

---

64 Vgl. Ferrari 2020, Merrin/Hoskins 2025.

65 Vgl. Ray 2021.

66 Vgl. Hüther 2022.

67 Dörr/Kowalksi 2022.

68 Vgl. Baumgärtel 2025a.

er auch 2017 schon als »Schattenpräsident«<sup>69</sup> bezeichnet wurde), sondern fest verankert über zahlreiche Vertraute – bis hin zum Vizepräsidenten.<sup>70</sup>

Peter Thiel hat nur selten direkt über Curtis Yarvin gesprochen. Öffentliche Äußerungen von Thiel zeigen jedoch eine auffällige inhaltliche Nähe zu Yarvins Kernthesen, insbesondere was die Kritik an der Demokratie und die Befürwortung technokratischer oder monarchischer Regierungsformen betrifft. Umgekehrt zitierte Yarvin zum Beispiel Thiels Aussage, dass Freiheit und Demokratie nicht miteinander vereinbar seien. Wie auch Yarvin betrachtet Thiel Demokratie als dysfunktional und unfrei. Thiel hat wiederholt durchblicken lassen, dass er eine starke, unternehmerisch geführte Exekutive für effektiver hält als pluralistische Demokratie; und er hat die besten Unternehmensgründer mit Diktatoren verglichen sowie herausgekehrt, dass Startups keine Demokratien seien, sondern von visionären Führern gelenkt werden müssten. Dies korrespondiert mit Yarvins Idee, dass der Staat durch einen allmächtigen CEO-Monarchen wie ein Unternehmen geführt werden sollte. Die Gleichsetzung von unternehmerischer Führungsstärke mit autokratischer Macht ist bei beiden unübersehbar. Ebenfalls teilen beide die Vorstellung eines Endes von Fortschrittsnarrativen, etwa indem sie die etablierte Vorstellung ablehnen, die westlichen Gesellschaften entwickelten sich stets positiv weiter. Wir hatten gesehen: Thiel warnt hier vor Stagnation in Technologie und Gesellschaft und zeigt sich pessimistisch, dass liberale Demokratien Fortschrittsversprechen einlösen können. Auch dies korrespondiert zu einer Aussage Yarvins: Dieser lehnt das grundlegende Versprechen des Liberalismus von einem unabwendbaren Weg in den Fortschritt ab. Thiel und Yarvin weisen beide Fortschrittsglauben als naiv zurück. – Nun ist ein undifferenzierter Fortschrittsglaube natürlich naiv, aber es ist eine deutliche Gemeinsamkeit zwischen beiden, wie sie ihre Ablehnung von Fortschrittsnarrativen begründen.

Inhaltlich lassen sich also durchaus Analogien und Gemeinsamkeiten zwischen beiden finden, während sich ablehnende oder kritische Aussagen Thiels über Yarvin gerade nicht finden lassen. Deutlich wird aber, dass, wenn Thiel auch kaum über Yarvin spricht, seine inhaltlichen Positionsnahmen stark mit den Ideen Yarvins übereinstimmen. Kurz gesagt bleibt Thiels Profil in Bezug auf Yarvin zustimmend bis schweigend, ohne erkennbare öffentliche Ablehnung. Dies ist umso auffälliger, da es durchaus indirekte Hinweise auf Thiels Wertschätzung gegenüber Yarvin gibt: Peter Thiel hat Projekte von Yarvin finanziell gefördert, zum Beispiel eines seiner Startups, und auch Personen aus Yarvins unmittelbarem Umfeld. Zudem sind Peter Thiel und Curtis Yarvin offenbar Teil

---

<sup>69</sup> Vgl. Lobe 2017

<sup>70</sup> Vgl. Baumgärtel 2025b.

gemeinsamer Netzwerke und Thiel lud Yarvin Berichten zufolge zu exklusiven, auch privaten Veranstaltungen ein. Auch Yarvin prahlte mit seinen Kontakten zu Thiel, so dass Yarvin teilweise als Haus-Philosoph Peter Thiels gilt. Hinzu kommt, dass Thiel in den letzten Jahren offenbar gezielt Politiker\*innen förderte, die von Yarvin beeinflusst sind, nicht zuletzt eben auch den US Vizepräsidenten J.D. Vance. Schließlich trägt Thiel aktiv zur Verbreitung von Yarvins Ideen bei: Dazu gehört auch die Finanzierung von rechtsintellektuellen und neoreaktionären Stimmen und Netzwerken, die sich öffentlich auf Yarvins Ideen beziehen, wie beispielsweise die National Conservatism Conference (NatCon). Es zeichnet sich damit das Bild ab, dass Thiel gewissermaßen hinter den Kulissen als ideeller und auch finanzieller Förderer oder Verbündeter von Yarvin fungiert, ohne sich öffentlich allzu deutlich hierzu bekennen zu wollen. Dabei sollte nicht unerwähnt bleiben, dass sich Thiel öffentlich gemäßigter äußert als Yarvin. Er distanziert sich gleichwohl nicht von beispielsweise völkisch-rassistischen Bemerkungen Yarvins (die allerdings länger zurückliegen), sondern kommentiert diese schlicht nicht. Deutlich wird aber, dass beide die Vision einer postdemokratischen Ordnung unter Führung von reichen Eliten teilen. Differenzen zwischen beiden sind eher dem Stil und dem Auftreten zuzuschreiben, was daran liegen mag, dass Thiel als Unternehmer mögliche Kunden nicht verprellen will, während Yarvin sich bewusst als provokanter Theoretiker inszeniert.

Eine naheliegende Frage ist, inwiefern Yarvins Denken Spuren in Palantirs Unternehmensphilosophie oder Strategie hinterlassen hat. Palantir wurde explizit dafür gegründet, um mit Technologie staatliche Aufgaben effizienter zu lösen, insbesondere der Terrorabwehr und Geheimdienstanalyse. Thiel und Karp sahen hier nach dem 11. September 2001 die Chance, den Westen zu unterstützen, indem das Silicon Valley die sich als überbordende Bürokratie auswirkende staatliche wie auch militärische Administration verbessern könnte.<sup>71</sup> Wiederkehrend scheint das Leitmotiv zu sein, technisches Know-how der Privatwirtschaft zum Retter des Staates zu machen, die Regierung also an eine Tech-Elite zu übergeben. Privatunternehmen sollen die Probleme lösen, an denen der Staat scheitert. Dies ist besonders deshalb bedenkenswert, weil die Software von Palantir im Ergebnis gewissermaßen hoheitliche Aufgaben übernehmen soll. Hinzu kommt, dass Palantir damit wirbt, gegen behördliche Trägheit und Regularien anzukämpfen, um effiziente Lösungen durchzusetzen. Die Rede vom »tiefen Staat« (also in der Administration angeblich verborgenen Verschwörungen) ähnelt dieser Semantik des Aufräumens und gegen Widerstände gebotenen Beschleunigens durchaus.

---

<sup>71</sup> Vgl. das Kapitel »A New Crusade« über Peter Thiel und die Gründung von Palantir in Lalka 2024, S. 239 ff. sowie Thiel 2014, S. 146 f. und Karp/Zamiska 2025, S. 139 ff.

Palantir zögerte vor diesem Hintergrund nicht, sich in Vergabeverfahren der US-Regierung einzuklagen. Sowohl Thiel und Karp als auch Yarvin haben offenbar die Vorstellung, als verkrustet denunzierte Verwaltungswege gelte es zugunsten effizienter Technologien schleunigst abzulösen – zumindest im ersten Schritt auf dem Weg zum Neokameralismus. Kurz: klassische Vorstellungen von staatlicher Bürokratie werden durch effiziente algorithmische Plattformen abgelöst. Auch hier muss allerdings eingeräumt werden, dass es keine direkten Aussagen gibt, die Yarvins Einfluss auf Palantir belegen. Das Unternehmen betont vielmehr den Nutzen seiner Software und spricht nicht über ideologische Ziele im engeren Sinn. Unübersehbar ist jedoch die Vorstellung, liberale Institution durch Technologie aufzurüsten oder doch zugleich abzulösen.

## 5. Autoritäre Ausnahmezustandsrhetorik, technokratische Herrschaftsszenarien – und die Belange ganz normaler Sicherheitsbehörden in Deutschland heute

Man vergisst leicht die schlichtweg marketingstrategischen Interessen der Protagonisten, lässt man sich auf die ideologischen Hinter- und Abgründe der durch Karp, Thiel und andere propagierten Krisendiagnosen näher ein. Vieles an den raunenden politischen Botschaften, an der autoritären Ausnahmezustandsrhetorik und den technokratischen Herrschaftsszenarien, dürfte schlicht Selbstinszenierung sein:<sup>72</sup> Man will als »intellektuelle« Stimme gelten, während man zugleich einfach um des Geschäfts willen gezielt auf (sicherheits)politische Stimmungslagen einwirkt. Beide Male geht es um Vermarktung eines Produkts – eines Produkts, das man in Deutschland freilich besser auf andere Weise vermarkten würde. Thiels philosophisches Interesse wirke, so der Soziologe und FAZ-Mitherausgeber Jürgen Kaube, »ein wenig wie die Begeisterung von Jungs, die Autoquartett spielen, ohne eine Fahrerlaubnis zu haben, nur dass auf den Spielkarten hier philosophische Namen stehen«.<sup>73</sup>

Wieviel Ideologie steckt nun aber im Code? Ist an der Entscheidung für hesenDATA mehr zu kritisieren als die Überweisung von Steuermillionen an eine Firma mit rechtslibertär-antidemokratischer Aura? Immerhin scheint Palantir Inc. mit mehreren deutschen Landesministerien verlässlich und augenscheinlich einigermaßen sachgerecht zusammenzuarbeiten. Dies zeigt, dass das Unternehmen zwar offensiv Infrastrukturen für den politischen Ausnahmezustand

---

<sup>72</sup> Vgl. auch Zorn 2025.

<sup>73</sup> Kaube 2025, S. 41.

feilbietet und verkauft. Es tritt aber doch so seriös auf, dass es im Zweifel bei einem ganz normalen Softwarekauf bleibt.

Glaut man den hessischen Beteiligten, dann würden sie lieber heute als morgen eine andere Software nutzen. Auch so kann eine Locked-in-Situation aussehen: Man kommt nicht von einem Anbieter nicht los, sondern man findet keinen anderen Anbieter als jenen einen. Die mit der Reminiszenz an Tolkiens Palantiri verbundene Idee der Mutprobe – wer stark genug ist, dem kann die große Macht, die den Steinen innewohnt, nichts anhaben, denn sie werden ihm »dienen« – lässt sich so womöglich auf die Situation des Palantir-Kunden übertragen: Für sich der Demokratie verpflichtet fühlende Entscheider\*innen wird es zur Mutprobe, sich auf das Unternehmen einzulassen: Man muss der (erhofften) Neutralität des Produkts das Wort reden. Man muss erklären, warum es nicht anders geht, und man muss der Öffentlichkeit die Sorge nehmen – vielleicht nicht vor dem sehr speziellen Image der Firma und ihrer Spitzenleute, aber doch davor, dass das Produkt selbst dem Rechtsstaat letztlich schadet.

Allerdings sollte man die Zwangslage dann auch offen zugeben: Man greift notgedrungen zum Produkt dieses Anbieters. Und dies auch, weil es der öffentlichen Hand jahrelang egal war, wie man die Polizei im Datenbank- und Softwarebereich ausstattet, so dass jetzt, wo man aufholen will, der Umgang mit den Altdatenbanken so komplex ist, dass es rein technisch an Alternativen fehlt. Dass Palantir sehr wohl weiß, sich als ganz normales Unternehmen zu »benehmen«, beantwortet die Frage gleichwohl nicht, inwieweit der Code tatsächlich doch Ideologie ist. Oder vielleicht auch werden könnte. Daran, dass die Vertreter der Ideologie in jedem Fall davon profitieren, an ganz normale Sicherheitsbehörden zu liefern, dürfte jedenfalls kein Zweifel bestehen.

## Quellen und Literatur

- Baumgärtel, Tilman, »Toxische Inspiratoren« (2025a), in: *Jungle World* 2025/21, 22.05.2025. <https://jungle.world/artikel/2025/21/maga-einfluss-ideologie-usa-toxische-inspiratoren> (01.10.2025).
- Baumgärtel, Tilman, »Technokratische Weltheilung« (2025b), in: *Jungle World* 2025/23, 05.06.2025. <https://jungle.world/artikel/2025/23/regierung-trump-ideologie-bewegung-dark-maga-technokratische-weltheilung> (01.10.2025).
- Brayne, Sarah, *Predict and surveil: Data, discretion, and the future of policing*, Oxford 2020.
- Chafkin, Max, *The Contrarian: Peter Thiel and Silicon Valley's Pursuit of Power*, New York 2021.
- Di Fabio, Udo, »Künstliche Intelligenz und vernetzte Wertschöpfung – untergräbt die digitale Entwicklung unsere ethischen und verfassungsrechtlichen Fundamente?«, in: Di Fabio,

- Udo/Dörr, Julian/Kowalski, Kowalski (Hg.): *Made in California. Zur politischen Ideologie des Silicon Valley*, Tübingen 2022, S. 215–225.
- Doherty, Brian, »Wait, Wasn't Peter Thiel a Libertarian?«, in: *reason*, August/September 2020. <https://reason.com/2020/08/02/wait-wasnt-peter-thiel-a-libertarian/> (01.10.2025).
- Dörr, Julian/Kowalski, Olaf, »Die politische Ideologie des Silicon Valley«, in: Di Fabio, Udo/Dörr, Julian/Kowalski, Kowalski (Hg.): *Made in California. Zur politischen Ideologie des Silicon Valley*, Tübingen 2022, S. 9–49.
- Ferrari, Elisabetta, »Technocracy Meets Populism: The Dominant Technological Imaginary of Silicon Valley«, in: *Communication, Culture and Critique*, Volume 13, Issue 1, 2020, S. 121–124.
- Golumbia, David, Cyberlibertarianism, *The Right-Wing Politics of Digital Technology* (2024a), Minneapolis 2024.
- Golumbia, David, »The Critique of Cyberlibertarianism« (2024b), in: *boundary 2*, Jg. 51, H. 2, 2024, S. 5–18.
- Griffin, Roger, *The nature of fascism*, London 1993.
- Harris, Mark, »How Peter Thiel's secretive data company pushed into policing«, in: *Wired*, 09.08.2017. <https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/> (01.10.2025).
- Hobe, Stephan, »Seasteading, Marskolonie und Erklärungen über neue ›Staaten‹ auf Hoher See und im Weltraum – Kennzeichen neuer Staatlichkeit?«, in: Di Fabio, Udo/Dörr, Julian/Kowalski, Kowalski (Hg.): *Made in California. Zur politischen Ideologie des Silicon Valley*, Tübingen 2022, S. 145–155.
- Hoppe, Hans-Hermann, *Democracy: The God That Failed*, New Brunswick 2001 (Englische Ausgabe).
- Hübel, Hagen, »Die dunkle Seite der Aufklärung: Curtis Yarvin und der Einfluss auf MAGA«, in: *Medium*, 22.02.2025. <https://medium.com/weitgedacht/die-dunkle-seite-der-aufkl%C3%A4rung-curtis-yarvin-und-der-einfluss-auf-maga-d72622597709> (01.10.2025).
- Hüther, Michael, »Public Valley: Marktwirtschaft und Demokratie in der digitalen Transformation«, in: Di Fabio, Udo/Dörr, Julian/Kowalski, Kowalski (Hg.): *Made in California. Zur politischen Ideologie des Silicon Valley*, Tübingen 2022, S. 119–143.
- Iliadis, Andrew/Acker, Amelia, »The seer and the seen: Surveying Palantir's surveillance platform«, in: *The Information Society*, Jg. 38, H. 5, 2022, S. 334–363.
- Karp Alexander C./Hiesserich, Jan/Cipierre, Paula, *Von Artificial Intelligence zu Augmented Intelligence – Was wir von der Kunst lernen können, um mit Software die Zukunft zu gestalten*, Frankfurt/New York 2023.
- Karp, Alexander C., Aggression in der Lebenswelt: Die Erweiterung des Parsonsschen Konzepts der Aggression durch die Beschreibung des Zusammenhangs von Jargon, Aggression und Kultur. Inauguraldissertation zur Erlangung des Grades eines Doktors der Philosophie im Fachbereich Gesellschaftswissenschaften der Johann Wolfgang Goethe Universität zu Frankfurt am Main 2002.
- Karp, Alexander C./Zamiska, Nicholas W., *The Technological Republic. Hard Power, Soft Belief and the Future of the West*, London 2025.
- Kaube, Jürgen, »Citizen Thiel«, in: *Frankfurter Allgemeine Sonntagszeitung*, 06.06.2025, S. 41 f.
- Knight, Emma/Gekker, Alex »Mapping interfacial regimes of control: Palantir's ICM in America's post-9/11 security technology infrastructures«, in: *Surveillance and Society*, Jg. 18, H. 2, 2020, S. 231–243.

- Lalka, Rob, *The Venture Alchemists. How Big Tech Turned Profits Into Power*, New York 2024.
- Land, Nick, *The Thirst for Annihilation. Georges Bataille and Virulent Nihilism*, London/New York 1992.
- Land, Nick, *Xenosystems*, o.O. 2024 [2013].
- Lobe, Adrian, »Sie nennen ihn den »Schattenpräsidenten«, in: *FAZ.NET*, 23.06.2017. <https://www.faz.net/aktuell/feuilleton/debatten/investor-peter-thiel-wirkt-als-berater-von-donald-trump-15074445.html> (01.10.2025).
- Merrin, William/Hoskins, Andrew, *SHARDED MEDIA. Trump's Rage Against the Mainstream*, Hampshire 2025.
- Mühlhoff, Rainer, *Künstliche Intelligenz und der neue Faschismus*, Ditzingen 2025.
- Rathje, Jan, »Cyberlibertarismus als Problem für liberale Demokratien«, in: *CeMAS-Blog*, 19.05.2025. <https://cemas.io/blog/cyberlibertarismus-als-problem-fuer-liberale-demokratien/> (01.10.2025).
- Ray, Emily, »Creature Comforts: Neoliberalism and Preparing for Disaster«, in: *New Political Science*, Jg. 43, H. 2, 2021, S. 171–188.
- Raymond, Eric S., »The cathedral and the bazaar«, in: *Knowledge, Technology & Policy*, Jg. 12, 1999, S. 23–49.
- Raymond, Eric S., *The Cathedral & The Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary*, Sebastopol 2001 [1999].
- Sacks, David O./Thiel, Peter, *The Diversity Myth. Multiculturalism and Political Intolerance on Campus*, Oakland 1995.
- Thiel, Peter, »The Education of a Libertarian«, in: *Cato Unbound*, 13.04.2009. <https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/> (01.10.2025).
- Thiel, Peter, *Zero to One. Notes on Startups, or How to Build the Future*, Peter Thiel with Blake Masters, New York 2014.
- Thiel, Peter, »Competition is for Losers«, in: *The Wall Street Journal*, 12.09.2014. <https://www.wsj.com/articles/peter-thiel-competition-is-for-losers-1410535536> (01.10.2025).
- Thiel, Peter, »The Straussian Moment«, in: Hamerton-Kelly, Robert (Hg.): *Politics & Apocalypse*, East Lansing 2007, S. 189–218.
- Winner, Langdon, »Cyberlibertarian myths and the prospects for community«, in: *SIGCAS Comput. Soc.*, Jg. 27, H. 3, 1997, S. 14–19.
- Yarvin, Curtis: »An Open Letter to Open-Minded Progressives. Chapter XII: What is to be done?«, in: *Unqualified Reservations*, 02.07.2008. <https://www.unqualified-reservations.org/2008/07/olxii-what-is-to-be-done/> (01.10.2025).
- Yarvin, Curtis: »Moldbug on Carlyle. Chapter 1: From Mises to Carlyle: My Sick Journey to the Dark Side of the Force«, in: *Unqualified Reservations*, 04.02.2010. <https://www.unqualified-reservations.org/2010/02/from-mises-to-carlyle-my-sick-journey/> (01.10.2025).
- Yarvin, Curtis: »Patchwork: A Political System for the 21st Century. Chapter 1: A Positive Vision«, in: *Unqualified Reservations*, 13.11.2008. <https://www.unqualified-reservations.org/2008/11/patchwork-positive-vision-part-1/> (01.10.2025).
- Yarvin, Curtis: »The Cathedral or the Bizarre«, in: *Tablet*, 31.03.2022. <https://www.tabletmag.com/sections/news/articles/the-cathedral-or-the-bizarre> (01.10.2025).
- Zorn, Daniel-Pascal, Dossier: »Peter Thiel – der Vermittler«, in: *Politik&Ökonomie. Beiträge zur politischen Ökonomie*, 02.06.2025. <https://politischeoekonomie.com/dossier-peter-thiel-der-vermittler/> (01.10.2025).

# Rechtspolitischer Rück- und Ausblick – hessenDATA und der schmale Grat zwischen polizeilicher Effizienz und Grundrechtsschutz

*Michael Bäuerle*

## 1. Einleitung

Seit dem Urteil des Bundesverfassungsgerichts vom 16.2.2023 sind in Bund und Ländern rege gesetzgeberische Aktivitäten und parlamentarische Diskussionen zu verzeichnen, die in den Medien aufmerksam beobachtet werden.<sup>1</sup>

Infolge des Urteils wurden zunächst die Normen in Hamburg und Hessen überarbeitet; es gelten nun in Hessen § 25a HSOG n. F. vom Juli 2023 und in Hamburg § 49 HmbPolDVG n. F. vom Februar 2025, wobei letzterer erneut der hessischen Regelung nachgebildet ist. Insoweit war die gesetzgeberische Tätigkeit keine Besonderheit, da die Anpassung von Sicherheitsgesetzen an Vorgaben des Bundesverfassungsgerichts und der Landesverfassungsgerichte mittlerweile zu einer Standardaufgabe der Gesetzgeber von Bund und Ländern geworden ist. Seit 1999 sind nicht weniger als 34 Entscheidungen alleine des Bundesverfassungsgerichts zu sicherheitsrechtlichen Vorschriften, insbesondere zu den Informationserhebungen, ergangen.<sup>2</sup> Diese – für einen einzelnen Rechtsbereich ungewöhnlich hohe – Zahl ist vor allem darauf zurückzuführen, dass das Bundesverfassungsgericht die Anforderungen an die Subsidiarität und die Beschwerdebefugnis bei Rechtssatzverfassungsbeschwerden gegen die regelmäßig (auch) angegriffenen verdeckten bzw. geheimen sicherheitsbehördlichen Eingriffe niedrig ansetzt, weil gegen solche Maßnahmen im Regelfall kein (einfach)gerichtlicher Rechtsschutz im Sinne des Art. 19 Abs. 4 GG zur Verfügung steht.<sup>3</sup> Allerdings hat das Bundesverfassungsgericht bisher in keinem Fall einen sicherheitsbehördli-

---

1 So führte eine Suche bei Google mit den Stichworten »Polizei Palantir« am 16.08.2025 zu einer unüberschaubaren Zahl von Beiträgen der öffentlich-rechtlichen und privaten (Leit-)Medien jüngerer und jüngsten Datums, die die politischen und parlamentarischen Diskussionen um den Einsatz des Programms in Bund und Ländern umfangreich dokumentieren und bewerten.

2 Vgl. näher Bäuerle 2025, S. 129, Fn. 17 und Fn. 23 m.w.N., neu hinzugekommen ist nunmehr noch der Beschluss des Gerichts vom 24.6.2025 (1 BvR 2466/19).

3 Vgl. dazu m.w.N. Bäuerle 2024, S. 13 ff.

chen Informationseingriff gänzlich verworfen;<sup>4</sup> so hat es auch im Fall des Palantir-Programms gleichsam einen Korridor für verfassungsgemäße Regelungen gelassen bzw. eröffnet.

In diesem Rahmen müssen sich nun auch geplante bzw. bereits erlassene Vorschriften des Bundes und anderer Länder bewegen. So hatte Bayern bereits im Juli 2024 eine Ermächtigungsgrundlage für die automatisierte Datenanalyse geschaffen, die sich Art. 61a BayPAG findet. Zeitgleich mit Hamburg hat auch Rheinland-Pfalz durch § 65a POG Rh.-Pf. eine solche Norm erlassen.<sup>5</sup>

Hinsichtlich der Automatisierten Datenanalyse mittels des Palantir-Programms befinden sich somit auf Landesebene fünf Vorschriften in Kraft. Allerdings setzen nur drei Bundesländer (Hessen, NRW und Bayern) diese Technik ein; in Rheinland-Pfalz und Hamburg sind die Normen gleichsam auf Vorrat geschaffen worden. Im Gesetzgebungsverfahren befinden sich entsprechende Regelungen in Sachsen-Anhalt und Baden-Württemberg.<sup>6</sup>

Auf der Bundesebene gab es zwei Anläufe, für das BKA und die Bundespolizei jeweils eine Regelung zur automatisierten Datenanalyse zu schaffen. Der erste stammte von der »Ampelkoalition« und kam im September 2024 noch in den Bundestag.<sup>7</sup> Nachdem die Koalition dann gescheitert war, gab es interessanterweise nochmal einen zweiten Entwurf, von den Fraktionen von SPD und den Grünen, der Ende Januar 2025 in den Bundestag eingebracht wurde, aber dann in der 20. Wahlperiode nicht mehr zur Abstimmung gelangte.<sup>8</sup>

Obwohl alle Gesetze und Gesetzentwürfe in Kenntnis des Urteils vom 16.2.2023 geschaffen wurden, zeigen sich inhaltlich deutliche Unterschiede hinsichtlich des Regelungsansatzes, der Terminologie, der Eingriffsschwellen und der Regelungsdichte.<sup>9</sup> Diese Divergenzen verweisen zum einen auf die – nicht völlig neuen – gesetzgeberischen Schwierigkeiten bei dem Versuch, »auf dem schmalen Grat zwischen verfassungsrechtlichen Geboten und Effizienzgewinn sicher zu wandeln.«<sup>10</sup> Nicht wenige der in Folge verfassungsgerichtlicher Entscheidungen neugefassten Regelungen zum Informationsrecht der Sicherheitsbehörden wurden bisher vom Bundesverfassungsgericht ein weiteres Mal beanstandet.<sup>11</sup>

---

4 Vgl. auch dazu m.w.N. Bäuerle 2025, S. 129.

5 Vgl. dazu und zum Folgenden auch Giogios, in diesem Band.

6 Vgl. auch dazu Giogios in diesem Band.

7 BT-Drucks. 20/12806.

8 BT-Drucks. 20/14704.

9 Vgl. dazu auch Giogios, in diesem Band.

10 Martini/Rusche-meier, in: Hoeren/Sieber/Holz-nagel 2024, Teil 29 Rn. 114.

11 Vgl. die Nachweise der entsprechenden (mit römischen Ziffern versehenen) Entscheidungen bei Bäuerle 2024, S. 88–95.

Im Fall der Automatisierten Datenanalyse verweist die Heterogenität der Gesetze und Gesetzentwürfe indessen auch auf die rechtspolitischen Herausforderungen, die die Digitalisierung und die mit ihr verbundene Verfügbarkeit von Massendaten an das Informationsrecht der Sicherheitsbehörden stellt. Mit dem folgenden Beitrag soll der Versuch unternommen werden, diese in Form eines rechtspolitischen Ausblicks zu skizzieren.<sup>12</sup>

## 2. Datafizierung der Gesellschaft und Polizeirecht

Seit der Umgang der Polizei mit personenbezogenen Daten infolge des sog. Volkszählungsurteils des Bundesverfassungsgerichts von 1983 als Grundrechtseingriff gilt, wurden in den Polizeigesetzen des Bundes und der Länder zahlreiche Normen geschaffen, die den Behörden die Erhebung, Speicherung und Verwendung personenbezogener Daten erlauben.<sup>13</sup> Diese Regelungen orientierten sich am »klassischen« Polizeirecht, das auf individuelle Eingriffe etwa in die Freiheit, die körperliche Unversehrtheit und die Privatheit der Wohnung zugeschnitten ist. Strukturell wurde die Datenerhebung als Einzelfallzugriff etwa auf die Personalien, die Eigenschaften und die Lebensumstände individualisierbarer Bürgerinnen und Bürger geregelt.

Zwar wurde gesetzgeberisch durchaus wahrgenommen, dass sich die Erhebung von Informationen infolge des technischen Fortschritts (etwa bei Telefonüberwachungen oder »großen Lauschangriffen«) oft nicht mehr auf einzelne Personen – polizeirechtlich gesprochen: Störer – beschränkt. Dem wurde jedoch dann mit der in den Gesetzen regelmäßig wiederholten Wendung Rechnung getragen, dass die Maßnahme auch durchgeführt werden dürfe, wenn durch sie Dritte unvermeidbar betroffen sind.<sup>14</sup>

Nach und nach wurden die Regelungen zur polizeilichen Datenverarbeitung sodann auch mit dem Datenschutzrecht – zunächst dem nationalen, sodann auch mit dem der EU – verschränkt, was ihnen zusätzliche Komplexität verlieh, an der auf den polizeilichen Einzelfallzugriff zugeschnitten Grundstruktur jedoch wenig änderte.

Diese wurde bis heute insbesondere nicht an die Tatsache der gesellschaftlichen Datafizierung, also dem exponentiellen Anstieg des verfügbaren Datenbestands infolge von Smartphones, sozialen Medien, Cloud- und Telekommunikationsdiensten sowie öffentlich verfügbaren Daten aus dem Internet ange-

---

<sup>12</sup> Vgl. zum Folgenden auch Butz 2023, S. 33 ff., insbesondere S. 44 ff.

<sup>13</sup> Vgl. für Hessen etwa die Regelungen der §§ 12 bis 29a HSOG.

<sup>14</sup> So z. B. in § 15c Abs. 2 Satz 4 HSOG.

passt. Dass in erheblichem Umfang individuelle und gesellschaftliche Beziehungen, Verhaltensweisen und Prozesse, letztlich also große Teile der Lebenswelt, digital nachvollziehbar geworden sind, spiegelt sich im Recht der polizeilichen Datenverarbeitung bis heute nicht grundsätzlich wider. Bezogen auf den einzelfallbezogenen Informationseingriff der Polizei hat lediglich das Bundesverfassungsgericht – immerhin, aber auch nur – betont, dass das Eingriffsgewicht im Fall einer großen »Streubreite« einer Maßnahme, also der (Mit-)Betroffenheit vieler Unbeteiligter, ansteigt, so dass an die Verhältnismäßigkeit strengere Anforderungen zu stellen sind.<sup>15</sup>

Der exponentielle Anstieg des verfügbaren Datenmaterials spiegelt sich indessen faktisch in einem erheblichen Anwachsen der polizeilichen Datenbestände wider, in denen polizeirelevante Vorgänge naturgemäß nicht mehr (nur) in Form von Aktenvermerken, Durchsuchungs- und Vernehmungsprotokollen anfallen, sondern vor allem als Auswertung von digitalen Geräten mit der Folge der Speicherung von Daten im Gigabyte-Maßstab.<sup>16</sup>

An diese Entwicklung hat sich zwar die informationstechnische Infrastruktur der Polizeien des Bundes und der Länder durch deren Informatisierung grundsätzlich angepasst. Entstanden ist dadurch indessen eine heterogene informationstechnische Struktur unterschiedlicher Datenbanksysteme und Datenformate und -typen.<sup>17</sup> Politisch sollte dem mit dem von den Innenministern geplanten IT-Großprojekt »Polizei 2020« entgegengewirkt werden, das die Schaffung eines sog. gemeinsamen Datenhaus der Polizei zum Ziel hat.<sup>18</sup> Dieses Projekt, mit dem die Polizei gleichsam im Massendatenzeitalter ankommen soll, harrt jedoch bis heute – wohl auch wegen der schwierigen Bund-Länder-Koordination – seiner Verwirklichung.

Der (alsbaldigen) Strukturierung der polizeilichen Datenbestände, also der (Forderung nach) automatisierter Datenanalyse, wie sie durch hessenDATA bewerkstelligt wird, kommt vor diesem Hintergrund höchste polizeipolitische Bedeutung zu. Die Forderung wird – ungeachtet verfassungsgerichtlicher Interventionen – auch die rechtspolitische Agenda weiter bestimmen.

---

<sup>15</sup> Vgl. etwa BVerfGE 125, 260 (305, m.w.N.).

<sup>16</sup> Vgl. zu dieser Herausforderung etwa die Ansätze der Zentralen Stelle für Informationstechnik im Sicherheitsbereich, siehe etwa [https://www.zitis.bund.de/DE/WasSonst/\\_documents/Fachartikel/jahrbuch-polizist-der-zukunft-1-2019.html](https://www.zitis.bund.de/DE/WasSonst/_documents/Fachartikel/jahrbuch-polizist-der-zukunft-1-2019.html) (01.10.2025).

<sup>17</sup> Vgl. Butz 2023, S. 36 und Bäuerle, hessenDATA in rechtssoziologischer Perspektive (in diesem Band).

<sup>18</sup> Auch dazu Butz 2023, S. 37.

### 3. Der rechtspolitische Pfad nach der verfassungsgerichtlichen Entscheidung vom 16.2.2023

Betrachtet man das Urteil des Bundesverfassungsgerichts vom 16.2.2023 vor diesem Hintergrund, kann davon ausgegangen werden, dass dem Gericht einerseits diese rechtspolitische Dringlichkeit nicht entgangen ist, dass es andererseits aber – anders als in früheren Entscheidungen – zu kleinteilige Vorgaben für die Gesetzgeber vermeiden wollte.

Zwar bleibt das Gericht zunächst seinen langjährigen Maßstäben für informationstechnische Eingriffe der Sicherheitsbehörden<sup>19</sup> treu, indem es eine hinreichend bestimmte, an die Eingriffstiefe angepasste gesetzliche Ermächtigung und deren Flankierung durch weitere Maßnahmen zum Schutz der individuellen informationellen Selbstbestimmung verlangt. Sodann trifft es jedoch zahlreiche »Je-desto«-Aussagen über eine mögliche verfassungskonforme Ausgestaltung der gesetzlichen Regelung, die den Gesetzgebern mehr (Interpretations-)Spielräume lassen, als dies bei früheren Entscheidungen oft der Fall war.

Die Heterogenität der nach dem Urteil entstandenen Regelungen und Regelungsentwürfe in Bezug auf die automatisierte Datenanalyse dürfte nicht zuletzt auf diesen Befund zurückzuführen sein.

Da auch das Gericht bisher an dem Konzept der individuellen Eingriffsdogmatik festhält, werden die Gesetzgeber den vorgegebenen Spielraum auf der Grundlage jeweils eigener Interpretation – etwa der bewirkten Eingriffsschwere – unterschiedlich nutzen, begleitet von einer rechtswissenschaftlichen Diskussion über die Frage, ob sie den Vorgaben des Gerichts entsprechen. Darüber wird sodann eine weitere Entscheidung des Gerichts Aufschluss geben, so dass sich das inzwischen eingeübte Wechselspiel zwischen Sicherheitsgesetzgeber und Bundesverfassungsgerichts insoweit fortsetzen wird.

Überlagert wird diese Diskussion im Fall der automatisierten Datenanalyse bisher aber noch von der politisch überaus umstrittenen, vom Bundesverfassungsgericht nur am Rande aufgegriffenen Frage, ob für die Erfüllung des prioritären polizeipolitischen Bedarfs auf ein Analysewerkzeug für Massendaten auf das Programm eines umstrittenen US-amerikanischen Herstellers gesetzt werden sollte,<sup>20</sup> wodurch die Kritiker insbesondere die nationale Datensouveränität gefährdet sehen.

---

19 Vgl. zum Folgenden im Einzelnen m.w.N. Bäuerle 2025, S. 129 ff.

20 Vgl. dazu auch den Beitrag von Brenneis/Denker/Gehring in diesem Band.

#### 4. Politikum Palantir

Diese Debatte bestimmt seit geraumer Zeit – politisch gut nachvollziehbar – zu einem guten Teil die gesetzgeberischen Aktivitäten, so dass die Diskussion um die Beschaffenheit einer rechtspolitisch und rechtsdogmatisch tragfähigen Rechtsgrundlage für ein solches System in den Hintergrund tritt.

Politisch thematisiert worden war die automatisierte Datenanalyse auf Bundesebene in diesem Zusammenhang erstmals schon im November 2023 durch einen Entschließungsantrag der CDU/CSU-Fraktion im Bundestag. Dieser war darauf zurückzuführen, dass die damalige Innenministerin entschieden hatte, für die Bundesbehörden nicht auf das Programm von Palantir zurückzugreifen. Sie hatte es damit abgelehnt auf den von Bayern 2022 abgeschlossenen Rahmenvertrag mit der Firma zurückzugreifen. Dieser Verzicht stieß auf Kritik in der Union, die daraufhin den Entschließungsantrag einbrachte, nach dem von Palantir nicht weniger als die »Handlungsfähigkeit der Strafverfolgungsbehörden« abhing.<sup>21</sup>

Daraufhin fand eine Anhörung im Bundestag (Innenausschuss) statt, in der sich im Wesentlichen die Polizeiangehörigen für die Beschaffung des Programms aussprachen und alle anderen – insbesondere die Experten – dagegen.<sup>22</sup> Auch im Bundesrat wurde die Frage wiederholt kontrovers diskutiert. Ein auf die Einführung des Programms gerichteter Entschließungsantrag Sachsen-Anhalts und Bayerns, dem sich Hessen und Berlin anschlossen, wurde schließlich angenommen. Dieser enthält die Forderung nach »interimsweise zeitnahe(r) Bereitstellung einer gemeinsam betriebenen automatisierten Datenanalyseplattform.« Zur Begründung dieser Forderung heißt es in dem Antrag:

»Um bestehende Fähigkeitenlücken der Polizeien des Bundes und der Länder bei der Informationsverarbeitung, Datenzusammenführung, Auswertung und Analyse unverzüglich zu schließen und gegebenenfalls weiteren Verzögerungen bei der Umsetzung eines gemeinsamen Datenhauses über das Jahr 2030 hinaus entgegenzuwirken, fordert der Bundesrat die Bundesregierung auf, die bereits im Jahr 2023 geplanten Aktivitäten einer gemeinsam finanzierten, zentral zu betreibenden, rechtlich zulässigen Interimslösung für eine automatisierte Datenanalyseplattform im Programm Polizei 20/20, aus der sich der Bund im Mai 2023 zurückgezogen hat, erneut aufzunehmen und zeitnah eine zentral betriebene, digital souveräne, wirtschaftlich tragbare und rechtlich zulässige automatisierte Datenanalyseplattform für alle Polizeien

---

21 BT-Drucks. 20/9495.

22 Dokumentiert unter <https://dip.bundestag.de/vorgang/handlungsf%C3%A4higkeit-der-straiverfolgungsbeh%C3%B6rden-sichern-entscheidung-des-bundesministeriums-des-innern/306393?f.deskriptor=Polizeiliches%20Informationssystem&rows=25&pos=3&ctx=e> (01.10.2025).

des Bundes und der Länder bereitzustellen. Darüber hinaus sind diese auch für sicherheitsrelevante Erkenntnisse und Informationen Verwaltungsbereichen zu öffnen und bereitzustellen.«<sup>23</sup>

Das Spannungsverhältnis zwischen den polizeipraktischen Interessen und der Wahrung der nationalen Datensouveränität wurde somit im Ergebnis nicht aufgelöst. Der Begriff »Interimslösung« deutet darauf hin, dass das Ziel eine deutsche oder europäische Lösung sein soll – also nicht Palantir – gleichzeitig soll diese Lösung jedoch »digital souverän« sein, was das Programm im Hinblick auf die nationale digitale Souveränität jedoch nicht wäre.

Dieser Gesichtspunkt war zuvor auch in einem Änderungsantrag der Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Saarland, Schleswig-Holstein und Thüringen, aufgegriffen worden. Dieser war auf eine Einfügung in den Text gerichtet, dass eine Lösung zu finden sei, die »eine Nutzung von Produkten des marktführenden US-amerikanischen Anbieters Palantir ausschließt«, hatte jedoch im Bundesrat keine Mehrheit gefunden.<sup>24</sup>

Auch der jüngste Beschluss der Innenministerkonferenz vom 13.6.2025 zur Thematik automatisierte Datenanalyse zeigt diese Ambivalenz, indem er zwar die nationale Datensouveränität betont, Palantir als Anbieter aber nicht ausschließt.<sup>25</sup> Während von Seiten der Sicherheitsbehörden und der Innenminister regelmäßig betont wird, dass die Firma Palantir das einzige Unternehmen sei, das ein für die Analyse der polizeilichen Datenbestände geeignetes Programm anbiete, wird dies von Oppositionspolitikern in Frage gestellt. So haben sich – wie das Bundesinnenministerium auf eine parlamentarische Frage einräumte<sup>26</sup> – mehrere europäische und deutsche Firmen an die Regierung und das Ministerium gewandt, um eine solche Lösung anzubieten; es gebe eine Liste mit den Kontaktaufnahmen, die jedoch als Verschlussache eingestuft wurde, so dass sie für die öffentliche Diskussion nicht zur Verfügung steht.

Dass es unabhängig von dieser Frage auf Bundesebene eine Regelung für BKA und Bundespolizei geben wird, ist nach dem Koalitionsvertrag sehr wahrscheinlich. In diesem heißt es:

»Für bestimmte Zwecke sollen unsere Sicherheitsbehörden, unter Berücksichtigung verfassungsrechtlicher Vorgaben und digitaler Souveränität, die automatisierte Datenrecherche

---

23 BT-Drucks. 58/25, S. 2.

24 Vgl. BR-Drucks 58/25.

25 Abzurufen unter [https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2025-06-13\\_DOK/beschl%C3%BCsse.pdf?\\_\\_blob=publicationFile&v=1](https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2025-06-13_DOK/beschl%C3%BCsse.pdf?__blob=publicationFile&v=1) (01.10.2025).

26 BT-Drucks. 32/396, S. 21.

und -analyse sowie den nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Internetdaten, auch mittels Künstlicher Intelligenz, vornehmen können.«<sup>27</sup>

## 5. Künstliche Intelligenz

Mit dem Verweis auf den Einsatz künstlicher Intelligenz, der in den Ländern bisher jeweils noch ausdrücklich ausgeschlossen war, taucht hier ein neuer – in der rechtspolitischen Debatte ebenfalls inzwischen virulenter – Gesichtspunkt auf. Insoweit hat das Land Hessen sich an die Spitze der Bewegung gesetzt, indem es bereits im Dezember 2024 die Möglichkeit zum Einsatz künstlicher Intelligenz im Rahmen automatisierter Datenanalysen geschaffen hat.<sup>28</sup>

Obwohl das Land Hessen im Verfahren über hessenDATA vor dem Bundesverfassungsgericht vorgetragen hatte, dass das Programm seinerzeit nicht KI-gestützt sei, hatte das Gericht in seiner Entscheidung sich vorsorglich bereits zu dieser Option geäußert und KI-gestützte Datenanalysen besonders strengen Anforderungen unterworfen; an diesen wird sich die geänderte hessische Vorschrift nun messen lassen müssen.<sup>29</sup> Gleiches gilt in absehbarer Zeit für die inzwischen aus der KI-VO resultierenden Anforderungen an KI-Systeme.<sup>30</sup>

Ebenso wie die Diskussion um Palantir als Anbieter überlagert somit nunmehr auch die Thematik des polizeilichen Einsatzes künstlicher Intelligenz die grundsätzliche Frage nach (alternativen) Regulierungsstrategien für die polizeiliche Informationsordnung in Zeiten von Big Data. Diese Themen bilden derzeit gleichsam die Stolpersteine bei dem gesetzgeberischen Versuch, »auf dem schmalen Grat zwischen verfassungsrechtlichen Geboten und Effizienzgewinn sicher zu wandeln.«<sup>31</sup>

## 6. Alternative Regelungsansätze?

Geht man davon aus, dass Big-Data und KI in der zukünftigen Polizeiarbeit in rechtstatsächlicher Hinsicht ebenso unvermeidbar wie unverzichtbar sein werden und erkennt an, dass die dem klassischen Polizeirecht entstammende ein-

---

27 Abzurufen unter [https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav\\_2025.pdf](https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf) (01.10.2025).

28 Vgl. näher auch hinsichtlich der verfassungsrechtlichen und europarechtlichen Problematik Bäuerle 2025, S. 130 f. m.w.N.

29 BVerfGE 165, 363 (408, 418, 428 f.).

30 Vgl. Bäuerle 2025, S. 131 f.

31 Martini/Rusche-meier, in: Hoeren/Sieber/Holz-nagel 2024, Teil 29 Rn. 114.

zelfallbezogene Eingriffsdogmatik des bisherigen Rechts der Informationsverarbeitung der Polizei unter diesen Gesichtspunkten nicht mehr gerecht wird, kann jedoch perspektivisch der grundsätzlichen Frage nach den rechtspolitischen Alternativen nicht ausgewichen werden.<sup>32</sup>

Voraussetzung für deren Entwicklung wäre indessen zunächst eine Analyse der tatsächlichen Bedeutung der polizeilichen Datenverarbeitung in der Informationsgesellschaft für deren Kernaufgaben, nämlich die Gefahrenabwehr und die Strafverfolgung.

Die strikte Trennung dieser im klassischen Polizeirecht durch die dogmatischen Strukturen und unterschiedliche Gesetzgebungskompetenzen separierten Bereiche ist hat sich in den letzten Jahrzehnten durch die Schaffung sogenannter Vorfeldstraftaten und die Einbeziehung der Verhütung von Straftaten in die Gefahrenabwehr bereits legislativ deutlich aufgeweicht. Es erscheint fraglich, ob sich die Trennung von Gefahrenabwehr und Strafverfolgung unter den Bedingungen einer durch die allgegenwärtige Generierung von Massendaten geprägten Gesellschaft aufrechterhalten lässt. Während sich bisher individuelle polizeiliche Informationseingriffen zumindest in ihrem Ausgangspunkt einer der beiden Aufgaben zurechnen ließen, wird es etwa bei den aus Digitalgeräten gewonnen (Massen-)Daten auf Dauer schlicht nicht möglich sein, diese zuverlässig jeweils der Strafverfolgung oder der Gefahrenabwehr zuzuordnen.

Vor diesem Hintergrund spricht einiges dafür, das Informationsrecht der Polizei zu einem eigenen Rechtsgebiet auszugestalten, das zwar die individuelle Eingriffsperspektive nicht aus dem Blick verliert, diese aber gleichsam generalisiert und auf die jeweiligen informationstechnischen Instrumente zuschneidet. Ein solches zwischen Datenschutz- und Technikrecht angesiedeltes Rechtsgebiet angesiedeltes Rechtsgebiet dürfte sich schon wegen der ubiquitären Notwendigkeit des bundesweiten Datenaustausches kaum noch zielführend jeweils eigenständig in 16 Bundesländern entwickeln lassen. Insoweit wäre die Schaffung einer Bundeskompetenz für das polizeiliche Informationswesen zu erwägen, ohne die auch die Verwirklichung des Programms »Polizei 2020« nur schwer vorstellbar scheint.

Ein weiterer wesentlicher Aspekt für diesen Regulierungsansatz wäre der Gesichtspunkt der Datenqualität (Datenwahrheit und -klarheit) in den polizeilichen Datenbeständen. Dieser dürfte in Zeiten von Massendaten eine nicht zu unterschätzende Bedeutung für die konkrete Alltagsarbeit der Polizei haben; insoweit würden objektive Analysen voraussichtlich die aus der Praxis vernehmbare Klage über eine mäßige Datenqualität wohl verifizieren. In den auf den einzelnen Informationseingriff zugeschnittenen bisherigen Regelungen der polizeilichen

---

32 Vgl. zum Folgenden näher Butz 2023, S. 33 ff., 44. ff.; Golla 2024, S. 229 ff., jeweils m.w.N.

Datenverarbeitung waren und sind zwar die Mittel und Instrumente der Datenerhebung sowie die Voraussetzungen für eine Speicherung von Daten geregelt, es fehlen aber Vorgaben, wie die durch solche Erhebungen und auf anderen Wegen alltäglich polizeilich bekannt werdenden lebensweltliche Vorgänge zu »datafizieren« sind. In der Folge werden viele tatsächliche Vorgänge von den vielen beteiligten Polizeibediensteten in unterschiedlichen Varianten und Terminologien in den polizeilichen Datenbestand integriert werden. Ein Schwerpunkt der Regelung des polizeilichen Informationswesens könnte daher in Regelungen über die Einspeisung und Validierung der bei den Polizeien anfallenden Informationen liegen<sup>33</sup>

In diesem Zuge ließe sich auch nach einem vom individuellen Informationseingriff abgekoppelten generellen Ansatz zur Beantwortung der Frage suchen, welche lebensweltlichen Vorgänge unter dem Gesichtspunkt der polizeilichen Aufgabenerfüllung<sup>34</sup> überhaupt Aufnahme in die polizeilichen Datenbestände finden sollen und müssen. Eine gegenüber den bisherigen Regelungen insoweit beschränkende Vorgabe könnte zugleich die vielbeschworene, die Polizeien tendenziell überfordernde, »Datenflut« reduzieren und die mit dieser ggf. korrespondierenden gesellschaftlichen Befürchtungen vor einer allwissenden und deshalb unter grundrechtlichen Gesichtspunkten bedenklichen Polizei.

Den letztgenannten Bedenken gegenüber einer hochtechnisierten Polizei könnte darüber hinaus durch die gesetzgeberische Schaffung eines vom Polizeiapparat unabhängigen Transparenz- und Aufsichtssystems Rechnung getragen werden, in dem – wie es im Europarecht inzwischen ohnehin gefordert wird – eingesetzte Algorithmen und KI-Systeme von unabhängiger Stelle einer objektiven Prüfung unterzogen werden, deren Ergebnisse öffentlich zu machen sind. Dieser Institution könnte etwa auch eine Befugnis zur regelmäßigen Kontrolle von Protokolldaten übertragen werden. Das infolge der Undurchschaubarkeit der technischen Vorgänge nach dem Bundesverfassungsgericht individuell hohe Eingriffsgewicht (bzw. dessen Unvorhersehbarkeit) ließe sich durch einen solchen Ansatz gleichsam generalisiert abmildern.

Als weiterer Regelungsgegenstand käme die Normierung von Voraussetzungen für den Zugang der Polizeibediensteten zu den Daten in Abhängigkeit von deren Aufgaben sowie die jeweils erforderliche Qualifikation in Betracht, also ein Regelungskonzept, das für den Bereich der automatisierte Datenanalyse inzwischen bereits verwirklicht oder geplant ist. Damit könnte je nach Ausgestaltung etwa einem Zugriff auf sensible Daten in polizeilichen Alltagssituationen – also gleichsam »Big Data im Streifendienst« – entgegengewirkt werden und damit zu-

---

<sup>33</sup> Dazu Golla 2024, S. 234 ff.

<sup>34</sup> Butz 2023, S. 41 ff. spricht in diesem Zusammenhang treffend von »polizeilicher Sozialkontrolle«.

gleich etwaigen Befürchtungen einer überbordender polizeilicher Sozialkontrolle »im Kleinen«. In diesen Bereich fiel auch eine – schon dem bisherigen Datenschutzrecht bekannte, aber derzeit recht großzügige – spezifische Regelung über die Dauer von Datenspeicherungen.

Denkbar wäre schließlich, die rechtlichen Vorgaben über Informationsrechte von Betroffenen über polizeiliche Datenverarbeitungen anzupassen. Empfehlenswert wäre es auf dieser Grundlage schließlich, die bisher noch ganz am individuellen Eingriffskonzept ausgerichtete und wenig IT-bezogene Polizeiausbildung zu reformieren.

## 7. Fazit

Wie sich gezeigt hat, ist die im Nachgang zur Entscheidung des Bundesverfassungsgerichts vom 16.2.2023 entstandene rechtspolitische Entwicklung von durchaus regen gesetzgeberischen Aktivitäten geprägt. Deren Diskussion wurde und wird zum einen von der Frage der politischen Vertretbarkeit der Beauftragung des Unternehmens Palantir und zum anderen von der Erforderlichkeit und Zulässigkeit des Einsatzes künstlicher Intelligenz bestimmt.

Die grundsätzlichen regulatorischen Fragen der Datafizierung der Polizeiarbeit stehen zwar auf der politischen Agenda, haben jedoch bisher noch keine Konkretisierung in Form rechtspolitischer Konzepte gefunden. Erste Skizzen finden sich in der rechtswissenschaftlichen Literatur, die zu recht auf die grundsätzliche Reformbedürftigkeit der polizeilichen Informationsordnung hinweist. Deren aus dem klassischen Polizeirecht stammende Ausrichtung am individuellen polizeilichen Informationseingriff und der darauf bezogenen Verhältnismäßigkeitsprüfung wird der rechtstatsächlichen Bedeutung eines der Sozialkontrolle dienenden Umgangs mit allgegenwärtigen Massendaten in Zeiten KI-gestützter Auswertungstools nur noch begrenzt gerecht.

Vor diesem Hintergrund war das Verfahren zur automatisierten Datenanalyse in Hessen nicht nur Anlass für die erstmaliger eingehende verfassungsgerichtliche Beschäftigung mit Big-Data und KI bei den Sicherheitsbehörden, es bietet vielmehr auch einen Anlass, die überkommenen Regelungskonzepte des polizeilichen Eingriffsrechts auf den Prüfstand zu stellen. Dies reicht bis hin zu den grundlegenden Prinzipien, wie der Trennung der Gesetzgebungskompetenz für Strafverfolgung und Gefahrenabwehr und der vorherrschenden einzelfallbezogene Eingriffsdogmatik. Zur Diskussion gestellt ist damit nicht weniger als Schaffung eines eigenen Rechtsgebiets, das durch seine Beziehung zur Technikregulierung auch disziplinübergreifende Ansätze beinhalten könnte, die dem deutschen Polizeirecht bisher fremd waren.

## Quellen und Literatur

- Bäuerle, Michael, *Das Informationsrecht der Sicherheitsbehörden zwischen Konstitutionalisierung und Europäisierung*, Frankfurt am Main 2024.
- Bäuerle, Michael, »Automatisierte und KI-gesteuerte Datenverarbeitung und -analyse bei den Sicherheitsbehörden«, in: *Zeitschrift für Datenschutz (ZD)* 2025, S. 128 ff.
- Butz, Felix, »Polizei und Massendaten: Kriminologische Überlegungen zum Wandel polizeilicher Sozialkontrolle«, in: Bliesener, Thomas/Deyerling, Lena/Dreißigacker, Arne/Henningsmeier, Isabel/Neumann, Merten/Schemmel, Jonas/Schröder, Carl Phillip/Treskow, Laura (Hg.): *Kriminalität und Kriminologie im Zeitalter der Digitalisierung*, Mönchengladbach 2023, S. 33 ff.
- Golla, Sebastian, *Die kriminalbehördliche Informationsordnung*, Trier 2024.
- Hoeren, Thomas/Sieber, Ulrich/Holznapel, Bernd (Hg.): *Handbuch Mutimediarrecht*, 62. Erg.-Lfg., München 2024.

# Mitglieder der Projektgruppe, Autorinnen und Autoren

*Dr. Michael Bäuerle, LL.M.* ist Professor für Öffentliches Recht an der Hessischen Hochschule für Öffentliches Management und Sicherheit und war Sprecher der ZEVEDI-Projektgruppe »Big Data und KI im Bereich der deutschen Sicherheitsbehörden« (KISib).

*Dr. Andreas Brenneis* ist Wissenschaftlicher Mitarbeiter am Institut für Philosophie an der Technischen Universität Darmstadt.

*Dr. Kai Denker* ist Wissenschaftlicher Mitarbeiter am Institut für Philosophie an der Technischen Universität Darmstadt und Verbundkoordinator im DatenTreuhand-Kompetenznetzwerk DaTNet.

*Dr. Petra Gehring* ist Professorin für Philosophie an der TU Darmstadt und war Ko-Sprecherin der ZEVEDI-Projektgruppe »Big Data und KI im Bereich der deutschen Sicherheitsbehörden« (KISib).

*Dr. Christian L. Geminn* ist Privatdozent für Öffentliches Recht und Recht der digitalen Gesellschaft an der Universität Kassel.

*Christopher Giogios* ist Rechtsanwalt in Bonn und war zuvor Wissenschaftlicher Mitarbeiter an der Professur für Öffentliches Recht an der Justus-Liebig-Universität Gießen und Koordinator der ZEVEDI-Projektgruppe »Big Data und KI im Bereich der deutschen Sicherheitsbehörden« (KISib).

*Dr. Nora Jansen* ist Disinformation Analyst and Policing Consultant und war im Rahmen eines ZEVEDI Young Investigator Fellowship Mitglied der ZEVEDI-Projektgruppe »Big Data und KI im Bereich der deutschen Sicherheitsbehörden« (KISib).

*Paul C. Johannes* ist geschäftsführender Gesellschafter der Datenrecht Beratungsgesellschaft (DRBG) und Rechtsanwalt.

*Dr. Lea Rabe, LL.M. (EULISP)* ist Wissenschaftliche Mitarbeiterin im Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel und Rechtsreferendarin am OLG Celle.

*Dr. Bettina Schöndorf-Haubold* ist Professorin für Öffentliches Recht an der Justus-Liebig-Universität Gießen.

*Burak Türkmén* ist studentische Hilfskraft an der Professur für Öffentliches Recht an der Justus-Liebig-Universität Gießen und wirkte als studentischer Mitarbeiter in der ZEVEDI-Projektgruppe »Big Data und KI im Bereich der deutschen Sicherheitsbehörden« (KISib) mit.