Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 J

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

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

Antrag der CDU/CSU Fraktion
Deutscher Bundestag

Drucksache 20/9495

Stellungnahme zur Anhörung im Ausschuss
für Inneres und Heimat am 22. April 20244

Prof. Dr. Clemens Arzt

Fachbereich Polizei und Sicherheitsmanagement der HWR Berlin
Gründungsdirektor Forschungsinstitut für Öffentliche und Private Sicherheit (FÖPS Berlin)

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Inhalt

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

I. Antrag der Fraktion der CDU/CSU

Der Antrag zielt darauf ab, „die Handlungsfähigkeit der Strafverfolgungsbehörden durch die Einführung und Nutzung einer Analyse-Software „Bundes-VeRA“ zu sichern und damit eine Entscheidung vom 23. Juli 2023 zu revidieren, „mit welcher die Hausleitung des BMI dem Bundeskriminalamt sowie der Bundespolizei die Nutzung der „Bundes-VeRA“ untersage. Zudem sei „im Zuge der Einführung der „Bundes-VeRA“ unverzüglich zu prüfen, inwiefern eine Gesetzesänderung (z.B. der StPO) für den Einsatz der Software zur Strafverfolgung vonnöten sei und gegebenenfalls eine entsprechende Gesetzesänderung auf den Weg zu bringen. In diesem Kontext wird auch die Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 (NJW 2023, 1196 ff.) zu automatisierten Datenanalyse oder -auswertung (Data-Mining) in Bezug genommen, welche nach dem Verständnis der Antragsteller „den Einsatz automatisierter Datenauswertung zur vorbeugenden Bekämpfung schwerer Straftaten explizit“ zulasse.

Die dem Antrag zugrundeliegenden politischen Differenzen sind ein wichtiger Hintergrund der heutigen Anhörung, können aber selbstredend nicht Gegenstand dieser Stellungnahme sein. Ich werde mich daher nachfolgend auf damit verbundene Rechtsfragen konzentrieren und hierzu eingangs die im Antrag angesprochene Entscheidung des BVerfG umreißen, die zur Erklärung der Verfassungswidrigkeit der entsprechenden gesetzlichen Regelungen zum Datamining in Hessen und Hamburg führte (II.). Sodann wird exemplarisch die derzeitige gesetzliche Regelung in NRW vorgestellt, zu der ebenfalls eine Klage vor dem Bundesverfassungsgericht anhängig ist (III.). Sollte eine solche Software im Bund eingeführt werden, bedarf dies vorab einer intensiven datenschutzrechtlichen Überprüfung im Rahmen der Vorgaben der §§ 67 und 68 des Bundesdatenschutzgesetzes (BDSG) sowie der JI-RL (IV.) und einer „verzahnten“ Entwicklung von möglicher gesetzlicher Regelung und Software sowie technisch-organisatorischer Regelungen „aus einem Guss“. Abschließend (V.) werde ich daher eine Empfehlung zum weiteren Vorgehen geben.

II. Entscheidung des BVerfG zu Data-Mining vom 16.2.2023

Hier kann die Entscheidung des Bundesverfassungsgerichts nicht im Detail vorgestellt werden. Es kann insoweit vertiefend auf die Stellungnahmen in dieser Anhörung und die aktuelle Ausarbeitung der Wissenschaftlichen Dienste des Deutschen Bundestages vom 17. Januar 2024 (WD 3 – 30000 – 145/23) verwiesen werden.

In den Leitsätzen der genannten Entscheidung fasst das Bundesverfassungsgericht die verfassungsrechtlichen Anforderungen zusammen und entwickelt hierbei seine Rechtsprechung im Kontext der Entscheidungen zum BKAG und ATDG

weiter. Folgende **Anforderungen an die Zulässigkeit einer automatisierten Datenanalyse oder Datenauswertung** fasst das Gericht dabei zusammen, die als „Leitlinien" für das weitere Vorgehen auf der Bundesebene Beachtung finden müssen:

- 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.

- Das **Eingriffsgewicht** einer automatisierten Datenanalyse oder -auswertung und die Anforderungen an deren verfassungsrechtliche Rechtfertigung **ergeben sich zum einen aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe**; insoweit gelten die Grundsätze der **Zweckbindung und Zweckänderung**.

- Zum andern hat die **automatisierte Datenanalyse oder -auswertung ein Eigengewicht**, weil die weitere Verarbeitung durch eine automatisierte Datenanalyse oder -auswertung spezifische Belastungseffekte haben kann, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen; insoweit ergeben sich aus dem Grundsatz der Verhältnismäßigkeit im engeren Sinne weitergehende Rechtfertigungsanforderungen.

- Die weitergehenden Anforderungen an die Rechtfertigung einer automatisierten Datenanalyse oder -auswertung variieren, da deren eigene Eingriffsintensität je nach gesetzlicher Ausgestaltung ganz unterschiedlich sein kann. Das **Eingriffsgewicht** wird insbesondere durch **Art und Umfang der verarbeitbaren Daten** und die **zugelassene Methode der Datenanalyse oder -auswertung** bestimmt. Der **Gesetzgeber kann die Eingriffsintensität** durch Regelungen zu Art und Umfang der Daten und zur Begrenzung der Auswertungsmethode **steuern**.

- 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.

- Grundsätzlich kann der **Gesetzgeber** den Erlass der erforderlichen Regelungen zu Art und Umfang verarbeitbarer Daten und zu den zulässigen Datenverarbeitungsmethoden zwischen sich und der **Verwaltung** aufteilen. Er muss aber sicherstellen, dass unter Wahrung des **Gesetzesvorbehalts** insgesamt ausreichende Regelungen getroffen werden.

- Der **Gesetzgeber** selbst muss indes die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst vorgeben.

- Soweit der Gesetzgeber die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigt, hat der **Gesetzgeber** zu **gewährleisten**, dass die **Verwaltung** die für die Durchführung einer automatisierten Datenanalyse oder -auswertung im Einzelfall maßgeblichen Vorgaben und **Kriterien in abstrakt-genereller Form** festlegt, verlässlich dokumentiert und in einer vom Gesetzgeber näher zu bestimmenden Weise **veröffentlicht**. Das sichert auch die verfassungsrechtlich gebotene Kontrolle, die insbesondere durch **Datenschutzbeauftragte** erfolgen kann.

III. Gesetzliche Regelung in NRW als Regelungsbeispiel

Die bestehende gesetzliche Reglung in **§ 23 Abs. 6 PolG NRW** zum automatisierter Abgleich und der Analyse von Daten gibt deutliche Hinweise auf eine unterkomplexe und verfassungsrechtlich kaum haltbare Ausgestaltung solch weitgehender polizeilicher Befugnisse:

> *(6) Die Polizei darf die nach § 22 rechtmäßig gespeicherten personenbezogenen Daten automatisiert zusammenführen. Sie darf personenbezogene Daten mit diesen zusammengeführten Daten abgleichen (§ 25 Absatz 1 Satz 2) sowie diese zusammengeführten Daten auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten aufbereiten und analysieren, soweit dies erforderlich ist*
> *1. zur Verhütung oder vorbeugenden Bekämpfung von in § 100a Absatz 2 der Strafprozeßordnung genannten Straftaten oder von Straftaten gemäß den §§ 176a, 176b, 176e, 177, 178, 180, 181a oder § 182 des Strafgesetzbuchs oder*

2. zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben oder Freiheit einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist.
Bei der Verarbeitung nach Satz 2 dürfen die nach Satz 1 zusammengeführten Daten nicht mittels statistisch-mathematischer Verfahren oder in sonstiger Weise selbständig auf Zusammenhänge analysiert werden. Die Abfrage ist zu protokollieren. 5Absatz 2 bleibt mit Ausnahme von Satz 1 Nummer 2 unberührt.

1. Entstehungsgeschichte der Regelung

Wie andere Landesregierungen auch (vgl. nur https://netzpolitik.org/2024/automatisierte-polizeidatenanalyse-bayern-testet-rechtswidrig-palantir-software/) war die Landesregierung in NRW der Auffassung, die Nutzung einer (angepassten) Software der Firma Palantir durch die Polizei bedürfe keiner neuen Rechtsgrundlage im PolG NRW (so der Innenminister in: APr 17/1375, 45). Sie änderte diese Position erst im Verlauf der politischen Diskussion und legte im Februar 2022 und damit kurz vor der Landtagswahl einen Gesetzentwurf für diese weitgehende Maßnahme vor. Ausweislich der Gesetzesbegründung (LT-Drs. 17/16517, 17 f.) werde damit allein „eine klarstellende Regelung zu bisher bereits nach § 23 rechtlich zulässigen automatisierten Zusammenführungsprozessen – insbesondere in der Fallgruppe der Zusammenführung von getrennten Daten in einem gemeinsamen Datensystem – getroffen."

Die **Gesetzesänderung** wurde im **Eilverfahren** vor der Wahl am 15.5.2022 durch das Parlament gebracht, ungeachtet **erheblicher datenschutzrechtlicher Bedenken** u.a. der Landesbeauftragten für Datenschutz in NRW (LDI). Kein unübliches Vorgehen in der Sicherheitsgesetzgebung, die nicht selten dem Kalkül zu unterliegen scheint, dass der Weg nach Karlsruhe zeitlich hinreichenden Spielraum zur Nutzung selbst evident verfassungswidriger Maßnahmen gibt.

Entgegen der Auffassung der Landesregierung hat die gesetzliche Neuregelung in NRW keine allein klarstellende Funktion (LDI NRW, LT NRW Stellungnahme 17/4970, 2), sondern führt ein **neues Instrument der Datenverarbeitung** ein. Dessen **Erprobung mit Echtdaten** war zudem datenschutzrechtlich nicht vom geltenden Recht gedeckt (LDI NRW, Schreiben v. 25.3.2021, LT NRW Vorlage 17/5078, 12). Es handelt sich um die **deutliche Erweiterung polizeilicher Befugnisse** zu Eingriffen in das Recht auf informationelle Selbstbestimmung. Die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW hatte zur Neuregelung unter anderem angemerkt: „Die vorgeschlagene Regelung dient der gesetzlichen Legitimierung des Einsatzes der in NRW sog. datenbankübergreifenden

Analyse und Recherche (DAR). Die DAR soll mittels einer Software der Firma Palantir durchgeführt werden. Dabei werden große Mengen personenbezogener Daten aus einer Vielzahl polizeilicher Datenbanken in zweckdurchbrechender Weise verarbeitet. Hierdurch wird in erheblicher Weise jedenfalls in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen eingegriffen“ (LDI NRW, LT NRW Stellungnahme 17/4970, 2; s. auch LDI NRW, Schreiben v. 25.3.2021, LT NRW Vorlage 17/5078, 3). Soweit Daten aus der **TK-Überwachung** oder der Wohnraumüberwachung in die Analyse einbezogen werden, sei zudem ein Eingriff in Art. 10 Abs. 1 und 13 Abs. 1 GG zu prüfen.

2. Anforderungen an die gesetzliche Regelung nach BVerfG

Die gesetzliche Regelung in NRW ist an den Maßstäben des **BVerfG** vom 16.2.2023 **zum Data-Mining** (s.o. II.) zu messen. Dabei ist zu beachten, dass sich die vom BVerfG beanstandeten Regelungen in § 25a HSOG und § 49 HmbPolDVG deutlich von § 23 Abs. 6 PolG NRW unterscheiden. Das BVerfG hob in seiner Entscheidung 2023 hervor, dass die automatisierte Datenanalyse oder -auswertung „eigene“, also neue und spezifische Belastungseffekte haben kann, die **über das Eingriffsgewicht der ursprünglichen Datenerhebung hinausgehen** (NJW 2023, 1196 (1201). Die Maßnahme ermögliche die Verarbeitung großer und komplexer Informationsbestände und durch eine verknüpfende Auswertung vorhandener Daten könnten neue persönlichkeitsrelevante Informationen gewonnen werden, die sonst so nicht zugänglich wären. Dies könne sich im Ergebnis einem **Profiling** annähern. Auch die verarbeitete **Datenmenge** sei relevant und bestimme das Eingriffsgewicht (a.a.O. S. 1203), das u.a. durch Eingrenzung auf bestimmte Personen, Aufbewahrungsfristen und Löschpflichten determiniert werde (ebd.). Zur Reduktion der Menge der verarbeiteten Daten trage auch bei, ob die genutzten Dateien automatisiert einbezogen werden oder für jeden Analyse- und Auswertungsvorgang händisch herangezogen werden müssten. Eingriffsverstärkend wirke eine **Verknüpfung mit dem Internet**, die eine Verarbeitung besonders großer Datenmengen praktisch fördere (ebd. S. 1204). Die Beschränkung von **Zugriffsrechten** und eine besondere Qualifizierung des zuständigen Personals könne die Menge der verarbeiteten Daten begrenzen (ebd.).

Das Eingriffsgewicht steige zudem mit dem **Einsatz komplexer Formen des Datenabgleichs**, wie etwa dem Ansatz statistischer Auffälligkeiten anstelle einer Begrenzung durch Suchbegriffe mit Bezug auf erkennbare Sachverhalte und tatsachengestützte Verbindungen zu einer konkret verantwortlichen Person. Damit steige das Risiko, dass Personen in weitere polizeiliche Maßnahmen einbezogen würden, die hierfür keinen zurechenbaren Anlass gegeben haben (ebd.). Relevant für das Eingriffsgewicht sei auch, ob Datenanalysen oder -auswertungen auf

personenbezogene Erkenntnisse oder bspw. nur auf **gefährliche oder gefährdete Orte** zielten (ebd. S. 1205). Werde **Software privater Akteure** oder anderer Staaten eingesetzt, bestehe zudem die Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte (ebd.). Die Fehleranfälligkeit und Mechanismen zu deren Entdeckung und Korrekturen hätten ebenfalls Auswirkungen auf das Eingriffsgewicht (ebd. S. 1207).

Eröffne der Gesetzgeber eine Befugnis zur vorbeugenden Bekämpfung von Straftaten im **Vorfeld einer konkretisierten Gefahr**, müsse er zur Wahrung der Verhältnismäßigkeit die Eingriffsintensität der Maßnahme reduzieren. Zudem müsse er die wesentlichen Grundlagen zur **Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden** selbst durch Gesetz vorgeben. Soweit dies nicht praktikabel erscheine, könne er die Polizei zur näheren Regelung organisatorischer und technischer Vorkehrungen ermächtigen. Er müsse aber sicherstellen, dass Art und Umfang der Daten und die Verarbeitungsmethoden selbst inhaltlich ausreichend, normenklar und begrenzt seien. Hierzu komme eine Verordnungsermächtigung in Betracht (a.a.O. S. 1207). Weitere Konkretisierungen durch die Polizei seien zulässig. Maßgebliche Konkretisierungen und Standardisierungen seien durch die Polizei nachvollziehbar zu dokumentieren und zu veröffentlichen. Dies sei auch wichtig für die **Kontrolle durch die Datenschutzbeauftragten**. Der **Gesetzgeber** müsse zudem die von ihm selbst normierten Angaben **hinreichend bestimmt und normenklar** regeln. Soweit sich Anforderungen bereits aus dem allgemeinen Datenschutzrecht ergäben, müsse auch hinreichend klar sein, was daraus für die praktische Ausgestaltung der Maßnahme folge (ebd.).

Der **Ausschluss von Daten aus der Wohnraumüberwachung** oder **Online-Durchsuchung** von einer Datenanalyse oder -auswertung zur (allein) vorbeugenden Bekämpfung von Straftaten sei mit Blick auf den Zweckbindungsgrundsatz ausnahmslos **gesetzlich zu regeln** (ebd. S. 1208). Auch Daten aus anderen schwerwiegenden Grundrechtseingriffen dürften nur unter engen Voraussetzungen genutzt werden. Dies müsse zudem durch gesetzliche Regelungen zur wirksamen Umsetzung dieser Anforderungen durch technische und organisatorische Vorkehrungen abgesichert werden. Hierzu gehöre etwa die vorab notwendige **Kennzeichnung und Abtrennung von Informationen aus eingriffsintensiven Maßnahmen**, um einen Zugriff hierauf zu verhindern. Der Einsatz **selbstlernender Systeme** und eine Beschränkung von Abgleichmöglichkeiten müsse im Gesetz ausdrücklich ausgeschlossen werden. Auch der Ausschluss maschineller Gefährlichkeitsaussagen über Personen im Sinne eines „**predictive policing**“ müsse vom Gesetzgeber selbst geregelt werden, um eine Verringerung des Eingriffsgewichts zu bewirken (ebd.).

3. Gesetzliche Ausgestaltung in NRW

Legt man diese Maßstäbe an die nordrhein-westfälische Regelung an, bestehen erhebliche Probleme mit der Verfassungsmäßigkeit der Maßnahme, die nachfolgend kurz dargestellt werden. Dabei ist zu berücksichtigen, dass eine umfassende Prüfung der Verfassungsmäßigkeit der Norm im Sinne der Rechtssprechung des BVerfG vom 16.2.2023 nur unter Hinzuziehung umfangreicher weiterer Informationen technischer und faktischer Natur sowie Kenntnis der genauen Abläufe von Maßnahmen im Sinne von Absatz 6, interner Verwaltungsvorgänge sowie interner Regelungen und Abläufe möglich ist. All dies ist mangels Veröffentlichung der notwendigen Informationen und Transparenz hier nicht möglich. Festgestellt werden kann nur, dass die vom BVerfG verlangten umfangreichen Regelungen durch den Gesetzgeber selbst oder eine explizite Delegation an den Verordnungsgeber oder die Polizei mit entsprechenden Veröffentlichungspflichten nicht hinreichend beachtet werden. Die Problematik gewinnt durch die Verwendung der Software eines ausländischen Herstellers deutlich an Gewicht, wie das BVerfG in seiner Entscheidung ebenfalls betont hat.

Automatisierte Zusammenführung

Nach Absatz 1 Satz 1 darf die Polizei zunächst die nach § 22 rechtmäßig gespeicherten personenbezogenen Daten automatisiert zusammenführen. Der Grundsatz der Zweckbindung wird dabei nach Ansicht der Landesregierung eingehalten, weil die automatisierte Zusammenführung als solche noch keine „Nutzung“ der Daten für die polizeiliche Aufgabenerfüllung beinhalte, sondern nur eine technische Voraussetzung für diese Nutzung darstelle (LT-Drs. 17/16517, 17). Diese Verneinung des Tatbestandes einer Datenverarbeitung ist wenig plausibel, da gerade die Zusammenführung verschiedener Daten zu neuen Erkenntnissen qua Herstellung von (Quer-)Bezügen führen soll. Die Zusammenführung erfolgt gezielt und allein zum Zwecke der weiteren Verarbeitung. Die folgende „weitere“ Verarbeitung ist nicht nur eine mögliche Folge unter vielen (vgl. BVerfG NJW 2019, 827 Rn. 43 – Kennzeichenerfassung II), sondern Zweck der „Zusammenführung“. Die „Zusammenführung“ einer Vielzahl personenbezogener Daten hat nach den Ausführungen der Landesregierung den Zweck einer besseren Verwendung, um das Auslesen und Abfragen durch die Polizei zu erleichtern. Die damit behauptete Trennung des Vorgangs der gezielten „Zusammenführung“ von Daten zur Verbesserung der Polizeiarbeit von einer weiteren „Nutzung“ ist künstlich; es handelt sich bereits bei der Zusammenführung nach S. 1 um einen Grundrechtseingriff.

Abgleich von Daten

Nach Absatz 1 Satz 2 darf die Polizei personenbezogene Daten mit den nach Satz 1 „zusammengeführten Daten abgleichen sowie diese zusammengeführten Daten auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen

Daten aufbereiten und analysieren“, soweit dies aus den sodann in Nr. 1 und 2 aufgeführten Gründen erforderlich ist. Die Zusammenführung nach Satz 1 dient indes der folgenden Durchführung der Maßnahmen nach Satz 2 und kann deshalb rechtlich nicht isoliert hiervon betrachtet werden (vgl. BVerfG NJW 2019, 827 Rn. 43 - Kennzeichenerfassung II). „Angebunden“ an das neue System ist nach diesseitiger Kenntnis rund ein Dutzend polizeilicher Informationssysteme, u.a. INPOL Zentral, ViVa (inklusive INPOL Land), IGVP und CASE NRW. Daneben können Daten aus externen Datenbeständen, auf die die Polizei Zugriff hat, im DAR-System genutzt werden. Hierzu gehören unter anderem Daten der Einwohnermeldeämter oder des Kraftfahrtbundesamtes (LDI NRW, Schreiben v. 25.3.2021, LT NRW Vorlage 17/5078, 2).

Die Nutzung von Daten jenseits polizeilicher Datenbestände stellt zugleich eine (neue) Datenerhebung und Zweckänderung dar, wenn nämlich Daten anderer Behörden wie bspw. Meldedaten, Kfz-Halterdaten oder Einträge im Waffenregister zum Abgleich übermittelt oder abgerufen werden. Auch die zielgerichtete Erhebung personenbezogener Daten in allgemein zugänglichen Bereichen sozialer Netzwerke im Internet stellt nach der Rechtsprechung des BVerfG in diesem Kontext einen Grundrechtseingriff dar. Für jede dieser Erhebungen bedarf es daher einer eigenständigen Erhebungsbefugnis (Golla, LT NRW Vorlage 17/5418, 15, 20, 33). Ob und insbesondere wie auch öffentlich zugängliche OSINT-Daten einbezogen werden, erscheint dabei unklar (vgl. Innenminister NRW, LT NRW Vorlage 17/5418, 14; s. auch Gutachten Golla, LT NRW Vorlage 17/5418, 12 ff.).

Hinzu kommen die Daten aus der Vorgangsverwaltung und damit eine Verarbeitung von Daten einer Vielzahl von Menschen, die hierzu keinen Anlass gegeben haben (vgl. BVerfG 13.2.2023 Rn. 126, 134 ff.). Zutreffend kritisiert daher die LDI NRW (LT NRW Stellungnahme 17/4970, 3), dass die DAR-Software auch Datenbestände durchsuche, die lediglich zur Vorgangsverwaltung und Dokumentation polizeilichen Handelns gespeichert werden und nicht selten Personen betreffen, die dort weder als Verantwortliche (Störer) noch als Verdächtige erfasst sind. Dies durchbricht den Grundsatz der Zweckbindung (vgl. BeckOK PolR Hessen/Bäuerle HSOG § 25a Rn. 24).

Zielrichtung der Maßnahme

Zulässig sind die Maßnahmen nach Satz 2 Nr. 1 zur Verhütung oder vorbeugenden Bekämpfung der in Nr. 1 genannten Katalogstraftaten, wobei neben den dort spezifisch aufgeführten Straftaten in Form einer Kettenverweisung auf den überaus weiten Katalog in § 100a Abs. 2 StPO verwiesen wird. Dabei ist nicht einmal klar, ob es sich um eine statische oder dynamische Verweisung handeln soll (vgl. GFF, LT NRW Stellungnahme 17/4971, 17). Mit der in der Gesetzesbegründung

angegebenen Zielrichtung der Maßnahme ist diese Weite der Kettenverweisung mit Blick auf die Eingriffsintensität der Maßnahme nicht vereinbar und unverhältnismäßig. Insbesondere aber ist die Eingriffsschwelle in S. 2 Nr. 1 deutlich niedriger als in Satz 2 Nr. 2, der eine (konkrete) Gefahr für hochrangige Rechtsgüter verlangt, was als Eingriffsschwelle nicht zu beanstanden sein dürfte (vgl. BVerfG NVwZ 2021, 226 Rn. 118; BVerfG 13.2.2023 Rn. 105).

Data-Mining

Gemäß S. 3 dürfen bei der Verarbeitung nach Satz 2 die nach Satz 1 zusammengeführten Daten nicht mittels statistisch-mathematischer Verfahren oder in sonstiger Weise selbständig auf Zusammenhänge analysiert werden. Mit dieser Regelung wird nach Ansicht des Gesetzgebers eine Datenverarbeitung durch Data-Mining im Sinne der zweiten ATDG-Entscheidung des BVerfG vom 10.11.2020 (NVwZ 2021, 226 Rn. 74) ausgeschlossen. Der Rechtsbegriff „selbständig“ meine „die rein automatisierte Auswertung von Datenbeständen ohne menschliches Zutun“. Die Vorschrift erlaube insbesondere keine automatisierte Entscheidungsfindung iSd § 46 Abs. 1 DSG NRW. Nicht ausgeschlossen seien dagegen „vom menschlichen Bearbeiter jeweils anhand von bereits vorliegenden oder im Zuge der Analyse festgestellten Erkenntnissen angestoßene weitere Analysevorgänge“ (LT-Drs. 17/16517, 18).

Hier wird zwar die Nutzung statistisch-mathematischer Verfahren ausgeschlossen. Welche damit genau gemeint sind und auf welchen Verfahren die Datenverarbeitung auf Grundlage des Art. 6 beruht, bleibt dabei indes im Dunkeln. Satz 3 schließt weiter aus, dass die zusammengeführten Daten „in sonstiger Weise selbständig auf Zusammenhänge analysiert werden“. Wollte man der Argumentation der Landesregierung folgen, die darauf abstellt, dass eigene und fremde Datenbestände immer dann nicht selbständig auf Zusammenhänge analysiert würden, wenn dies von menschlicher Hand „angestoßen“ werde, würden im Umkehrschluss nur dann Analysevorgänge den Beschränkungen zum Data-Mining in der Entscheidung zum Antiterrordateigesetz II des BVerfG (BVerfG NVwZ 2021, 226) und in der Entscheidung zur automatisierten Datenanalyse vom 16.2.2023 unterfallen, wenn gleichsam das Analysesystem sich selbst „anstieße“, vorhandene Datenbestände zu durchsuchen und auszuwerten. Oder aber es fände nach Absatz 6 nur ein einfacher Datenabgleich statt, der bereits in § 25 spezialgesetzlich geregelt ist. Beides kann den Einwand eines übermäßig in die Grundrechte eingreifenden Data-Mining nicht widerlegen.

Protokollierung

Nach Satz 4 ist die Abfrage zu protokollieren. Es fehlt hierfür jedoch eine präzisierende und rechtlich hinreichend bestimmte Festlegung im Gesetz selbst zum Protokollierungsumfang und zu den zu protokollierenden Daten.

Erkennbarkeit des Grundrechtseingriffs

Betroffene Personen haben von der Datenverarbeitung regelmäßig keine Kenntnis. Dies gilt selbst dann, wenn die verarbeiteten Daten ursprünglich offen erhoben wurden. Dass diese Daten für andere Zwecke weiterverwendet werden, ist für die Betroffenen nicht transparent. Es handelt sich somit um eine nicht offene, heimliche oder verdeckte Maßnahme, wodurch das Eingriffsgewicht weiter erhöht ist“ (LDI NRW, LT NRW Stellungnahme 17/4970, 3; ebenso Golla, LT NRW Vorlage 17/5418, 13 f.). Dennoch fehlen Vorgaben für eine kurzfristige Löschung der Erkenntnisse aus der Auswertung, soweit nicht dargelegt werden kann, dass diese für die Aufgabenerfüllung zwingend erforderlich sind (GFF, LT NRW Stellungnahme 17/4971, 15). Mangels Benachrichtigungspflicht über die Erfassung einer Person im Rahmen der Maßnahme (vgl. § 48 DSG NRW) wird auch die Transparenz der Datenverarbeitung vernachlässigt. Dies wird durch das Fehlen einer klar geregelten Anordnungsbefugnis oder deren Externalisierung auf die Gerichte sowie eine fehlende gesetzlich verankerte Einbeziehung der Datenschutzaufsicht weiter verstärkt (vgl. GFF, LT NRW Stellungnahme 17/4971, 14 f. unter Hinweis auf § 25a HSOG; kritisch dazu auch BeckOK PolR Hessen/Bäuerle HSOG § 25a Rn. 54).

4. Fazit

Es zeigt sich, dass eine automatisierte Datenanalyse oder -auswertung (Data-Mining) nur schwer mit grundrechtlich Anforderungen kompatibel auszugestalten ist. Die Anforderungen des BVerfG in der Entscheidung vom 16.2.2023 konnten mit Blick auf den zeitlichen Ablauf vor der Wahl vom Landesgesetzgeber in NRW nicht berücksichtigt werden. Hinreichende Geduld wäre hier vermutlich für den Bestand des Gesetzes vor eben diesem Gericht besser gewesen.

IV. Allgemeine datenschutzrechtliche Anforderungen

Die verfassungsrechtlichen Anforderungen an die Zulässigkeit einer automatisierten polizeilichen Datenanalyse oder Datenauswertung aus dem Grundrecht auf informationelle Selbstbestimmung und anderen Grundrechten werden oben und in den Stellungnahmen bspw. des Bundesdatenschutzbeauftragten, des Kollegen Löffelmann, der GFF und anderer Sachverständiger in dieser Anhörung dargestellt. Nicht zuletzt der Bundesdatenschutzbeauftragte hat in seiner Stellungnahme darauf hingewiesen, dass im Falle der Einführung einer solchen Analysesoftware

die Entwicklung einer eigenen Software-Lösung vorzugswürdig wäre, wobei er die Notwendigkeit einer solchen Software ausdrücklich offengelassen hat.

Dass das Bundesdatenschutzgesetz und die dort verankerten datenschutzrechtlichen Anforderungen nicht nur bei der Nutzung einer neuen Technologie im „Regelbetrieb“ gelten, wird polizeiliche immer wieder „übersehen“ und es werden Neuentwicklungen mit „echten“ Daten oder im Echtbetrieb der Polizeien getestet (s.o. III), ohne dass hierfür eine Rechtsgrundlage vorläge. Diese Praxis muss endlich durch die Polizeien selbst oder die Datenschutzbehörden beendet werden.

In diesem Kontext sei insbesondere an den seit 2017 geltenden **§ 67 BDSG** zur unter im Gesetz näher bestimmten Voraussetzungen zwingend notwendigen Durchführung einer **Datenschutz-Folgenabschätzung** (und die entsprechenden Landesregelungen) „erinnert“,, die bis heute in den Innen- und Polizeibehörden mit Blick auf die hier diskutierte **besonders eingriffsintensive Maßnahme** offenbar in Hessen, Hamburg, NRW und Bayern auf wenig Beachtung stieß oder deren Ergebnisse zumindest niemals transparent der Öffentlichkeit vorgestellt wurde.

§ 67 BDSG gibt für die Datenschutz-Folgenabschätzung vor

> *(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich* ***eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge****, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.*
> (…)
> *(4) Die Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:*
> *1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,*
> *2.eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,*
> *3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und*
> *4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.*

> *(5) Soweit erforderlich, hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Folgenabschätzung ergeben haben.*

§ 67 BDSG konstituiert damit eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung nach den tatbestandlichen Voraussetzungen der Norm und diese ist gerade im polizeilichen Bereich zudem nach Art. 27 JI-RL Pflicht, wenn „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen**“ besteht. In diesem Falle hat „der Verantwortliche **vorab** eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge **für den Schutz personenbezogener Daten**“ durchzuführen.

Nach der Gesetzesbegründung zu § 67 BDSG ist die Datenschutz-Folgenabschätzung ein „zentrales **Element der strukturellen Stärkung des Datenschutzes**“. Dabei soll „nicht eine Einzelverarbeitung, sondern lediglich die **Verwendung maßgeblicher Systeme und Verfahren** zur Verarbeitung personenbezogener Daten mithilfe einer Datenschutz-Folgenabschätzung **vorab** in den Blick genommen werden“ müssen. Kriterium dafür, ob eine Vorababschätzung der Risiken durchzuführen ist, soll nach der Gesetzesbegründung die „**Eingriffsintensität** der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein“ (BT-Drs. 18/11325, S. 117).

In diesem Kontext ist auch auf **§ 68 BDSG** hinzuweisen, welcher der Umsetzung des Art. 28 JI-RL dienen soll. „Die **Vorkonsultation** (…) der oder des **Bundesbeauftragten** dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die **ein erhöhtes Gefährdungspotential** für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung (§ 67)“, führt die Gesetzesbegründung (a.a.O.) weiter aus.

Wer wollte nach der Entscheidung des BVerfG vom 10.11.2020 (ATDG II) und der vom 16.2.2023 zum Data-Mining in Hessen und Hamburg das Vorliegen der tatbestandlichen Voraussetzungen des § 67 bzw. des Art. 27 Abs. 1 JI-RL ernsthaft verneinen? Offenkundig kann Data-Mining (wie auch immer bezeichnet) „eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge“ haben.

Hinzu kommt, dass im polizeilichen Bereich verbreitet „**besondere Kategorien personenbezogener Daten**“ („sensible Daten“) im Sinne des Art. 10 der Richtlinie

(EU) 2016/680 (JI-Richtlinie) verarbeitet werden, wofür **besondere Schutzvorkehrungen** gegen eine unzulässige Verarbeitung zu beachten sind (zur mangelnden Beachtung bindenden Rechts in diesem Bereich vgl. Arzt, Polizeiliche Verarbeitung „besonderer Kategorien personenbezogener Daten“ - Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, Die Öffentliche Verwaltung 2023, 991 ff.).

V. Empfehlungen für das weitere Vorgehen

In der Entwicklung neuer Technologien für die Sicherheitsbehörden werden die datenschutzrechtlichen Anforderungen immer wieder „ausgeblendet“ und allenfalls am Ende oder im Rahmen der sogenannten Begleitforschung (ELSI) bearbeitet (vgl. Arzt/Heesen/Rappold/Schuster, Neue Überwachungstechnologien und "Begleitforschung", Bürgerrechte und Polizei / CILIP 134, 2024, 57 ff.). Soweit auf die hier diskutierte Anwendung zum Data-Mining nicht aus grundsätzlichen Erwägungen verzichtet wird, was aus Sicht des Grundrechtsschutzes unzweifelhaft zu begrüßen wäre (so auch Ruf/GFF in dieser Anhörung), sollte endlich das Bundesdatenschutzgesetz ernst genommen werden (s.o. IV.) und ein breiter und öffentlicher Diskurs mit rechtlichem, sozialwissenschaftlichem, zivilgesellschaftlichem und polizeilichem Sachverstand organisiert werden, der ergebnisoffen die Einführung solch weitgehender Überwachungstechnologien diskutiert.

Danach kann im Falle einer positiven Entscheidung für ein polizeiliches Data-Mining im Anschluss an die abschließenden Bemerkungen des Kollegen Löffelmann in seiner Stellungnahme „eine Konsolidierung der erforderlichen Rechtsgrundlagen und Anforderungen an den Algorithmus [herbeigeführt werden], anstatt ein Produkt „auf Vorrat“ zu erwerben, das dann möglicherweise aus rechtlichen Gründen nicht oder nur eingeschränkt Verwendung finden kann.“

Berlin, 20. April 2024

gez. Prof. Dr. Clemens Arzt