Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 D

GESELLSCHAFT FÜR FREIHEITSRECHTE

17. April 2024

Stellungnahme

zu dem 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 im Innenausschuss des Deutschen Bundestags am 22. April 2024

von Dr. Simone Ruf,
Gesellschaft für Freiheitsrechte e.V.

A. Zusammenfassung

Die CDU/CSU-Bundestagsfraktion zielt mit ihrem Antrag vom 27. November 2023 unter dem Titel „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ (im Folgenden „**der Antrag**“) insbesondere darauf ab, dem Bundeskriminalamt und der Bundespolizei den Einsatz der Datenanalyse-Software VeRA, die auf Palantir Gotham beruht, zu ermöglichen.

Der Einsatz der Datenanalyse-Software Bundes-VeRA des US-amerikanischen Herstellers Palantir ermöglicht mittels sog. „Datamining“ tiefgreifende Grundrechtseingriffe und ist nach verfassungsgerichtlicher Rechtsprechung nur unter strengen Voraussetzungen zulässig.

Weder für das Bundeskrminalamt noch für die Bundespolizei existieren Rechtsgrundlagen, die zum Einsatz der Software zur Gefahrenabwehr oder Strafverfolgung ermächtigen.

Möchte der Gesetzgeber künftig den Einsatz legitimieren, müsste er eine hinreichend bestimmte und normenklare Rechtsgrundlage in den einschlägigen Gesetzen (BKAG, BPolG, StPO) schaffen. Dabei sind insbesondere die im Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 (1 BvR 1547/19 und 1 BvR 2634/20) zur automatisierten Datenanalyse (im Folgenden „**Datenanalyse-Urteil**“) vorgegebenen verfassungsrechtlichen Grenzen zu wahren, die je nach Eingriffsgewicht der Regelung im Einzelfall variieren.

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

Auch wenn damit die Einführung einer Rechtsgrundlage grundsätzlich möglich ist, ist dennoch davon abzuraten. Mit dem Einsatz der Software gehen schwere Grundrechtseingriffe, erhebliche Diskriminierungs- und Stigmatisierungsrisiken sowie Bedenken hinsichtlich der Datensicherheit und der allgemeinen Missbrauchsgefahr einher. Darüber hinaus ist die Effizienz der Software, abgesehen von anekdotischen Erfolgsgeschichten, nicht nachgewiesen.

Sollte sich der Gesetzgeber trotz der mit dem Datamining einhergehenden schwerwiegenden Grundrechtseingriffe dazu entschließen, eine solche Regelung zu schaffen, sollten ausreichende Einschränkungen getroffen werden, die verhindern, dass Unbeteiligte fälschlicherweise verdächtigt werden und die sicherstellen, dass Diskriminierung verhindert wird. Dazu bedarf es weitreichender Einschränkungen der Art und des Umfangs der verarbeitbaren Daten und der Auswertungsmethode. Es wird außerdem empfohlen, die verfassungsrechtlichen Grenzen nicht auszureizen und Datenanalysen nur bei konkreten Gefahren für überragend wichtige oder besonders gewichtige Rechtsgüter zuzulassen.

Jedenfalls ist davon abzuraten, auf kommerzielle Anbieter wie Palantir zurückzugreifen. Diese streben Gewinnmaximierung an und arbeiten mit vielen anderen Vertragspartner*innen zusammen, die ein Interesse an den Daten aus Deutschland haben könnten, sodass damit große Risiken für Datensicherheit und Datenschutz einhergehen. Darüber hinaus führt der Betriebsgeheimnisschutz, auf den sich kommerzielle Anbieter berufen, zu einem hohen Maß an Intransparenz und erschwert Betroffenen nachträglichen Rechtsschutz. Mithin wäre eine staatlichen Eigenentwicklung zu bevorzugen, um Transparenz sicherzustellen und Abhängigkeit zu verhindern. Bis dahin stünden Sicherheitsbehörden zahlreiche andere Ermittlungs- und Überwachungsbefugnisse zur Verfügung, die zur Bekämpfung und Verhinderung schwerer Kriminalität eingesetzt werden dürfen.

B. Bewertung

1. Schwerwiegende Grundrechtseingriffe durch Datenanalyse

Der Einsatz von VeRA kann zu schwerwiegenden Eingriffen in die Grundrechte vieler Menschen führen. Durch sogenanntes „Datamining“ werden in komplexen Abgleichschritten polizeiliche Datenbestände zusammengeführt, verknüpft und daraus neues persönlichkeitsrelevantes Wissen generiert. Dies geht weit über das hinaus, was einzelne Polizeibeamt*innen leisten können und birgt das Risiko der Erstellung ganzer Persönlichkeitsprofile. Angesichts der Heimlichkeit der Maßnahme können Betroffene regelmäßig nicht gegen ungerechtfertigte Datenanalysen vorgehen. Dies verschärft den Eingriff. Da polizeiliche Datenbestände auch viele Daten von

Personen enthalten, die polizeilich noch nie Anlass für Gefahrenabwehr- oder Ermittlungsmaßnahmen gegeben haben, besteht ein hohes Risiko, dass diese durch die Einbeziehung ihrer Daten in Datenanalysen fälschlicherweise als Störer*innen oder Verdächtige qualifiziert werden.

2. Keine bestehenden Rechtsgrundlagen im Bundeskriminalamtgesetz, Bundespolizeigesetz und in der Strafprozessordnung

Weder auf präventiver noch auf repressiver Ebene existieren derzeit Rechtsgrundlagen, die dem Bundeskriminalamt oder der Bundespolizei den Einsatz von VeRA oder einer anderen Datenanalysesoftware erlauben.

Da Datenanalysen besonders schwere Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) darstellen und ihnen ein besonderes Eigengewicht zukommt, das über die bloße Weiterverarbeitung von Daten hinausgeht[1], verbietet sich ein Rückgriff auf datenschutzrechtliche Generalklauseln, wie § 12 BKAG oder § 29 BPolG (bzw. § 42 BPolG-E[2]) .

Auch speziellere Regelungen der Datenverarbeitung im Bundeskriminalamtgesetz, im Bundespolizeigesetz und in der Strafprozessordnung betreffen andere Maßnahmen und ermächtigen nicht zum Einsatz solcher Analysetools.

§ 34 BPolG (bzw. § 57 BPolG-E[3]) ermächtigt lediglich dazu, personenbezogene Daten mit dem Inhalt von Dateien zum Zweck der Feststellung zu vergleichen, ob darin bereits personenbezogene Daten einer Person gespeichert sind[4], und berechtigt nicht zu einer darüberhinausgehenden Analyse.

Rasterfahndungen sind sowohl auf präventiver Ebene (§ 48 BKAG) als auch auf repressiver Ebene (§ 98a StPO) vorgesehen. Diese Befugnisse ermächtigen aber nicht zur Durchführung von Datenanalysen, da diese keinen festgelegten Suchkriterien bzw. keinem begrenzenden Auswerteraster folgen. Datenanalysen sind deutlich komplexer und erschöpfen sich nicht in einfachen Abgleichen. § 98a StPO knüpft an ein „Verdächtigenprofil“ im Sinne der auf den Täter

[1] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 67 ff.
[2] BT-Drs. 20/10406, S. 38.
[3] BT-Drs. 20/10406, S. 48.
[4] Wehr, in: Nomos-BR, BPolG, 3. Aufl. 2021, § 34 Rn. 1.

vermutlich zutreffenden Prüfungsmerkmale an.[5] Eine Datenanalyse geht hingegen darüber hinaus und kann unter anderem dazu dienen, genau diese Prüfungsmerkmale erst zu generieren. Weiterhin werden bei der Datenanalyse – je nach Konfiguration – teilweise oder zum Großteil Datenbestände der Polizei, also „justizinterne" Daten verarbeitet. Der Abgleich mit „internen" Daten richtet sich aber nach § 98c StPO, der § 98a StPO insofern verdrängt.[6]

Da § 98c StPO an nur wenige Voraussetzungen geknüpft ist, kann er nur geringfügige Grundrechtseingriffe rechtfertigen.[7] Weil automatisierte Datenanalysen aber schwere Grundrechtseingriffe darstellen, können sie nicht auf § 98c StPO gestützt werden.

Eine Nutzung der Software wäre entsprechend erst und nur dann möglich, nachdem der Gesetzgeber eine den Anforderungen aus dem Datenanalyse-Urteil genügende Eingriffsgrundlage im Bundespolizeigesetz und Bundeskriminalamtgesetz (zu präventiven Zwecken) sowie in der Strafprozessordnung (zu repressiven Zwecken) geschaffen hat. Vorher wäre auch nach der im Antrag unter Nr. 1 geforderten Genehmigung des Bundesministeriums des Inneren und für Heimat eine Nutzung unzulässig.

Es ist äußerst bedenklich, dass der Antrag nahe legt, eine derart eingriffsintensive Software ohne die Schaffung einer speziellen gesetzlichen Grundlage einzuführen. Auch in Hessen und Nordrhein-Westfalen wurde von den jeweiligen Landesdatenschutzbeauftragten kritisiert, dass die Software über einen langen Zeitraum ohne Rechtsgrundlage unter dem Deckmantel eines „Pilotprojekts" eingesetzt wurde. Das Bundesverfassungsgericht hat mit seinem Datenanalyse-Urteil nunmehr aber verbindlich festgestellt, dass der Einsatz solcher Software nur auf hinreichend bestimmte, normenklare Rechtsgrundlagen, die spezifisch Datenanalysen betreffen, gestützt werden kann.[8]

3. Gründe gegen die Schaffung einer Rechtsgrundlage

Von der Einführung einer Ermächtigungsgrundlage in den entsprechenden Gesetzen ist abzuraten.

[5] Vgl. Gerhold, in: BeckOK StPO, 50. Ed. 1.1.2024, § 98a Rn. 8.
[6] Gerhold, in: BeckOK StPO, 50. Ed. 1.1.2024, § 98a Rn. 4 f.
[7] Gercke, in: Gercke/Temming/Zöller, StPO, 7. Aufl. 2023, § 98c Rn. 3; Gerhold, in: BeckOK StPO, 50. Ed. 1.1.2024, § 98c Rn. 1.
[8] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 55, 110 ff.

Dass Datenanalysen schwerwiegende Grundrechtseingriffe ermöglichen, hat auch das Bundesverfassungsgericht in dem dem Datenanalyse-Urteil zu Grunde liegenden Verfahren betont, in dem es unter anderem um die Rechtsgrundlage für den Einsatz der Software hessenDATA ging, die genauso wie VeRA auf Palantir Gotham beruht.[9] Durch die Analysesoftware können Polizeibehörden neue persönlichkeitsrelevante Informationen erlangen. Die Software führt nicht nur vorhandene Daten zusammen, sondern kann Querverbindungen herstellen und Muster erkennen. Damit besteht die Gefahr der Erstellung umfassender Persönlichkeitsprofile.

a) Risiko falscher Verdächtigung

Mit dem Einsatz sind erhebliche Risiken verbunden. Besonders problematisch ist das **Risiko für objektiv Unbeteiligte**, Ziel weiterer polizeilicher Aufklärungs- oder gar imperativer Maßnahmen zu werden. Polizeiliche Datenbanken enthalten eine große Menge an Daten unbeteiligter Personen, insbesondere von Anzeigenerstatter*innen, Zeug*innen oder Hinweisgeber*innen. So reicht es schon aus, einen Auskunftsantrag bei Polizeibehörden zu stellen, um in deren Vorgangsverwaltungssysteme aufgenommen zu werden. Insbesondere im Rahmen der Vorgangsverwaltung ist eine vorherige Aussonderung oder Kategorisierung der Vorgangsdaten Unbeteiligter praktisch nicht möglich, da für diese Sachverhalte eine abschließende Beurteilung oft noch aussteht. Auch im Rahmen von Funkzellenabfragen werden massenhaft Verkehrsdaten Unbeteiligter erhoben. Aber auch für Menschen, die tatsächlich Anlass zu Ermittlungen oder Gefahrenabwehrmaßnahmen gegeben haben, besteht ein erhöhtes Risiko, von diesem Anlass losgelöst, in ganz anderen Kontexten verdächtigt zu werden, wenn die Software fälschlicherweise Verknüpfungen erstellt oder sie zufällig wegen bestimmter, lediglich korrelierender Merkmale in ein von der Software generiertes Muster passen.

b) Diskriminierungsgefahr

Polizeilichen Datensätzen sind Diskriminierungen immanent, die durch den Einsatz von Künstlicher Intelligenz und komplexer Analysen verstärkt würden. Es besteht die Gefahr, dass ganze Personengruppen unter Generalverdacht gestellt und stigmatisiert werden.

Der Hersteller bewirbt sein Produkt Palantir Gotham als ein kommerziell verfügbares KI-fähiges Betriebssystem.[10] Der Einsatz **Künstlicher Intelligenz** ist mit besonders großen Gefahren und Diskriminierungsrisiken verbunden. Das hat auch das Bundesverfassungsgericht im

[9] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, insb. Rn. 104 ff., 125 ff.
[10] Zitiert nach https://www.palantir.com/de/platforms/gotham/ (Stand: 17. April 2024).

Datenanalyse-Urteil festgestellt, indem es die Verhinderung der Herausbildung und Verwendung diskriminierender Algorithmen als spezifische Herausforderung bewertet.[11]

Die Herausbildung und Verwendung diskriminierender Algorithmen kann derzeit aber kaum verhindert werden. Gerade wenn der Staat nicht am Entwicklungsprozess beteiligt ist, um beispielsweise Einfluss auf Trainingsdaten nehmen zu können, ist dies ausgeschlossen. Schädlich ist auch, dass die polizeilichen Datenbanken, die einer Datenanalyse zugrundeliegen, regelmäßig nicht um strukturelle Diskriminierungen bereinigt werden.

Auch weitreichende Transparenzregelungen im Sinne sogenannter „Explainable AI", also erklärbarer KI, wären dann sowohl bei der Verwendung selbstlernender Systeme als auch bei komplexen deterministischen Systemen angezeigt. Der Gerichtshof der Europäischen Union hat darauf hingewiesen, dass gerade im Hinblick auf die Gewährleistung von effektivem Rechtsschutz und Kontrolle transparent und nachvollziehbar sein muss, wie eine Software zu dem jeweiligen Ergebnis im Einzelfall kommt. Angesichts der für die Funktionsweise von Technologien der künstlichen Intelligenz kennzeichnenden mangelnden Nachvollziehbarkeit kann es sich hingegen als unmöglich erweisen, den Grund zu erkennen, aus dem ein bestimmtes Programm einen Treffer erzielt hat.[12]

c) Predictive Policing

Problematisch ist weiterhin, dass die Software auch dafür eingesetzt werden kann, Gefahren zu erkennen, bevor konkrete Anhaltspunkte dafür vorliegen. Dann bewegen sich Polizeibehörden aber unterhalb der Schwelle einer konkreten oder konkretisierten Gefahr. Zwar ist auch ein Einsatz zur vorbeugenden Bekämpfung von Straftaten bei hinreichenden Einschränkungen verfassungsrechtlich nicht ausgeschlossen.[13] Die Grenzen zu einem Predictive Policing, das unter Umständen darin münden kann, maschinell Gefährlichkeitsprognosen über Personen zu erstellen[14], ist damit aber aufgeweicht. Eine gänzlich anlasslose automatisierte Auswertung personenbezogener Daten durch Polizeibehörden zur vorbeugenden Bekämpfung von Straftaten ist jedenfalls verfassungsrechtlich unzulässig.[15]

[11] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
[12] Vgl. EuGH, Urteil v. 21. Juni 2022, C-817/19 (Fluggastdatensätze), Rn. 195.
[13] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 107.
[14] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 98.
[15] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 108.

d) Kein nachgewiesener Mehrwert

Insoweit der Antrag zur Begründung anekdotisch auf Erfolge der Software abgestellt, ist anzumerken, dass nicht nachgewiesen ist, ob die genannten Erfolge wirklich kausal auf den Einsatz der Software zurückzuführen sind oder (auch) durch andere Ermittlungsbefugnisse erzielt wurden. Es ist nicht ausreichend dargelegt, ob die Software tasächlich einen Mehrwert bei der Verhinderung und Aufklärung schwerer Verbrechen hat. Der Antrag legt die Effizient mithin nicht ausreichend dar. Dies wäre aber in Anbetracht der offenkundigen Gefahren und Risiken notwendig.

Darüber hinaus ist zu betonen, dass in der mündlichen Verhandlung zum Datenanalyse-Urteil die Vertreter*innen der hessischen Polizeibehörden und des Innenministeriums immer wieder betonten, dass der Mehrwert der Software insbesondere in der übersichtlichen und durchsuchbaren Auswertung der bestehenden Datenbanken durch hessenDATA lag. Derartige Übersichtlichkeit und Durchsuchbarkeit lässt sich aber auch realisieren, ohne zugleich eingriffsintensive und riskante Analysetools einzuführen, die über das Ziel hinaus schießen.

Im Übrigen stehen den Polizeibehörden bereits umfangreiche Ermittlungs- und Gefahrenabwehrbefugnisse zur Verfügung, die zum Teil intensive Grundrechtseingriffe zulassen.

Vor diesem Hintergrund sollten keine Rechtsgrundlagen geschaffen werden, die den Einsatz von VeRA ermöglichen.

4. Anforderungen an eine Rechtsgrundlage

Sollte sich der Gesetzgeber dennoch entschließen, eine Rechtsgrundlage für den Einsatz automatisierter Anwendungen zur Datenanalyse zu schaffen, muss er neben den Mindestanforderungen, die die Richtlinie (EU) 2016/680 vom 27. April 2016 (im Folgenden „**JI-RL**“)[16] vorgibt, die verfassungsrechtlichen Grenzen einhalten, die sich aus dem Verhältnismäßigkeitsgrundsatz ergeben. Diese hat das Bundesverfassungsgericht im Datenanalyse-Urteil teilweise ausformuliert.

[16] 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.

Wenn im Antrag ausgeführt wird, dass durch den Einsatz ein verbesserter polizeilicher Informationsaustausch ermöglicht würde (Nr.5), ist darauf hinzuweisen, dass das Bundesverfassungsgericht für Übermittlungsbefugnisse enge Grenzen aufgezeigt hat.[17] Diese Anforderungen dürfen nicht durch den Einsatz von Software wie VeRA umgangen werden. Darüber hinaus ist schon unklar, wie eine Analysesoftware zum verbesserten Informationsaustausch beitragen soll, da sie der Auswertung und nicht der Übermittlung von Daten dient.

a) Einhaltung der Grundsätze der Zweckbindung

Da automatisierte Anwendungen zur Datenanalyse sowohl zweckwahrende als auch zweckändernde Weiterverarbeitungen ermöglichen, sind die verfassungsrechtlichen Grundsätze der Zweckbindung, insbesondere der **Grundsatz der hypothetischen Datenneuerhebung** zu beachten.[18] Eine grundrechtskonforme Ausgestaltung erfordert zwingend auch die technische Umsetzung der Zweckbindung in der Praxis, zum Beispiel mittels Kennzeichnung. Diese kann sich als durchaus aufwändig gestalten.

b) Variable Eingriffsvoraussetzungen nach Eingriffsgewicht

Weil automatisierten Anwendungen zur Datenanalyse aber über die bloße Weiterverbreitung vorhandener Daten eigene Belastungseffekte zukommen, da im Sinne eines Datamining neues persönlichkeitsrelevantes Wissen erzeugt werden kann, müssen darüber hinaus bei den Eingriffsvoraussetzungen weitere verfassungsrechtliche Grenzen beachtet werden. Diese sind variabel und hängen von der Eingriffsintensität ab.[19]

Maßgeblich für die Eingriffsvoraussetzungen ist das **Eingriffsgewicht, das der Gesetzgeber durch einschränkende Regelungen steuern kann**.[20] Dann sollten aber mindestens Regelungen getroffen werden, um die oben genannten Risiken und Gefahren zu reduzieren.

Konkret sollten Datenbestände, die typischerweise eine Vielzahl an **Daten Unbeteiligter** enthalten, ausgeschlossen werden. Dies betrifft Vorgangsdaten und Verkehrsdaten, vor allem solche, die aus Funkzellenabfragen stammen, aber auch Asservate. Bei Datenkategorien, die

[17] BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 275 ff.; BVerfG, Beschluss des Ersten Senats vom 10. November 2020, 1 BvR 3214/15, Rn. 99 ff.
[18] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 55 ff.
[19] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 103 ff.
[20] Vgl. dazu näher BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 79 ff.

besonders sensible Daten nach Art. 10 JI-RL darstellen, ist jeweils zu hinterfragen, ob ihre Einbeziehung unbedingt erforderlich ist und vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt. Zu den besonders sensiblen Daten gehören unter anderem auch biometrische Daten. Gerade deren Ausschluss kann eingriffsmildernd wirken.[21] Auch **Daten aus schwerwiegenden Grundrechtseingriffen** sollten ausgeschlossen werden. Dazu gehören zum Beispiel Daten aus Telekommunikationsüberwachung, Onlinedurchsuchung oder akustischer Wohnraumüberwachung. Es sollte außerdem sichergestellt sein, dass frei verfügbare Daten aus dem Internet nicht einbezogen werden. Weiterhin sollten Beschränkungen im Hinblick auf die einzusetzende **Methode** vorgenommen werden. In der Rechtsgrundlage sollte durch eine hinreichend bestimmte Regelung sichergestellt sein, dass VeRA nicht mit polizeilichen Daten „weiterlernen" darf.

Zwar erlaubt das Bundesverfassungsgericht den Einsatz unter bestimmten Voraussetzungen auch unterhalb der Gefahrenschwelle der konkreten Gefahr.[22] Jedoch muss der Gesetzgeber die verfassungsrechtlichen Spielräume nicht zwangsläufig bis an ihre Grenzen ausreizen. Um den mit Datenanalysen verbundenen Risiken und Gefahren für Grundrechte vorzubeugen, sollten die Eingriffe nur beim Vorliegen einer **konkreten Gefahr für überragend wichtige oder besonders gewichtige Rechtsgüter** erlaubt sein.

Darüber hinaus ergeben sich unabhängig von dem Umstand, wie eingriffsintensiv sich die Befugnis darstellt, in jedem Fall aus dem Verhältnismäßigkeitsgrundsatz Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle.[23] An dieser Stelle sollte eine **verpflichtende Kontrolle** durch mindestens eine*n (behördlichen oder unabhängigen) Datenschutzbeauftragte*n vorgesehen sein.

5. Spezifische Gefahren des Rückgriffs auf private Softwareanbieter

Zwar hat das Bundesverfassungsgericht im Datenanalyse-Urteil den Einsatz von Software privater Anbieter nicht grundsätzlich ausgeschlossen.[24] Die Entwicklung und Verwendung eines eigenen Analysetools würde aber einige Risiken in Bezug auf Datensicherheit und Datenschutz minimieren.

[21] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 87.
[22] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20.
[23] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.
[24] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

Das Risiko defizitärer **Datensicherheit** ist bei (ausländischen) Unternehmen deutlich höher als bei der Entwicklung eigener Software. Denn private Unternehmen unterliegen in einem höheren Maße Anreizen, die Daten mit anderen zu verbinden oder Dritten zur Verfügung zu stellen.

So hat auch das Bundesverfassungsgericht angemerkt, dass mit dem Einsatz von Software privater Anbieter die **Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte** verbunden ist.[25]

Zwar hat das Frauenhofer Institut für Sichere Informationstechnologie die Software VeRA teilweise untersucht und dabei keine sogenannte Backdoor festgestellt. Allerdings wurden nur Teilaspekte der Software überprüft, die Untersuchungsberichte sind nicht öffentlich und weiterhin wird mit jeder Weiterentwicklung der Software eine erneute Überprüfung notwendig.

Mit IT-Outsourcing geht auch ein hohes Maß an **Intransparenz und Abhängigkeit** einher. Denn die Funktionsweise des Analyseverfahrens ist für den Staat nicht einsehbar. Im Streitfall werden Privatunternehmen in der Regel mit Blick auf den Betriebsgeheimnisschutz eine Aufklärung der Funktionsweise ihrer Software verhindern. Es ist unklar, wie dann beispielsweise sichergestellt sein soll, dass sich im Rahmen der Konfiguration und Vorprogrammierung der Analyseschritte, welche seitens des Herstellers erfolgt, keine diskriminierenden Algorithmen herausbilden. Das Ausmaß staatlicher Einflussnahme mittels Ausschreibungen ist vor diesem Hintergrund denkbar gering.

Gerade das Argument der hohen **Kosten einer Eigenentwicklung**, wie es im Antrag vorgebracht wird, lässt außer Acht, dass auch der Einsatz privater Software mit immensen Kosten und Abhängigkeit verbunden ist.

So hat sich in Nordrhein-Westfalen, das ebenfalls eine auf Palantir Gotham beruhende Software mit dem Namen DAR nutzt, herausgestellt, dass sich die Kosten für das Gesamtprojekt statt ursprünglich auf 14 Millionen Euro nunmehr auf insgesamt 39 Millionen Euro belaufen.[26]

Langfristig ist zudem zu befürchten, dass derzeit geschaffene Abhängigkeiten zukünftig zu **erheblichen Preissteigerungen** durch den privaten Anbieter führen können. Bereits in Hessen,

[25] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
[26] Hell/Kartheuser, NRW-Polizei: Knapp 40 Millionen Euro für umstrittene Palantir-Software, WDR vom 25. September 2022, abrufbar unter https://www1.wdr.de/nachrichten/landespolitik/nrw-polizei-datenbank-software-palantir-kosten-100.html#:~:text=Mittlerweile%20kostet%20das%20Gesamtprojekt%20das%20Land%20NRW%20insgesamt%2039%20Millionen%20Euro (Stand: 17. April 2024).

Nordrhein-Westfalen und Bayern wird Software eines einzigen Herstellers genutzt. Durch den Rahmenvertrag wird dessen Marktposition noch weiter ausgebaut. Es ist kaum ersichtlich, dass die verwendenden Polizeibehörden zukünftig den Anbieter wechseln wollen. Zumindest wäre ein solcher Wechsel aber mit erheblichen Kosten verbunden. Die daraus resultierende Abhängigkeit versetzt den privaten Anbieter in die Lage, seine Preise zukünftig erheblich zu erhöhen, sodass sich die Kosten für den Staat über die Zeit auftürmen können. Vor allem im Hinblick auf zwingende sicherheitsrechtliche Updates oder zusätzliche Komponenten ist der Staat dann an die Preisvorstellung des Anbieters gebunden.

Schließlich lagert der Staat durch den Rückgriff auf private Anbieter hoheitliche Maßnahmen zu Lasten des Grundrechts- und Datenschutzes auf Private aus. Aufgrund der damit einhergehenden Risiken für einen effektiven Grundrechts- und Datenschutz ist staatlichen **Eigenentwicklungen der Vorzug** zu geben.[27] Es wäre ein fatales Signal, wenn Versäumnisse des Staates, rechtzeitig eigene, rechtssichere Strukturen zu schaffen, zu Lasten des Grundrechtsschutzes gingen.

[27] So auch Kugelmann/Buchmann, GSZ 2024, 1 (6).