20. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 74. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 22. April 2024, 14:00 Uhr
Konrad-Adenauer-Str. 1, 10557 Berlin
Paul-Löbe-Haus, Raum E 800

Vorsitz: Petra Pau, MdB

Tagesordnung - Öffentliche Anhörung

Einziger Tagesordnungspunkt **Seite 5**

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-Drucksache 20/9495

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Rechtsausschuss
Ausschuss für Digitales
Haushaltsausschuss

Berichterstatter/in:
Abg. Sebastian Fiedler [SPD]
Abg. Dr. Stefan Heck [CDU/CSU]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]
Abg. Manuel Höferlin [FDP]
Abg. Dr. Christian Wirth [AfD]
Abg. Martina Renner [Die Linke]

Inhaltsverzeichnis

Stellungnahmen der Sachverständigen

Unangeforderte Stellungnahme

Dem Ausschuss sind die Stellungnahmen teilweise in nicht barrierefreier Form zugeleitet worden.

Anwesende Mitglieder des Ausschusses

	Ordentliche Mitglieder	**Stellvertretende Mitglieder**
SPD	Baldy, Daniel Hartmann, Sebastian	
CDU/CSU	Heck, Dr. Stefan Oster, Josef	
BÜNDNIS 90/DIE GRÜNEN	Emmerich, Marcel Notz, Dr. Konstantin von	
FDP	Höferlin, Manuel	
AfD	Janich, Steffen Wirth, Dr. Christian	Benkstein, Barbara
Die Linke	Pau, Petra	
BSW	Ernst, Klaus	
fraktionslos		

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 22. April 2024, 14.00 Uhr
„Polizeiliche Analyse-Software Bundes-VeRA“

Stand: 11. April 2024

Prof. Dr. Clemens Arzt[3)]
Hochschule für Wirtschaft und Recht Berlin

Dr. Hans Christoph Atzpodien[4)]
Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V., Berlin

Susanne Dehmel[1)]
Bitkom e.V., Berlin

Prof. Dr. Markus Löffelmann[1)]
Hochschule des Bundes für öffentliche Verwaltung, Berlin

Prof. Ulrich Kelber[5)]
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn

Dirk Peglow[2)]
Bundesvorsitzender, Bund Deutscher Kriminalbeamter e.V., Berlin

Simone Ruf[3)]
Verfahrenskoordinatorin, Gesellschaft für Freiheitsrechte e.V., Berlin

Christine Skropke[1)]
secunet Security Networks AG, Essen

Klaus Teufele[2)]
Abteilungsdirektor, Bayerisches Landeskriminalamt, München

Dr. Roland Wagner[2)]
Landespolizeivizepräsident, Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz, Wiesbaden

---

1) Vorschlag SPD
2) Vorschlag CDU/CSU
3) Vorschlag BÜNDNIS 90/DIE GRÜNEN
4) Vorschlag FDP
5) Gemäß § 69a Abs. 3 GO-BT

Einziger Tagesordnungspunkt

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-Drucksache 20/9495

AVors. **Petra Pau** (Die Linke): Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen, ich eröffne die 74. Sitzung des Ausschusses für Inneres und Heimat und begrüße Sie alle sehr herzlich. Der Kollege Höferlin hat übermitteln lassen, dass er in der Anreise ist und es sicherlich, wenn ich hier alle Regularien erledigt habe, geschafft haben wird, dann auch an der Sitzung teilzunehmen.
Mein Name ist Petra Pau. Ich bin die derzeit amtierende oder Altersvorsitzende des Ausschusses für Inneres und Heimat und werde die öffentliche Anhörung der Sachverständigen leiten. Ich danke Ihnen allen, dass Sie uns als Sachverständige zur Verfügung stehen und unserer Einladung nachgekommen sind, um uns mit Ihrer Expertise zu bereichern, aber vor allem auch die Fragen der Kolleginnen und Kollegen des Ausschusses für Inneres und Heimat und auch der mitberatenden Ausschüsse zu beantworten. Ich begrüße daher zunächst die von den Fraktionen benannten und hier anwesenden Sachverständigen: Herrn Dr. Hans Christoph Atzpodien, Frau Susanne Dehmel, Herrn Prof. Dr. Markus Löffelmann hier auf der anderen Seite Herrn Prof. Ulrich Kelber als Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Herrn Dirk Peglow, Frau Simone Ruf, Frau Christine Skropke, Herrn Klaus Teufele und Herrn Dr. Roland Wagner. Habe ich irgendjemanden übersehen? Das ist nicht der Fall, also seien Sie uns alle herzlich willkommen. Professor Dr. Clemens Arzt musste leider seine Teilnahme kurzfristig absagen. Begrüßen darf ich dann für die Bundesregierung Frau Parlamentarische Staatssekretärin Rita Schwarzelühr-Sutter aus dem Bundesministerium des Inneren und für Heimat. Die Sitzung wird live im Parlamentsfernsehen und auf der Homepage des Deutschen Bundestages übertragen und ab morgen über die Mediathek für die Öffentlichkeit zum Abruf bereitgestellt. Wir hatten schriftliche Stellungnahmen erbeten. Ich bedanke mich bei allen Sachverständigen herzlich für die eingegangenen Stellungnahmen. Diese sind an alle Ausschussmitglieder verteilt worden und werden auch dem Protokoll unserer heutigen Sitzung beigefügt. Ich gehe davon aus, dass Ihr Einverständnis zur Durchführung der öffentlichen Anhörung auch die Aufnahme der Stellungnahmen in eine Gesamtdrucksache umfasst. Von der heutigen Anhörung wird ein Wortprotokoll erstellt und Ihnen zur Korrektur übersandt. Im Anschreiben werden Ihnen die Details zur Behandlung mitgeteilt. Die Gesamtdrucksache, bestehend aus Protokoll und schriftlichen Stellungnahmen, wird im Übrigen auch ins Internet eingestellt. Für die Anhörung ist die Zeit von 14 bis 16 Uhr vorgesehen. Da wir um 14:05 Uhr begonnen haben, setze ich Ihr Einverständnis voraus, dass wir diese fünf Minuten natürlich entsprechend draufschlagen können. Und meiner Ankündigung gemäß ist der Kollege Höferlin nach Abwicklung all dieser organisatorischen Hinweise auch eingetroffen und wir können mit der Anhörung beginnen.

Einleitend möchte ich den Sachverständigen die Gelegenheit geben, in einer kurzen Einleitung, die drei Minuten nicht überschreiten sollte, zum Beratungsgegenstand Stellung zu beziehen. Ich bitte Sie ausdrücklich, sich angesichts der Vielzahl von Sachverständigen an dieses Zeitfenster zu halten, damit ausreichend Zeit für Fragen durch die Abgeordneten besteht. Ihre umfassenden schriftlichen Stellungnahmen sind den Ausschussmitgliedern zugegangen und auch bekannt. Nach den Eingangsstatements werden wir orientiert an Fraktionsrunden mit der Befragung der Sachverständigen beginnen. Ich bitte, dass die Fragesteller diejenigen Sachverständigen ausdrücklich benennen, an die Sie Ihre Fragen richten wollen. Für alle noch einmal, zu den Frageregeln gilt: In der ersten Fraktionsrunde kann jeder Fragesteller entweder zwei Fragen an einen Sachverständigen oder eine Sachverständige stellen oder je eine Frage an zwei Sachverständige. Für die Fragen gilt eine Zeitbegrenzung von zwei Minuten. Die Auskunftsperson

antwortet unmittelbar auf die Frage. Für die Antwort auf jede Frage stehen ebenfalls zwei Minuten zur Verfügung. In der zweiten Fraktionsrunde werde ich angesichts der fortgeschrittenen Zeit situativ entscheiden, ob das Zeitfenster weiterhin zwei oder nur noch eine Frage pro Fraktion zulässt. Wenn Sie damit einverstanden sind, werden wir so verfahren. Dann werden wir jetzt entsprechend der alphabetischen Reihenfolge die Sachverständigen aufrufen, ich darf Herrn Dr. Atzpodien um seine Eingangsstellungnahme bitten.

SV **Dr. Hans Christoph Atzpodien** (BDSV, Berlin): Vielen Dank Frau Vorsitzende, meine Damen und Herren Abgeordneten, ich vertrete den Bundesverband der deutschen Sicherheits- und Verteidigungsindustrie, zu dem die Firma Palantir seit Ende letzten Jahres nicht mehr gehört, sie ist ausgetreten aus Gründen, die wir nicht im Einzelnen kennen und insofern vertrete ich diejenigen Unternehmen, die sich sozusagen als Wettbewerber von Palantir hier um eine Lösung, wie wir sie heute diskutieren, sehen. Da gibt es zum einen das sogenannte NaSA-Konsortium, das steht für „Nationale Souveräne Analyseplattform“ mit den Häusern SecoNet, Plath Innosystec, Conet und Rola. Und dann gibt es ein zweites Angebot unter dem Kurztitel RAP – Aufbau einer „Recherche- und Analyseplattform für die Polizei“ und der Leitung von Evident mit verschiedenen Mittelständlern und einen Dritten, der mir ausdrücklich gesagt hat, dass er nicht genannt werden möchte, weil er sich noch sozusagen in der Reserve hält. Warum eine deutsche Lösung, ganz kurz noch mal, auch unter Bezug auf das von mir eingereichte Stellungnahmepapier? Ich möchte vor allem verweisen auf das Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie von 12. Februar 2020. Dort werden Krypto und KI ausdrücklich als nationale Schlüsseltechnologien bezeichnet, die man nach Artikel 346 des Vertrages über die Arbeitsweise der Europäischen Union national beschaffen will. Wenn man das postuliert hat, dann wäre unsere Position, das bitte auch zu tun. Dem gegenüber erscheint aus der Sicht meiner Mitgliedsfirmen die Palantir Software „Gotham“ oder „Gotham“ weniger verfügbar und Plug & Play-Ready, als sie immer beworben wird. Im Übrigen sind wir der Meinung, es sollte das Ziel sein, dass man auch auf Bundesebene nicht von einem einzigen Monopolisten abhängig ist, der im Übrigen auch noch ein und US-Unternehmen ist. Ich erinnere daran, wir haben ein Präsidentschaftswahlkampf vor uns und da könnte ein Mensch gewinnen, der im Krisenfall „America First“ sagt. Eine nationale Lösung würde unseres Erachtens, aus der Sicht unserer Mitgliedsunternehmen, mehr Flexibilität bieten. Auch mit Blick auf ein übergreifendes System in Kontext des militärischen, wie auch des zivilen Nachrichtenwesens und des Sicherheitseinsatzes. Und im Übrigen glauben wir, dass wir auch mit den genannten Gruppierungen hinreichend nah an einer Lösung sind, in einem Fall mit erklärtermaßen noch geringem Entwicklungsaufwand, der nötig ist und vergleichsweise auch geringen Kosten. Im anderen Fall schon mit einer militärischen Lösung und einem Prototypen für den polizeilichen Einsatz, also nah an sozusagen einer Praxislösung. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Herzlichen Dank auch für die Einhaltung der Zeit. Frau Susanne Dehmel hat das Wort.

SV **Susanne Dehmel** (Bitkom, Berlin): Vielen Dank für die Möglichkeit zur Stellungnahme für den Bitkom. Da Verschiedene unserer über 2 000 Mitgliedsunternehmen auch im Bereich Sicherheit und Software grundsätzlich für die Beschaffung solcher Software in Frage kommen, nehmen wir generell keine Stellung zu einzelnen Angeboten, wohl aber an dieser Stelle zu den abzuwägenden Faktoren. Übergeordnetes Ziel muss die Automatisierung von Verwaltungsauswertungsprozessen sein, die eine schnelle und medienbruchfreie Übermittlung von Daten innerhalb der Bundesländer, bundesländerübergreifend, aber auch zwischen Bundesländern und Bund ermöglicht. Daher ist es grundsätzlich schon sinnvoll und wünschenswert, dass sich Länder und Bund auf gemeinsame Standards und die Beschaffung entsprechender Lösungen verständigen, die genau das ermöglichen. Zurzeit sehen wir, dass die Sicherheitsbehörden zu solchem Austausch nur eingeschränkt in der Lage sind. Allein die Auswertung von Verdachtsfällen im Bereich Geldwäsche

ist durch die Masse der Daten schwierig, sodass die Verfolgung nur rudimentär folgen kann. Handlungsoptionen für die Beschaffung solcher IT-Auswertungstools sind im Wesentlichen die eigene Entwicklung, die Entwicklung mit Partnern, entweder im Wege der Auftragsvergabe oder der Kooperation oder die Beschaffung bestehender Lösungen am Markt. Alle Optionen haben ihre Vor- und Nachteile und sie müssen unter Betrachtung einmal der kurzfristigen, aber auch der mittel- und langfristigen Bedarfe und der entstehenden Risiken und Chancen abgewogen werden. Die Erstellung eigener Lösungen kann dauerhaft erhebliche Personal-, Material- und finanzielle Ressourcen binden und unter Umständen deutlich teurer als die Beschaffung marktverfügbarer Lösungen sein, ohne unbedingt in Sachen Erprobungen/Updates deswegen wettbewerbsfähig sein zu müssen. Gleichzeitig wird die Beschaffung von bestehenden Lösungen in der Regel schneller und zeitsparender sein, kann aber unter Umständen Kosten und Verfügbarkeit auf Dauer nicht unbedingt garantieren bzw. ist schwerer zu planen möglicherweise. Die Erstellung von Softwarelösungen im behördlichen Auftrag kann nur dann gelingen, wenn ausreichend Haushaltsmittel und notwendige Ressourcen bei den für die Projekte jeweils zuständigen Behörden da sind. Speziell im sicherheitspolitischen Bereich muss eine besonders kritische Risikoabwägung stattfinden. Eine vollständige Neuentwicklung von bereits am Markt befindlichen Lösungen kann zwar sehr kosten- und zeitintensiv sein, kann aber auch einen Mehrwert haben, wenn es um Kernkomponenten der nationalen Sicherheit geht. Denn digitale Souveränität bedeutet auch eigene Fähigkeiten eben in den bereits erwähnten Schlüsseltechnologien und dort über die entsprechenden Fähigkeiten zu verfügen. Es muss deswegen auch ein Anbieter-Ökosystem in Deutschland zu solchen Schlüsseltechnologien geben. Das kann es nur geben, wenn es auch dauerhaft durch den Staat als Ankerkunden mit gefördert wird. Danke.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Wir machen weiter mit Prof. Kelber.

SV **Prof. Ulrich Kelber** (BfDI): Sehr geehrte Frau Vorsitzende, meine Damen und Herren Abgeordnete, vielen Dank für die Möglichkeit, Stellung zu nehmen. Komplexe Auswerte- und Analysesysteme werben mit dem Versprechen, dem zu prüfenden Versprechen, sofort Abhilfe schaffen zu können. Sie greifen aber eben auch sehr intensiv in Grundrechte von Bürgerinnen und Bürgern ein und deswegen bedarf es einer speziellen rechtlichen Grundlage, um sie zum Einsatz zu bringen. Ein solches Gesetz liegt aktuell weder für das Bundeskriminalamt noch für die Bundespolizei vor. Die Software VeRA aus Bayern könnte deswegen – aktuelle Rechtslage – nicht zum Einsatz kommen, sondern eine solche Rechtsgrundlage müsste geschaffen werden. Das Bundesverfassungsgericht hat Anfang des letzten Jahres klargestellt, dass komplexe Auswertung und Analysen nicht grundsätzlich unzulässig sind, sondern es hat dem Gesetzgeber einen Werkzeugkasten zur Verfügung gestellt, um solche gesetzlichen Grundlagen schaffen zu können. Das schließt aber immer ein, dass diese Werkzeuge an Bedingungen gebunden sind. Kurzfassung: Umso intensiver eine Technologie, eine Technik in Grundrechte eingreift, desto klarer muss der Gesetzgeber selbst die Voraussetzungen und Schwellen festlegen und darf dies nicht auf die Anwendungsebene übertragen. Die Frage für die Verhältnismäßigkeit ist natürlich die Prüfung, ob ein polizeifachlicher Bedarf für die Analysen vorliegt. Insbesondere die Analyse- und Auswertungsmöglichkeiten, um Zusammenhänge zwischen Tat-Tat- und Tat-Täter-Beziehungen zu erstellen. In den polizeilichen Datenbanken, die grundsätzlich jetzt diejenigen wären, die zusammen verbunden würden, sind keineswegs nur Straftäter*innen und Verdächtige gespeichert, sondern auch Daten von Bürgerinnen und Bürgern, die nie einen Tatverdacht ausgesetzt worden sind, als Zeuginnen und Zeugen, Erstatter*innen von Anzeigen, Geschädigte, Opfer eines Sexualdeliktes. Solche Systeme sorgen ja erstmal für Musterbeziehungen und sind nicht in dieser Unterscheidung, wie sonst in Vorgangssystemen, einzuteilen. Das heißt, diese Festlegung, welche personenbezogenen Daten überhaupt auswertefähig sein müssen, muss auch am Anfang solcher Überlegungen stehen. Im Projekt Polizei 20 ist ein umfangreicher Bereich vorgesehen für die Auswertung und Analyse

solcher Daten, die dann im gemeinsamen Datenhaus zur Verfügung stehen. Die entscheidende technische Stärke von VeRA, sehr unterschiedliche heterogene Systeme zusammenzufassen, auch enthaltene heterogene Inhalte, wäre dann in dieser Form nicht mehr notwendig. Von daher: Die gründliche Prüfung, ob im Vorgriff auf P20 und ergänzend zu dem, was dort möglich ist, mit einem Drittsystem so etwas zu tun, müsste am Anfang der Überlegungen stehen und nicht schon die Voraussetzung sein. Aus Gründen der digitalen Souveränität wäre eine Eigenentwicklung vorzuziehen.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Wir wechseln auf die andere Seite zu Herrn Prof. Dr. Markus Löffelmann.

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin): Sehr geehrte Frau Vorsitzende, meine Damen und Herren Abgeordneten, vielen Dank für die Einladung. Dass eine moderne Polizei über moderne Formen der Datenverarbeitung und -analyse verfügen können muss, ist, denke ich, eine Selbstverständlichkeit, über die auch hier weitgehend Einigkeit herrscht. Darüber hinaus gibt es einen breiten Konsens, dass solche Systeme auch bund- und länderübergreifend vereinheitlicht sein sollten. Das war Gegenstand der Saarbrückener Agenda und auch das Projekts Polizei 2020. Aus einer juristischen Perspektive, und allein dazu kann ich beitragen, ist freilich die rechtliche Ausgestaltung – Herr Kelber hat es auch gerade schon angesprochen – solcher Systeme von ganz entscheidender Bedeutung. Und auch darüber gab es im Ansatz in der Vergangenheit keinen Dissens. Ich möchte gerne die Gelegenheit nutzen, aus dem Whitepaper des BMI von 2017, Seite 24, zu zitieren. Da heißt es: „Die technische Realisierung der gesetzlichen Datenschutzbestimmungen, wie sie sich aus dem neuen BKAG ergeben, ist Vorgabe für die Modernisierung der Informationssysteme der deutschen Polizeien. Der Grundsatz der hypothetischen Datenneuerhebung ist als zentrales Element des Urteils des Bundesverfassungsgerichts effektiv und effizient in der zu entwickelnden IT-Architektur Polizei 2020 umzusetzen.“ Nun hat das Bundesverfassungsgericht in den vergangenen Jahren seine Rechtsprechung zu Datenverarbeitungen sehr stark weiterentwickelt und den Gesetzgeber dabei immer wieder aufgefordert, eigenverantwortlich präzise Entscheidungen zu treffen. In seiner Entscheidung zur automatisierten Datenverarbeitung vom vergangenen Jahr hat es zahlreiche Gesichtspunkte aufgezeigt, die der Gesetzgeber dabei zu beachten hat, ohne aber ein konkretes Regelungsmodell vorzugeben. Und das, glaube ich, stellt den Gesetzgeber vor eine große Herausforderung. Wenn wir uns nun die existierenden Rechtsgrundlagen ansehen, die es in einigen Ländern gibt, sehen wir ein ganz heterogenes Bild: In Nordrhein-Westfalen eine Regelung gegen die schon eine Verfassungsbeschwerde anhängig ist, in Hessen eine neue Regelung gegen die massive Bedenken vorgebracht werden. In Bayern und in Rheinland-Pfalz gibt es aktuelle Gesetzgebungsverfahren, die die völlig disparat sind und die auch große Schwierigkeiten aufwerfen. Meines Erachtens wäre es für eine Konsolidierung des Rechtsrahmens für diese Datenanalyse notwendig, auf zwei Ebenen zu denken. Zum einen müssten Art, Umfang der zu verwendenden Daten und die zu verwendenden Methoden einheitlich festgelegt werden, denn das ist der Ausgangspunkt für alle weiteren Regelungen, und der richtige Regelungsort dafür wäre eigentlich das BKAG, wenn dem BKA eine Schlüsselrolle bei der Bereitstellung dieser Technologie zukommen soll. Und dann müssten zum anderen in den Fachgesetzen der verschiedenen Polizeien Eingriffsschwellen geregelt werden. Warum? Weil die automatisierte Datenverarbeitung zugleich eine Neuerhebung von Erkenntnissen ist und deshalb der Befugnisse bedarf. Und ich kann mir auch gut vorstellen, dass auf dieser Ebene in den Fachgesetzen ein gewisser Regelungsspielraum besteht, um Eigeninteressen der jeweiligen Polizeien zur Geltung kommen zu lassen. Ich bedanke mich.

AVors. **Petra Pau** (Die Linke): Herzlichen Dank. Das Wort hat Herr Dirk Peglow.

SV **Dirk Peglow** (BDK, Berlin): Herzlichen Dank Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, es freut mich sehr, dass ich die Gelegenheit habe, mal das Thema vielleicht ein bisschen aus Sicht der kriminalpolizeilichen Praxis zu beleuchten. Ich habe extra zwei Zitate

mitgebracht, die leider Gottes immer mehr repräsentativen Charakter gewinnen für die kriminalpolizeiliche Arbeit. Eines beginnt damit, dass eine junge Kollegin mir sagte: Ich gehe abends nach Hause und denke darüber nach, was ich heute alles nicht erkannt habe, ob ich etwas nicht veranlasst habe, was dazu geführt hätte, ein Kind aus dieser schrecklichen Situation zu befreien und dem Täter an der Fortsetzung seiner furchtbaren Taten zu hindern. Das nächste Zitat ist von einem Kollegen: Wenn ich Nachrichten schaue und dort eine Meldung zu einem Terroranschlag kommt, denke ich sofort, hoffentlich war es keiner von meinen Leuten. Ich mache mir dann Sorgen, dass ich Dinge übersehen habe, die dazu führten, dass Menschen zu Schaden gekommen sind. Zwei Zitate junger Polizeibeamter, die aus meiner Sicht sehr gut beschreiben, unter welchen Druck bereits junge Kolleginnen und Kollegen stehen. Zwei Zitate, die aber auch verdeutlichen – und das ist wirklich ein Thema – wie wichtig es ist, den Ermittlerinnen und Ermittlern die bestmöglichen Werkzeuge für ihre Arbeit zur Verfügung zu stellen, in rechtlicher und technischer Hinsicht. Erfolgreiche polizeiliche Arbeit ist immer ein Zusammenspiel mehrerer kriminalistischer Fertigkeiten und Methoden, die fallbezogen angewandt werden müssen. Die Veränderung des Kriminalitätsgeschehens, insbesondere die Verlagerung von Kriminalität aus dem analogen in den digitalen Raum – wir kennen das alle – hat leider Gottes zur Folge, dass die Analyse- und Auswertekompetenzen immer mehr zum entscheiden Faktor werden, Straftaten zu verhindern oder Gefahrenlagen zu erkennen. Vor diesem Hintergrund erachte ich die nachfolgenden Grundaussagen für die heutige Anhörung aus Sicht der polizeilichen Praxis für besonders bedeutsam. Die Notwendigkeit einer datenbankübergreifender Analyseplattform ist aus fachlicher Sicht alternativlos und muss sich anbieterunabhängig an den Bedarfen der Kolleginnen und Kollegen ausrichten, die diese Systeme im täglichen Dienst verwenden. Das Bundesverfassungsgericht, das ist eben hier schon genannt worden, hat klargestellt, dass die automatisierte Datenauswertung zur vorbeugenden Bekämpfung schwerer Straftaten zulässig ist. Das hat auch zugleich die verfassungsrechtlichen Hürden für eine Nachbesserung bestehender gesetzlicher Normen, wie auch für notwendige gesetzgebende Initiativen in den Ländern definiert. Die Vorgaben sind bei der rechtlichen und technischen Umsetzung zu beachten. In Hessen sind die notwendigen Anpassungen bereits erfolgt. Ich komme aus Hessen, deswegen weiß ich, wovon ich spreche. Digitale Souveränität bedeutet aus Sicht der polizeilichen Praxis zunächst die Hoheit über die verfügbaren polizeilichen Daten sicherzustellen und diese rechtskonform zu verarbeiten. Für meine Kolleginnen und Kollegen kann die Entwicklung von IT-Lösungen in eigener digitaler Kompetenz nicht zur Folge haben, dass die bereits in der NRW und Hessen und demnächst in Bayern im erfolgreichen Betrieb befindlichen Systeme nicht eingeführt werden, weil man auf die Implementierung souveräner Systeme unbestimmte Zeit warten muss. Wir sollten alle so ehrlich sein und feststellen, dass jedenfalls nach meiner Erfahrung, bis zum heutigen Tag keine vernünftige Alternative zu dem aktuellen Produkt vorhanden ist. Aber ich muss einschränkend sagen, dass wir natürlich uns alle freuen würden, auch aus Sicht der polizeilichen Sachbearbeitung, wenn ein digitales souveränes System irgendwann mal eingeführt wird. Es kann nur nicht zur Folge haben, dass wir das Funktionierende abschalten, bis das neue kommt. Danke schön.

AVors. **Petra Pau** (Die Linke): Danke schön. Das Wort hat Frau Simone Ruf.

SV **Simone Ruf** (GFF, Berlin): Sehr geehrte Abgeordnete, vielen Dank für die Einladung. Die Gesellschaft für Freiheitsrechte rät von der Einführung von Bundes-VeRA ab. Es gibt derzeit keine Rechtsgrundlage für BKA und Bundespolizei, auf die sich der Einsatz stützen ließe. Das heißt, eine Genehmigung durch das BMI würde nicht dazu führen, dass der Einsatz erlaubt wäre. Man müsste vielmehr zuerst eine Rechtsgrundlage dafür schaffen. Aus dem Urteil des Bundesverfassungsgerichts vom Februar 2023 ergibt sich, dass es verfassungsrechtlich grundsätzlich zulässig wäre. Man müsste dann die darin vorgezeichneten Grenzen wahren und darin aufgezeigte Anforderungen an die Rechtsgrundlage erfüllen. Wir raten dennoch davon ab, eine Rechtsgrundlage für Bundes-

VeRA zu schaffen, und zwar aus folgenden Gründen: Zunächst muss man sich klarmachen, was die Software potenziell alles kann. Es werden hier nicht nur getrennte Datenbanken zusammengeführt, sondern durch sogenanntes Data-Mining werden die Daten analysiert, um Muster zu erkennen und neue Beziehungen zu bilden. Das heißt, der Einsatz ermöglicht es, neues persönlichkeitsrelevantes Wissen aus dem vorhandenen Daten zu generieren, das sonst verborgen bliebe. Wir sprechen also nicht nur von einer Weiterverarbeitung der Daten, sondern von spezifischen Belastungseffekten, die durch Data-Mining entstehen können. Allen voran besteht die Gefahr, dass ganze Persönlichkeitsprofile erstellt werden können. Darüber hinaus haben wir es hier aber mit einer enormen Streubreite zu tun, denn aus grundrechtlicher Perspektive sind nicht nur Zielpersonen einer Analyse betroffen, sondern alle, deren Daten in die Datenanalyse einbezogen werden, was mich gleich zum nächsten Punkt bringt. Der Einsatz birgt ein hohes Risiko falscher Verdächtigungen. Warum? Bei der Polizei liegt eine Vielzahl von Daten Unbeteiligter vor. Das betrifft vor allem Funkzellenabfragen und Vorgangsdaten. Das heißt, das Risiko ist recht hoch, dass Unbeteiligte fälschlicherweise als Störer*innen oder Verdächtige von der Software identifiziert werden, und zwar vor allem dann, wenn komplexe Algorithmen der Auswertung zugrunde liegen, die nicht nachvollziehbar sind. Weiter hat der Einsatz großes Diskriminierungs- und Stigmatisierungspotenzial. Polizeilichen Datensätzen sind Diskriminierungen immanent. Die verstärken sich durch den Einsatz künstlicher Intelligenz und komplexer Analysen und werden mit steigender Komplexität weniger nachvollziehbar. Darauf hat auch das Bundesverfassungsgericht verwiesen. Es besteht also die Gefahr, dass ganze Personengruppen unter Generalverdacht gestellt und stigmatisiert werden. Der Eingriff verschärft sich dadurch, dass es sich hier um heimliche Maßnahmen handelt und damit erhebliche Rechtsschutzdefizite einhergehen. Und schließlich ist auch der Mehrwert fraglich. Auf der einen Seite haben wir offenkundig handfeste schwerwiegende Grundrechtseingriffe mit erheblicher Streubreite und auf der anderen Seite anekdotisch anmutende Erzählungen über die Effizienz der Software. In rechtlicher Hinsicht stellt sich also schon die Frage, ob eine derartige Befugnis überhaupt erforderlich ist. Jedenfalls raten wir davon ab, auf private Softwareanbieter zurückzugreifen. Das Bundesverfassungsgericht hat es zwar nicht ausgeschlossen, aber auch darauf hingewiesen, dass damit die Gefahr unbemerkter Manipulation und des unbemerkten Zugriffs auf Daten durch Dritte verbunden ist. Und auch wir sehen hier große Gefahren in Hinblick auf Datensicherheit, Intransparenz und Abhängigkeit. Gerade die Abhängigkeit wird dazu führen, dass auch die Kosten in die Höhe schießen werden, wenn ein Anbieter die Preise letztlich diktieren kann. Danke schön.

AVors. **Petra Pau** (Die Linke): Vielen Dank und wir machen weiter mit Frau Christine Skropke.

SV **Christine Skropke** (secunet, Essen): Sehr geehrte Frau Vorsitzende, meine Damen und Herren, ich danke Ihnen für die Gelegenheit, zu diesem wichtigen Thema Stellung zu nehmen. Als Mitarbeiterin der secunet möchte ich das Thema aus einer primär technologischen und industriepolitischen Sicht darstellen. Sicherheit und der Schutz der Bevölkerung sind Kernaufgaben des Staates. Es steht außer Frage, dass die dafür zuständigen Behörden mit allen verfügbaren modernen Technologien zur Unterstützung ihrer Arbeit ausgestattet werden sollten. Was sind technologische Grundvoraussetzungen, nationale hoheitliche Bereiche müssen sicherstellen, dass Daten und Informationen sowie die Kontrolle über den Zugriff stets mit der höchst verfügbaren und vertrauenswürdigen Sicherheitstechnologie vor Sabotage, Spionage und Datenmissbrauch geschützt sind. Die Software allein einmalig auf Sicherheit zu prüfen, stellt keine ausreichende Vertrauenswürdigkeitsüberprüfung dar. Ebenso unerlässlich ist die Einbettung der Software in hochsichere Cloud- und Netzwerkinfrastrukturen. Industriepolitisch betrachtet: Wir machen Forschungsförderung in Deutschland. Wir betreiben Gründungsförderung. Gleichzeitig definieren wir Strategiepapiere, wie von Herrn Dr. Atzpodien schon benannt, zu wichtigen Kompetenzen, Schlüsseltechnologien und kennzeichnen ganze Branchen als national relevant. Und Unternehmen dieser

Branchen müssen national geschützt und gefördert werden, so heißt es in den Strategiepapieren. Keine Frage, Gründungsförderung und Kapitalgeber sind wichtig, aber das Wichtigste für die Entwicklung sind Beauftragungen. Sie ermöglichen die praktische Anwendung, aber auch gemeinsame Weiterentwicklung mit den Bedarfsträgern. Die Unternehmen wachsen wirtschaftlich stabil, stellen nationale Fähigkeiten sicher und leisten wertvolle Beiträge beim Setzen neuer technologischer Standards. Technologiehoheit und ielfalt verhindern die Abhängigkeit von Drittstaaten oder einzelnen Anbietern. So kann Deutschland digital souverän werden und bleiben. Es fehlt generell an einer langfristigen Bedarfsplanung. Das Projekt Bundes-VeRA wäre prädestiniert die erwähnten nationalen Strategien in eine operative Wirtschaftspolitik umzusetzen. Daher verwunderte es, dass bei der europäischen Ausschreibung kein deutsches oder zumindest europäisches Konsortium ausgewählt wurde oder – sofern die Fähigkeiten zum Zeitpunkt der Ausschreibungserstellung noch nicht sichtbar oder verfügbar waren – die deutsche Industrie nicht frühzeitig in die Bedarfsermittlung und deren möglichen Realisierung eingebunden wurden. Als Fazit kann ich sagen, dass das Programm P20 der Reset-Button für die IT-Infrastruktur der deutschen Polizei ist. Im Sinne einer nachhaltigen nationalen Industriestrategie sollte insbesondere bei den kritischen Teilprojekten auf digital souveräne Lösungen nationaler Hersteller gesetzt werden. Die Vergabe an außereuropäische Anbieter von Einzellösungen mag kurzfristig attraktiv erscheinen, mittel- und langfristig aber ignoriert diese nicht absehbare finanzielle, technische und letztlich auch geopolitische Risiken. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Und es geht weiter mit Herrn Klaus Teufele.

SV **Klaus Teufele** (BLKA, München): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete. Mein Name ist Klaus Teufele, ich bin Polizeibeamter des Bayerischen Landeskriminalamts in München und bedanke mich sehr herzlich für die Gelegenheit, hier heute auch etwas zur Bundes-VeRA sagen zu dürfen. „Greift die Kreuzfahrer und Juden an, nehmt sie ins Visier.“ Mit diesen Worten forderte Al-Ansari, der Sprecher des islamischen Staates Provinz Khorasan, bereits unmittelbar nach dem furchtbaren menschenverachtenden Terrorangriff auf die Konzerthalle in Moskau seine Anhänger zu weiteren Angriffen/Übergriffen in Europa und den USA auf. Neben der islamistischen Bedrohung, neben dem internationalen Terrorismus, ist es aber auch die Schwerkriminalität, die organisierte Kriminalität, die die anhaltend hohe Gefährdungslage in Deutschland beeinflusst. Der rechtsextreme Angriff auf die Synagoge in Halle, der Mord an dem Kassler Regierungspräsidenten Lübke, aber auch der sexuelle Missbrauch an Kindern und die in Massen verbreiteten Inhalte dieser Missbräuche, sind Ausdruck oder Teil unserer Sicherheitslage. Ziel muss es sein, Anschläge bereits frühzeitig zu erkennen und zu verhindern. Ziel muss es sein, Kinder aus diesem Missbrauch herauszuholen und weitere Missbräuche zu verhindern. Dafür braucht die Polizei aber das notwendige Werkzeug. Daten, polizeiliche Daten, sind ein wesentlicher Mehrwert, mit dem wir hier arbeiten, um Tat-Täter-Zusammenhänge erkennen zu können, mögliche Anschlagsziele identifizieren oder die Täter identifizieren zu können. Die Daten, die die Polizei derzeit hat, liegen historisch bedingt, aber in sehr unterschiedlichen Datenformaten, in sehr unterschiedlichen Fachverfahren, sehr breit gestreut, zur Verfügung. Eine Abfrage, eine Recherche, eine Informationsgewinnung, was weiß denn die Polizei überhaupt, bedeutet heute, dass diese Daten manuell abgeglichen werden müssen, recherchiert, bewertet und die Zusammenhänge manuell zusammengetragen werden müssen, mit der Frage, ob sie überhaupt erkannt werden. Das erfordert nicht nur viel Personal, sondern auch viel Zeit. Zeit, die nicht zur Verfügung steht. Diese Gefährdungslagen können sich jederzeit konkretisieren. Die Bayrische Polizei hat sich deshalb im Jahr 2021 bereits dazu entschlossen, eine verfahrensübergreifende Recherche- und Analyseplattform einzuführen. Mit diesem Bedarf stehen wir aber nicht alleine. In Nordrhein-Westfalen und Hessen gibt es diese Systeme bereits und alle anderen Bundesländer haben polizeilicherseits bereits erklärt, dass dieser Bedarf besteht. Damit war es für uns auch nicht verwunderlich, dass wir von

Seiten des Zentralprogramms des BMIs auch die Bitte bekommen haben, unsere Ausschreibung insoweit zu öffnen, dass auch die Beschaffung einer Bundes-VeRA möglich wird. Das haben wir gemacht. Wichtigster Gesichtspunkt war dabei unter anderem die Gefährdungslage, ist sie heute, ist sie jetzt. Wir haben keine Zeit, wir müssen reagieren. Und damit war wichtigster Punkt ein bestimmtes System, eine leistungsstarke Software, die im Einsatz bereits erprobt ist. Das war gemeinsames Verständnis des Zentralprogramms und der Bayerischen Polizei. Wir haben eine europaweite Ausschreibung durchgeführt. Von 13 Firmen, die Interesse gezeigt haben, haben wir drei zur Abgabe eines Angebots aufgefordert und letztlich das Angebot der Firma Palantir bezuschlagt. Als leistungsstärkstes und wirtschaftliches Angebot bezuschlagt. Heute sind wir der Überzeugung, dass es die richtige Entscheidung war. Ich kann Sie nur bitten, auch auf Bundesebene die Voraussetzungen für den Einsatz der Bundes-VeRA zu schaffen. Als Polizeibeamter bin ich überzeugt, wir brauchen dieses Werkzeug und wir brauchen es zeitnah. Danke.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Herr Dr. Roland Wagner hat das Wort.

SV **Dr. Roland Wagner** (HMdI, Wiesbaden): Vielen Dank Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, wenn wir uns die Frage stellen, wofür steht die Polizei, dann ist die Antwort simplifiziert. Effektive Gefahrenabwehr und konsequente Strafverfolgung, wobei idealerweise, da sind wir uns einig, mehr Gefahren abgewehrt werden, als später Straftäter verfolgt werden müssen. Und die Gefahrenlage ist, um die Worte der Bundesinnenministerin nach den Anschlägen in Moskau zu zitieren, akut. Wir haben in unserer Gesellschaft im Moment sehr viel Nährboden für Gefahrenlagen, die Zahl der Straftaten steigt, wir haben den Ukrainekrieg, genauso wie den Nahostkonflikt und zudem eine steigende Radikalisierungsbereitschaft. Auftrag der Polizei ist es, die Bürgerinnen und Bürger zu schützen, Gefahren von ihnen abzuwenden und ein Leben in Sicherheit zu ermöglichen. Erfolgskritische Faktoren für eine effektive Gefahrenabwehr wiederum sind, erstens ein professioneller Umgang mit großen Datenmengen und zweitens Geschwindigkeit beim Erkennen von kriminellen Netzwerken oder einfacher, Herr Teufele hat es gerade ebenfalls gesagt, Zeit. Als Beispiel für den Umfang mit Datenmengen kann ich Ihnen unsere BAO-Fokus, das ist die besondere Aufbauorganisation zur Bekämpfung des sexuellen Missbrauchs, ein paar Zahlen nennen, 83 000 Asservate wurden in drei Jahren gesammelt. 21 200 Asservate allein in 2023. Wir haben aktuell 8 700 aktive Fälle und einer hat im Schnitt 3,2 Terabyte, pro Fall. Das können Sie händisch auf gar keinen Fall mehr auswerten oder analysieren, geschweige dann relevante Verknüpfungen zu anderen Tätern herstellen. Wir aber wollen die Netzwerke identifizieren und bekämpfen. Der zweite kritische Faktor ist die Zeit. Laufender Missbrauch oder Terrorabwehr duldet keine Minute Verzögerung, da sind wir uns glaube ich alle einig. Auch die Kollegen Peglow und Teufele haben es gerade gesagt. Den Unterschied dabei machen aber oft wenige Stunden. Daher brauchen wir Werkzeuge, die es uns jetzt und nicht morgen oder übermorgen, sondern *jetzt* ermöglichen, die vorhandenen Daten schnell, sicher und umfassend zu analysieren. Und es muss uns gelingen, die richtigen Schlüsse daraus zu ziehen, um Weiteres zu verhindern. Darin sind sich übrigens alle Polizeien des Bundes und der Länder fachlich einig. Nach meiner Auffassung haben wir ein solches Werkzeug mit der Analyseplattform Hessen Data oder eben der Bundes-VeRA, denn es ist eine schnelle Analyse bereits vorhandener und rechtmäßig erhobener polizeilicher Daten möglich. Das ist rechtlich zulässig. Das hat das Bundesverfassungsgericht entschieden und der hessische Gesetzgeber hat eine an der Entscheidung ausgerichtete Norm getroffen. Durch Fraunhofer SIT wurde moderner Datenschutz und IT-Sicherheit geprüft und – wichtig – es gibt gegenwärtig keine Alternative und sie ist ehrlich gesagt auch nicht in Sicht. Denn digitale Souveränität darf an dieser Stelle nicht falsch verstanden werden. Ich bin sehr für deutsche und europäische Produkte, wenn sie verfügbar sind und den gleichen Nutzen bringen. Das ist Teil der Digitalstrategie der Polizei in Hessen, die ich maßgeblich verantworte. Das Streben nach digitaler Souveränität darf aber nicht dazu führen, dass wir Gefahren für die Bürgerinnen und Bürger

zulassen, die wir anders verhindern können. Der Einsatz wäre, bei allem Streben nach digitaler Souveränität, zu hoch. Daher, die Sicherheit der Bürgerinnen und Bürger duldet keinen Aufschub und kein Zuwarten, weshalb ich mich sehr für die Ausstattung aller Polizeien des Bundes und der Länder mit der Analyseplattform VeRA ausspreche, um die Handlungsfähigkeit der Strafverfolgungsbehörden zu sichern. Vielen Dank!

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Ich erinnere an unsere Frageregeln. In der ersten Runde kann jeder Fragesteller entweder zwei Fragen an einen Sachverständigen oder je eine Frage an zwei Sachverständige richten. Für die Fragen gilt eine Zeitbegrenzung von zwei Minuten und die Auskunftspersonen antworten jeweils unmittelbar auf die Frage. Auch hier stehen ebenfalls zwei Minuten zur Verfügung. Herr Kollege Hartmann, bitte.

Abg. **Sebastian Hartmann** (SPD): Frau Vorsitzende, herzlichen Dank für die Möglichkeit. Zunächst mal an die Sachverständigen, herzlichen Dank für die wirklich umfänglichen Stellungnahmen, die auch aufzeigen, wie groß eigentlich die Spannbreite zwischen Datenschutz, Rechtsgrundlagen und sofortigem Handeln, also dem Vollzug, ohne jedes Zögern, deutlich machen. Deswegen erlaube ich mir den Hinweis, dass wir das als Gesetzgeber sehr ernst nehmen und gerade auch als Koalition hier vor allem in den Punkt der Rechtsgrundlagen sind. Also deswegen auch nochmal danke an den Bundesdatenschutzbeauftragten und Herrn Professor Dr. Löffelmann, an den die Frage auch gleich gehen wird. Also ohne Rechtsgrundlage wird das nicht gehen. Die Verhinderung der Tat und am Ende auch die Verfolgung und wirklich auch Aburteilung ist sehr entscheidend, darum das vorweg geschoben. Und die Kollegen von der Union, sich so einseitig vor ein amerikanisches Unternehmen spannen zu lassen, ist ein Widerspruch zur deutschen digitalen Souveränität. Und darum geht die zweite Frage auch gleich an Frau Skropke, denn es ist ja so, als ob es auf dem ganzen globalen Markt offensichtlich nur ein US-amerikanisches Unternehmen nach Ihrer Lesart gibt. Und wenn ich nach den Berichten in Bayern schaue, wird sogar die Rechtsgrundlage, auf denen das angewandt wird, der Testbetrieb, in Frage gestellt. Also ganz so einfach ist die Sachlage nicht. Deswegen geht die erste Frage an Frau Skropke. Sie sind Vertreterin eines namhaften Unternehmens, das anstelle vieler – wir haben das bei Bitkom gehört – heute hier anwesend ist. Wenn Sie die digitale Souveränität, auch ihre Leistungen beurteilen, Sie sind hier nicht in der Werbeshow, haben Sie auch in der Stellungnahme deutlich gesagt, Sie waren bislang nicht befasst damit. Nach unserem Kenntnisstand gibt es zwei oder drei Strukturen oder Konsortien, die sich eine solche eigenständige Lösung vorstellen könnten. Können Sie das bitte mal in einen zeitlichen Bezug stellen? Was wäre daran zu tun? Was wäre aber auch anzupassen bei amerikanischen Lösungen? Was wäre anzupassen, um überhaupt in einen Betrieb zu kommen? Sonst entsteht ja der Eindruck, als ob heute etwas verfügbar ist, was sofort per Knopfdruck da ist. Bayern investiert seit Jahren fünf Millionen Lizenzgebühren, um es nicht anwenden zu können. Und die zweite Frage an Herrn Professor Dr. Löffelmann. Sie haben in Ihrem Sachverständigenschreiben noch mal deutlich gesagt, welche Mindestanforderungen muss eigentlich ein Gesetzgeber, und da würde ich differenzieren zwischen dem Bundes- und den Landesgesetzgebern, eigentlich erfüllen? Und welche Streitpunkte sind jetzt schon gegeben bei den vorhandenen Rechtsgrundlagen und der guten Ordnung, teilweise angemerkt, vier Länder wollen die Palantir-Lösung in Deutschland nicht und die stolze Republik Frankreich verzichtet komplett auf Palantir und setzt auf eigenständige nationale Regelungen, gerade deswegen.

AVors. **Petra Pau** (Die Linke): Danke, wir beginnen mit Frau Skropke.

SV **Christine Skropke** (secunet, Essen): Ja, vielen Dank. Souveräne Lösungen haben wir verfügbar in Deutschland, Wir haben die Möglichkeit, Konsortien zu bilden. Es gibt schon seit einem Jahr einen Zusammenschluss von Unternehmen, die sich dort darauf verständigt haben, eine Lösung bauen zu können. Es bedarf einer Anschubfinanzierung, wenn ich das so konkret direkt sagen darf. Es sind deutsche Unternehmen, die alle sicherheitsüberprüft sind, die alle in Sicherheitsumgebungen für

Bund oder Länder tätig sind mit den verschiedenen Disziplinen, die so etwas in sechs bis zwölf Monaten aufbauen könnten. Dazu würde ich gerne noch betonen, dass wir eine außerordentliche KI-Forschung in Deutschland haben, auf die wir sehr stolz sind und ich glaube, dass man hier auch sehr wohl in Start-Ups mal reinschauen könnte, die hier solche Dinge auch aufbauen können. Was die digitale Souveränität angeht, glaube ich, muss man auch immer darauf schauen, mit welchem Bibliotheken und Datenbanken KI-Systeme eigentlich arbeiten. Ich glaube, das ist sehr wichtig, dass die genau angesehen werden. Hier gab es auch vorher schon Stellungnahmen dazu. Wie ist das mit der Gleichbehandlung und auch vor allen Dingen der Anonymisierung und Pseudonymisierung der Daten? Das ist ganz erheblich. Also in Deutschland haben wir Unternehmen, die das leisten können. Die Einbindung von amerikanischen Unternehmen kann erfolgen, wenn es gesicherte Schnittstellen gibt. Aber man muss immer berücksichtigen, dass es immer noch in Amerika die Möglichkeit gibt, dass ein Präsident sagt, wir greifen jetzt auf alle Daten zu. Ich glaube, hier darf man nicht unterschätzen, was also der Rückfluss an Daten auf amerikanische Systeme ermöglicht oder ermöglichen könnte, wenn in Amerika die Gesetze geändert würden. Danke.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Herr Professor Löffelmann.

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin)**:** Ja vielen Dank für diese sehr komplexe Frage. Das Bundesverfassungsgericht, das ist eine zentrale Aussage dieses Judikats von 2023, hat deutlich gemacht, dass automatisierte Datenanalysen eine sehr große Anwendungsbreite haben, sehr unterschiedliche Eingriffsintensitäten hervorrufen können. Das hängt davon ab, welcher Art die Daten sind, die verarbeitet werden, welchen Umfang das hat und welche Analysemethoden verwendet werden. Dem muss man, und das ist eigentlich der zentrale Punkt, nun Eingriffsschwellen gegenüberstellen. Man braucht also ein Stufensystem von Eingriffsschwellen und dieses Stufensystem ist ganz eng und unmittelbar mit dem verknüpft, was eine solche Maßnahme kann und darf, mit der Funktionalität dieser Maßnahme. Ich habe mal versucht ein solches Stufensystem zu visualisieren. Ich weiß nicht, ob das hier erkennbar ist. Ja, was man machen könnte und was vielleicht unverzichtbar ist, aber in den gegenwärtigen Rechtsgrundlagen überhaupt nicht auftaucht, ist, dass man die zu verarbeitenden Daten zunächst einmal kategorisiert. Hier kann man fünf Kategorien sehen. Da gibt es nichtpersonenbezogene Daten. Die kann man praktisch für alles verwenden. Es gibt Daten, die sind gesperrt, weil sie aus einer eingriffsintensiven Maßnahme stammen, wie Wohnraumüberwachung, Online-Durchsuchung, und dazwischen muss man eben je nach Herkunft der Daten, ihrer intrinsischen Sensibilität oder dem Verantwortungsprinzip, die Daten einer Kategorie zuordnen. Das könnte/sollte man in einem BKAG machen. In den Fachgesetzen der Länder und des Bundes müssten Eingriffsschwellen definiert werden. Und dann sieht man hier, würden bestimmte Datentöpfe durch bestimmte Eingriffsschwellen abgedeckt werden. Das Besondere an einem solchen Stufenkonzept wäre nun, dass die ordinale Stufe der Eingriffsschwelle immer eins höher liegt als die Schutzwürdigkeit der Daten. Denn man muss auch die eigenständige Eingriffsintensität der automatisierten Analyse abwägen. In aller Kürze, ich glaube, so ein Konzept ist dringend erforderlich, aber ich kann im gegenwärtigen Recht nirgendwo auch nur Ansätze für ein Konzept erkennen.

AVors. **Petra Pau** (Die Linke): Eine Bitte, Herr Professor Löffelmann, können Sie uns diese Visualisierung im Nachgang mit zur Verfügung stellen? Dann würde sie Bestandteil des Protokolls (*vgl. Grafik: „Stufenkonzept automatisierte Datenanalyse“ in der schriftlichen Stellungnahme von Prof Dr. Markus Löffelmann).*

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin)**:** Selbstverständlich, das mache ich gerne.

AVors. **Petra Pau** (Die Linke): Herzlichen Dank. Dann kommen wir zur CDU/CSU-Fraktion. Das Wort hat der Kollege Dr. Heck.

Abg. **Dr. Stefan Heck** (CDU/CSU): Ja, auch von unserer Seite herzlichen Dank an alle Sachverständigen für Ihre Ausführungen. Uns geht es nicht darum, irgendein Unternehmen zu bevorzugen. Uns

geht es um die Sicherheit der Bürgerinnen und Bürger. Wir haben zur Kenntnis zu nehmen, dass es eine Ausschreibung gegeben hat, federführend von der Bayerischen Polizei. Deswegen meine erste Bitte an Herrn Teufele: Könnten Sie nochmal die Rahmenbedingungen dieser Ausschreibung darlegen? Wie war insbesondere der Bund daran beteiligt? Wie war der Weg dorthin? Und können Sie sich eigentlich erklären, warum sich der Bund dann offenbar entgegen den fachlichen Boten, insbesondere des BKA, entschieden hat, die dann erfolgte Ausschreibung nicht weiter zu verfolgen und das Produkt nicht abzurufen? Das ist meine erste Frage. Die zweite Frage geht an Herrn Dr. Wagner. Sie haben ja sehr eindrucksvoll dargelegt, wie zeitkritisch viele polizeilichen Ermittlungen sind. Haben Sie Kenntnis darüber, wie lange es dauern würde, eine eigene Entwicklung im Rahmen des Programms P20 vorzunehmen? Wie weit sind wir da? Wie viel Zeit würde noch vergehen, bis die wirklich so weit wäre, dass sie von der Polizei auch eingesetzt werden kann?

AVors. **Petra Pau** (Die Linke): Herr Teufele, Sie haben das Wort.

SV **Klaus Teufele** (BLKA, München): Vielen Dank. Damit zu der ersten Frage. Rahmenbedingungen. Ausgehend vom fachlichen Bedarf haben wir hier natürlich aufgrund der zu erwartenden Kostengröße eine europäische Ausschreibung durchgeführt, die auf Basis von Leistungsbeschreibungen, Eignungskriterien etc. durchgeführt wurde. An der Erstellung der Leistungsbeschreibung, an der Festlegung der Eignungskriterien, war bereits das Zentralprogramm, war das BMI, beteiligt. Das heißt, wir haben diese Kriterien gemeinsam festgelegt. Genauso, wie wir gemeinsam festgelegt haben, dass aufgrund des akuten Handlungsbedarfs auch eine Software benötigt wird, die jetzt in den Einsatz gebracht werden kann, die wir jetzt brauchen. Die Ausschreibung selbst wurde auch gemeinsam durchgeführt in einer gemeinsamen Bewertungskommission. Das heißt, wir haben das nicht allein getan, sondern haben das auch gemeinsam mit dem Zentralprogramm gemacht und sind hinterher auch zur gemeinsamen Entscheidung gekommen, dass das Produkt der Firma Palentir zu bezuschlagen ist. Vom Rahmenkonstrukt sah die Ausschreibung vor, dass die Bayerische Polizei unmittelbar abrufen kann, dass andere Bundesländer auch unmittelbar abrufen können, dass aber hier auch der Bund für uns alle gemeinsam, für alle Bundesländer gemeinsam, Bundes-VeRA abrufen kann. Was wiederum für alle Beteiligten nicht bedeutet, dass es jeder sofort einsetzen muss, sondern schlicht und einfach einsetzen kann. Aber das noch zu einem deutlich günstigeren Preis, weil nur eine Installation damit benötigt werden würde. Waren wir überrascht? Natürlich waren wir überrascht. Die Leistungsbeschreibung hat das Produkt hervorgebracht, dass alle Kriterien erfüllt. Es war das wirtschaftlichste Angebot. Für uns äußerst überraschend, dass am Ende der Bund VeRA nicht abgerufen hat.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Herr Dr. Wagner, Sie haben das Wort.

SV **Dr. Roland Wagner** (HMdI, Wiesbaden)**:** Vielen Dank Frau Vorsitzende, vielen Dank Herr Abgeordneter für die Frage. Ich würde gerne eine allgemeine Antwort vorweg mal als Frage formulieren. Weil ich mir nämlich gar nicht sicher bin, ob überhaupt eine eigene Entwicklung im Moment möglich ist. Denn wir haben drei Vergabeverfahren gehabt, was Analyseplattformen angeht. Hessen als erstes, Nordrhein-Westfalen als zweites und Bayern, wie gerade von Herrn Teufele umfassend dargestellt, dann für das Programm 2020 und der Vertrag läuft ja noch. Vor dem Hintergrund, wenn wir eine identische Analyseplattform ausschreiben würden, wäre es zumindest nach meinem Verständnis nicht ganz vergaberechtskonform. Denn der Rahmenvertrag läuft fünf Jahre, ist 2022 bezuschlagt worden und hat dann – meine ich – noch mal eine Abrufoption auf vier Mal ein Jahr. Vor dem Hintergrund wäre das schon allein die Frage, was zu einer zeitlichen Verzögerung in meinen Augen führen würde. Denn ich gehe davon aus, dass man sich auf jeden Fall juristisch wehren würde gegen so etwas. Aber es geht meiner Meinung nach noch viel weiter, denn die Verfügbarkeit ist ja gerade auch in Zeiten sich anspannender Haushaltslagen eine Kostenfrage. Auch das hat Herr Teufele gerade angeschnitten. Würde ein zentraler Abruf erfolgen, wäre es, was die Implementierung und die Basisdaten angeht,

deutlich günstiger für die Länder. Insofern auch eine Kostenfrage und damit bestimmt auch eine Beschleunigung. Und dann kommt natürlich noch mehr hinzu. Wenn man keine fertige Software hat, muss man sie entwickeln. Ganz klar, unabhängig davon, ich habe keinen Kenntnisstand, wie weit die einzelnen Konsortien sind. Teilweise wollten die ja noch anonym bleiben. Neben diesen Entwicklungen kommen dann natürlich die Implementierungskosten hinzu, die, wenn sie nicht aus dem Programm 2020 sind, externen Sachverstand mit polizeilichen übereinander bringen müssen. Das ist mit Sicherheit nicht ganz einfach. Und dann natürlich solche Dinge wie Schulungen und Abstimmungsbedarfe in den Ländern, die jenseits des Programms, wie gesagt, wenn Sie einen Externen mit dazu nehmen, wird es immer etwas aufwendiger. Nochmal, nicht falsch verstehen. Ich bin für eine Eigenentwicklung, aber für den Einsatz einer Eigenentwicklung aber dann, wenn es das gleiche kann und die Bürgerinnen und Bürger gleich gut schützt und vor dem Hintergrund gilt das, was ich vorhin gesagt habe. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Danke. Für die Fraktion BÜNDNIS 90/DIE GRÜNEN hat der Kollege Dr. von Notz das Wort.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Frau Vorsitzende, meine Damen und Herren, herzlichen Dank für die Stellungnahmen. Wichtiges Thema in schwierigen Zeiten. Dem umfangenen Betrachter drängt sich ein bisschen die Frage auf, warum es das eigentlich nicht längst gibt. Alle 16 Länder hacken ihre Daten da rein und ich glaube, die traurige Antwort ist, weil 16 Länder sehr unterschiedliche Systeme betreiben. Die können teilweise überhaupt nicht Daten miteinander austauschen, weil alle irgendwie eine andere Lösung haben. Es ist schon kurios, dass wir jetzt angesichts dieser Entwicklung der letzten 30 Jahre überlegen, welchen privatwirtschaftlichen Unternehmen wir ein paar Milliarden Euro geben, damit diese Daten zusammengeworfen werden können. Das aber eher eine politische Anmerkung. Sei es drum. Ich frage mich halt, es klang ja an in den Stellungnahmen, da sind ja alle möglichen Daten drin. Da sind Wohnraumüberwachungsdaten drin, da sind gesundheitliche, medizinische Untersuchungen drin, Obduktionsberichte, weil die Polizeivertreter hier mehrfach angesprochen haben, Kindesbrauch, die Opfer, einfach die medizinischen Berichte darüber, mit all den Daten, die da drin sind. Und wir lassen ja Beamtinnen und Beamte einen Eid schwören, damit sie auch mit solchen Daten umgehen können als Exekutive. Jetzt frage ich mich, wie ist das, wenn wir all diese Daten einem privatwirtschaftlichen Unternehmen geben? Vielleicht können Herr Löffelmann und Frau Ruf mal auf diese Frage eingehen, was das eigentlich für verfassungsrechtliche Implikationen hat, wenn ein privatwirtschaftliches Unternehmen eine solche Datenmacht bekommt. Jetzt wurde gesagt, es ist ein amerikanisches Unternehmen. Ich finde, das ist noch unter vielen Varianten die günstigste. Aber sagen wir mal, Elon Musk steigt da nächste Woche ein. Ja, kann ja sein. Der sagt, kaufe ich mich ein. So, alle bayerischen Opferdaten zu Elon Musk. Oder, mein letzter Punkt, die Polizeibeamten, ja, ich frage mich, die Gewerkschaftsvertreter der Polizei tragen hier vor, sie sind dafür. Sie gucken sich die Geschichte mit Egisto Ott in Österreich an, wo der russische Nachrichtendienst Datenabfragen abkauft. Alle ermittelnden Beamten sind da mit ihren Daten drin.

AVors. **Petra Pau** (Die Linke): Kollege.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Kann das in Ihrem Sinne sein oder muss dafür nicht aus Sicherheitsgründen eine nationale Antwort gefunden werden? Herzlichen Dank.

AVors. **Petra Pau** (Die Linke): Prof. Löffelmann, Sie haben das Wort.

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin)**:** Vielen Dank für die Frage. Das Bundesverfassungsgericht spricht in seiner Entscheidung diese Möglichkeit des Missbrauchs bei einer Auslagerung der Datenverarbeitung an private oder auch an ausländische Stellen explizit an. Und das ist deshalb mit Sicherheit ein Gesichtspunkt, der zumindest regulativ aufgefangen werden müsste, indem man eben entsprechende Schutzvorkehrungen schafft. Aus den mir bekannten

Gesetzesvorhaben gibt es zum Beispiel den Ansatz, dass man die ganze Software in einem System betreibt, das vom Internet komplett getrennt wird und dann gewissermaßen in einem Stand-Alone-System betrieben wird. Das wirft natürlich auch Folgeprobleme auf. Auch Software muss gewartet werden, muss weiterentwickelt werden. Also letzten Endes wird man, wenn man nicht die eigene technische Expertise hat, nicht davon ausgenommen sein, dass man fremden Personen darauf Zugriff gewährt. Und ja, dann greift die Notwendigkeit, dass der Staat sich schützend vor die Bürger stellt, was die Verarbeitung dieser Daten anbelangt. Also das hat eine normative Komponente, das hat sicher auch eine technische Komponente. Auf jeden Fall glaube ich, dass das sehr, sehr schwierig ist. Ich bin selbst in meinem früheren Leben Staatsanwalt und Richter gewesen und ich muss sagen, mich hat es immer mit einem gewissen Unbehagen erfüllt, zu hören, dass in der bayerischen Justiz die entsprechenden Server für die elektronische Akte und dergleichen nicht selbst betrieben werden, sondern an Private ausgelagert werden. Und wenn man dann auf einmal auf seinem PC die Aufforderung hat, man soll irgendetwas in der Cloud speichern, dann gehen bei mir die Warnglocken an. So viel, das ist jetzt keine wahnsinnig rechtliche Bewertung, aber vielleicht ein bisschen Erfahrungshintergrund.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Frau Ruf.

SV **Simone Ruf** (GFF, Berlin): Ja, dem kann ich mich eigentlich nur anschließen und würde da auch noch mal die Schutzvorkehrungen hervorheben wollen und da vielleicht noch eine zusätzliche anführen. Dass man eben auch Zugriffsbeschränkungen vorsehen sollte in der Rechtsgrundlage, die dann nur besonders qualifizierten Mitarbeiter*innen Zugriff erlauben. Das könnte wiederum an bestimmte Qualifikationen, Ausbildungen, Fortbildungen geknüpft sein. Und nochmal, um den Aspekt der Datensicherheit insgesamt aufzugreifen. Wir haben jetzt ja in Bayern den Fall, dass VeRA getestet wurde. Hier sehe ich schon ein großes Problem, dass die Berichte nicht öffentlich sind und man müsste diese Tests wohl laufend wiederholen. Nur mit einmal Testen kann man sich ja vorstellen, dann kommt ein neues Update, eine neue Komponente rein. Damit ist es nicht getan und das müsste auf jeden Fall in regelmäßigen Abständen sichergestellt sein, sodass es hier auch normativ irgendwo verankert sein müsste. Danke.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Für die AfD-Fraktion fragt der Abgeordnete Herr Dr. Wirth.

Abg. **Dr. Christian Wirth** (AfD): Vielen Dank fürs Wort, vielen Dank auch an die Sachverständigen. Wir haben eben gehört, dass man hier natürlich eine europäische oder eine deutsche Lösung bevorzugt. Das sehen wir auch so, aber man spricht die ganze Zeit von mittel- bis langfristig. Ich habe noch keine Zeiten gehört, wann so ein System zur Verfügung stehen würde. Auf der anderen Seite arbeiten wir ja, oder in Bayern, seit etwa zwei Jahren relativ erfolgreich mit dem System. In Hessen und Nordrhein-Westfalen wird auch damit gearbeitet. Vor dem Hintergrund, dass Frau Ruf meinte, dass die aufgeführten Ermittlungserfolge lediglich anekdotischen Charakter haben sollen, möchte ich Herrn Wagner und Herrn Peglow vielleicht mal fragen in der Praxis, was die Software bisher bewirkt hat. Und was würde es bedeuten, diese Software nicht einzusetzen, wenn wir noch mittel- oder langfristig warten, sprich einige Jahre warten, bis vielleicht ein deutsches System zur Verfügung steht? Danke.

AVors. **Petra Pau** (Die Linke): Dr. Wagner bitte.

SV **Dr. Roland Wagner** (HMdI, Wiesbaden)**:** Ja, vielen Dank. In meiner schriftlichen Stellungnahme hatte ich ja zwei Fälle aufgeführt, die exemplarisch darstellen sollten, wo der Vorteil ist. Nämlich genau da, wenn sich ganz kleine Puzzleteile in riesigen Datenmengen verstecken. Und das ist ja genau das, womit wir, so hatte ich auch versucht meine Stellungnahme aufzubauen, wenn wir mit den aktuellen Datenmengen konfrontiert sind. Wie gesagt, 3,2 Terabyte in einem Fall von sexuellem Missbrauch. Dann kommt es vielleicht genau auf das eine Bild an, ob ein laufender Missbrauch entdeckt wird oder ob er eben weiterläuft. Und ich finde, da können wir nicht zuwarten, keinen Tag, keine Woche, keinen Monat, überhaupt

nicht. Weil wenn ein Kind leiden muss, weil wir die richtige Analyse nicht fahren können, dann ist das zumindest aus polizeilicher Sicht ein absolut unannehmbarer Zustand. Genauso in Fällen, die wir aktuell bearbeiten. Was Geldautomatensprengungen angeht, sind es komplexe Täternetzwerke, mit denen wir es zu tun haben. Wenn es dort Asservate gibt, sind auch die voll von Daten. Und dann kommt es eben auf die kleinen Puzzleteile an, ob man ein Täternetzwerk aufdecken kann oder ob es Einzeltäter bleiben, weil man eben die Hintergründe nicht entdecken kann. Und vor dem Hintergrund ist die Analysesoftware ganz aktuell und jetzt nach meiner Meinung sehr, sehr wichtig. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Danke schön. Herr Peglow.

SV **Dirk Peglow** (BDK, Berlin): Ja, herzlichen Dank. Vielleicht beschreibe ich Ihnen das mal aus Sicht der Sachbearbeitungserfahrung von vor gar nicht so vielen Jahren, 15 Jahre. Da hat man Ermittlungsverfahren gehabt, wo man im Grunde genommen als sachleitender Ermittler oder Ermittlerin sich viele Dinge merken konnte. Also ich kann mich jetzt noch an Beschuldigtendaten erinnern aus dem Ende der 90er Jahre, die habe ich noch im Kopf. Das ist heute nicht mehr vergleichbar mit dem, was wir jetzt aktuell machen. Dr. Wagner hat dazu schon einiges gesagt. Es geht aber auch darum, Operativkräfte in entsprechenden Gefahrenlagen zu steuern und hier kommt es auf Sekunden an. Das heißt, eine Einsatzleiterin, ein Einsatzleiter muss innerhalb kürzester Zeit Entscheidungen treffen, ob wir links- oder rechts herum gehen. Polizeiliches Arbeiten ist vielfach eben nicht so viel von Diskussionen und auch nicht von „Wünsch-dir-was“, sondern von „So ist es“ geprägt und dieses „So ist es“ muss entschieden werden. Und dazu brauche ich einigermaßen vernünftige Daten, die ich dann auch sehr schnell in kurzer Zeit zusammenbringe und die richtigen Entscheidungen treffe. Denn eins ist uns allen auch klar: Wenn die falsche Entscheidung getroffen wird, werden die, die Verantwortung für diese Einsätze haben, gefragt werden, warum die falsche Entscheidung getroffen wurde und möglicherweise Dinge nicht abgewehrt werden konnten. Das sollte man sich immer in Erinnerung rufen. Also die Zeiten, wo wir sechs, sieben Leitz-Ordner im Regal haben und das mehr oder weniger uns aneignen, was da drinsteht, die sind eben vorbei. So einfach ist das. Es klingt profan, es ist aber tatsächlich die Realität. Ich kann immer nur wieder sagen, die Sachbearbeiterinnen und Sachbearbeiter haben teilweise überhaupt gar keine Zeit, komplexe Analyse- und Auswertungsverfahren zu machen. Also der Trend polizeilicher Arbeit geht immer mehr auch dahin, dass wir Analystinnen und Analysten einstellen, die mit einem ganz anderen ermittlungstaktischen Ansatz, mit einem ganz anderen Erkenntnishintergrund an solche Auswertungen und Analysen gehen. Wir haben in der Sachbearbeitung eine ganze Menge zu tun und brauchen auch diese Expertise und die entsprechenden Systeme, um dann den Sachverstand zusammenzubringen und zum Ergebnis zu kommen.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Für die FDP-Fraktion fragt der Kollege Höferlin.

Abg. **Manuel Höferlin** (FDP): Danke Frau Vorsitzende. Ich weiß nicht, ob mich das jetzt beruhigt, dass Palantir uns sagt, ob wir links- oder rechts herum gehen und man sich dann darauf 100 Prozent verlässt. Ich habe zwei Fragen an Herrn Dr. Atzpodien. Die Einlassungen an verschiedenen Stellen heute klingen so an, als gäbe es nur ein einziges System, nämlich das von Palantir, das derzeit lauffähig ist und solche Aufgaben zu Analyse von großen Datenmengen machen kann. Alles andere wären Dinge für mittlere- bis langfristige Projekte, so klingt es, wenn ich vor allem die Vertreter der Polizeien höre. Ich wundere mich darüber deshalb, weil allein mir mindestens eins, eigentlich zwei Systeme bekannt sind, die derzeit sogar bei Bundesbehörden im Einsatz sind, zum Beispiel bei Nachrichtendiensten und beim Verfassungsschutz, die auch Datenanalysen machen. Und ich frage mich dann, sind das irgendwie Spielereien oder sind das echte Systeme? Und auch in Frankreich höre ich, wird Palantir gerade aktuell aus den Systemen entfernt und mit einer eigenen Software, die lauffähig ist, ersetzt. Vielleicht können Sie dazu etwas sagen. Sie haben ja gesagt, Sie vertreten eigene Unternehmen im Bereich. Gibt es wirklich keine einzige Software und

was machen andere Unternehmen da? Vor dem Hintergrund des Strategiepapiers geht es ja um Schlüsseltechnologien. Also ganz konkret, sind Ihnen Unternehmen bekannt – Sie müssen sie ja nicht nennen – aber die Frage, gibt es wirklich nichts anderes, was in Ministerien oder Behörden sonst aktiv eingebunden ist und funktioniert? Und die zweite Frage. Sie sagen, dass man sich in Bayern, obwohl die Anschaffung des Palantir-Produkts zurückliegt, noch immer in der Entwicklungs- und Testphase befindet. Dort werden immer noch Dinge fertig getestet. Auch öffentliche Äußerungen sind so. Es werden noch Datenmengen für einen zukünftigen zuverlässigen Betrieb unabdingbar getestet. Heißt das, der Bund müsste auch noch jahrelang mit echten Menschen Daten testen, bevor man dann eine lauffähige, zuverlässige Nutzung hat? Vielleicht können Sie dazu noch was sagen, wie man einen zuverlässigen, bundesweiten Betrieb damit gewährleisten kann.

AVors. **Petra Pau** (Die Linke): Bitte, Herr Dr. Atzpodien.

SV **Dr. Hans Christoph Atzpodien** (BDSV, Berlin)**:** Herr Abgeordneter Höferlin, vielen Dank für die beiden Fragen. Zu der ersten Frage. Ich hatte ja eingangs gesagt, dass Palantir nicht zu unseren Verbandsmitgliedern, nicht mehr zu unseren Verbandsmitgliedern gehört. Insofern kann ich mich hier etwas, sozusagen, einseitiger äußern, als vielleicht meine Nachbarin Frau Dehmel das kann. Ich habe diese Informationen natürlich bekommen von unseren Mitgliedsunternehmen, also ich habe nicht von Palantir etwas gehört. Das kann ich kann ich hier deutlich sagen. Aber ich habe etwas gehört von den Unternehmen, die bei uns Mitglieder sind und die weisen darauf hin – ich spreche jetzt mal unter der Kontrolle des Herrn aus Bayern –, dass eben das System von Palantir in der Tat noch auch nach der Umsetzung noch Entwicklungsaufwand gehabt habe. Ihre Frage ging aber darauf, welche Systeme von unseren Mitgliedsunternehmen sind schon im Einsatz und ich kann sagen, in Teilen, also zum Beispiel, was Massendatenspeicherung angeht, sind Systeme im Einsatz oder eben im militärischen Bereich. Ich hatte das erwähnt in meiner mündlichen Aussage. Es sind Systeme im Einsatz, die aus Sicht unserer Mitgliedsunternehmen sehr leicht adaptiert werden können, auch in den polizeilichen Einsatz. Vielleicht mit einer entsprechenden Testphase, aber ohne da wirkliche Risiken einzugehen, was die Funktionalität angeht. Zweiter Punkt. Sie hatten auf das Thema „Echte Menschendaten“ abgehoben. Ich habe mich dazu nochmal versucht schlau zu machen. Beide Gruppen, von denen ich hier berichtet hatte, die eben von sich sagen, dass sie relativ, sehr lösungsnahe Angebote machen können, sagen, dass man aus ihrer Sicht nicht mit echten Menschendaten testen muss, sondern – und das sei gerade der Vorteil bei einer Standardlösung –, dass man zwar einen Testaufwand treiben muss, aber das mit den legal zur Verfügung stehenden Daten – und da beziehe ich mich auch auf das, was der Bundesdatenschutzbeauftragte gesagt hat – hier durchaus machen kann. Also nicht unbedingt mit echten Menschendaten, sondern mit legal zur Verfügung stehenden Daten und dass der Testaufwand relativ überschaubar ist, weil wir eben schon sehr lösungsnahe Angebote haben. Danke.

AVors. **Petra Pau** (Die Linke): Ich danke Ihnen. Da wir uns alle in der ersten Runde im Großen und Ganzen an die Vorgaben gehalten haben, können wir in eine zweite Runde mit jeweils zwei Fragen nach dem bekannten Prozedere einsteigen, wenn das so gewünscht ist. Für die SPD beginnt der Kollege Fiedler.

Abg. **Sebastian Fiedler** (SPD): Vielen Dank nochmal, ich versuche so ein bisschen zu extrahieren, welche Punkte am Ende für mich noch relevant sind, neben der Feststellung, dass wir immer noch ein Musterpolizeigesetz benötigen, deshalb würde ich meine Fragen an Herrn Atzpodien und Frau Dehmel noch mal richten, auch vor dem Hintergrund der vielen Industriegespräche, die ich beim Europäischen Polizeikongress geführt habe, die mir andere Geschichten zu den Ausschreibungsverfahren erzählen, was auch immer da jetzt dran sein will. Es scheint mir die Geschwindigkeit der Einführung eines anderen Systems, von dem Sie gerade sagten, dass sie jedenfalls existent sind, der entscheidende Punkt zu sein. Ich würde auf Europol nochmal verweisen wollen, von denen ich

hörte, dass dort auch nicht Palantir im Einsatz ist und das aus meiner Sicht eine der zentralen Auswertungs- und Analyse-Behörden Europas gerade ist. Also ich glaube für uns ist das der entscheidende Punkt und die Diskrepanz. Wir hörten von Frau Skropke, deswegen frage ich nochmal, sechs bis zwölf Monate sagen Sie, wenn Sie uns bitte noch mal eine Einschätzung dazu geben können, wie lange würde es dauern, bis – ich lasse diese rechtliche Komponente mal weg –ein technisches System mit vergleichbaren Fähigkeiten, läuft? Also das würde ich an Sie beide noch mal fragen wollen. Das ist für mich die Kernfrage, die noch überbleibt, bisher.

AVors. **Petra Pau** (Die Linke): Herr Dr. Atzpodien.

SV **Dr. Hans Christoph Atzpodien** (BDSV, Berlin)**:** Vielen Dank Herr Abgeordneter Fiedler, für die Frage. Also ich würde es noch mal ganz klar sagen und für das eine kann ich ja nur auf Frau Skropke verweisen. Ich meine bei Nationale Souveräne Analyseplattform (NaSA) ist secunet eines der maßgeblich beteiligten Unternehmen und Frau Skropke selber hat ja sozusagen den zeitlichen Aufwand genannt, der aus meiner Sicht sehr überschaubar ist. Bei dem zweiten Angebot, ich hatte das erwähnt, Aufbau einer Recherche- und Analyseplattform für die Polizei, abgekürzt RAP, gibt es das als militärische Lösung bereits und es muss also sozusagen nur noch adaptiert werden auf die Polizei und da gibt es also nach deren Auskünften, die mir vorliegen bereits einen Prototypen, also von daher sind wir in beiden Fällen nah an der Lösung. Der Dritte, wie gesagt, erklärt mir das auch, aber möchte nicht genannt werden, aus Gründen, die ich jetzt nicht weiter erläutern kann, weil ich sie auch nicht kenne. Aber es gibt einen Dritten und das ist ein namhaftes Unternehmen aus Süddeutschland. So von daher kann ich nur sagen, gibt es, ich wiederhole mich noch mal, sehr einsatznahe Lösungen offenbar. Umgekehrt wird von diesem Unternehmen berichtet, sei Palantir nicht so Plug & Play, wie es von den Anwendern dargestellt wird. Aber das sage ich auch wertfrei, weil ich nur das wiedergeben kann, was man mir erzählt. Danke.

AVors. **Petra Pau** (Die Linke): Vielen Dank, Frau Dehmel.

SV **Susanne Dehmel** (Bitkom, Berlin): Ja, also an der Stelle kann ich auch auf Aussagen von anwesenden Anbietern verweisen, was Frau Skropke gesagt hat, alles weitere ist schwer aus Verbandssicht einzuschätzen. Also wir haben natürlich eine Reihe von Unternehmen, wo ich sagen würde, die müssten in der Lage sein, so etwas in überschaubarer Zeit zu entwickeln und da gab es auch Gespräche. Aber wie lange das genau dauert, hängt eben nicht nur allein von den Anbietern ab, sondern hängt auch davon ab, wie die öffentliche Hand in der Lage ist, im Zweifelsfall entsprechend die Leistungsbeschreibung zu machen und das Ganze auch zu unterstützen. Behördlicherseits, finde ich, sind insofern schon auch die Bedarfe auf Behördenseite relevant und auch die rechtliche Grundlage ist nicht ganz außer Acht zu lassen bei der Überlegung, weil die Erfahrung so ein bisschen zeigt, dass es da ganz schön viele Zeitfaktoren gibt, die entstehen können. Ich würde mal sagen, was die Kompetenz und die Kapazität deutsche Anbieter angeht, da stehen wir nicht schlecht da. Aber die Frage ist, wie man so etwas aufsetzt. In dem Zusammenhang wäre meine Empfehlung auch, dass man zukünftig vielleicht einen verbesserten Marktdialog im Voraus mit den entsprechenden nationalen Unternehmen führt, sozusagen vorkommerzielle Beschaffungsverfahren, wo man sich mal anguckt, welche Kompetenzen sind wo vorhanden und auch schon mal spezifiziert, wie sich die Bedarfe auf Seiten der Sicherheitsbehörden entwickeln. Das gibt es teilweise auch im Verteidigungsbereich und ich glaube, das sollte man sich auch zukünftig nochmal stärker in der Richtung angucken.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Für die CDU/CSU-Fraktion hat der Kollege Dr. Heck das Wort.

Abg. **Dr. Stefan Heck** (CDU/CSU): Ja, vielen Dank, ich würde gerne die Euphorie, die Sie hier teilweise haben hinsichtlich der zeitlichen Zusagen und den Optimismus teilen. Von daher würde ich gerne mal einen etwas ungewöhnlichen Vorschlag machen in dieser Fragerunde. Gibt es

irgendjemanden von Ihnen, ich gucke jetzt mal Frau Skropke, Frau Dehmel, Herrn Dr. Atzpodien an, der uns sagen kann, zu dem Zeitpunkt X, um die Frage von Herrn Fiedler noch mal etwas zu schärfen, steht ein Produkt zur Verfügung, das jedenfalls ein ähnliches Leistungsniveau hat wie Palantir Hessen Data, das in den Polizeien der Länder gerade eingesetzt wird? Gibt es jemanden, der sich dazu traut eine Aussage zu machen, hier in einer öffentlichen Anhörung des Deutschen Bundestages? Dann finde ich, sollten wir die Gelegenheit nutzen und wir würden das auch gerne dann so für die Öffentlichkeit festhalten. Die zweite Frage geht an Herrn Teufele. Herr Dr. von Notz hat ja eben so ein bisschen das Bild an die Wand gemalt, was eigentlich passiert, wenn auf Umwegen Daten an anderer Stelle landen, dort, wo wir sie nicht haben wollen. Es ist ja eine Besorgnis, die, wenn sie zutreffend wäre, man sehr ernst nehmen müsste. Deswegen wollte ich Sie fragen, wie haben Sie denn dagegen Vorkehrungen getroffen? Haben Sie dort Eigenuntersuchung vorgenommen? Gibt es dort Externe, die sich damit beschäftigt haben und zu welchem Ergebnis sind die gekommen? Wie verhindern Sie ganz konkret, dass bei Ihrer Anwendung in Bayern Daten abfließen?

AVors. **Petra Pau** (Die Linke): Gut, etwas unkonventionell, aber lösbar. Ich würde jetzt erstmal Herrn Teufele das Wort geben und ansonsten stünde auch die Parlamentarische Staatssekretärin zur Verfügung etwas dazu zu sagen. Herr Teufele.

SV **Klaus Teufele** (BLKA, München): Vielen Dank für die Frage. Es ist eine Frage der IT-Sicherheit und vielleicht ist auch ein bisschen digitale Souveränität. Das nehmen wir wichtig, das ist uns wichtig, das ist mit die oberste Messlatte. Die Software befindet sich im Rechenzentrum der bayrischen Polizei und nur im Rechenzentrum der bayrischen Polizei. Wir entscheiden, was hier eingespielt wird, was hier nicht eingespielt wird, auch wenn es um Updates oder Ähnliches geht. Es ist nicht nur so, dass es keinen Zugang zum Internet gibt, selbstverständlich nicht, sondern im Gegenteil. Auch Dinge, die reinkommen, laufen durch einen sehr dedizierten Sicherheitsprozess und es wird von uns detailliert geprüft, was die Software tut, was sie nicht tut. Also diese Updates, die kommen, was sie können oder nicht können. Erst recht die polizeilichen Daten. Sie sind ausschließlich im Rechenzentrum der Bayerischen Polizei. Nur hier haben wir die Daten und wir geben keinerlei Daten nach außen, allein durch den Betrieb innerhalb des IT-Sicherheitsbetriebs wäre es schon gesichert, dass keine Daten raus gehen, aus dieser Software, egal was die Software denn möchte. Und das machen wir nicht nur für Palantir, das machen wir für unsere gesamte Software, in der personenbezogene Daten liegen. Darüber hinaus haben wir an der Stelle auch noch eine Quellcodeuntersuchung veranlasst. Zur Frage vorhin, warum wir so lange brauchen: Ja, die hat auch relativ viel Zeit gebraucht, um hier einfach nochmal die abschließende Sicherheit zu haben, dass die Software keine unzulässige Funktionalität hat. Es wurde keinerlei Funktionalität entdeckt, die eine Backdoor oder irgendeine Möglichkeit bietet, hier Daten nach außen abfließen zu lassen. Es sind unsere Daten, es bleiben unsere Daten.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Darf ich eine kurze Verständnisfrage stellen?

AVors. **Petra Pau** (Die Linke): Ja, wir sind auch gut in der Zeit, machen Sie das.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Herr Teufele, ich verstehe nicht ganz, wie kommen denn die Daten da rein und wie können die Ermittler, wenn ich Herrn Peglow mal zitieren kann, die in der Situation im Einsatz sind und jetzt entscheiden müssen, ob sie nach links oder rechts gehen sollen, wie kommen die denn an die Analyseergebnisse, die bei Ihnen in einem Stand-alone-Rechner sind? Also wie funktioniert das denn überhaupt?

SV **Klaus Teufele** (BLKA, München): Ich habe nicht von einem Stand-alone-Rechner gesprochen, ich habe gesagt, gesichert im Rechenzentrum der bayrischen Polizei.

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ja, aber auf den haben Zehntausende Zugriff.

SV **Klaus Teufele** (BLKA, München)**:** Nein, auf diesen Rechner hat die bayrische Polizei Zugriff.– –

Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Ja, zehntausende von Beamten.

SV **Klaus Teufele** (BLKA, München): – –und die Daten kommen aus den Umgebungen der Bayerischen Polizei, aus den Verfahren der Bayerischen Polizei und bleiben innerhalb der Bayerischen Polizei. Zugriff haben dediziert Berechtigte der Bayrischen Polizei und es wird aufgrund des Funktionsumfangs, weil wir es auch nicht so brauchen, ein sehr kleiner Kreis der bayrischen Polizeibeamten sein.

AVors. **Petra Pau** (Die Linke): Gut, bevor Frau Staatssekretärin das Wort bekommt, von den Sachverständigen hat sich Herr Dr. Atzpodien gemeldet. Gab es noch andere Sachverständige, die sich auf diese unkonventionelle Fragestellung einlassen wollten? Dann haben Sie das Wort.

SV **Dr. Hans Christoph Atzpodien** (BDSV, Berlin)**:** Ja, ich mache es auch ganz kurz, ich finde die Frage absolut berechtigt. Das ist eine Kernfrage, Herr Abgeordnete Fiedler hat die im Prinzip ja auch schon gestellt. Ich kann Ihnen als Verbandsvertreter – und da bin ich ganz transparent – nur das vortragen, das habe ich gemacht, was mir meine Mitglieder, die dort relevant sind, in diesem Thema berichten. Es gibt hier am Tisch ein Konsortium, das ist hier persönlich vertreten durch Frau Skropke. Die Empfehlung wäre vielleicht Frau Skropke noch mal genau diese Frage zu stellen. Ich glaube, das gibt vielleicht am ehesten den Aufschluss, den sie sich erhoffen.

AVors. **Petra Pau** (Die Linke): Ich würde vorschlagen, weil man keine Hellseherin sein muss, um zu erkennen, dass wir genügend Zeit haben. Ich würde vorschlagen, dass wir das im Moment noch zurückstellen. Wir werden ganz zum Schluss noch eine Runde haben mit übrig gebliebenen Fragen. Wir bleiben jetzt erstmal noch in der Fraktionsrunde, Frau Staatssekretärin.

PStn **Rita Schwarzelühr-Sutter** (BMI): Vielen Dank Frau Vorsitzende und liebe Kolleginnen und Kollegen, sehr geehrte Damen und Herren. Zeit spielt ja durchaus eine Rolle und jetzt wurde mehrfach gefragt, Plug & Play und es geht los. Ich will aber hier auch noch mal Plug & Play realistisch einordnen, weil P20 ist mehr als nur das Analyse- und Software-Tool und insofern ist es mir hier wichtig, dass ich noch mal darstelle, dass wir dabei sind, das Datensystem „Ökohaus“ aufzubauen und will das einfach noch mal zeitlich einordnen, damit es nicht so ein Bild gibt, wie wenn jetzt Palantir zur Verfügung steht, dass wir den Stecker einstecken und dann läuft es. Das VeRA ist dann noch ein bisschen mehr.

AVors. **Petra Pau** (Die Linke): Gut, ich würde vorschlagen, Sie gedulden sich, vielleicht kommen dann auch noch andere Aspekte dazu. Wir machen weiter mit BÜNDNIS 90/DIE GRÜNEN und der Kollege Emmerich fragt diesmal.

Abg. **Marcel Emmerich** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Frau Vorsitzende. Die sicherheitspolitischen und auch die verfassungsrechtlichen Bedenken sind ja jetzt schon vielfach geäußert worden. Ich würde gerne noch mal mehr ins Detail gehen und habe da eine Frage an Sie, Frau Ruf. Die Gesellschaft für Freiheitsrechte hat ja auch gegen diese automatisierte Datenerhebung vor dem Bundesverfassungsgericht geklagt. Und in Hessen und Hamburg sieht man ja, dass man da auch Recht bekommen hat. Jetzt meine Frage. Mit welcher Begründung haben Sie denn diese Verfassungsbeschwerden eingelegt und welche Kritikpunkte treffen auch in diesem Zusammenhang auf die Bundes-VeRA zu? Können Sie das noch mal genauer erörtern? Und ja, wie bewerten Sie dann überhaupt die Nutzung von Bundes-VeRA in Anbetracht von diesen Bedenken? Also ist es überhaupt möglich ohne Rechtsgrundlage?

SV **Simone Ruf** (GFF, Berlin): Also ohne Rechtsgrundlage ist es sowieso nicht möglich, um das gleich mal vorwegzustellen. In dem Verfahren haben wir insbesondere gerügt, dass die Vorschriften, die jeweils die Rechtsgrundlage waren für den Einsatz – in Hamburg wurde es ja noch nicht eingesetzt – derart daten- und methodenoffen ausgestaltet waren, dass sie schwerwiegende Grundrechtseingriffe ermöglicht haben. Also dass sich letztlich all die Gefahren und Risiken, die ich eingangs schon dargestellt hatte, realisieren können und jedenfalls eine große Gefahr bestand, weil

umfassend alle Datentöpfe einbezogen werden und auch die Methode einfach nicht begrenzt war. Und gleichzeitig waren aber die Eingriffsschwellen in den Rechtsgrundlagen viel zu niedrig, viel zu sehr ins Vorfeld von Gefahren verschoben und auch die Rechtsgüter, die es nach der Rechtsvorschrift zu schützen galt, waren viel zu unbestimmt ausgestaltet. Und dann kam noch dazu, dass es keine Verfahrenssicherungen gab, keine Benachrichtigungspflichten, keine Auskunftsrechte, die datenschutzrechtliche Kontrolle war defizitär ausgestaltet, also einiges. Die Kritikpunkte ließen sich natürlich jederzeit je nach der Ausgestaltung der jeweiligen Rechtsgrundlage, übertragen. Im Grundsatz ist es ja dasselbe Prinzip. In NRW haben wir auch noch eine Verfassungsbeschwerde anhängig und auch die Neuregelung in Hessen sieht nicht verfassungskonform aus. Genau, deswegen vielleicht noch, um da anzuschließen, um da wirklich eine rechtssichere Grundlage auch hinzubekommen, die sich auch technisch realisieren lässt, weil da würde ich auch noch mal anknüpfen an diese Darstellung von gerade eben: Kategorisierung ist superwichtig, Kennzeichnung ist wichtig, aber es reicht nicht aus, es einfach nur in der Rechtsgrundlage festzuschreiben, sondern es muss gerade auch technisch möglich sein, das Ganze auch umzusetzen.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Das Fragerecht geht an die AfD-Fraktion, Dr. Wirth, Sie haben das Wort.

Abg. **Dr. Christian Wirth** (AfD): Vielen Dank. Also ich glaube, wir haben alle verstanden, dass eine deutsche Lösung wünschenswert ist. Wir haben auch verstanden, dass dringender Handlungsbedarf besteht und bestehen bleibt und nicht zugewartet werden kann. Und daher schließe ich mich der allgemeinen Frage an, wann könnte man starten mit einem solchen deutschen Projekt und ist es nicht möglich bis dahin eventuell Palantir bundesweit einzusetzen, wobei natürlich die Politik gefragt ist, also wir, hier eine rechtssichere Regelung herbeizuführen? Vielen Dank.

AVors. **Petra Pau** (Die Linke): Haben Sie eine Adressatin oder einen Adressaten? Gibt es eine Sachverständige oder einen Sachverständigen, der oder die etwas sagen kann? Dann haben Sie jetzt das Wort.

SV **Christine Skropke** (secunet, Essen): Ja, vielen Dank. Also ich kann ganz konkret sagen, dass das Konsortium NaSA seit einem Jahr bereits am Thema und an der Prüfung Thema arbeitet und mit vielen Sicherheitsbehörden in Gesprächen war. Es gibt auch einen Zeitplan, der sagt, dass in zwölf Monaten Testbetrieb, Installationen und so weiter realistisch sind. Ich möchte aber wirklich darauf hinweisen, was Frau Dehmel auch gesagt hat, dass natürlich die behördliche Seite hier entsprechend auch mitarbeiten muss und das Ganze natürlich auch in der Definition, in der Aufgabenbeschreibung etc. natürlich auch parallel mitlaufen muss. Vielleicht, damit sie auch die Namen haben, damit das nicht mehr so anonym ist, also wer steht hinter NaSA? Das ist secunet mit Cloud- und IT-Sicherheit-Krypto-Lösungen, die natürlich die sicheren Netze darstellen.

Abg. **Sebastian Hartmann** (SPD): Was ist NaSA?

SV **Christine Skropke** (secunet, Essen): Ach so, Entschuldigung, dass die Nationale Souveräne Analyseplattform. Genau. Was wichtig ist, wenn ich jetzt diese Firmen nenne. Es sind mehrere Firmen, es sind deutsche Firmen, dass dieses Konsortium sehr stark den Wert auf einen Plattformgedanken legt, das heißt, offen ist für weitere Partner, für Technologien, für Erweiterungen und nicht in einen Login reindenkt. Und ich möchte ja eigentlich, ich habe bewusst versucht keine Werbung für dieses Projekt zu machen, aber zumindest möchte ich einmal alle Beteiligten hier nennen. Neben secunet ist das SAP, ist das Rola, ist das Innosystec, die zur Firma Plath gehört, die Bundesdruckerei und Conet. Also alles Partner, die mit dem Bund und mit vielen Ländern zusammenarbeiten. Herr Teufele, wir sind uns ja auch sehr vertraut in Bayern, da gibt es ja auch einige gute Zusammenarbeit, wo wir doch, glaube ich, in diesem Kreis auch gegebenenfalls erweitert noch um andere Unternehmen, die ja noch Kompetenzen mit einbringen können, wirklich sagen können, das sind erprobte und auch, ich sage mal, bekannte, vertrauenswürdige Unternehmen, die den Umgang mit deutschen Sicherheitsbehörden auch seit vielen Jahren gewohnt sind.

AVors. **Petra Pau** (Die Linke): Herzlichen Dank. Kollege Höferlin.

Abg. **Manuel Höferlin** (FDP): Danke schön Frau Vorsitzende. Ja, Frau Skropke, dann stelle ich meine Frage auch nochmal an Sie. Sie haben jetzt gerade auch ganz nebenbei von einem wichtigen Punkt gesprochen, nämlich von offenem Datenaustausch in der Plattform und von keinem Login-Effekt. Ich will jetzt nicht, dass Sie sich über andere Mitbewerber zu tief auslassen, aber es ist ja schon ein Unterschied, ob ich eine Software habe, bei der später andere Unternehmen Daten austauschen können. Ich frag mich auch noch wie in Bayern die Daten in das Rechenzentrum reinkommen, wenn es keine Außenverbindung geben soll. Also wahrscheinlich ist gemeint, dass es eine gute Sicherheitslösung gibt, dass da keine unberechtigten Zugriffe stattfinden können. Aber natürlich sind solche Datenpools zugänglich von außen, also sonst laufen natürlich die Daten nicht rein und natürlich sind sie auch zugänglich, um Daten abzufragen. Wenn man das bundesländerübergreifend mit dem Bund macht, kann man das auch nicht alles im bayerischen Rechenzentrum hosten und jeder Beamte aus Schleswig-Holstein geht mal kurz ins bayerische Rechenzentrum, um die Daten abzurufen, sondern natürlich ist das übers Internet erreichbar. Es ist nur eben getunnelt und verschlüsselt. Mit allen Sicherheitslücken, die dann auch da sein könnten, will ich das nur eben vorwegsagen. Die Frage an Sie, wie sieht es aus mit Offenheit im Sinne von Anbindung weiterer Softwarekomponenten in eine solche Plattform? Wie sieht das aus bei Palantir? Ihrer Erfahrungen nach, wie sieht denn das Preismodell von Palantir im Moment aus? Ich höre, Palantir macht extreme Aufschläge im Moment, gigantische Aufschläge. Liegt es an der Marktsituation? Ist das bei Ihnen auch so, dass Sie plötzlich das zwei- oder dreifache des Preises nehmen müssen, was Sie noch vor einem Jahr kalkuliert haben? Ist die Marktlage – das können Sie als Marktteilnehmer vielleicht sagen – denn so schlimm, dass man plötzlich wahnsinnige Aufschläge nehmen muss? Und ich habe noch eine Frage an Herrn Kelber. Ich höre, dass Europol ja Palantir nicht mehr benutzt, vor allen Dingen nicht nur Preisqualität als Kriterium für den Rauswurf der Software, sondern vor allen Dingen auch datenschutzrechtliche Gründe angegeben hat. Gibt es aus Ihrer Sicht dort auch Probleme beim Einsatz einer Softwareplattform Palantir aus den US-amerikanischen Bereich? Bei der Verwendung der Daten hinsichtlich Software-Updates kann man mit Sicherheit sagen, dass es eine Lücke in der Software nicht gibt oder kann man darauf testen, weil das war auch so eine Einlassung, man könne ausschließen, dass es eine Lücke gibt. Das ist mir, ich komme aus der IT, neu, dass man das so sicher sagen kann bei einer Software, die nicht im Quelltext vorliegt und das ist bei Palantir nicht der Fall.

AVors. **Petra Pau** (Die Linke): Gut, als Erstes hat Frau Skropke das Wort.

SV **Christine Skropke** (secunet, Essen): Ich kann zum Preismodell vom Palantir nichts sagen. Da bitte ich auch um Verständnis, dass wir hier diese Marktdaten auch nicht weiter vertiefen. Ich denke, es ist sicherlich immer wieder ein Risiko, wenn man an einem einzigen Anbieter hängt und hier natürlich die Lizenzmodelle dann, ich sag mal, freier verändert werden können. Wenn man natürlich einen offeneren Markt hat, hat man auch mehr Wettbewerb und dann entstehen natürlich auch unter dem Wettbewerb wieder andere Preismodelle. Das vielleicht einfach nochmal vorausgesagt. Was schwierig ist, wenn Sie sagen, wird sowas teurer in der Entwicklung. Und da haben sicherlich auch die Verbände Erfahrungen. Da sind wir immer wieder in den Gesprächen mit Bedarfsträgern, wenn während der Entwicklungsphase Änderungen reinkommen. Das heißt, wenn die Bedarfe nochmal nachjustiert werden, dann kann es dazu kommen, dass natürlich auch Produkte oder Lösungen am Ende auch teurer werden, wenn man nicht bei der ersten Definition bleibt, worauf ein Anbieter oder ein Konsortium die Lösung drauf baut. Ich hoffe, dass das Ihre Fragen weitestgehend so beantwortet.

Abg. **Manuel Höferlin** (FDP): Nach den offenen Schnittstellen hatte ich auch gefragt.

SV **Christine Skropke** (secunet, Essen): Als Plattform wollen wir offene Schnittstellen darstellen, aber natürlich mit entsprechender IT-Sicherheit hinterlegt. Sie hatten das vorhin schon gesagt, es gibt hier jetzt schon einen Datenaustausch zwischen den Bundesländern, den Polizeibehörden, auch den Sicherheitsbehörden, die immer mit

entsprechenden hochkryptierten, hochsicheren Leitungen entsprechend gesichert sind. Und das würde in unserer Plattform, in den Plattformgedanken, natürlich analog auch so stattfinden.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Prof. Kelber.

SV **Prof. Ulrich Kelber** (BfDI): Vielen Dank. Ich habe leider keine öffentlich zitierbaren Informationen dazu zur Verfügung. Allerdings geht der zuständige Datenschutzbeauftragte für Europol, mein europäischer Kollege, nach genau denselben Prüfkriterien vor wie ich.

AVors. **Petra Pau** (Die Linke): Danke schön. Ich schaue jetzt in die Runde, ich habe Sie gesehen, Herr Peglow, oder war das eine Meldung? Nicht. Ich schaue jetzt in die Runde. Gibt es weiteren Fragebedarf aus den Fraktionen? Die SPD? Die Union? Okay, dann bleiben wir in der üblichen Reihenfolge. Kollege Hartmann, beginnen Sie?

Abg. **Sebastian Hartmann** (SPD): Ja, Frau Vorsitzende, Frau Vizepräsidentin, herzlichen Dank. Wir haben ja jetzt hier nicht nur die Bandbreite von Rechtsgrundlagen bis Haushaltsmittelverfügbarkeit, sondern auch, wer bietet wie viel, wie sind die Namen und wer sagt ja, wer sagt nein und das könnte zu einer gewissen Unübersichtlichkeit führen, die jetzt beunruhigen könnte. Da würde ich das doch gerne mal zuspitzen, weil wir der Gesetzgeber sind, möglicherweise auch der Haushaltsgesetzgeber, wenn es jetzt zur Vergabe kommt. Deswegen will ich das auf zwei Themenkomplexe machen. Offensichtlich gibt es Unternehmen, die sagen, man könnte das in sechs bis zwölf Monaten machen. Das amerikanische Konsortium sagt, unseres ist sofort verfügbar. Wir wissen aber auch aus öffentlich zugänglichen Quellen, dass in Bayern auch Lösungen jahrelang Lizenzgebühren verlangten, ohne dass sie in die Anwendung kamen. Ich glaube man kann mir hier öffentlich nicht widersprechen, auch nicht öffentlich nicht widersprechen. So, das muss man festhalten, weil sonst im Raum steht, wir würden als Gesetzgeber unsere Aufgabe nicht gerecht, nämlich die Sicherheit der Bürgerinnen und Bürger dieses Landes zu garantieren. Ich möchte das hier in aller Klarheit in der Öffentlichkeit auch nochmal darstellen. Uns geht es am Ende auch darum, Strafverfolgung im Rechtsstaat zu ermöglichen. Und dazu muss Beurteilungsfähigkeit da sein und zumindest dieses Mindestmaß an digitaler Souveränität brauchen wir, um den Prozess als solchen beurteilen zu können, wo die Daten liegen. Wir haben dafür eine öffentliche Einrichtung, das ist der Datenschutzbeauftragte Uli Kelber, dem ich für die hervorragende Zusammenarbeitet in den vergangenen Jahren auch danke. In seiner Stellungnahme ist etwas enthalten, ähnlich wie bei Prof. Dr. Löffelmann, was sind die Mindestanforderungen, die der Bundesgesetzgeber regeln muss, um solche Lösungen rechtssicher in einem Rechtsstaat anwenden zu können? Und das ist die Mindestvoraussetzung auch mit dem Blick auf die Ländergesetze. Und mich würde auch mal interessieren, wie Sie als Datenschutzbeauftragter die Urteile des Verfassungsgerichts zur automatisierten Datenverarbeitung wahrnehmen, was da auch mehr möglicherweise kommen kann, ich will nicht suggestiv fragen, aber an mehr aufkommt, wenn es ein automatisiertes Verfahren ist. Das würde mich noch mal wirklich zur Zuspitzung zum Schluss interessieren. Und dann möchte ich gerne an den Vertreter der Wirtschaft noch mal das Wort geben. Fallbeispiel: Wenn wir uns entschieden haben, eine bestimmte Technologie nicht einzuführen, eine bestimmte Entwicklung nicht vorzunehmen, was vergeben wir uns? Das ist ja nicht nur die Beherrschbarkeit, sondern dass Sie ein bisschen etwas die Lage beschreiben. Deswegen will ich auch öffentlich bekennen, mir ist der NaSA-Ansatz sehr gut bekannt. Mir sind auch durch andere Gespräche mehrere Konsortien in Deutschland gut bekannt, das sind namhafte deutsche Unternehmen der deutschen Steuer, die zahlen ja auch Steuern und müssen vor allen Dingen unserem Rechtsstaatpflichtprinzipien unterliegen.

AVors. **Petra Pau** (Die Linke): Schauen Sie auf die Zeit.

Abg. **Sebastian Hartmann** (SPD): Können Sie mir das mal darlegen, wie sich das entwickelt hat aus Sicht der Wirtschaft? Vielleicht auch an Beispielen, die jetzt schon funktioniert haben.

AVors. **Petra Pau** (Die Linke): Gut, wir beginnen mit Prof. Kelber.

SV **Prof. Ulrich Kelber** (BfDI): Vielen Dank. Ich war damals auch Sachverständiger bei dem Verfahren. Wir haben versucht, an Beispielen aus unserer Kontrollpraxis natürlich deutlich zu

machen, wo die Probleme beim Einsatz solcher Datenanalysen vorliegen. Mir persönlich hat das natürlich Spaß gemacht, weil meine berufliche Herkunft kommt ja genau aus dem Bereich KI und Datenanalyse. An dem Punkt, ähnlich wie die Polizeibeamten, sehen auch wir die besonders pathologischen Beispiele. Also wir haben natürlich die Beispiele, wo es total schiefgelaufen ist oder wo Grundrechte missachtet worden sind, was von automatisierten Mustererkennungen, die wiederum zu verlängerten Speicherungen führen können bei beispielsweise Kreuztreffern in Funkzellenabfragen beim Senken von Schwellen. Man ist wegen eines Kleinstdeliktes – das Übermalen eines Hakenkreuzes auf einer Parkbank – im System, dann eine Kontaktperson zu dieser Person, dann vielleicht eine Anzeigenerstellung und dann geht es über diese Mustergeschichte auch weiter. Das sind natürlich Fälle, die wir sehen an dem Punkt. Und deswegen noch vor der eigentlichen Gesetzgebungstechnik also: Datum, Schwelle Übertragung, Analyse, Sichtweise, Zugangsbeschränkung, liegt ja die Frage, welche Daten will ich eigentlich miteinander verknüpfen und welche nehme ich, obwohl irgendwo mal ein Zufallstreffer auch noch kommen könnte, raus, weil die Verhältnismäßigkeit nicht mehr gewährleistet ist? Diese erste Überlegung, die nimmt natürlich dem Gesetzgeber außerhalb des Gesetzgebungsrechtes auch niemand ab und die ist auch nicht in Wochenfrist zu machen. Die Qualität von Daten natürlich, wir haben gerade in diesen historisch gewachsenen Datenbanken teilweise extrem schlechte Qualität, das wird besser, das sehen wir auch, aber die Verknüpfung einer schlechten Datenbank kann auch den gesamten Datenbestand ein Stückchen weit vergiften.

AVors. **Petra Pau** (Die Linke): Danke. Herr Dr. Atzpodien.

SV **Dr. Hans Christoph Atzpodien** (BDSV, Berlin)**:** Ja, vielen Dank Herr Abgeordneter Hartmann für die Frage. Das gibt mir Gelegenheit, neben dem NaSA-Konsortium, was ja hier am Tisch mit Frau Skropke vertreten ist, auch noch mal das andere Konsortium unter der Führung der Firma Evident, früher Atos, mit einer Reihe von qualifizierten deutschen Mittelständern und der Frauenhofer Organisation bewusst zu erwähnen. Dort kommt man eben von einer militärischen Lösung, die bereits vorhanden ist und von der klar gesagt wird, dass man sie mit den bestehenden Prototypen für die polizeiliche Anwendung auch sehr schnell in die polizeiliche Anwendung adaptieren kann. Und ich und nehme das Stichwort, das Sie gegeben haben, auch noch mal auf, „Schlüsseltechnologien“, das ist ja nicht von ungefähr damals in zweiter Auflage schon in dem Papier von 2020 definiert worden. Die erste Auflage kam 2015 für den militärischen und 2016 für den übrigen Sicherheitsbereich. Die Überlegung war ja ganz bewusst zu sagen, was sind Technologien, bei denen ich nationale Souveränität behalten möchte, aus gutem Gründen, und wenn ich das möchte – und da wurde eben krypto- und KI-gestützte Anwendungen definiert – wenn ich das möchte, was tue ich dann, damit ich das tun kann? Es steht in dem Papier drin und es ist immerhin von der Bundesregierung beschlossen und es ist vielleicht demnächst in der Überarbeitung aber eher noch extensiver als restriktiver, drin, dass man eben, wenn die Möglichkeit besteht, dann solche Lösungen aus diesem Grunde auch national beschaffen will und umgekehrt man natürlich auch guckt, was passiert, wenn zum Beispiel dann ausländische Investoren in solchen Unternehmen investieren wollen. Und diese beiden Dinge können ja nicht einfach sozusagen nichtssagend sein, sondern die müssen meines Erachtens und unseres Erachtens gerade hier in diesem Bereich besonders gewürdigt werden und insbesondere dann, wenn eben auch Lösungen zur Verfügung stehen, die bereits sehr anwendungsnah sind. Immer natürlich auch unter Anerkennung der Tatsache, dass es um Lösungen gehen muss. Ganz klar.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Für die Fraktion BÜNDNIS 90/DIE GRÜNEN hat der Kollege Emmerich das Wort. Entschuldigung, jetzt war ich doch zu schnell, nachdem wir so sensationell schnell in die dritte Runde gekommen sind. Entschuldigen Sie, Herr Dr. Heck, Sie sind dran.

Abg. **Dr. Stefan Heck** (CDU/CSU): Kein Problem. Ja, ich habe eine Frage an Herrn Peglow und eine Frage an Herrn Dr. Wagner. Herr Peglow vielleicht, ich wollte Ihnen gerne Gelegenheit geben, noch mal Stellung zu nehmen. Sie haben ja einen guten Überblick über die Marktlage, sprechen mit vielen Kollegen, die mit diesem Programm auch befasst

sind. Wie schätzen Sie den Wettbewerb, den wir momentan haben ein? Ist dieser Zeitplan realistisch? Wie ist Ihre Einschätzung hinsichtlich der Marktreife anderer Produkte? Und ist es eigentlich zutreffend, weil wir gerade über Haushaltsfragen gesprochen haben auf Nachfrage des Kollegen Hartmann, dass durch den Nichtabruf der Bundes-VeRA nun für diejenigen Polizeien der Länder, die sich für einen Abruf entscheiden, deutlich höhere Kosten entstehen, als wenn das BMI bei seiner ursprünglichen Zusage geblieben wäre? Herr Dr. Wagner, Frau Ruf hat eben die Gesetzeslage in Hessen angesprochen, es gab dazu ja auch Gerichtsurteile. Könnten Sie uns noch mal erläutern, wie sich das auf die praktische Anwendbarkeit auswirkt? Es gab ja Anpassungen auch in den hessischen Gesetzen, wenn ich es richtig sehe, ist es jetzt nicht mehr möglich, Hessen Data anzuwenden? Ist es anders möglich? Wie wirkt sich das aus?

AVors. **Petra Pau** (Die Linke): Herr Dr. Wagner.

SV **Dr. Roland Wagner** (HMdI, Wiesbaden)**:** Dann fang ich an, vielen Dank. Also nach dem Urteil des Bundesverfassungsgerichts war ja klar, die automatische Datenanalyse folgt einem legitimen Zweck, ist geeignet und erforderlich. Die Verhältnismäßigkeit, das ist korrekt, musste nachgeschärft werden, unter anderem auch, insofern ist es richtig, weil Teile der alten Normen von dem, § 25a HSOG (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung), zu unbestimmt waren. Das liegt ein bisschen historisch betrachtet an dem Umstand, dass sozusagen die Einführung der Software mit dem damaligen Paragraphen gewachsen ist. Das wurde geheilt, am 12. Juli 2023, meine ich, ist § 25a HSOG neu in Kraft getreten. Sehr dezidiert angelegt an die Vorschriften des Bundesverfassungsgerichts. Man hat dort versucht, auch die einzelnen Punkte, die das Gericht in der sehr umfassenden Entscheidung aufgeführt hat, von Eingriffstiefe über Veranlasserprinzip, über Bestimmtheitsgrundsätze, alles das, was heute auch schon mal angeklungen ist, dezidiert zu regeln, sodass im Moment in drei Varianten die Norm anwendbar ist bzw. die Analyse, nämlich zur Abwehr einer konkreten Gefahr, zur Abwehr einer konkretisierten Gefahr und auch zur vorbeugenden Bekämpfung von Straftaten, wobei dabei immer der Grundsatz folgt, je tiefer es in die Daten reingeht, desto weniger Kolleginnen und Kollegen haben Zugriff. Gegenwärtig haben ungefähr 2 000 Kolleginnen und Kollegen in Hessen Zugriff auf Hessen-Data, von 20 000 Beamtinnen und Beamten, die in Hessen insgesamt Dienst versehen. Die Voraussetzungen sind streng geregelt nach einem Rollen- und Rechtekonzept, und auch die Zugriffskontrolle ist dort geregelt, sodass es eigentlich nicht auf einen Zugriff auf unberechtigte Daten kommen kann, denn alles wird protokolliert und der Datenschutzbeauftragte des Polizeipräsidiums Frankfurt hat da ein Auge drauf. Vor diesem Hintergrund sehen wir im Moment keine Einschränkungen, wir sehen es durchaus als regelbar an, in Gefahrenabwehrgesetzen, aber auch in der Strafprozessordnung, was die Repression angeht. Dort Regelungen zu schaffen, die eine vernünftige Arbeit auf sauberer, rechtlicher Grundlage mit einer Auswerte- und Analyseplattform ermöglichen. Vielen Dank.

AVors. **Petra Pau** (Die Linke): Danke und Entschuldigung Herr Peglow, aber wir hatten das hier nicht ordentlich registriert. Sie haben das Wort.

SV **Dirk Peglow** (BDK, Berlin): Herzlichen Dank. Ja, Herr Heck, ich also ich war mal vor vielen, vielen Jahren beteiligt in einem Projekt zur Neubeschaffung einer TKÜ-Anlage, also Telekommunikationsüberwachungsanlage, für das Land Hessen. Wir haben damals mit Anbieterunternehmen die Möglichkeit einer Implementierung eines Polygrafen in eine TKÜ-Anlage diskutiert und ich habe nach erstauntem Zuhören von 15 Minuten der Fachleute dann irgendwann als der Vertreter der Anwender*innen-Anforderungen gesagt, dass ich das für wenig sinnvoll halte, weil bei einem Großteil der Gespräche, die wir abhören, sich die Menschen anlügen. Insofern hilft uns das dann diese Implementierung dieser Technik auch nicht weiter. Was ich damit sagen will, wir haben bei der Polizei ganz viele Menschen, ganz viele Kolleginnen und Kollegen, die bei P20 zumindest ein Stirnrunzeln ins Gesicht bekommen. Ich glaube daran, ich halte das für einen Paradigmenwechsel in der Sicherheitsarchitektur der deutschen Polizei und zwar für alle Kolleginnen und Kollegen. Wenn wir hier über Marktsondierung reden, sollten wir natürlich immer im Zweiklang auch, Frau Skropke, davon gehe ich aus, dass Sie das berücksichtigen, darüber nachdenken, dass das alles abhängig davon ist, dass P20 mit dem Öko-Datenhaus der Polizei nach vorne kommt. Also das ist

ein wesentliches Kriterium, wenn wir über Fremdvergaben anderer Anbieterunternehmen reden. Das muss im Gleichklang mit P20 laufen und das ist die Voraussetzung. Und dann reden wir darüber, welches System wir da möglicherweise in eigener digitaler Souveränität aufsetzen. Das sollte man bedenken. Ich habe ganz viele Kontakte zu Menschen, Unternehmen, auch zu EVIDENT, die sagen, das machen wir! Bloß aus Sicht der polizeilichen Praxis warten wir schon seit 2016, beginnend Saarbrücker-Agenda. Wir haben PIAF, die Entwicklung dauert. Wir haben als polizeiliche Praktikerinnen und Praktiker seit mehreren Jahren immer wieder mit Verzögerungen zu tun, wenn es um die Einführung von IT-Tools geht. Das ist leider so, hat aber unterschiedliche Gründe, die nicht unbedingt bei den Kolleginnen und Kollegen liegen, die bei P20 engagiert sind. Die haben nämlich eine ganze Menge zu bedenken, das sollte man an dieser Stelle auch mal respektieren. Heißt unterm Strich, wir sind oder der BDK ist grundsätzlich dafür, dass natürlich digitale Souveränität eine Rolle spielen muss, selbstverständlich. Aber es kann, wie gesagt nochmal, nicht zur Folge haben, dass wir Dinge abschalten, die jetzt laufen. Schön wäre oder wir hätten uns gewünscht, eine Parallelentwicklung, also das eine System weiter bleibt und derzeit hat P20 und haben andere eben im Einvernehmen mit Unternehmen, denen wir vielleicht eher trauen, eine Möglichkeit, was zu entwickeln, was digitale Souveränität heißt und was auch entsprechend konform ist mit den Vorgaben der Datenschutzbeauftragten und den rechtlichen Vorgaben, die wir haben.

AVors. **Petra Pau** (Die Linke): Vielen Dank. Der Kollege Emmerich hat das Wort.

Abg. **Marcel Emmerich** (BÜNDNIS 90/DIE GRÜNEN): Vielen Dank Frau Vorsitzende, ich habe noch mal zwei Fragen, einmal an Frau Ruf und einmal an Herr Kelber. Einmal an Sie, Frau Ruf, ich wollte da eh schon mal nachhaken, weil Sie das vorhin schon gesagt haben, dass Sie weiterhin anzweifeln, dass die Rechtsgrundlage in Hessen ausreicht und Herr Dr. Wagner hat ja gesagt, dass alle Probleme geheilt seien. Da ist dann natürlich noch mal interessant zu hören, dass Sie auch diese Meinung teilen, das wäre diese eine Frage an Sie. Und die andere Frage an Sie, Herr Kelber, es ging ja auch immer um gesellschaftliche Risiken von solchen Analyseplattformen, gerade auch mit Blick auf künstliche Intelligenz. Können Sie dazu etwas sagen im Blick auf Diskriminierungspotenziale, die durch solche Analyseplattformen entstehen können?

AVors. **Petra Pau** (Die Linke): Frau Ruf.

SV **Simone Ruf** (GFF, Berlin): Ja, dann fang ich an. Die Ansicht teile ich gar nicht, das Hauptproblem in der Neuregelung, würde ich sagen, liegt darin, dass eigentlich alles auf die Verwaltung, also auf die Polizeien verschoben wurde, indem man sie umfänglich dazu ermächtigt, Verwaltungsvorschriften zu erlassen, in denen dann letztlich alles an Verhältnismäßigkeitserwägungen austariert werden soll. Die Vorschrift ist erst mal bisschen länger, man liest sie, dann denkt man, es ist irgendwie besser geworden, aber eigentlich ist sie dann relativ inhaltsleer. Die Gefahrenschwellen passen dann auch nicht mehr, weil dann ist es trotzdem wieder ein schwerwiegender Eingriff. Vor allem wenn man bedenkt, dass hier wieder einfach umfassend alle Datentöpfe zusammengeführt werden. Es sind auch wieder die Vorgangsdaten dabei und es sind auch wieder die Verkehrsdaten dabei. Dann sind die Vorgangsdaten für Unbeteiligte ausgeschlossen, was eigentlich faktisch, was nicht möglich ist, weil ein Vorgangsbearbeitungssystem ja gerade darauf zielt, dass man noch nicht groß kategorisiert in Personengruppen, sodass das letztlich ein Pseudoausschluss am Ende sein wird. Die Gefahrenstellen sind so weit vorne, dass man sogar mit wirklichen Bagatelldelikten Zielperson von der Analyse werden kann. Vor allem wenn dann noch an die Straftaten, die es zu verhüten gilt, auch an Vorfeldtatbestande angeknüpft wird. Dann ist man natürlich immer noch mal ein Stück weiter vorne. Man kann sich das schon fragen, was dann eigentlich noch der Anlass ist, den man geben muss, damit so eine Datenanalyse durchgeführt werden kann. Und ja, dann auch die Kontrolle ist meiner Meinung nach nicht hinreichend ausgestaltet, es wird kein Datenschutzbeauftragter verpflichtet. Das hätte man auf jeden Fall anders ausgestalten müssen. Ja, so in Kürze, würde ich sagen, man könnte hier noch sehr viel weiter machen.

AVors. **Petra Pau** (Die Linke): Wir merken uns, dass Prof. Löffelmann dazu noch was beizutragen hat, aber erstmal ist Prof. Kelber dran.

SV **Prof. Ulrich Kelber** (BfDI)**:** Vielen Dank. Solche Auswertesysteme sind natürlich immer besonders gut bei sehr gleichartigen Daten, die in sehr großer Menge vorliegen. Das war das Beispiel, es kommen terabyteweise Missbrauchsfotos herein, da Strukturen zu erkennen, Wiederholungen zu erkennen, Hintergründe oder Ähnliches wird ja zum Glück auch schon gemacht, zur Geschwindigkeitssteigung und zur Entlastung der Personen. Schwieriger wird es immer dann, wenn die Daten heterogener sind, eigentlich in der Auswertung Kontextbezogenheit benötigen. Ich will das mal im Beispiel erläutern, das jetzt so auch nicht mehr aktuell ist: Ein KI-System, das von Fotos ballspielender Kinder lernen soll. Ob das am Ende auf die Gravitation käme, es Ballwürfe nimmt oder vermutet, dass Kinder einfach immer Bälle in Bögen werfen, ist nicht klar, wenn das System nicht schon im Modelldesign darauf vorbereitet wurde, bestimmte Zusammenhänge auch zu erkennen. Also das Modelldesign ist das erste entscheidende. Das nächste ist natürlich die Qualität der Daten, weil durchaus KI auch eine konservative Technologie dahingehend ist, dass sie Strukturen, die sie vorfindet, interpretiert und wiederholt. Das heißt, wenn sie in Fällen, wo Verdächtige, Beteiligte, Kontaktpersonen in Vermutungen hineingenommen werden und die eventuell nicht völlige Gleichverteilung über Gruppen, Orte oder Ähnliches haben, dann repetiert das System mit einer hohen Gefahr diese Verzerrungen und interpretiert es auch in Zusammenhängen. Das ist systemimmanent. Dem müssen Sie mit entsprechenden Designs, mit entsprechenden Kontrollen in der Entwicklung und auch im weiteren Verlauf auf jeden Fall entgegenwirken! Sie brauchen aber natürlich solche Technologien für die Interpretation. Aber um zurückzukommen auf die Frage: Ich muss auch was an der Qualität der Datentöpfe tun und ich muss mich eventuell bewusst gegen die Hinzunahme bestimmter Daten entscheiden und das ist in der heutigen Situation schwierig, weil in bestehenden Systemen manche dieser Daten einfach wild nebeneinander liegen. Das wird besser werden, ist aber aktuell leider das Problem.

AVors. **Petra Pau** (Die Linke): Ich habe es so ein bisschen laufen lassen, weil ich das Gefühl hatte, dass das für alle an dieser Stelle nochmal aufklärend ist. Wir haben die Situation, dass die FDP in jedem Fall noch das Fragerecht wahrnehmen will und das Prof. Löffelmann zu der eben gestellten Frage noch eine kurze Ergänzung machen möchte. Kollege Höferlin, ist das okay?

Abg. **Manuel Höferlin** (FDP): Ja, meine Frage geht eh an Prof. Löffelmann. Von daher …

AVors. **Petra Pau** (Die Linke): Ach so. Na, dann lässt sich das vielleicht lösen.

Abg. **Manuel Höferlin** (FDP): Womöglich ist das fast das, was er sagen möchte, weil er vorhin sehr stark auf die Daten und Datenarten abgestellt hat mit seinem Bild. Auch das hat ja Herr Kelber gerade noch mal ausgeführt und wir haben auch an verschiedenen Stellen jetzt gehört, dass es durchaus einen Unterschied macht, wenn man solche polizeilichen Systeme mit einer Datenanalyse macht, wenn man sich vorher Gedanken macht, für welche Art der Abfrage, welche Datentöpfe denn überhaupt zur Verfügung stehen. Und deswegen würde ich mich freuen, wenn Sie die mindestens zwei Minuten, die Ihnen die amtierende Vorsitzende gibt, wenn es noch weitere Fragen gibt, vielleicht noch länger, dafür nutzen könnten, da nochmal Ausführungen zu machen, was da vielleicht auch gesetzgeberisch noch für Voraussetzungen nötig sind.

SV **Prof. Dr. Markus Löffelmann** (HS Bund, Berlin): Vielen Dank Herr Abgeordneter, jetzt glaube ich fast, Sie können Gedanken lesen. Also ich wollte noch mal auf den meines Erachtens sehr wichtigen Punkt hinweisen, weil das Stichwort „Qualität der Daten“ gefallen ist, dass der wunde Punkt der bisher vorliegenden gesetzlichen Regelungen meines Erachtens darin liegt, dass dort global ganze Datenbestände in Bezug genommen werden. Wenn man hier die Regelungen in Hessen liest, da heißt es, Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen. Da sind alle Daten vereint in einem Vorgangsverarbeitungssystem, die in einem Vorgang eben anfallen. Das sind sehr heterogene Daten. Das können nicht-personenbezogene, personenbezogene sein, das können Gesundheitsdaten sein, biometrische Daten, Verkehrsdaten, alles Mögliche. Und ich denke, der

Gesetzgeber wird sich diese Frage stellen müssen, das ist genau das, was das Bundesverfassungsgericht fordert. Welche Arten von Daten dürfen eigentlich in eine automatisierte Datenanalyse eingegeben werden? Wie sensibel sind diese Daten aus sich heraus? Aus welchen Datenerhebungsmaßnahmen stammen sie? Denn das ist der Kerngedanke des Grundsatzes der hypothetischen Datenneuerhebung. Ich hatte ja in meinem Eingangsstatement auch aus dem White Paper zitiert, dass man sich dazu bekennt. An diesem Grundsatz kommt man nicht vorbei, aber dann muss man sich eben genau diese Frage stellen: Wo kommt das Datum her? Wie, in welche Kategorie ordne ich das jetzt ein? Da sehe ich auch einen gewissen Spielraum, wie man das macht. Es gibt auch dazu rechtliche Vorgaben. Ja, das ist eine komplexe Angelegenheit. Also die Art der Daten. Das ist das eine. Das andere ist der Umfang der Daten, das kann man begrenzen, geografisch begrenzen, zeitlich begrenzen, anlassbezogen oder auf bestimmte Personenkreise bezogen begrenzen. Und das dritte ist die Methode der Datenanalyse. Auch hier sehe ich eine große Vielfalt von denkbaren Methoden automatisierter Analyse, von einer rein deskriptiven, über eine Textanalyse, Netzwerkanalyse, eine voraussagende Analyse, die Prognosen erlaubt. Also da gibt es wohl, ich bin kein Techniker, aber eine ganze Reihe von Methoden, die auch zu unterschiedlichen Eingriffsintensitäten führen. Und das sind die entscheidenden Fragen, die kann nur der Gesetzgeber beantworten und die gehen natürlich Hand in Hand mit der Funktionalität, ich habe es vorhin schon einmal gesagt, einer solchen Software. Also man müsste sich idealerweise fragen, was die Software können soll und was sie dürfen soll. Das ist der Ausgangspunkt für die Beantwortung der Frage kaufen und anpassen oder lieber selber machen.

AVors. **Petra Pau** (Die Linke): Vielen Dank! Ich schaue jetzt in die Runde, plagt eine Fraktion, einen Abgeordneten, eine Abgeordnete noch eine weitere Frage, dann würde ich diese noch zulassen, damit wir alle hier sehr zufrieden aus dieser Anhörung herausgehen. Wenn das nicht der Fall ist, danke ich erst einmal den Sachverständigen sowohl für die ausführlichen Stellungnahmen als auch dafür, dass Sie hier Rede und Antwort gestanden haben. Ich habe vorhin den Hinweis gegeben, dass Ihnen das Protokoll der Anhörung zugeschickt wird, versehen mit Hinweisen, wie das weitere Verfahren ist. Wir freuen uns dann auf die Auswertung der vollständigen Unterlagen. Ich schließe die Sitzung. Danke auch allen anderen Beteiligten.

Schluss der Sitzung: 15:54 Uhr

Petra Pau, MdB
Altersvorsitzende

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

An den Stellvertretenden Vorsitzenden des
Ausschusses für Inneres und Heimat
Herrn Prof. Dr. Lars Castellucci

per E-Mail: innenausschuss@bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
E-MAIL Referat32@bfdi.bund.de
INTERNET www.bfdi.bund.de
DATUM Bonn, 16.04.2024
GESCHÄFTSZ. 32-642-1/028#0065

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Einladung zur öffentlichen Anhörung im Innenausschuss am 22. April 2024**
BEZUG 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
ANLAGEN Stellungnahme

Sehr geehrter Herr Professor Dr. Castellucci,

zunächst bedanke ich mich für die Einladung zur öffentlichen Anhörung im Innenausschuss am 22. April 2024. Die Teilnahme wurde bereits zugesagt.

Anbei übersende ich meine schriftliche Stellungnahme mit der Bitte um Weiterleitung an die Mitglieder des Ausschusses.

Mit freundlichen Grüßen

[redacted]

Ulrich Kelber

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 16.04.2024

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestags
am 22. April 2024

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

(BT-Drs. 20/9495)

Graurheindorfer Straße 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

1. Ausgangslage

Mit dem Gesamtprogramm Polizei 20/20 (P 20) haben sich die Innenminister des Bundes und der Länder 2016 darauf geeinigt, die polizeiliche IT-Landschaft grundlegend zu modernisieren. Kern von P 20 ist das „gemeinsame Datenhaus“ der Polizeibehörden des Bundes und der Länder. Das Datenhaus soll durch eine mandantenfähige Trennung sicherstellen, dass jeder Teilnehmer – also jede Polizeibehörde – personenbezogene Daten entsprechend seiner jeweiligen rechtlichen Grundlagen speichert bzw. verarbeitet und dabei gesetzliche Speicherschwellen und den Grundsatz der Zweckbindung einhält.

Ein weiteres Ziel von P 20 ist es, den Datenbestand – innerhalb der gesetzlichen und verfassungsrechtlichen Grenzen – von vornherein auswertbar und analysefähig auszurichten. Deshalb werden alle Daten im gemeinsamen Datenhaus gespeichert, nicht mehr in vielen unterschiedlichen Systemen. Zu diesem Zwecke wird es innerhalb von P 20 eine Domäne „Analyse und Auswertung“ geben.

Die derzeit betriebenen Systeme werden teilweise als Interimssysteme in das Projekt P20 überführt, um eine Zwischenlösung bereitstellen zu können, bis das Datenhaus fertiggestellt ist. Dies betrifft etwa verschiedene Vorgangsbearbeitungssysteme und Fallbearbeitungssysteme. Natürlich wird auch das bisherige INPOL-Zentral übergangsweise weiterbetrieben. Um in dieser Zeit auch innerhalb der Domäne „Analyse und Auswertung“ weitergehende Möglichkeiten zu haben, nutzen bereits einige Teilnehmer einzelne Werkzeuge und Tools, die jeweils Teile der geplanten Domäne „Analyse und Auswertung“ abdecken.[1] Als Beispiel: die hessische Polizei nutzt ein Softwareprodukt der Firma Palantir mit der Bezeichnung hessenData. Unter dem Namen DAR nutzt die Polizei in Nordrhein-Westfalen ebenfalls ein solches Produkt.

Das Bayerische Landeskriminalamt führte im Jahr 2022 eine europaweite Ausschreibung für ein Auswerte- und Analysesystem durch. Das Ausschreibeverfahren zu einer verfahrensübergreifenden Auswertung und Analyse wurde zugunsten einer Software der Firma Palantir Technologies GmbH entschieden. Dieses Analysetool wird in Bayern als verfahrensübergreifendes Recherche- und Analysesystem kurz „VeRA“ bezeichnet. VeRA ist daher der gebräuchliche Begriff für die Softwareprodukte „Foundry“ und „Gotham“ der Firma Palantir.

Durch Abschluss eines Rahmenvertrages eröffnete die bayerische Polizeibehörde anderen Polizeibehörden des Bundes und der Länder die Möglichkeit, ohne ein gesondertes Ausschreibeverfahren

[1] Fachlicher Bebauungsplan des Programms P 20 S. 65

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

ebenfalls das Softwareprodukt der Firma Palantir zu nutzen. Insoweit wird von einer sog. „Bundes-VeRA“ gesprochen.

Das Bundesministerium des Innern und für Heimat (BMI) hatte zunächst Interesse an VeRA bekundet, sich letztlich aber gegen das Produkt entschieden.

2. Funktionalitäten von VeRA

VeRA eröffnet umfangreiche Analysemöglichkeiten.

Ziel von VeRA bzw. ähnlichen Produkten der Firma Palantir ist es, umfangreiche und zu verschiedenen Zwecken betriebene polizeiliche Datenbestände zusammenzuführen, zu verknüpfen und auszuwerten. Je nach Bedarf des jeweiligen Nutzers können unterschiedliche Datenbanken und Systeme angebunden werden.

Neben polizeilichen Datenbanken wie Vorgangsbearbeitungssystemen und polizeilichen Informationssystemen (z.B. INPOL-Zentral) können auch externe Datenbanken in eine Analyse einbezogen werden. Hier kommen als Beispiele Datenbanken des Einwohnermeldeamtes und des Kraftfahrtbundesamtes in Betracht.

Polizeiliche Datenbanken enthalten nicht nur Speicherungen über Personen, die Gegenstand polizeilicher Ermittlungen sind, bzw. waren, sondern auch personenbezogene Daten von Betroffenen, die zu keinem Zeitpunkt einem strafrechtlichen Anfangsverdacht ausgesetzt waren. Unbeteiligte Dritte wie z. B. Opfer, Hinweisgeber, Zeugen und Anzeigenerstatter werden ebenfalls in polizeilichen Datenbanken gespeichert. Diese Daten können unter Umständen sehr sensibel sein, man denke nur beispielsweise an elektronische Vernehmungsprotokolle der Opfer von Sexualstraftaten.

3. Rechtfertigung von Auswerte- und Analyseverfahren

Auswerte- und Analyseverfahren sind nicht grundsätzlich unzulässig, bedürfen aber spezifischer Grundlagen. Diese liegen derzeit weder für das BKA noch für die Bundespolizei vor.

Das BVerfG hat in seiner Entscheidung vom 16.02.2023[2] ausgeführt, dass eine automatisierte Datenauswertung und Analyse nicht grundsätzlich unzulässig ist. Es hat aber klargestellt, dass sie ein

[2] 1 BvR 1547/19, 1 BvR 2634/20

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

eigenständiger Grundrechtseingriff sein kann, der deshalb auch einer eigenständigen Rechtsgrundlage bedarf. Der Gesetzgeber muss die Voraussetzungen und Bedingungen der Datenanalyse normenklar bestimmen. Umso schwerer die von der Datenanalyse ausgehenden Grundrechtseingriffe sind, desto höhere Schwellen muss der Gesetzgeber festlegen.

Gegenstand des Verfahrens waren seinerzeit landesgesetzliche Normen, auf dessen Grundlage die Polizei Hessen unter dem Namen hessenDATA Software der Firma Palantir einsetzte. Ebenfalls waren gesetzliche Regelungen Gegenstand des Verfahrens, die der Polizei Hamburg den Einsatz einer entsprechenden Software ermöglichen könnte. Diese bestimmten jedoch keine ausreichenden Schwellen und Grenzen.

In seinem Urteil hat das Bundesverfassungsgericht zum einen umfangreiche Kriterien aufgestellt, durch welche die Eingriffsintensität von Datenauswertungen und Analysen bestimmt werden kann. Zum anderen hat es Vorgaben aufstellt, durch welche ein Eingriff in das Recht auf informationelle Selbstbestimmung gerechtfertigt sein kann.

Die besondere Eingriffsintensität von automatisierten Auswerte- und Analysemöglichkeiten wird schon dadurch verdeutlicht, dass das Bundesverfassungsgericht einen Grundrechtseingriff in zweifacher Hinsicht angenommen hat. Zum einen stelle die Nutzung der Daten über den ursprünglichen Zweck hinaus einen Grundrechtseingriff dar. Zum anderen liege ein weiterer Eingriff in der automatisierten Datenanalyse selbst.

Für die Bestimmung des Eingriffsgewichts hebt das BVerfG zwei Kriterien besonders hervor. Das sind *„Art und Umfang der Daten“* sowie die *„Analysemethoden“.*

Um die besondere Tragweite für den Bereich der Bundespolizeibehörden verstehen zu können, muss man wissen, dass die Polizeien umfangreiche Daten zu unterschiedlichen Personen in vielen Dateien speichern. Die Speicherung erfolgt zu unterschiedlichen Zwecken und derzeit noch in verschiedenen Dateisystemen.

In den Vorgangsbearbeitungssystemen - als Kernsysteme der Polizeien - werden beispielsweise neben Daten von Beschuldigten auch sensible Informationen von Opfern, von Zeugen und von Hinweisgebern zu unterschiedlichen Zwecken gespeichert. Es handelt sich also auch um einen umfangreichen Datenbestand von unbescholtenen Bürgerinnen und Bürgern. Diese personenbezogenen Daten würden potentiell mit VeRA ausgewertet und dann ggf. länger gespeichert werden. Vor diesem Hintergrund ist es offensichtlich, dass derart intensive Grundrechtseingriffe nicht auf Generalklauseln gestützt werden können. Daneben darf nicht vergessen werden, dass auch bei Daten

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

von Beschuldigten und Verdächtigten sich bei weitem nicht jeder Verdacht bestätigt. Viele Personen sind weiter gespeichert, auch wenn das Verfahren eingestellt oder sie freigesprochen wurden.

Es bleibt festzuhalten, dass das BVerfG mit seinem Urteil vom 16.02.2023 einen umfangreichen „Werkzeugkasten“ zur Verfügung gestellt hat, dessen Inhalt für eine spezialgesetzliche Grundlage genutzt werden muss.

4. Datenschutzrechtliche Herausforderungen

a. Bedarf einer Analysesoftware:

Zunächst obliegt es nicht dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, polizeifachliche Bedarfe zu erkennen und zu benennen.

Unabhängig davon bestehen aktuell bereits Auswerte- und Analysemöglichkeiten, die sowohl das BKA als auch die Bundespolizei unterstützen, Tat-Tat und Tat-Täter-Beziehungen in allen Phänomenbereichen zu erkennen. Hierzu werden die einheitlichen Fallbearbeitungssysteme genutzt (sog. eFBS).

b. Spezialgesetzliche Grundlage:

Wird ein darüberhinausgehender Bedarf für eine komplexere Auswertung und Analyse festgestellt, ist zunächst zu eruieren, ob eine gesetzliche Grundlage einen solchen Einsatz und damit Eingriff in das Recht auf informationelle Selbstbestimmungsrecht überhaupt rechtfertigen würde.

Eine den Vorgaben des Urteils des BVerfG vom 16.02.2023 entsprechende spezialgesetzliche Regelung der Polizeibehörden des Bundes (Bundeskriminalamt und Bundespolizei) liegt derzeit weder für VeRA noch für vergleichbare Produkte vor. Der Gesetzgeber hat vor dem Einsatz von Auswerte- und Analysesystemen eine entsprechende gesetzliche Grundlage zu schaffen. Anderenfalls würde das „Pferd von hinten aufgezäumt werden“ und eine Datenverarbeitung verstieße bereits gegen den Gesetzesvorbehalt.

Innerhalb des Gesetzgebungsverfahrens müssen u.a. entsprechend der Vorgaben des Bundesverfassungsgerichts folgende Fragen zuvor geklärt werden, bevor ein Auswerte- und Analysesystem in den Wirkbetrieb geht:

- Welche Datenbanken werden einbezogen?
- Werden nur Daten analysiert, die die jeweilige Behörde selbst erhoben hat?

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

- Werden polizeiliche Daten übergreifend ausgewertet, die mit unterschiedlichen Zielsetzungen gespeichert werden (z.B. entweder nur Daten von Personen, die zur Verfolgungsvorsorge im INPOL gespeichert sind oder aber auch Zeugendaten aus den Vorgangsbearbeitungssystemen?)
- Werden externe Datenbanken einbezogen?
- Werden Daten aus sozialen Netzwerken einbezogen?
- Werden Daten von Nachrichtendiensten einbezogen?
- Werden Daten von ausländischen Behörden berücksichtigt?
- Werden Daten aus Wohnraumüberwachungen und Onlinedurchsuchungen einbezogen?
- Werden Daten automatisiert oder manuell einbezogen?
- Wer hat Zugriff auf das Analysetool?
- Wie komplex ist der dahinterstehende Algorithmus und wie ist es um die Nachvollziehbarkeit der Datenanalyse bestellt?

Aus diesen Antworten ergeben sich die Anforderungen an eine spezialgesetzliche Grundlage.

c. Polizeiliche Generalklauseln

Auf allgemeine polizeiliche Generalklauseln (z. B. § 16 Abs. 1 und Abs. 4 BKAG) lässt sich eine derartige Analysemöglichkeit jedenfalls nicht stützen. Schon die spezielleren Vorschriften aus dem hessischen bzw. hamburgischen Polizeirecht waren zu allgemein gehalten. Als praktisches Beispiel wird auf den Beratungs- und Kontrolltermin zu sog. Funkzellendatenbanken im BKA verwiesen.[3]

In dieser Funkzellendatenbank speichert das BKA personenbezogene Daten, die die Strafverfolgungsbehörden im Bund und Ländern durch Funkzellenabfragen – zu Rufnummern, IMEI, IMSI, LAC-Cell-ID, Datum, Uhrzeit, Gesprächsdauer, Gesprächsrichtung – erhoben haben. Das BMI stützt die Speicherung auf die Generalklausel des § 16 Abs. BKAG und den Abgleich auf § 16 Abs. 4 BKAG. Das Eingriffsgewicht kommt einer Rasterfahndung gleich und kann nicht auf Generalklausel gestützt werden. Ich habe die Einstellung dieser Dateien angeordnet. Ein Klageverfahren hiergegen ist derzeit vor dem Verwaltungsgericht Köln anhängig.

Produkte der Firma Palantir, bzw. VeRA könnten im Verhältnis zur Funkzellendatenbank noch deutliche größere Datenmengen intensiver auswerten und analysieren. Mit VeRA könnte sog. „Data-Mining“ betrieben werden. Dieses umfasst nach der Definition der Bundesregierung Verfah-

[3] 30. Tätigkeitsbericht des BfDI, Nr. 8.2.4

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

ren und Methoden, „mit deren Hilfe bereits vorhandene große Datenbestände, zumeist auf statistisch-mathematischen Verfahren basierend, selbstständig auf Zusammenhänge analysiert werde, um auf diesem Wege „neues Wissen“ zu generieren“.[4]

Es bedarf daher unbedingt spezialgesetzlicher Regelungen, um eine Auswertung und Analyse rechtskonform umzusetzen.

d. Zweckbindungsgrundsatz:

Aus datenschutzrechtlicher Betrachtung ist es zudem erforderlich zu klären, welche Vorkehrungen zur Sicherung des Grundsatzes der Zweckbindung getroffen werden. Der Zweckbindungsgrundsatz ist ein Grundpfeiler des deutschen und europäischen Datenschutzrechts.[5] Er dient insbesondere dazu, die Verhältnismäßigkeit staatlichen Handelns sicherzustellen und Bürger vor ungerechtfertigten Grundrechtseingriffen zu schützen.

Mit P 20 sollen künftig alle Daten der Polizeibehörden in einem gemeinsamen Datenhaus gespeichert werden. Das Datenhaus wäre faktisch die Grundlage für Auswerte und Analysemöglichkeiten. Durch die einheitliche Datenbasis im Datenhaus bestünde grundsätzlich die Möglichkeit, dass sämtliche Daten miteinander abgeglichen, kombiniert und verknüpft werden. Gerade vor diesem Hintergrund ist es essentiell, sicherzustellen, dass der Grundsatz der Zweckbindung eingehalten wird. Selbstverständlich sind die oben genannten rechtlichen und verfassungsrechtlichen Vorgaben innerhalb des neuen Datenhauses zu beachten.

e. Unterlaufen von gesetzlichen Schwellen

Durch komplexe Auswerte- und Analyseverfahren könnten gesetzliche Schwellen unterlaufen werden. In dem polizeilichen Informationsverbund INPOL-Z werden personenbezogene Daten zur Fahndung und zur Vorsorge gespeichert. Hierfür bestehen bestimmte gesetzliche Schwellen in §§ 18, 19, 29, 31 Bundeskriminalamtsgesetz (BKAG). Zum einen ist die sog. Verbundrelevanz – länderübergreifende, internationale oder erhebliche Bedeutung – bei einer Speicherung zu beachten. Eine weitere Schwelle ist die sog. Negativprognose. Eine Speicherung zur Vorsorgezwecken ist daher nur dann rechtmäßig, wenn zuvor geprüft wurde, ob eine weitere Speicherung wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstige Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind.

[4] BT-Drs. 17/11582, S. 3
[5] https://www.bfdi.bund.de/SharedDocs/Kurzmeldungen/DE/2021/07_Positionspapier-Zweckbindung-Polizei.html

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Diese gesetzlichen Schwellen dürfen durch Auswerte- und Analysemöglichkeiten nicht unterlaufen werden.

5. Digitale Souveränität

In den Datenbanken der Polizeibehörden des Bundes und der Länder werden umfangreiche Daten von unterschiedlichsten Personenkreisen gespeichert. Von „einfachen“ Daten bis hin zu besonders sensiblen Daten werden Daten von Verdächtigen, Beschuldigten und verurteilten Straftätern und teilweise von unbescholtenen Bürgern gespeichert. Vor diesem Hintergrund und mit Blick auf mögliche Gefahren für die Sicherung dieser sensiblen Daten ist die digitale Souveränität der Bundesbehörden ein verfassungsrechtliches Gebot. Das Bundesverfassungsgericht weist zutreffend darauf hin, dass beim Einsatz von Software privater Akteure oder anderer Staaten die Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte besteht.[6]

Aus datenschutzrechtlicher Sicht ist es daher zu begrüßen, wenn das Programm P 20 eine eigene Softwarelösung entwickelt. Der Schutz der Grundrechte der betroffenen Personen ist Aufgabe des Staates und kann durch eigene digitale Lösungen am besten sichergestellt werden. Anderenfalls besteht das Risiko, Abhängigkeiten mit privaten Anbietern einzugehen, die nicht immer vorhersehbar sein können. Unbemerkte Manipulation und Zugriffe sind nicht auszuschließen. Um eine verfassungsrechtlich nicht hinnehmbare Abhängigkeit der Polizeibehörden zu vermeiden, sind Eigenentwicklungen grundsätzlich vorzugszugswürdig.[7]

[6] 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
[7] Kelber/Bortnikov, Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten, NJW 2023, 2002)

Graurheindorfer Str. 153 FON +49 (0)228-997799-0 E-MAIL poststelle@bfdi.bund.de
53117 Bonn INTERNET www.bfdi.bund.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 B

Bayerisches Landeskriminalamt

Öffentliche Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am Montag, dem 22. April 2024 von 14.00 bis 16.00 Uhr

Stellungnahme AD Klaus Teufele, Bayerisches Landeskriminalamt

---

Stellungnahme zum Antrag der Fraktion CDU/CSU:

Handlungsfähigkeit der Strafverfolgungsbehörden sichern - Entscheidungen des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren (BT-Drucksache 20/9495)

Die Sicherheitslage in Deutschland ist von einer anhaltend hohen Gefährdung durch den internationalen Terrorismus, die Organisierte Kriminalität und die Schwere Kriminalität geprägt. Der Anschlag auf das Veranstaltungszentrum Crocus City Hall am 22.03.2024 in Moskau mit über 140 Toten, gefolgt vom Aufruf des Sprechers der Terrormiliz ISPK (Islamischer Staat Provinz Khorasan) zu Anschlägen auf Christen und Juden verdeutlicht die nach wie vor vom Islamischen Staat ausgehende Gefährdung. Die rechtsextremen Angriffe auf die Synagoge in Halle, der Mord am Kassler Regierungspräsidenten Lübcke, die beinahe zum Alltag gehörenden Meldungen über Sprengungen von Geldautomaten und nicht zuletzt der sexuelle Missbrauch von Kindern und Verbreitung der Inhalte über das Internet als andauerndes Massendelikt sind Beispiele, vor denen wir nicht die Augen verschließen dürfen.

Die Polizei braucht das notwendige Handwerkszeug, um den in der analogen wie in der digitalen Welt agierenden Tätern habhaft werden zu können. Ziel muss es sein, Anschlagspläne möglichst frühzeitig zu erkennen und zu beenden, oder aber auch Kinder aus Missbrauchssituationen herauszuholen und die dafür verantwortlichen Täter zu identifizieren.

Wesentliche Bedeutung haben hierbei auch die bei der Polizei bereits vorliegenden Daten. Diese Informationen liegen allerdings in unterschiedlichsten polizeilichen IT-Verfahren und müssen von den Nutzenden derzeit einzeln abgefragt und die Ergebnisse händisch miteinander abgeglichen werden, um Zusammenhänge erkennen zu können. Grund hierfür ist eine historisch gewachsene, heterogene polizeiliche Datenbankstruktur, die mit den unterschiedlichsten Datenformaten und Datenbankarchitekturen aufgebaut wurde. Recherchen müssen manuell

angestoßen, Mehrfachabfragen mit ein und demselben Datum in unterschiedlichsten Systemen/Datenbanken durchgeführt werden. Die Abfragen und verlässliche Zusammenführung der Daten nehmen dabei viel Zeit in Anspruch – Zeit, die bei diesen Gefahrenlagen nicht zur Verfügung steht. *„Die Polizei weiß erst nach Tagen, was die Polizei weiß“* - die Täter agieren hingegen vernetzt in Echtzeit. Die Gefahrenlagen erfordern eine sofortige Reaktionsfähigkeit der Polizei, nicht erst nach Tagen. Ganz zu schweigen von den hohen personellen Ressourcen, die für die Vielzahl an Einzelabfragen eingesetzt werden müssen. Letztlich bleibt auch das Risiko, durch die fehlende Zusammenführung und die verteilten Abgleiche Ermittlungsansätze und Tatzusammenhänge nicht oder nur eingeschränkt erkennen zu können.

Die Zeit drängt. Die Gefahrenlagen sind tagesaktuelle Realität und erfordern möglichst zeitnah die Bereitstellung einer verfahrensübergreifenden Recherche- und Analyseplattform. Die Bayerische Polizei hat deshalb bereits im Jahr 2021 beschlossen, eine solche Plattform einzuführen. Neben der Zusammenführung der vorhandenen Daten muss diese Plattform polizeiliche Analysen funktional unterstützen und Auswertungen in Echtzeit ermöglichen. Ausgehend vom Bedarf einer möglichst frühzeitigen Einsatzfähigkeit und langfristigen Betriebsstabilität entschied sich die Bayerische Polizei für die Ausschreibung einer am Markt vertriebenen und im Einsatz bereits erprobten Standardsoftware.

Der fachliche Bedarf an einer verfahrensübergreifenden Analyseplattform besteht aber nicht nur in Bayern. In Hessen und NRW ist eine derartige Plattform längst eingeführt. Abfragen in den polizeifachlichen Gremien ab 2020 haben ergeben, dass der dringende Bedarf an einer verfahrensübergreifenden Analyseplattform in allen Bundesländern besteht.
Damit war es nur folgerichtig, dass die Bayerische Polizei keinen Alleingang bei der Ausschreibung der Analyseplattform beschritten hat. Alle Vergabeunterlagen (Verträge, Leistungsbeschreibung, Kriterienkatalog) wurden auf Bitte des beim Bundesministerium des Innern und für Heimat angesiedelten Zentralprogramms Polizei 20/20 gemeinsam mit Vertretern des Zentralprogramms erarbeitet und abgestimmt.

Dabei wurde auch einvernehmlich bestätigt und für potentielle Anbieter letztlich verbindlich festgelegt, dass es sich bei der Analyseplattform um eine auf dem Markt vertriebene Standardsoftware handeln muss, die unmittelbar eingesetzt werden kann. Diese muss für eine Mehrzahl von Kunden am Markt verfügbar sein – und nicht eigens erst für den Auftraggeber entwickelt werden. Für die Durchführung des Vergabeverfahrens wurde eine gemeinsame Bewertungskommission mit Vertretern des BMI sowie des Bayerischen Landeskriminalamts gebildet. Das ausgeschriebene Vertragskonstrukt wurde mit dem Bund extra so gewählt und abgestimmt, dass sowohl der sofortige Einsatz der Plattform in Bayern als auch der nachfolgende Einsatz der Bundes-VeRA möglich ist (Mantelrahmenvertrag mit jeweiligen EVBIT-Systemverträgen). Die gemeinsame Verwendung der Bundes-VeRA würde nicht nur den Datenaustausch und die Zusammenarbeit in bundesweiten Ermittlungskomplexen erheblich erleichtern, sie wäre schlicht auch finanziell deutlich günstiger.

Im Januar 2021 erfolgte in Abstimmung mit dem Zentralprogramm Polizei 20/20 die Veröffentlichung der europaweiten Ausschreibung im EU-Amtsblatt
Insgesamt 13 interessierte Unternehmen haben Teilnahmeanträge mit entsprechenden Unterlagen zur Eignungsprüfung eingereicht. Drei Bewerber erfüllten die Mindestanforderungen an die Eignung. Die anderen Bewerber konnten wegen fehlender oder nicht ausreichender Referenzen für die weiteren Vergabeschritte nicht berücksichtigt werden. Die drei Bewerber wurden zur Abgabe eines Erstangebots aufgefordert. Alle drei Bewerber reichten verhandlungsfähige, indikative Erstangebote ein.

Die drei Bewerber wurden von der gemeinsamen Bewertungskommission des Zentralprogramms Polizei 20/20 und des Bayerischen Landeskriminalamtes im weiteren Fortgang für das Verhandlungsverfahren eingeladen. Nach den ersten Verhandlungen wurden die drei Bewerber im September 2021 zur Abgabe eines verbindlichen Folgeangebots aufgefordert. Ein Bewerber teilte mit, dass er sich gezwungen sehe, von einer Angebotsstellung abzusehen. Die beiden verbliebenen Bewerber übermittelten jeweils Folgeangebote. Einer der beiden verbliebenen Bewerber teilte wenige Tage später mit, dass er zum Zeitpunkt der

Angebotsabgabe mehrere A-Kriterien noch nicht erfüllen könne. Er musste sein Folgeangebot schließlich zurückziehen.

Als Bewerber übrig blieb alleine die Firma Palantir Technologies GmbH. Die hypothetische Prüfung der verbindlichen Folgeangebote bestätigte darüber hinaus die Wirtschaftlichkeit des Angebots Firma Palantir Technologies GmbH. Nach abschließenden Verhandlungen übermittelte die Firma Palantir Technologies GmbH ihr finales Angebot, welches nach materieller und formeller Prüfung den Zuschlag erhielt.

Wir sind der Überzeugung, dass wir mit der Firma Palantir Technologies GmbH nicht nur eine leistungsstarke Firma ausgewählt haben, die alle Ausschreibungskriterien erfüllt.
Nach unseren bisherigen Erfahrungen im Projektverlauf (Anbindung der Quellsysteme, Test der fachlichen Funktionalitäten) sind wir vielmehr auch der Überzeugung, dass die aktuell bestmögliche verfügbare Software für eine polizeiliche Recherche- und Analyseplattform ausgewählt wurde.

gez.
Teufele

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 C

Dr. Roland Wagner

Dr. Roland Wagner c/o Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz, D-65185 Wiesbaden

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

Antrag der CDU/CSU-Bundestagsfraktion: „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Inneren und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ (20/9495), Anhörung des Ausschusses für Inneres und Heimat am 22. April 2024

Wiesbaden, 17. April 2024

Sehr geehrte Damen und Herren Abgeordnete,

für die Einladung, zum Antrag 20/9495 „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Inneren und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren“ vor dem Ausschuss für Inneres und Heimat des Deutschen Bundestages Stellung zu nehmen, darf ich mich sehr bedanken.

In dienstlicher Funktion bin ich als Landespolizeivizepräsident zuständig für die Sicherheit und den Schutz der etwas mehr als sechs Millionen hessischen Bürgerinnen und Bürger. Um dies zu gewährleisten, verrichten gut 20.000 Mitarbeiterinnen und Mitarbeiter tagtäglich Ihren zunehmend komplexer werdenden Dienst. Hierbei muss die Polizei vor allem in Zeiten der Digitalisierung und Globalisierung in der Lage sein, die exponentiell steigenden Datenmengen schnell und gezielt analysieren zu können, um regionale und überregionale Tat- und Täterzusammenhänge zu erkennen. Denn

es zeigt sich leider vermehrt: Es sind die kleinen Details, die oft den Unterschied zwischen einer verhinderten und einer vollendeten Tat ausmachen.

Zum Antrag der CDU/CSU-Bundestagsfraktion: „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Inneren und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren" – nehme ich wie folgt Stellung:

Vorbemerkung/Grundsätzliches

Einen ersten Grundpfeiler der Historie zum Thema polizeilicher Analysekompetenz stellt die Innenministerkonferenz im Jahr 2016 dar. Im Zuge dieser Innenministerkonferenz haben am 30. November 2016 die Innenminister der Länder sowie der damalige Bundesinnenminister die Saarbrücker Agenda unterzeichnet. Sie beschreibt die Neuausrichtung der Informationsarchitektur der Polizeien des Bundes und der Länder. Wesentliche Leitlinien waren dabei:

1. Jede Polizistin und jeder Polizist hat nach Maßgabe der rechtlichen Rahmenbedingungen jederzeit und überall Zugriff auf diejenigen Informationen, welche für ihre/seine Aufgabenerfüllung erforderlich sind.
2. Die zukünftige IT der Polizei ist einfach und anwenderfreundlich. Sie wird kontinuierlich dem jeweiligen Stand der Technik und den Anforderungen der IT-Sicherheit angepasst.
3. Polizeiliche IT-Angebote, die Bund und Länder gleichermaßen betreffen können, werden nur einmal entwickelt und stehen den Bedarfsträgern in den Ländern und im Bund zur Verfügung. Dadurch können Anforderungen aufgrund aktueller Entwicklungen zeitnah, flexibel und zuverlässig umgesetzt werden.
4. Die Grundlage für eine digitale, medienbruchfreie Vernetzung der Polizei mit ihren nationalen und internationalen Partnern wird geschaffen.

Anlass war die sich weltweit immer schneller ändernde Sicherheitslage. Denn die zunehmende digitale Vernetzung und Transformation unserer Gesellschaft stellten uns bereits damals vor neue sicherheitspolitische Herausforderungen. Die Geschwindigkeit der Veränderung hat sich seitdem noch einmal deutlich erhöht.

Die vernetzte Welt ermöglicht Kriminalität in einer neuen Dimension, über Grenzen hinweg und jederzeit. Man erkannte bereits damals die defizitäre Informationsarchitektur der Polizei und verständigte sich ausdrücklich auf eine

zukünftige IT der Polizei, welche kontinuierlich an den Stand der Technik, die Anforderungen der IT-Sicherheit sowie den Datenschutz angepasst wird, um die Polizistinnen und Polizisten in die Lage zu versetzen, auf diejenigen Informationen zugreifen zu können, die sie für ihre Aufgabenerfüllung dringend benötigen.

Nur kurze Zeit später, am 19. Dezember 2016, steuerte ein islamistischer Terrorist einen Sattelzug in eine Menschenmenge auf dem Berliner Breitscheidplatz. Er tötete 13 Menschen und verletzte weitere 67. Sie alle waren und sind Bürgerinnen und Bürger, die zuvor auf dem Weihnachtsmarkt zusammen mit Freunden und Familien die vorweihnachtliche Zeit genossen haben. Anis Amri war den Sicherheitsbehörden bekannt. Es gab mehrere Informationen aus unterschiedlichen Datenquellen, aber niemand konnte die Zusammenhänge erkennen.

Dieser und viele nachfolgende Anschläge wie in Halle auf eine Synagoge, beim Rosenmontagsumzug in Volkmarsen, der Terrorakt in Hanau oder die Umsturzpläne der Reichsbürgerszene, um nur einige traurige Beispiele zu nennen, stellen die Sicherheitsbehörden seitdem vor große Herausforderungen – mit deutlichem Einfluss auf das Sicherheitsgefühl der Bevölkerung.

Einher gehen der starke und wiederum schnelle gesellschaftliche Wandel, auch aufgrund steigender Radikalisierungsbereitschaft. Durch den Ukraine-Krieg und vor allem durch den Nahost-Konflikt hat sich die Sicherheitslage jüngst weiter verschärft. Die Wahrscheinlichkeit von Terroranschlägen hat sich nochmals deutlich erhöht.

Zentrales Ziel / Rechtsstaatlicher Auftrag

Dies alles verdeutlicht aus polizeilicher Sicht: Die Gefahr besteht nicht nur in ferner Zukunft, sie besteht nicht nur abstrakt. Sie kann sich vielmehr jederzeit konkretisieren. Angesichts dessen wird deutlich, wie wichtig es ist, unsere Innere Sicherheit zu stärken, um unsere Bevölkerung vor schwerwiegenden Gefahren zu schützen. Unser wesentliches Ziel, der Kern der Aufgaben unserer Sicherheitsbehörden ist es, Straftaten und Anschläge nicht nur zu verfolgen und aufzuklären, sondern möglichst vor der Tat einzuschreiten; wir wollen Gefahren abwehren, wir wollen die Menschen schützen bevor sich ein Anschlag oder eine andere Gefahrenlage realisiert.

Zentrale Frage: Einzeltäter vs. Täternetzwerk

Dabei hat sich spätestens seit dem Anschlag in den USA am 11. September 2001 und durch die schrecklichen Taten des NSU in Deutschland eine Frage – und vor allem die schnelle und zielsichere Antwort darauf – als wesentlich für den Erfolg oder Misserfolg unserer Bemühungen herausgestellt: Haben es die Sicherheitsbehörden mit Einzeltätern oder mit Täternetzwerken zu tun?

Dies zu erkennen und aus der Erkenntnis schnell und zielgerichtet die richtigen Maßnahmen abzuleiten, macht den entscheidenden Unterschied bei der Gefahrenabwehr aus. Insbesondere bei der Bekämpfung des Terrorismus, des Extremismus, aber auch bei der Bekämpfung der Schweren und der Organisierten Kriminalität wird die schnelle und umfassende Analyse eines Tatgeschehens zur zentralen Bedingung erfolgreicher Polizeiarbeit. Gerade hier sind unsere höchsten Rechtsgüter durch skrupelloses, oftmals menschenverachtendes Vorgehen in erheblichem Maße gefährdet. Dabei ist Zeit der entscheidende Faktor.

Dem Faktor der beschränkten Zeit stehen in der Regel gigantische Datenmengen gegenüber, die ausgewertet und miteinander in Verbindung gebracht werden müssen, um die handelnden Personen zu identifizieren, sie von der Tatausführung abzubringen und so Gefahren für die Bürgerinnen und Bürger abzuwehren.

Eine händische Auswertung der entstehenden Datenmengen ist längst nicht mehr möglich: Im Bereich der Bekämpfung des Missbrauchs von Kindern umfasst ein Vorgang im Durchschnitt ein Datenvolumen von 3,2 TB.

Ein Vorgang mit 3,2 TB entspricht etwas mehr als 5160 CD-Roms oder circa 745 DVDs. Den – natürlich rein rechnerischen – Vergleich mit Papierakten können wir indes bereits nicht mehr vornehmen. Mediendateien wie Bilder, Videos, Grafiken, Tonaufnahmen und dergleichen liegen darüber hinaus in unzähligen Formaten vor. Hinzu kommen spezifische Datenformate, die mit der hochfrequenten Nutzung von Smartphones, Tablets, Laptops und dergleichen einhergehen.

In einer einzelnen Datei in diesen Mengen könnte der Hinweis auf einen aktuellen Gefahrenüberhang und damit auf einen laufenden Missbrauch eines Kindes enthalten sein. Wenn wir den oben formulierten Anspruch der Gefahrenabwehrbehörden ernst nehmen, zeigt dies die dringende Notwendigkeit der schnellen und umfassenden

Datenanalyse, der – und das möchte ich an dieser Stelle betonen – ohnehin vorhandenen polizeilichen Datenbestände. Denn es geht bei der in Rede stehenden Analysefähigkeit nicht um Datengewinnung, sondern in erster Linie um die Auswertung bereits vorliegender Daten.

Das Grundproblem aller Sicherheitsbehörden ist jedoch, dass diese polizeilichen Datenbestände in einzelnen polizeilichen Datentöpfen separiert gespeichert sind. Es handelt sich um einzelne, teils historisch gewachsene, nicht originär verknüpfte Datensilos. Jedes dieser Silos muss manuell einzeln betrachtet werden, um dann zu versuchen, die gewonnenen Informationen miteinander zu vergleichen. Die entscheidenden Erkenntnisse aus diesen Daten sind also nicht schnell verfügbar und auch von Menschen auf Grund der Menge und Komplexität nicht mehr verarbeitbar.

Es ist daher mehr denn je dringend geboten, unsere polizeilichen Analyse- und Auswertestellen, unsere Ermittlerinnen und Ermittler personell, organisatorisch und insbesondere technisch zu stärken. Anders ist der Umgang mit derartigen Datenmengen nicht mehr möglich.

In Hessen erfolgte 2017 die Einführung der Auswerte- und Analyseplattform hessenDATA, mit der wir unmittelbar auf die Anschläge in Berlin, in Würzburg und bei unseren europäischen Nachbarn reagiert haben. Wir begegnen damit aber auch unseren eigenen Defiziten, die wir in der Bekämpfung des Terrorismus in der Vergangenheit ausgemacht haben. Dies gilt allen voran für die Geschehnisse um den Nationalsozialistischen Untergrund: Grundlage polizeilicher Entscheidungen muss immer eine sorgfältige und umsichtige Beurteilung der Lage sein. Je schlechter die Informationslage, umso höher das Risiko fehlerhafter Entscheidungen.

Es ist meine tiefe Überzeugung, dass wir unsere Sicherheitsbehörden befähigen müssen, gute Entscheidungen zu treffen. Entscheidungen, die im Sinne der Sicherheit unserer Bürgerinnen und Bürger sind und welche die Handlungsfähigkeit unserer Polizistinnen und Polizisten sicherstellen. Liegen der Polizei nicht die relevanten Informationen vor oder – noch fataler – kann die Polizei mit den ihr zur Verfügung stehenden Daten nicht richtig umgehen, ist eben diese Handlungsfähigkeit maßgeblich eingeschränkt. Im schlimmsten Fall können dann Anschläge oder schwere Straftaten nicht rechtzeitig verhindert werden. Wie bereits dargelegt, ist es elementar wichtig, schnell zu erkennen, ob Täter allein agieren oder ob sie Teil einer organisierten

kriminellen Gruppierung sind, ob und welche Sympathisanten, Unterstützer oder Mittäter im Umfeld zu finden sind und welche Gefahren wiederum von ihnen ausgehen. Die Bestätigung einer Einzeltätertheorie oder deren Widerlegung ist dabei in den letzten Jahren zu einem der höchsten Ansprüche an die Polizei geworden. Zu erkennen, ob ein Anschlag bevorsteht, ob ein laufender Angriff tatsächlich beendet wurde oder ob es weitere Ziele gibt, kann letztlich von einer einzigen Information abhängen, die der Polizei zwar möglicherweise vorliegt, aber eben auch erkannt und interpretiert werden muss.

Die folgenden Beispiele verdeutlichen, welche Relevanz das Instrument hessenDATA für die Hessische Polizei entfaltet hat. Sie sind exemplarisch für die verschiedenen Dimensionen und Aspekte polizeilicher Gefahrenabwehr zu verstehen. Gemeinsam führen sie klar vor Augen, wie wichtig diese Möglichkeit der Datenanalyse ist.

Konkrete Fallbeispiele

1. **Anschlagsverhinderung Eschwege**

Im Rahmen der internationalen Zusammenarbeit wurde das Polizeipräsidium Nordhessen durch das BKA im November 2017 über die Vorbereitungen eines Anschlags informiert. Die Informationen stammten aus den Posts eines Facebook-Profils eines 17-Jährigen aus Eschwege. Erste Ermittlungen in Social Media erhärteten den Tatverdacht: Der Eschweger beschäftigte sich seit 2017 mit dem IS und sympathisierte seitdem mit dessen Ideologie.

Die im Anschluss beschlagnahmten 25 Social Media Accounts wiesen einen umgerechneten Umfang von ca. 100.000 DIN A4-Seiten bzw. 150 Aktenordner auf. Fünf Ermittlerinnen und Ermittlern und zwei Dolmetschern gelang es mit Hilfe der Analyseplattform hessenDATA innerhalb von drei Tagen, die Informationen zu strukturieren und die relevanten Informationen zusammenzustellen: Die große Faszination für den sogenannten Islamischen Staat und für dessen menschenverachtende Ideologie sowie die Überzeugung, der Jihad sei ein geeignetes Mittel im Kampf gegen Anders- oder Nichtgläubige, spiegelten sich in den fast 250.000 Chatbeiträgen wider. Weitere Brisanz erfuhr der Fall durch Informationen über

Kontakte zu einem britischen Gefährder und erste Probezündungen von Sprengkörpern.

In einer sofort veranlassten Durchsuchungsmaßnahme konnten innerhalb kürzester Zeit ein zur Veröffentlichung bestimmtes Bekennervideo und Sprengstoff sichergestellt werden. In der Beschuldigtenvernehmung gestand der Jugendliche die Anschlagsabsichten. Durch einen Kontakt im Irak sollte demnach dem Jugendlichen eine Sprengstoffweste übergeben werden, die dann im direkten Anschluss an einer vorgegebenen Örtlichkeit gezündet werden sollte.

2. Länderübergreifende Ermittlungen zu einem pädokriminellen Netzwerk

Der Polizei in Nordrhein-Westfalen (NW) gelang es, ein Netzwerk aus Pädokriminellen aufzudecken, der sogenannte Bergisch-Gladbach-Komplex. Die Maßnahmen der Ermittlerinnen und Ermittler führten dabei auch auf die Spur eines hessischen Mittäters. Gegen ihn und einen Haupttäter aus NW konnte der Verdacht des gemeinschaftlichen sexuellen Missbrauchs eines Kindes begründet werden. Daraufhin wurde seitens der Hessischen Polizei eine besondere Aufbauorganisation ins Leben gerufen, um weitere fortwährende Realmissbräuche zu verhindern. Ein exakter Zeitpunkt konnte jedoch von dem Kind nicht benannt werden und die Täter schwiegen zu den Vorwürfen.

Im Verlauf der Ermittlungen entschlossen sich die Beamtinnen und Beamten in Hessen zu einer Analyse der Daten von insgesamt 61 Asservaten mit mehreren Millionen Datensätzen mithilfe der Analyseplattform hessenDATA. Ziel war die Verhinderung weiterer Missbrauchstaten. Die Analyse erbrachte zunächst folgendes Ergebnis:

Beide Täter hielten sich zur gleichen Zeit in einem gleichnamigen (Name: Spain) WLAN-Bereich auf. Mithilfe der Auswertung von Geodaten in den Metadaten der zur fraglichen Zeit aufgenommenen Bilder konnte der WLAN-Bereich auf der Insel Mallorca in Spanien lokalisiert werden. Weitere darauf basierende Ermittlungen (Emails, Hotelbuchungen) bestätigten den gemeinsamen Aufenthalt der beiden Haupttäter auf der spanischen Insel und den Missbrauch des Schutzbefohlenen.

Die Analyse der Daten führte zu weiteren Ermittlungserfolgen: Es konnte erstens der Nachweis mehrerer Missbrauchstaten zum Nachteil von Kindern, die von mehreren Tätern gemeinschaftlich begangen wurden, erbracht werden. Zweitens konnte der Verdacht wegen des sexuellen Missbrauchs von weiteren Kindern im Alter von zwei bis elf Jahren begründet werden. Darüber hinaus wurde drittens bekannt, dass einem Täter ca. drei Monate zuvor ein 4-jähriges männliches Pflegekind anvertraut wurde. Die Maßnahmen mündeten viertens in einem weiteren Fall des sexuellen Missbrauchs eines Kindes, bei dem zur Tatbegehung die gefährliche – auch als Vergewaltigungsdroge bekannte – Substanz GBL eingesetzt wurde. Ein fünfter Ermittlungszweig führte zur Rettung eines einjährigen Pflegekindes aus den Händen eines weiteren Sexualstraftäters, welches ihm zwei Wochen zuvor anvertraut wurde.

Ohne die Nutzung von hessenDATA hätte die entscheidende Information über den Aufenthalt zur gleichen Zeit innerhalb eines WLAN-Netzes beider Hauptbeschuldigter nicht in kürzester Zeit erlangt werden können. Ohne die Nutzung von hessenDATA wären die weiteren Ermittlungen nicht in der Weise und in der Zeit herangereift, dass in letzter Konsequenz Missbrauchshandlungen verhindert wurden. Die Kinder hätten nicht schnellstmöglich aus der Hand ihrer Peiniger befreit werden können.

Die Beispiele könnten problemlos um eine Vielzahl weiterer ergänzt werden. An ihnen wird der Nutzen und die Bedeutung der Analysefähigkeit deutlich. Fachlich sind sich hierin alle Länder- und die Bundesbehörden einig.

Datenschutzrechtliche Aspekte und IT-Sicherheit

Bereits im Jahr 2018 entwickelte das Land Hessen auf Anregung und mit Unterstützung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit den §25a HSOG als spezialgesetzliche Regelung für die Automatisierte Anwendung zur Datenanalyse.

Die Norm ermächtigt die Hessische Polizei, in begründeten Einzelfällen zur Abwehr konkreter Gefahren für hochrangige Rechtsgüter die bereits vorhandenen polizeilichen Daten automatisiert zu analysieren, die dringend zur ganzheitlichen Beurteilung der Lage benötigt werden. Damit hat Hessen ein rechtliches Fundament für den ermittlungs- und auswertungsunterstützenden Einsatz moderner Technologie

geschaffen. Das Bundesverfassungsgericht hat mit Urteil vom 16.02.2023 (Az.: 1 BvR 1547/19, 1 BvR 2634/20) auf Grundlage des § 25a HSOG für Rechtsklarheit gesorgt und festgestellt, dass der Einsatz einer automatisierten Datenanalyse oder -auswertung grundsätzlich zulässig ist. Der hessische Gesetzgeber hat die Vorgaben, die das Gericht hierfür gemacht hat, unmittelbar aufgenommen und mit einer Novelle umgesetzt.

Selbstredend sind höchste Standards in Sachen IT-Sicherheit und Datenschutz notwendig. Moderner Datenschutz vollzieht sich in der Nutzung der Plattform selbst, bei jedem Nutzer, an jedem Tag und bei jedem Einsatz.

Dies bestätigend, wurde im Jahr 2023 durch das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) eine umfangreiche Quellcode-Prüfung des bayerischen Systems durchgeführt. Diese ergab, dass bezüglich des Systems keine Schwachstellen identifiziert werden konnten, die einen unzulässigen Abfluss von Daten unter Umgehung von Zugriffsbeschränkungen oder einen unautorisierten Zugriff von außen ermöglichen.

Europaweites Vergabeverfahren

Bund und Länder hatten sich zudem auf eine gemeinsame Beschaffung verständigt. Bereits im Jahr 2020 wurde durch den Verwaltungsrat des Polizei-IT-Fonds beschlossen, dass Bayern eine Öffnungs- und Nachnutzungsklausel in die Ausschreibung des Projekts „VeRA“ aufnimmt. Nach Bedarfsabfrage wurde Anfang des Jahres 2021 die Ausschreibung europaweit veröffentlicht und im März 2022 der Zuschlag an eine Firma erteilt. Im Ergebnis konnte nur ein Anbieter den Anforderungen gerecht werden.

Fazit

Moderne Kriminalitätsbekämpfung und höchste Ansprüche an den Datenschutz setzen den Einsatz moderner Technologie voraus, um den bestmöglichen Schutz der Bevölkerung zu ermöglichen.

Unsere Polizei muss in die Lage versetzt werden, zur Abwehr von Gefahren für höchste Rechtsgüter die eigenen Datenbestände schnell und effizient zu sichten, um auf dieser Grundlage die richtigen polizeilichen Entscheidungen treffen zu können. Darauf haben die Menschen in Hessen und Deutschland einen Anspruch. Sie zu schützen ist unsere Pflicht.

Die Analyseplattform „VeRA" sollte dabei ein wesentlicher Baustein der gemeinsamen Sicherheitsarchitektur der Länder und des Bundes unter dem Dach von P20 werden.

Eine wesentliche Leitlinie der Saarbrücker Agenda war und ist, jeder Polizistin und jedem Polizisten die Daten zur Verfügung zu stellen, die für die polizeiliche Aufgabenerfüllung benötigt werden. Dies wird in Hessen, Nordrhein-Westfalen und Bayern durch die Einführung einer Analyseplattform sichergestellt.

Die fachliche Lücke an Analysefähigkeiten in den Polizeien der Länder und des Bundes, die durch ein Fehlen eines solches Analysewerkzeugs entsteht, ist groß und gefährdet ganz aktuell die Sicherheit der Bürgerinnen und Bürger.

Das Streben nach digitaler Souveränität ist wichtig, nach hiesiger Einschätzung perspektivisch alternativlos und Teil der Digitalstrategie der hessischen Polizei. Dies bedeutet jedoch ausdrücklich nicht, zwingend erforderliche Technologien nicht zu nutzen, wenn sie derzeit von deutschen Firmen nicht geliefert werden können. Ein gegenwärtiges Zuwarten auf eine mögliche Entwicklung entsprechender Analysefähigkeiten ist aufgrund der bestehenden Herausforderungen und der Gefährdungslage fachlich keine Alternative.

Im Ergebnis ist es aufgrund des dargestellten Mehrwertes vielmehr fachlich dringend notwendig, die Polizeien der Länder sowie des Bundes unmittelbar mit einer Analyseplattform zu befähigen und die Handlungsfähigkeit unserer Sicherheitsbehörden bestmöglich auszubauen.

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).

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 E

Bundesverband der Deutschen
Sicherheits- und Verteidigungsindustrie e.V.

Dr. Hans Christoph Atzpodien, Hauptgeschäftsführer BDSV e.V., Berlin

Stellungnahme für die Anhörung des Innenausschusses des Deutschen Bundestages zum Projekt „VeRA“ am 22.04.2024

Für die beteiligten Mitglieder des Bundesverbandes der Deutschen Sicherheits- und Verteidigungsindustrie e.V. Berlin, nehme ich wie folgt Stellung:

I. Vorbemerkung

1. Der Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V. (BDSV) umfasst derzeit 218 Mitgliedsunternehmen, denen gemeinsam ist, dass sie Ausrüster staatlicher Sicherheitsorganisationen sind, sei es von Streitkräften oder von Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Unsere Mitgliedsunternehmen erfüllen darüber hinaus die satzungsmäßige Anforderung, wonach sie über sicherheits- oder verteidigungsindustrielle bzw. damit zusammenhängende digitale Wertschöpfung in Deutschland verfügen müssen. Ausländische Unternehmen oder solche mit ihrem Hauptsitz im Ausland können ebenfalls Mitgliedsunternehmen des BDSV sein, sofern sie die o.g. Wertschöpfungsvoraussetzung erfüllen. Die Fa. Palantir war bis zum 31.12.2023 Mitglied des BDSV, ist jedoch aus bei uns nicht bekannten Gründen per Jahresende 2023 aus dem BDSV ausgetreten, so dass wir bezogen auf die Fa. Palantir keiner Interessenbindung unterliegen.

2. Der BDSV kann an dieser Stelle auch deshalb umso überzeugender als Interessenvertretung deutscher digitaler Kompetenzen auftreten, weil es aus unserer Sicht ein klares Ziel der Bundesregierung sein muss, gemeinsam mit der darauf spezialisierten Industrie gerade unter den gegenwärtigen geopolitischen Rahmenbedingungen die technologische Souveränität in wesentlichen Bereichen der staatlichen Sicherheit zu gewährleisten. Dies gilt für alle einschlägigen Bereiche von der Aufbereitung, Speicherung und hochsicheren Übertragung von Daten bis hin zur Analyse großer und kleiner Datenmengen in strukturierter und unstrukturierter Form und aller Formate, angereichert durch modernste Verfahren aus den Bereichen Kryptologie, Künstlicher Intelligenz etc. In diesem Zusammenhang sei daran erinnert, dass gerade die deutschen industriellen Kompetenzen im Bereich Kryptologie und sicherheitsbezogener Künstlicher Intelligenz zu den sog. „Schlüssel-technologien“ gehören, die das von der Bundesregierung am 12.02.2020 verabschiedete „Strategiepapier zur Stärkung der Sicherheits- und Verteidigungsindustrie“ als nationale Souveränitätstechnologien im Sinne von Art 346 AEUV eingestuft hat. Auch dieses Strategiepapier gebietet eine nationale Vergabe von Aufträgen, wenn diese die Beschaffung entsprechender Schlüsseltechnologien für unsere staatlichen Sicherheitsorgane beinhalten. Die derzeit laufende Aktualisierung dieses Strategiepapiers durch die Ressorts BMWK, BMVg und BMI wird im Zweifel sogar noch zu einer Verstärkung der nationalen Bedeutung von Schlüsseltechnologien führen, weil dies wiederum der geopolitischen Lage und den entsprechenden Ableitungen aus der Nationalen Sicherheitsstrategie geschuldet ist. Würde man entgegen diesen strategischen „Pflöcken“ die bestehenden deutschen Kompetenzen in wesentlichen

Bereichen der digitalen Souveränität nicht honorieren, sondern sich stattdessen US-amerikanischen Herstellern anzuvertrauen, wäre dies als geradezu „strategievergessen“ einzustufen.

3. Dies gilt umso mehr, als in Deutschland die Kompetenzen für eine nationale, den Interessen digitaler und technologischer Souveränität genügende Lösung auf Seiten der von uns vertretenen Industrie eindeutig bestehen.

II. Randbedingungen und Gründe für eine nationale Lösung zur Datenanalyse

1. Es gibt nationale Lösungen, welche für andere Bereiche bereits unter Vertrag sind oder zumindest als Projektskizze existieren. Im Verhältnis zu den langlaufenden und wesentlich teureren Projekten der Fa. Palantir ist der vorgeschobene Grund der „Preis-Realisierungszeit“ kein tragfähiges Argument, sondern vielmehr ein weiteres und von Palantir seit Jahren im europäischen Markt vehement platziertes „Verkaufskonzept“.

2. Da – wie bereits erwähnt - die vorliegende Stellungnahme nicht die wettbewerblichen Interessen der Fa. Palantir berücksichtigen muss, können insoweit die Fakten in Bezug auf das Palantir-Produkt „Gotham“ klar benannt werden: „Gotham“ ist eben keine sogenannte „plug-and-play-Solution, also ein Produkt, das unmittelbar nach Kauf vollumfänglich technologisch, datenschutz- und prozesskonform sowie kundenspezifisch passend zur Verfügung steht. Bei allen Projekten der Fa. Palantir in Deutschland (siehe Bundesländer NRW, Hessen, Bayern) handelt es sich um langjährig laufende Entwicklungs- und Anpassungsprojekte, die bereits in der „Bauphase“ durch erhebliche Preissteigerungen gekennzeichnet sind. Hierzu können durch eine simple Internetrecherche („Palantir Kosten“) umfangreiche Informationen gesichtet werden. Insbesondere das Land NRW mit dem dortigen Palantir-Projekt „DAR“ ist ein Beispiel für ein typisches, kostenintensives und intransparent geführtes mehrjähriges Einführungsprojekt. Die fehlenden polizeirechtlichen und datenschutzrechtlichen Anspruchsgrundlagen bilden eine weitere Problematik. Hierzu ist auf die einschlägigen und hinlänglich bekannten Verfassungs-beschwerden zu verweisen. Das Argument, dass mit der Palantir-Lösung „Gotham“ eine sofort einsatzfähige Software zur Verfügung stehen würde, ist demnach eher ein Marketing- und Verkaufsargument und entspricht nicht den Realitäten in den langjährigen Projekten der drei vorgenannten Bundesländer. In Bayern ist man auch Jahre nach der Anschaffung von „VeRA“ noch in der Entwicklungs- und Testphase. Während dieser Phase wurden jedoch jährlich fünf Millionen Euro für nicht im Einsatz befindliche Lizenzen an die Fa. Palantir gezahlt. International ist dies ebenfalls der Fall. Unter anderem aus diesem Grund wurde die Palantir-Lösung bei EUROPOL, aber auch bei vielen weiteren internationale Behörden, wieder gekündigt. Frankreich hat sich vor einigen Monaten komplett von Palantir losgesagt und setzt auf nationale Lösungen.

3. Die wesentlichen Gründe dafür, nochmals Zeit und Geld in einem überschaubaren Rahmen aufzuwenden, um eine nachhaltig tragfähige industrielle und zugleich nationale Umsetzungsmöglichkeit für das Projekt „VeRA“ auf Bundesebene zu schaffen, liegen aus unserer Sicht in folgenden Aspekten:

a) Nationale Lösungen mit einem offenen Plattformansatz, auf Basis von Standardtechnologien, erlauben eine besondere Flexibilität und können je nach Bedarf und Herausforderung angepasst, ergänzt und/oder erweitert werden. Damit können sowohl Behörden im Bereich der Polizeien als auch im Gesamtsystem des militärischen Nachrichtenwesens angesprochen werden; es können dort untereinander fachliche sowie wirtschaftliche Synergieeffekte erzielt werden. Eine Service-Schicht erlaubt die Anbindung der verschiedensten Quellen und Tools, eingebettet in eine hoch-sichere Infrastruktur. Eine Plattform erlaubt auch anderen nationalen Partnern und Unternehmen sowie staatlichen Organisationen weitere Datenquellen und Analysemodule anzubinden und zu integrieren.

b) Es muss im deutschen Interesse liegen, nicht sowohl auf der Länder- wie auch der Bundesebene von einem einzigen Monopolisten Palantir abhängig zu sein. Zwar könnte aus funktionalen Gründen ein Interesse an einer einheitlichen Bund- und Länder-übergreifenden Lösung bestehen; dem müssen allerdings die beim „single sourcing“ üblicherweise anzutreffenden Risiken und Abhängigkeiten gegenübergestellt werden (Kostenrisiken, Risiken des Scheiterns, Risiko einer allmählichen konzeptionellen Abhängigkeit etc.). Hierbei ist auch zu berücksichtigen, dass ein nationaler Anbieter den Transparenzregeln des deutschen öffentlichen Preisrechts unterliegt, während Palantir dies nicht automatisch, sondern nur im Fall einer ausdrücklichen Unterwerfung und Übernahme der Preisrechtsgrundsätze tut. Falls Palantir in Deutschland einen Monopol-Status erreichen würde, wäre Preiserhöhungen Tür und Tor geöffnet.

c) Ein entscheidender Vorteil einer nationalen Lösung besteht in der gesicherten Kontrolle über den Datenfluss (analog zu Frankreich). Es muss ausgeschlossen sein, dass Daten auf Servern in den USA gespeichert werden, d.h. gerade in einem möglichen Krisenfall ein komplett souveräner, unter alleiniger Kontrolle der deutschen Behörden stattfindender Datenzugriff nicht sichergestellt sein mag. Dies wäre im Fall der Beauftragung deutscher Unternehmen anders.

d) Wie aus öffentlich verfügbaren BT-Dokumenten (z.B. Drucksache 20/8390 v. 18.09.2023) hervorzugeht, scheint das Bundesministerium des Innern derzeit für die Umsetzung des Projektes „VeRA“ auf Bundesebene eine behördliche Eigenentwicklung zu präferieren. Solche Eigenentwicklungen sind jedoch zumeist mit Risiken im Bereich der inhaltlichen Umsetzung und der aufzuwendenden Kosten belastet. Daher bietet sich demgegenüber ein privatwirtschaftlich getragener, gleichwohl aber strikt nationaler Ansatz an, um sowohl das Kosten- und Implementierungsrisiko unter Kontrolle zu halten, gleichzeitig aber auch den nationalen Schutzinteressen in vollem Umfang Rechnung zu tragen. Wie langjährige Erfahrungen mit ähnlichen Projekten erwiesen haben, können hoheitliche Souveränitätserfordernisse auch dann gewahrt werden, wenn private Unternehmen an der Projekt-Implementierung beteiligt sind, sofern sie sich dabei entsprechend strengen Geheimschutzanforderungen unterwerfen.

e) Schließlich sei nochmals auf den schon zuvor erwähnten Aspekt des „Strategiepapiers zur Stärkung der Sicherheits- und Verteidigungsindustrie“ vom 12.02.2022 verwiesen (Fundstelle: https://www.bmwk.de/Redaktion/DE/ Downloads/S-T/strategiepapier-

staerkung-sicherits-und-verteidigungsindustrie. pdf?__blob =publicationFile&v=4). In diesem Papier, welches sich im Gefolge der Nationalen Sicherheitsstrategie vom Juni 2023 und der veränderten geopolitischen Herausforderungen aktuell zwischen den zuständigen Ressorts der Bundesregierung in der Überarbeitung befindet, werden die nationalen Technologie-Kompetenzen in den Bereichen Krypto und Künstliche Intelligenz ausdrücklich als nationale Schlüsseltechnologien eingestuft. Dort heißt es: „Die Verfügbarkeit der identifizierten sicherheits- und verteidigungsindustriellen Schlüsseltechnologien ist aus wesentlichem nationalem Sicherheitsinteresse zu gewährleisten." Um dies auch im deutschen Vergaberecht zu konkretisieren, hat die Bundesregierung mittels § 107 Abs. 2 GWB deutlich gemacht, dass „sicherheits- und verteidigungsindustrielle Schlüsseltechnologien" im Fall von Beschaffungen durch die nationalen Sicherheitsbehörden als Fall der Betroffenheit wesentlicher Sicherheitsinteressen nach Artikel 346 AEUV behandelt werden sollen. Dem sollte sich auch das BMI sowie die in der Beauftragung verantwortlichen Bundesländer im Fall „VeRA" verpflichtet fühlen.

III. Fazit der vorliegenden Stellungnahme:

Der BDSV plädiert mit Blick auf die Bearbeitung des Projektes „VeRA" auf Bundesebene für eine stringent nationale Lösung, allerdings nicht auf der Grundlage einer behördlichen Eigenentwicklung, sondern auf der Basis einer nationalen Analyseplattform. nationaler, privater Anbieter mit entsprechendem Track-Record.

Sehr geehrte Ausschuss-Mitglieder, nationale Souveränität bedeutet nicht, alles selbst machen zu müssen, aber es bedeutet, im Zweifel alles selbst machen zu können. Beim Thema Analyseplattform stehen wir gerade an einer Wegscheide, und die Entscheidungen (oder Nicht-Entscheidungen) von heute bestimmen darüber, ob wir morgen souverän handeln können. Bitte setzen Sie sich in diesem Sinne für eine deutsche Lösung ein, und zwar gerade in Zeiten, in denen wir mit Sorge auf eine nächste Präsidentschaft Trumps in den USA blicken.

Hochschule des Bundes
für öffentliche Verwaltung

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 F

POSTANSCHRIFT HS BUND, POSTFACH 40527, 10063 BERLIN

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

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

DATUM Berlin, 17.04.2024

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

Stellungnahme zum Antrag der Fraktion der CDU/CSU

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

BT-Drs. 20/9495

A. Vorbemerkung

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

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

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

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

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

II. Anforderungen an ein Regelungskonzept

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

1. Unzulässige Einsatzweisen

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

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

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

2. Verarbeitung großer Datenmengen und Einsatz Künstlicher Intelligenz

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

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

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

3. Stufensystem der Eingriffsintensität

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

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

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

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

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

4. Differenzierte Eingriffsschwellen

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

5. Prozedurale Flankierungen

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

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

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

6. Regelungstechnische Ausgestaltung

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

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

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

III. Schlussfolgerung

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

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

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

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

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

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

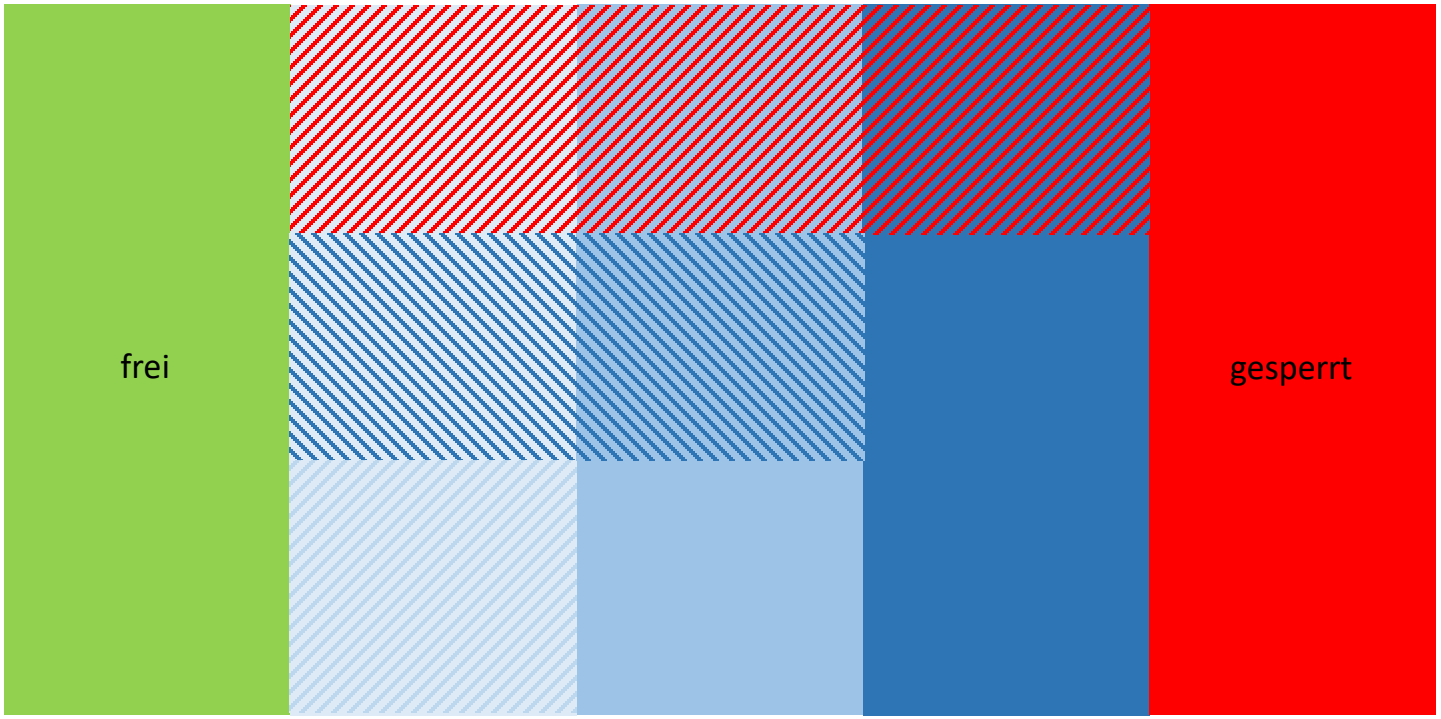
übersichtlichen und hastigen Gesetzgebungsverfahrens[49] und hat erneut eine rechtstechnisch und verfassungsrechtlich angreifbare Norm hervorgebracht.[50] Gegen die von Anfang an umstrittene Regelung zum Data-Mining nach § 23 Abs. 6 PolG NW wurde eine – nach den bisher vom BVerfG entwickelten Maßstäben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

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

(Prof. Dr. Markus Löffelmann)

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

Stufenkonzept automatisierte Datenanalyse



FachG

ES:

4 bes. hoch

3 hoch

2 erheb-lich

EI: 0 npbD 1 leicht 2 mittel 3 schwer 4 bes. schwer

BKAG

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 G

bitkom

Stellungnahme

< April 2024>

Anhörung des Innenausschusses des Deutschen Bundestages zum Projekt „VeRA“ am 22.04.2024

Bitkom nimmt grundsätzlich keine Stellung zu den Angeboten einzelner Mitgliedsunternehmen, um hier Neutralität zu wahren.

Zentrale Herausforderung im Umgang mit großen Datenmengen

- Weltweit beträgt das Datenvolumen etwa 64,2 Zettabyte. 2025 werden es laut Europäischer Kommission bereits 175 Zettabyte sein. Das Verarbeiten großer Datenmengen ist bereits heute eine große Herausforderung für die Sicherheitsbehörden, da der Großteil davon unstrukturierte Daten sind. Allein in der Polizei Niedersachsen sind etwa 7,5 Petabyte Daten gespeichert. Diese Menge an Daten würde etwa 150 Millionen Aktenschränke füllen.

- Durch den weiteren Anstieg an Sensoren, mobilen Endgeräten (Smartphones, Tablets, etc.) sowie den Kapazitäten auf Speichermedien, wird diese Herausforderung weiter steigen. Hinzu kommt, dass sich Kriminalitätsphänomene immer weiter in den digitalen Raum verlagern und Sicherheitsbehörden stärker mit Daten in digitaler Form konfrontiert sind. (z.B. Daten aus Ermittlungen, Anzeigen, Kinderpornographie, Cybercrime usw.) Dies erfordert den Aufbau von weiteren Behördenkompetenzen, u. a. in der digitalen Forensik, Open Source Intelligence (OSINT) und der Analyse.

- Es stellen sich technische Fragen nach Speicherkapazitäten, Rechenkapazitäten sowie geeigneter Software zur Auswertung dieser Daten. Diese Herausforderungen können nur im Dreiklang aus Politik (Rahmensetzung), Behörden (Durchführung) und Wirtschaft (Digitale Kompetenzen und Ressourcen) konstruktiv und kooperativ gelöst werden.

- Eine Vernetzung von Analyse und Auswertung soll Schnelligkeit schaffen und Redundanzen verhindern und muss gleichzeitig mit einem aktiven Wissensmanagementsystem ausgestattet sein. Die eingesetzte Software muss daher große Datensätze strukturiert und nutzerfreundlich bearbeiten können. Dadurch entstehende Datenräume müssen auf gemeinsamen Standards (oder Werten, Technologien, Schnittstellen) basieren und die Transaktion von Daten erlauben und befördern. [1]

- Derzeit sind die Sicherheitsbehörden dazu nur eingeschränkt in der Lage. So sind die Behörden allein am Beispiel der Verfolgung aller Verdachtsfälle im Bereich Geldwäsche durch die Masse an Daten gelähmt, sodass eine Verfolgung nur rudimentär erfolgt, bzw. Erfolge bei der Polizei eher im geringfügigen Bereich liegen. Auch ist die Bearbeitung und Verfolgung eingehender digitaler Anzeigen kaum noch möglich, geschweige denn ein Feedback an die Anzeigenden. Die Folge ist ein zunehmender Verlust von Vertrauen der Bevölkerung in die Fähigkeiten der Sicherheitsbehörden. Die digitale Arbeitsfähigkeit staatlicher Einrichtungen sicherzustellen ist letztlich

Das für Sicherheitsbehörden auszuwertende Datenvolumen steigt stetig. Die meisten Daten sind dabei unstrukturiert. Die Fähigkeit zur vernetzten Analyse & Auswertung ist zentral für das Funktionieren des Staatsgefüges und derzeit nur eingeschränkt möglich.

[1] Herausforderungen der Polizei durch die digitale Transformation | Positionspapier 2023 | Bitkom e. V.

eine Voraussetzung für das Vertrauen der Bürgerinnen und Bürger in staatliche Institutionen.

- Ziel muss die Automatisierung von Verwaltungsprozessen sein, die eine medienbruchfreie Übermittlung von Daten innerhalb der Bundesländer, zwischen den Bundesländern und letztlich bis hin zum Bund ermöglicht. Diese Daten müssen analysiert und die Ergebnisse zeitnah der Justiz zur Einleitung möglicher Strafverfolgungsmaßnahmen bereitgestellt werden können.

- Eine solche Software muss aber nicht nur die Nutzung des Potentials der Datenanalyse für die Polizeiarbeit ausschöpfen, sie muss auch den Erfordernissen des Daten- und Grundrechteschutzes sowie der Informationssicherheit gerecht werden. Der verantwortungsvolle, sichere und rechtmäßige Umgang mit Daten durch Sicherheitsbehörden und eine zeitgemäße gesetzliche Regelung sind die Schlüssel für Innovationen und Vertrauen in eine moderne Polizeiarbeit. Weiterhin sind Souveränitätsaspekte zu berücksichtigen.

Software im Bereich der Sicherheitsbehörden muss grundsätzlich den Erfordernissen des Daten- und Grundrechteschutzes sowie der Informationssicherheit gerecht werden.

Bedeutung digitale Souveränität

- Digitale Souveränität bedeutet nicht Autarkie, sondern unabhängige digitale Selbstbestimmung: Es geht darum, die Wahl zu haben etwa zwischen eigenen Lösungen (z.B. eigenständige Lösungen der Behörden) und denen vertrauensvoller (auch internationaler) Partnerinnen und Partner (marktverfügbar oder als beauftragte Entwicklung).

- Digitale Souveränität ist die Möglichkeit zur digitalen Handlungs- und Gestaltungsfreiheit. Das bedeutet Mitgestaltungs- und Innovationsspielräume zu erhalten. Die Fähigkeit international auf Augenhöhe Schlüsseltechnologien, Geschäftsmodelle und Ökosysteme mitzugestalten, sowohl durch Forschung als auch durch Entwicklung, in der Mitgestaltung internationaler Standards und als Kunde und Partner.[2]

- Aus sicherheitspolitischer Perspektive muss in besonders kritischen Bereichen immer eine Risikoabwägung stattfinden. So ist eine vollständige Neuentwicklung von bereits auf dem (globalen) Markt verfügbaren Lösungen zwar sehr kosten- und zeitintensiv, kann aber nach Abwägung aller Chancen und Risiken einen Mehrwert haben, wenn es um Kernkomponenten im Bereich der nationalen Sicherheit geht. Andererseits lassen sich solche komplexen Systeme immer weniger in Eigenentwicklungen aufbauen oder gar betreiben. Gerade hinsichtlich geeigneter Software sollten neben der Digitalwirtschaft auch innovative Forschungsinstitutionen einbezogen werden, um Zugang zu zukunftsfähigen Lösungen zu erhalten.

- Europa und Deutschland müssen dort technologische Kernkompetenzen weiter ausbauen, wo Expertise, Marktanteile und Innovationskraft vorhanden sind, bzw. in der Zukunft entwickelt werden können. Das umfasst die Fähigkeit, die weltweit bereits bestehenden und neu entstehenden Technologien auf ihre Vertrauenswürdigkeit hin zu bewerten und in die eigenen Produkte, Prozesse, Organisationen und in die Gesellschaft zu integrieren, um dadurch Wertschöpfung zu erzielen und die Wachstums- und Wettbewerbsfähigkeit der deutschen und europäischen Wirtschaft in Kernfeldern abzusichern und auszubauen. Schlüsseltechnologien müssen daher systematisch betrachtet und entwickelt werden, so dass rechtzeitig eigene Kompetenzen in besonders wichtigen Bereichen aufgebaut werden können. Dazu gehört auch der Aufbau und Erhalt eines entsprechenden Anbieterökosystems in Europa in Bereichen, die als Schlüsseltechnologie identifiziert wurden.

Digitale Souveränität bedeutet nicht Autarkie, sondern unabhängige digitale Selbstbestimmung. Dies umfasst die Fähigkeit zwischen vertrauensvollen Partnern zu wählen.

[2] Vgl. auch Bitkom 2020.

Lösungsansätze bei großen Datenmengen

- **Monetäre Herausforderungen meistern:** Die öffentliche Haushaltslage ist angespannt. Notwendige Investitionen sind dadurch schwieriger durchzuführen. Gleichwohl steht der Haushalt gestiegenen Anforderungen gegenüber, u. a. an die Öffentliche Sicherheit und an den Schutz kritischer Infrastrukturen. Digitale Lösungen müssen daher verstärkt Interoperabilität, auf Basis offener Standards, gewährleisten.

- **Personelle Voraussetzungen und Qualifikationen von Behördenpersonal:** Gleichzeitig ändert sich das Aufgabenprofil der Beschäftigten der Sicherheitsbehörden. Sie werden zusätzlich zu ihren Tätigkeiten, zukünftig u. a. stärker mit dem Auswerten großer Datenmengen konfrontiert sein. Die Ausbildung muss daher in diesem Bereich angepasst werden. Es sollten auch andere Möglichkeiten in Betracht gezogen werden: Der Quereinstieg (entsprechend ausgebildeter Personen) oder das Einkaufen von externer Fachexpertise sind Möglichkeiten, diesen Herausforderungen zu begegnen.

- **Management der Sicherheitsbehörden-Landschaft**
  Die föderale Struktur in der Bundesrepublik macht die Koordinierung von Aktivitäten der Sicherheitsbehörden nicht leicht. Gerade, weil insbesondere die Polizeiarbeit in die Zuständigkeit der Länder fällt. Nicht alle Daten stehen allen Beteiligten in Bund und Ländern immer zur Verfügung, sodass bei übergreifenden Kriminalitätsphänomenen zum Teil nicht die richtigen Analysen durchgeführt- und Schlussfolgerungen in Ermittlungsprozessen gezogen werden können. Das gilt sowohl im nationalen Raum (über Grenzen der Bundesländer), als auch im internationalen Raum (über Ländergrenzen). **Eine zentrale Analyse unter den gegebenen Sicherheitsaspekten, könnte einen großen Mehrwert für die Sicherheitsbehörden enthalten. Gleichzeitig könnten Infrastrukturen dadurch effizienter genutzt werden. Bislang ist eine zentrale, länderübergreifende Datenverarbeitung nur eingeschränkt möglich.**

  Dabei ist die Anpassungsfähigkeit und Erweiterbarkeit von IT-Lösungen, unter Einbeziehung der Nutzenden, wichtig. So lassen sich Abhängigkeiten zu einzelnen Anbietern vermeiden.

Eine übergreifende Analysefähigkeit kann großen Mehrwert für die Sicherheitsbehörden bieten.

IT-Lösungen sollten anpassbar und erweiterbar sein, um nicht in Abhängigkeiten zu einzelnen Anbietern zu geraten.

Dabei ist die Orientierung an den Bedürfnissen der Nutzenden essentiell.

Optionen für die Sicherheitsbehörden zum Erhalt relevanter Fähigkeiten

a) Die Erstellung von Eigenlösungen durch die Sicherheitsbehörden

- Grundsätzlich können die Behörden selbst am besten beurteilen, welche Lösungen sie benötigen. Die Erstellung eigener Lösungen kann jedoch dauerhaft erhebliche Personal-, Material- und finanzielle Ressourcen binden und kann unter Umständen deutlich teurer als die Beschaffung marktverfügbarer Lösungen sein, ohne gleichzeitig in Sachen Erprobung und Updates wettbewerbsfähig zu sein.

- Hinzu kommt, dass sich die technologischen Innovationszyklen immer schneller vollziehen. Dies bedingt eine permanente Betreuung technischer und rechtlicher Aspekte, um rechtssichere Lösungen zu erstellen. Dies bedeutet eine starke Bindung von Fachpersonal, welches perspektivisch immer schwerer zu finden sein wird.

- Zu bedenken ist, dass Software nie „zu 100 % fertig“ ist. Sie muss dauerhaft weiterentwickelt und betreut werden, in enger Abstimmung mit relevanten Stakeholdern wie Endnutzenden, Datenschutz- und Informationssicherheitsbeauftragten usw. Personal und Haushaltsmittel müssen also von der Planung über die initiale Entwicklungsphase bis hinein in den Betrieb und die Wartung der Software in auskömmlicher Weise zur Verfügung stehen.

b) Die Erstellung von Innovationslösungen durch die Sicherheitsbehörden mit der Wirtschaft und Wissenschaft

- Die Erstellung von Softwarelösungen im behördlichen Auftrag kann nur gelingen, wenn ausreichende Haushaltsmittel und notwendige Priorisierungen von Projekten in den einzelnen zuständigen Landespolizeien oder im Bund vorliegen.

- Kernherausforderung ist hier, dass Bedarfe, Aufgaben einzelner Polizeien und dazu nötige Ressourcen (Personal, Finanzen, politische Zielsetzung etc.) meist getrennt sind. Es bedarf daher stets einer Koordinierung verschiedener Akteure, was Prozesse in die Länge zieht und Enttäuschungen bei den Nutzenden erzeugt.

- Das Programm P20 (früher P2020) sollte diese Herausforderung lösen, wobei sich die Bundesländer teilweise schwertun, um das Programm mit Impulsen zu beleben. (nötige personelle Faktoren auf Landesebene). Auch bleibt das Programm hinter den Erwartungen zurück. Dabei geht es u.a. um Priorisierungen, wo es unterschiedliche Auffassungen gibt.

- Chancen bestehen durch die Einbeziehung aufgebauter Reallabore, u.a. der GovTechCampus in Berlin.

- Lösungen in Reallaboren lassen sich schneller skalieren. Zur Umsetzung stellen Experimentierklauseln zentrale Bausteine dar, um den Rechtsrahmen innovationsoffen und zukunftsorientiert zu gestalten. Bei der Formulierung von rechtssicheren und innovationsoffenen Experimentierklauseln kann eine Handreichung des Bundesministeriums für Wirtschaft und Klimaschutz helfen.[3] Dabei sollte ein einfacher und transparenter Zugang zum Reallabor für alle relevanten Stakeholder (Sicherheitsvorkehrungen inkl.), u. a. für Industrie, Wissenschaft und andere Teilstreitkräfte vorhanden sein. Dabei darf es zu keinen Wettbewerbsnachteilen kommen, etwa durch die strenge Auslegung von Compliance-Regeln. Ggf. bedarf dies auch der Anpassung von Doktrinen. Es dürfen keine Denkverbote bestehen und die Verantwortlichen sollten die Möglichkeit haben, mit eigenen Mitteln zu wirtschaften.
  Dazu bedarf es eines eindeutigen politischen Mandats für den GB BMI.

- Das Reallabor sollte auch über ausreichende solvente Mittel, z. B. Handgeld, Studienmittel oder weitere niederschwellige Sofortmaßnahmen verfügen. Reallabore sind unter dem HUB-Gedanken zu führen, wobei die Sicherheitsbehörden ihren Bedarf und dazugehörige Lösungen suchen (pull) und diese gemeinsam mit der Industrie oder Wissenschaft, unter Einbezug der Nutzenden, entwickelt. Umgekehrt sollte es jedoch auch möglich sein, dass die Industrie proaktiv Lösungsansätze einbringt. Teststellungen müssen skalierbar sein und stets Klarheit über Zielsetzung, Finanzierung und Betriebszeit, auch über Haushaltsjahre hinweg, sicherstellen.
  Operationelle Feldtests (Praxis) müssen ebenso durchführbar sein, wie digitale Simulationen im AR- und VR-Bereich (Simulation), um wo immer möglich auch eine regulatorische Basis zu schaffen. Es bedarf zudem transparenter Vorgaben zur Evaluation von Ergebnissen, über Skalierungsmöglichkeiten der Innovation nach dem Reallabor, sowie Vorgaben zur Veröffentlichung von Ergebnissen und der Einbindung relevanter Partner. Dabei sollten Unternehmen erarbeitete Lösungen auch weiter vermarkten können. Es sollte aber auch Klarheit darüber herrschen, wer Zugriffs- und Eigentumsrechte auf Daten und Lizenzen, sowie ungenutzte digitale Kapazitäten hält.

Grundsätzlich besteht die Option Lösungen selbst zu erstellen, entwickeln zu lassen oder marktverfügbar zu kaufen.

Dies bedingt einen funktionierenden Marktdialog, und den Zugriff auf ein leistungsfähiges Ökosystem aus Staat-Wirtschaft-Wissenschaft.

Die Faktoren Zeit-Kosten-Personal sind dazu abzuwägen.

[3] Reallabore – Recht flexibel (bmwk.de)

c) Der Einkauf marktverfügbarer Lösungen durch die Sicherheitsbehörden

- Grundsätzlich sollten marktverfügbare Lösungen im Fokus stehen, um doppelte Entwicklungen (das Rad neu erfinden) zu vermeiden und Ressourcen zu sparen. Voraussetzung dazu ist, dass die Anforderungen an Datenschutz, Informationssicherheit, Transparenz, Interoperabilität sowie Gerichtsfestigkeit der Ergebnisse gesichert werden können.

- Unternehmen benötigen dazu relevante Erfahrungen über Bedarfe und Anforderungen im Umgang mit Sicherheitsbehörden.

- Wichtig ist dabei einen „Lock-In" zu vermeiden oder zumindest zu reduzieren. Eine einmalig gekaufte Lösung darf zu keiner dauerhaften Abhängigkeit von einem bestimmten Lieferanten führen.

- Der Kauf marktverfügbarer Lösungen bedingt einen funktionierenden Marktdialog. Der Markt benötigt Kenntnis darüber, welche Fragestellungen für die Sicherheitsbehörden von Relevanz sind, inkl. eines Feedbacks zu eigenen Lösungsansätzen durch die Behörden.

- Dazu genügt es nicht nur den Markt nach Lösungen zur durchsuchen oder durch Roadshows Ideen der Sicherheitsbehörden zu forcieren. Es gilt einen strukturierten Dialogansatz zwischen Staat-Wirtschaft-Wissenschaft zu implementieren, um Bedarfe der Sicherheitsbehörden mit Kapazitäten, Best Practice etc. der Wirtschaft und Wissenschaft abzugleichen.

- Vor dem Hintergrund der digitalen Souveränität gilt es zu priorisieren, welche Schlüsselaspekte national, europäisch oder international bei befreundeten Nationen beschafft werden können. Dies erfordert auch eine leistungsfähige nationale industrielle Basis. Neue Technologien kommen meist aus dem zivilen Bereich. Daher müssen diese unter Achtung geltenden Rechts in Sicherheitsbehörden adaptiert werden können. Dabei gilt es auch, verfügbare Forschungsansätze in die Praxis zu integrieren.

- Insbesondere die Digitalwirtschaft ist auf Effektivität und Effizienz ausgerichtet. Lösungsansätze werden in wenigen Stunden erdacht und in wenigen Wochen umgesetzt. Produkte bzw. Gewerke werden jedoch erst entwickelt, wenn ein skalierbarer Markt (ausreichender Bedarf, gemessen an Finanzvorlumen, Verständnis zu realem Bedarf von Nutzenden etc.) vorhanden ist. Gelingt dies nicht, so werden sich innovative Unternehmen weiterhin dem zivilen Sektor zuwenden.

- Vergabestellen müssen diesem Umstand Rechnung tragen, u.a. im Bereich der Bearbeitungszeiten, aber auch der Form der Ausschreibung. Ggf. existieren sogar Lösungsansätze, die durch zu enge oder unattraktive Ausschreibungsbedingungen nicht zum Tragen kommen.

- Ein Vorschlag zum verbesserten Marktdialog ist die Durchführung von Marktschautagen zu Themen von Interesse im Rahmen vorkommerzieller Beschaffungsverfahren (PCP). Bei PCP „kaufen öffentliche Auftraggeber Research & Development (R & D) von mehreren konkurrierenden Anbietern, um alternative Lösungsansätze zu vergleichen und das beste Preis-Leistungs-Verhältnis zu ermitteln, das der Markt liefern kann, um seinen Bedürfnissen gerecht zu werden. R & D gliedert sich in Phasen (Lösungsdesign, Prototyping, ursprüngliche Entwicklung und Validierung bzw. Tests einer begrenzten Reihe von ersten Produkten), wobei die Anzahl konkurrierender R&D-Anbieter nach jeder R&D-Phase reduziert wird."[4] Dieses Verfahren wird u. a. auch erfolgreich durch die Cyberagentur des Bundes genutzt, wodurch sich hier Erfahrungswerte adaptieren lassen. Wichtig ist dabei, dass mittels veröffentlichter und konkreter Problembeschreibung die Industrie zum Pitch für die (Teil-)Lösung aufgefordert ist.

[4] Pre-Commercial Procurement - European Commission (europa.eu)

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Stephan Ursuleac | Bereichsleiter Verteidigung & Öffentliche Sicherheit
s.ursuleac@bitkom.org

Verantwortliches Bitkom-Gremium

AK Öffentliche Sicherheit

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 H

Christine Skropke

secunet Security Networks AG

Kurfürstenstraße 58

45138 Essen

E-Mail: christine.skropke@secunet.com

Öffentliche Anhörung: Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des BMI bezüglich der polizeilichen Analyse-Software Bundes-VeRA

Montag, 22. April 2024, 14:00h bis 16:00h
Paul-Löbe-Haus, Raum E 800, Konrad-Adenauer-Str. 1, 10557 Berlin

**Sachverständigenstellungnahme von Christine Skropke,
Leiterin Public Affairs bei der secunet Security Networks AG**

Aufklärung zu möglichen finanziellen Interessensverknüpfungen:

Die secunet Security Networks AG war weder im Bereich der Projekte Polizei 2020 noch an der öffentlichen Ausschreibung zur polizeilichen Analyse-Software Bundes-VeRA beteiligt. Aufgrund der neuen Ausgangslage wurde secunet Anfang 2023 eingeladen, seine Expertise im Bereich IT-Sicherheit in die Interessensgemeinschaft NASA (Nationale souveräne Analyseplattform) mit einzubringen. Bei einer möglichen Pilotierung würde secunet einen entsprechenden Anteil im Projekt realisieren.

Gesamtgesellschaftliche Perspektive

1. Die Sicherheit und der Schutz der Bevölkerung gehören zu den Kernaufgaben des Staates. Die dafür zuständigen Behörden sollten mit allen verfügbaren modernen Technologien zur Unterstützung ihrer Arbeit ausgestattet werden können.

Technologische Grundvoraussetzungen

2. Ein Analyse-System für die Arbeit moderner Sicherheitsbehörden muss technologisch offen konzipiert werden, damit auch neue (Zukunfts-) Technologien eingebunden werden können. So kann sichergestellt werden, dass die Bedarfsträger auch langfristig stets über die erforderlichen Fähigkeiten zur bestmöglichen Erfüllung ihres Auftrages verfügen.

3. Nationale hoheitliche Bereiche müssen sicherstellen, dass Daten und Informationen sowie die Kontrolle über den Zugriff auf die Anwendungen stets mit der höchst verfügbaren und vertrauenswürdigen Sicherheitstechnologie vor Sabotage, Spionage und Datenmissbrauch geschützt sind. Die Software allein einmalig auf Sicherheit zu überprüfen, stellt keine ausreichende Vertrauenswürdigkeitsüberprüfung dar. Ebenso unerlässlich ist die Einbettung der Software in sichere Cloud- und Netzwerkinfrastrukturen.

4. Mit Blick auf den bspw. erst kürzlich verabschiedeten AI Act der Europäischen Kommission sind alle aktuellen gesetzlichen regulatorischen Vorgaben in Hard- und Software entsprechend zu erfüllen.

Industriepolitische Perspektive

5. Sicherheitspartnerschaft und Partner der nationalen Sicherheitsbehörden

   Deutschland verfügt über eine weltweit hoch geachtete und anerkannte Forschung im Bereich der Sicherheitstechnologien ebenso wie im Bereich KI – sowohl in der Grundlagenforschung als auch bei der angewandten Forschung. Zahlreiche Inkubatoren, gefördert durch das Bundesministerium für Bildung und Forschung (BMBF), unterstützen jungen kreative Köpfe, aus der Forschung heraus Unternehmen zu gründen.

   Gleichzeitig legen seit Jahren die Bundesregierungen verschiedenster Koalitionen in ihren Strategiepapieren fest, dass die Sicherheits- und Verteidigungsindustrie mit ihren unterschiedlichsten Kompetenzen zu den Schlüsseltechnologien für Deutschland gehören und die Unternehmen dieser Branchen national geschützt und gefördert werden müssen.

   Für ein Unternehmen sind Gründungsförderungen und Kapitalgeber wichtig, aber das wichtigste für die Weiterentwicklung wichtiger technologischer Lösungen und Anwendungen sind Beauftragungen. Nur so kann ein Unternehmen seine Technologien in die praktischen Anwendungen bringen und diese gemeinsam mit den Bedarfsträgern weiterentwickeln. So werden diese Unternehmen gleichzeitig wirtschaftlich stabil und stellen nationale Fähigkeiten hinsichtlich Know-how oder entsprechender Fachkräfte sicher.

   Daraus entstehen dann wichtige nationale oder vielleicht sogar europäische Öko-Systeme, die auch wertvolle Beiträge leisten, wenn es um das Setzen neuer technologischer Standards geht. Technologiehoheit und -vielfalt verhindern die Abhängigkeit von Drittstaaten oder einzelnen Anbietern (Vendor-Lock-in). So kann Deutschland digital souverän werden und bleiben.

Auszug aus der Nationalen Sicherheitsstrategie von 2023

a. „Cybersicherheit ist untrennbar mit unserer digitalen Souveränität verbunden. Dieser Anspruch wird uns bei der gezielten Förderung von Technologien und bei der Weiterentwicklung von Sicherheitsstandards leiten. Die Bundesregierung wird hierfür auch die Zusammenarbeit mit der Industrie in den relevanten internationalen Gremien stärken."

   (Quelle: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland – Nationale Sicherheitsstrategie, 2023, S. 59)

b. „Die Bundesregierung wird überprüfen, bei welchen Schlüsseltechnologien nationale und europäische Fähigkeiten zum Schutz unserer technologischen und digitalen Souveränität nötig sind. Die Bundesregierung wird gezielt Anbieter kritischer Schlüsseltechnologien mit geeigneten Maßnahmen, z. B. durch staatliche Ankeraufträge, unterstützen, um eigene Fähigkeiten zu Forschung und Entwicklung in kritischen Technologien zu erhalten und weiterzuentwickeln."
   (Quelle: Nationale Sicherheitsstrategie, S. 58)

c. „Die Bundesregierung wird die Cybersicherheitsstrategie der Bundesregierung weiterentwickeln und dabei auch die Cybersicherheit der Bundesverwaltung umfassend stärken."
   (Quelle: Nationale Sicherheitsstrategie, S. 61)

Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie (BMWK) von 2020

Strategiepapier zu Schlüsseltechnologien „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie", Bundesministerium für Wirtschaft und Klimaschutz (BMWK), 2020, schreibt die relevanten Technologien (u.a. Krypto) und deren Erhalt in Deutschland vor. Darin enthalten ist nicht nur entsprechende Forschungsförderung, sondern auch der Erhalt der Industrien.

> „Die Verfügbarkeit der identifizierten sicherheits- und verteidigungsindustriellen Schlüsseltechnologien ist aus wesentlichem nationalen Sicherheitsinteresse zu gewährleisten, abhängig von der Einordnung der Technologie gegebenenfalls auch im Rahmen von europäischen/transatlantischen Kooperationen und diesbezüglichen bi- und multilateralen Vereinbarungen."
>
> (Quelle: Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie, 2020, S. 3 mit Grafik)

Ähnliche Aussagen siehe auch:

- Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (BMI)
- Digitalstrategie der Bundesregierung
- Verteidigungspolitische Richtlinien 2023 des Bundesministeriums der Verteidigung (BMVg)

6. Leider müssen wir als deutsche IT- und Sicherheitsindustrie zunehmend feststellen, dass diese Partnerschaften oder Förderungen in Form von Aufträgen an nationale Anbieter häufig nicht in Betracht gezogen werden. Dabei lässt das Europäische Vergabeverfahren eine rein nationale Vergabe bei „Ausschreibungen für die nationale Sicherheit“ formal zu (siehe Vertrag über die Arbeitsweise der Europäischen Union, kurz: AEUV, Art. 346).

7. Es fehlt an generell an einer langfristigen Bedarfsplanung. Das Projekt für die Analyse-Software Bundes-VeRA wäre prädestiniert, die o.g. nationalen Strategien in eine operative Wirtschaftspolitik umzusetzen. Daher verwunderte es, dass bei der Europäischen Ausschreibung:
    a. kein deutsches oder zumindest europäisches Konsortium/Anbieter ausgewählt wurden,
    b. oder, sofern die Fähigkeiten zum Zeitpunkt der Ausschreibungserstellung noch nicht sichtbar / verfügbar waren, die deutsche oder auch europäische Industrie nicht frühzeitig in die Bedarfsermittlung und deren möglichen Realisierung eingebunden wurden.

8. Auch auf europäischer Ebene lösen solche deutschen Vergabepraktiken Verwunderung aus. Gespräche auf Verbandsebenen mit bspw. der Generaldirektion Migration und Inneres der Europäischen Kommission (DG Migration and Home Affairs) haben ergeben, dass die EU sehr wohl auch finanzielle Fördermittel bereitstellen würden für innovative polizeiliche Technologieentwicklungen für die EU und ihre Mitgliedsstaaten.

9. Deutschland würde sich mit der Förderung deutscher Technologien insbesondere für Sicherheitsorganisationen in keiner Weise „beschädigen“. Stattdessen würde es auf exakt gleiche Strategien setzen, die in Staaten wie den USA, Korea, China oder Frankreich regelmäßig Anwendung finden. Palantir wurde seinerzeit vom Pentagon (Ministry of Defense), CIA und NSA finanziell gefördert, und sowohl für die Geheimdienste als auch für das Militär eingesetzt.

Fazit:

Das Programm P20 als Zukunftsprogramm der deutschen Polizei ist der Reset-Button für die IT-Infrastruktur der deutschen Polizei des 21. Jahrhunderts. Im Sinne einer nachhaltigen nationalen Industriestrategie sollte insbesondere bei den kritischen Teilprojekten, wie z.B. den Analyse- und Auswertefähigkeiten, auf digital souveräne Lösungen nationaler Hersteller gesetzt werden. Die Vergabe an außereuropäische Anbieter von Einzellösungen mag kurzfristig attraktiv erscheinen, ignoriert jedoch mittel- und langfristige nicht absehbare finanzielle, technische und letztlich auch (geo-)politische Risiken.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 I

Bund Deutscher Kriminalbeamter

BDK | Wollankstraße 135 | D-13187 Berlin

An den Deutschen Bundestag

Sekretariat PA 4 Innenausschuss
z.Hd. Herrn Oberregierungsrat Daniel Kruppert

per E-Mail: innenausschuss@bundestag.de

Der Bundesvorsitzende

Ansprechpartner/in: Dirk Peglow
Funktion: Bundesvorsitzender

E-Mail: dirk.peglow@bdk.de
Telefon: +49 30 2463045-0

Datum: 17.04.2024

Stellungnahme des Bund Deutscher Kriminalbeamter e.V. (BDK) zum 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, Drucksache 20/9495

Sehr geehrte Abgeordnete,
sehr geehrte Damen, sehr geehrte Herren,

ich bedanke mich für die Gelegenheit, zu dem Antrag der Fraktion von CDU/CSU für den Bund Deutscher Kriminalbeamter e.V. (BDK) Stellung nehmen zu dürfen, den wir ausdrücklich begrüßen.

Voranstellen möchten wir, dass Entscheidungen zum Einsatz von Analyseplattformen bei den Polizeibehörden den dringenden Bedarfen der Ermittlerinnen und Ermittler entsprechen und produktneutral erfolgen müssen. Zugleich weisen wir darauf hin, dass jede Verzögerung bei der flächendeckenden Implementierung solcher Plattformen erhebliche Auswirkungen für die Analysekompetenz der deutschen Polizei hat.

1. Veränderung des Kriminalitätsgeschehens – Erkenntnisdefizite

Die Beschäftigten der Strafverfolgungsbehörden müssen sich in nahezu allen kriminalpolizeilichen Arbeitsbereichen seit Jahren einer massiven Verlagerung des Kriminalitätsgeschehens aus der analogen in die digitale Welt stellen. Diese Verlagerung hat zur Folge, dass sich

bekannte Kriminalitätsphänomene verändern, neue hinzukommen und zugleich die polizeiliche Sachbearbeitung immer kürzer werdenden Veränderungszyklen unterliegt.

Die polizeilichen Sachbearbeiterinnen und Sachbearbeiter sind tagtäglich mit der Herausforderung konfrontiert, dass sowohl die technische Entwicklung aber auch die extreme Anpassungs- und Innovationsfähigkeit weltweit agierender krimineller Akteure zu einem Wandel in der Kriminalitätsbekämpfung geführt haben, dem die Polizeiorganisation standhalten muss.

Zugleich müssen unsere Kolleginnen und Kollegen befürchten, dass der hierfür erforderliche polizeiliche Handwerkskasten durch aktuelle Gesetzgebungsverfahren immer mehr zu einem Erste-Hilfe-Set wird, das aus Sicht der Fachlichkeit nicht geeignet ist, eine zukunftsfähige Kriminalitätsbekämpfung zu gewährleisten.

2. Die Saarbrücker Agenda als Grundlage einer digitalen und medienbruchfreien Vernetzung der Polizei

Am 30.11.2016 verständigte sich die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) anlässlich ihrer Herbstsitzung in Saarbücken darauf, das Informationsmanagement der Polizeien des Bundes und der Länder einer grundlegenden Modernisierung und Vereinheitlichung zu unterziehen. Vermutlich allen Beteiligten dürfte damals schon bewusst gewesen sein, dass die Umsetzung dieses Vorhabens eher Jahrzehnte als Jahre dauern wird.

Das in der Folge initiierte Bund-Länder-Projekt „Programm Polizei 2020“ sollte - entgegen immer wieder zu vernehmenden kritischen Stimmen - nicht etwa das Jahr der beabsichtigten Umsetzung zum Ausdruck bringen. Vielmehr steht der mittlerweile gekürzte Projektname „P20“ für die Anzahl der Projektpartner, die sich aus 16 Länderpolizeien, dem Bundeskriminalamt, der Bundespolizei, dem Zoll und der Polizei beim Deutschen Bundestag zusammensetzen.

In der 2016 formulierten „Saarbrücker Agenda“ wurde die Zielsetzung der „Schaffung einer gemeinsamen, modernen, einheitlichen Informationsarchitektur“ festgelegt, die es allen Polizistinnen und Polizisten ermöglichen soll, „jederzeit und überall Zugriff auf die zur Aufgabenerfüllung erforderlichen Informationen“ zu erhalten.[1]

Tragend für die formulierte Zielsetzung war der ernüchternde Befund einer sehr heterogenen polizeilichen IT-Landschaft mit zahllosen Einzelanwendungen und unterschiedlichen Vorgangsbearbeitungs- und Analysesystemen.

[1] saarbruecker-agenda.pdf (bund.de)

Diese waren und sind bis heute nur unzureichend miteinander verbunden, gewährleisten den Austausch polizeilicher Informationen nicht im erforderlichen Umfang und haben zur Folge, dass erlangte Daten mehrfach in unterschiedliche Systeme eingegeben werden. Getreu dem vielfach angewendeten „Paragraphen 1 – jeder macht seins“ wurden (und werden) IT-Anwendungen in einzelnen Bundesländern entwickelt und als Insellösungen“ mit der Folge betrieben, dass polizeiliche Informationen, die in Bayern vorhanden sind, den Kolleginnen und Kollegen in Hamburg nicht unmittelbar zur Verfügung stehen.

Der kurze Rückblick auf die Entstehungsbedingungen von P20 gibt vielen polizeilichen Praktikerinnen und Praktikern Anlass zu der Frage, wann die in Aussicht gestellte „digitale und medienbruchfreie Vernetzung der Polizei“ kommen wird.

Aus Sicht des BDK sollte die in Teilen berechtigte Kritik an P20 jedoch berücksichtigen, dass es sich eben nicht „nur“ um ein IT-Projekt handelt, sondern um eine grundlegende Neugestaltung der deutschen Sicherheitsarchitektur, die Auswirkungen auf nahezu alle Prozesse polizeilicher Arbeit für mehr als 320.000 Beschäftigte haben wird. Zugleich gilt es zu beachten, dass die beabsichtige Harmonisierung der polizeilichen IT-Landschaft im laufenden Betrieb erfolgen muss und daher einer Operation am offenen Herzen gleicht.

Bei allem Respekt vor dem Umfang des Gesamtprojektes muss man sich jedoch darüber im Klaren sein, dass in vielen Bereichen der kriminalpolizeilichen Sachbearbeitung wenig Verständnis für die Zeiträume vorhanden ist, die Beschaffungsmaßnahmen zu IT-Anwendungen in Anspruch nehmen.

Es ist unseren Kolleginnen und Kollegen, die z.B. in den Deliktsbereichen sexualisierter Gewalt gegen Kinder oder der Bearbeitung des Erwerbs und Besitzes von Missbrauchsdarstellungen, der Bekämpfung organisierter Kriminalität oder des Terrorismus tätig sind, nicht zu vermitteln, dass die Beschaffung entsprechender Auswerte- und Analysetools von der Bedarfserhebung bis zur tatsächlichen Nutzung zum Teil mehrere Jahre dauert. In gleicher Weise haben Ermittlerinnen und Ermittler im Bereich der Auswertung und Analyse der Messengerdienste Sky ECC, Encrochat und Anom einen akuten Bedarf, ihre Analyse- und Auswertekompetenzen durch den Einsatz modernster Technologien zu verbessern.

3. Ausschreibung einer verfahrensübergreifenden Recherche- und Analyseplattform (VeRA) durch das Landeskriminalamt des Freistaates Bayern

Bezogen auf P20 erachten wir daher die am 13.01.2021 erfolgte europaweite Ausschreibung des bayerischen LKA mit folgendem Wortlaut als hochrelevant:

„Die Beschaffung einer verfahrensübergreifenden Recherche- und Analyseplattform (VeRA) für die Polizei des Freistaates Bayern (Primärauftraggeber) sowie mit der unverbindlichen Abrufoption unter der Rahmenvereinbarung für die Polizeien der Länder (...) und für die Bundesbehörden Bundeskriminalamt (BKA) und Bundespolizei (BPOL), Zollkriminalamt (ZKA) (Länder und Bundesbehörden jeweils als Sekundärauftraggeber) im Rahmen des Programms Polizei2020 zur Kooperation der deutschen Polizei- und Sicherheitsbehörden für die Modernisierung des polizeilichen Informationswesens von Bund und Ländern."

Maßgeblich und richtungsweisend für künftige Beschaffungsverfahren war an dieser Art der Ausschreibung, dass durch die darin aufgenommene „unverbindliche Abrufoption" (Rahmenvereinbarung) über P20 den Polizeien der Länder und des Bundes die Möglichkeit eröffnet worden wäre, die Anwendung zu nutzen, ohne gesonderte Vergabeverfahren zu eröffnen. Hiermit wäre der Philosophie von P20 Rechnung getragen worden, neue Anwendungen von einem oder mehreren Bundesländern entwickeln oder beschaffen zu lassen und sodann allen anderen zur Verfügung zu stellen.

Der bayerische Projektleiter Jürgen Brandl erklärte im März 2022 gegenüber der WELT, dass das Unternehmen Palantir Technologies GmbH den Zuschlag für das „Verfahrensübergreifende Recherche- und Analysesystem (VeRA)" des Bayerischen Landeskriminalamts (BLKA) erhalten habe.[2]

Am 08.07.2022 wurde der bayerische Innenminister Joachim Hermann in einer Pressemeldung des Landeskriminalamtes Bayern mit der Ankündigung gegenüber dem Innausschuss des Bayerischen Landtages zitiert, dass die Software des Unternehmens Palantir vor ihrer Einführung einer umfänglichen Überprüfung unterzogen wird, mit der das renommierte Fraunhofer Institut SIT beauftragt wird.[3]

Im März 2023 teilte das Landeskriminalamt Bayern mit, dass die in Auftrag gegebene Überprüfung der Software nach Auskunft des Fraunhofer Institutes ergeben hat, dass sie „datenschutzrechtlich unbedenklich" ist und eingesetzt werden darf. Weiter wurde erklärt, dass keine Funktionalitäten festgestellt wurden, die einen unzulässigen Abfluss von Daten unter Umgehung von

[2] Bayern: Palantir bekommt Zuschlag vom LKA - WELT

[3] Die Bayerische Polizei - Projekt VeRA: Zuschlag für die Untersuchung des Quellcodes erteilt (bayern.de)

Zugriffsbeschränkungen oder einen unautorisierten Zugriff auf das System von außen ermöglichen“.[4]

4. Urteil des Bundesverfassungsgerichts zum Einsatz von Analyseplattformen

Mit seinem Urteil vom 16.02.2023 hat der Erste Senat des Bundesverfassungsgerichts entschieden, dass die in Hamburg und Hessen bestehenden gesetzlichen Grundlagen für den Betrieb von Analyseplattformen verfassungswidrig sind. (1 BvR 1547/19, 1 BvR 2634/20).[5]

Entscheidungsgrundlage waren zwei Verfassungsbeschwerden, mit denen sich u. a. die Gesellschaft für Freiheitsrechte, die Humanistische Union sowie der Verband der Internetwirtschaft gegen die landesgesetzlichen Ermächtigungen in Hamburg und Hessen zur automatisierten Datenauswertung wandten.

In den von Prof. Dr. Tobias Singelnstein und Jun.-Prof. Dr. Sebastian Golla verfassten Beschwerdeschriften wurde wesentlich geltend gemacht, dass die Regelungen des § 25 a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) sowie der § 49 des Hamburgischen Gesetzes über die Datenverarbeitung bei der Polizei (PolDVG) u. a. das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) und, soweit betroffen, das Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) und das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) verletzen.

Im Unterschied zur hamburgischen Regelung, die mangels bisheriger Anwendung für nichtig erklärt wurde, entschied der Erste Senat, dass die gesetzliche Vorschrift im hessischen Polizeigesetz mit der Verfassung unvereinbar ist und ordnete eine befristete Fortgeltung bis zum 30.09.2023 an. Grund hierfür war die Bewertung, dass eine Nichtigerklärung und damit sofortige Ungültigkeit den „Schutz überragender Güter des Gemeinwohls die Grundlage entziehen würde und eine Abwägung mit den betroffenen Grundrechten ergibt, dass der Eingriff für eine Übergangszeit hinzunehmen ist“.[6]

An die Entscheidung zur Fortgeltung wurden Bedingungen geknüpft, die einzuhalten sind, bis eine verfassungsgemäße Ausgestaltung der Eingriffsermächtigung hergestellt ist, ohne aber darin eine gesetzliche Neuregelung zu präjudizieren. So wurde festgelegt, dass künftig konkrete Tatsachen den Verdacht begründen müssen, dass eine besonders schwere Straftat nach § 100 b Abs. 2 StPO (bisher § 100 a Abs. 2 StPO) begangen wurde und mit weiteren gleichgelagerten Straftaten zu rechnen ist, die Leib, Leben oder den Bestand oder die Sicherheit des Bundes oder eines Landes gefährden.[7]

---

[4] https://www.polizei.bayern.de/aktuelles/pressemitteilungen/045266/index.html

[5] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

[6] Ebd. Seite 57

[7] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html, Seite 5

Mit dem Urteil hat das Bundesverfassungsgericht klargestellt, dass die automatisierte Datenauswertung zur vorbeugenden Bekämpfung schwerer Straftaten zulässig ist. Es hat zugleich die verfassungsrechtlichen Hürden für eine Nachbesserung bestehender gesetzlicher Normen, wie auch für notwendige gesetzgebende Initiativen in den Ländern definiert.

5. Untersagung der Nutzung der Bundes-VeRA durch Frau Bundesinnenministerin Faeser

Die Entscheidung von Frau Bundesinnenministerin Faeser dem BKA und der Bundespolizei die Einführung einer Analyse-Plattform, der sogenannten „Bundes-VeRA“, zu untersagen ist ein erstaunlicher Vorgang in vielfacher Hinsicht, der erhebliche Auswirkungen für die Auswerte- und Analysekompetenz der deutschen Polizei haben wird.

Frau Ministerin Faeser setzte sich nicht nur über das Votum der gesamten Fachlichkeit hinweg, da alle 16 Bundesländer sich im Verwaltungsrat des Polizei-IT-Fonds, dem das BMI vorsitzt, für die dringliche Notwendigkeit der Einführung von VeRA ausgesprochen hatten. Sie ignorierte auch die Ziele der eingangs erwähnten „Saarbrücker Agenda“, deren Kernelement die Schaffung einer gemeinsamen und modernen, einheitlichen Informationsarchitektur der deutschen Polizei ist.

Vor allem bei der Bekämpfung der Organisierten Kriminalität und des Terrorismus, aber auch bei Ermittlungen im Bereich des sexuellen Missbrauchs von Kindern und dem Erwerb und Besitz von Missbrauchsdarstellungen sexualisierter Gewalt gegen Kinder und Jugendliche sind die Ermittlerinnen und Ermittler auf das schnelle Erkennen von Tat- und Täterzusammenhängen angewiesen.

Ihre Entscheidung berücksichtigte nicht, dass eines der priorisierten Tätigkeitsfelder von P20 sich mit der Stärkung der Auswertung- und Analyse durch Analysetechniken (-plattformen) befasst. Hier wurde eine verfahrensübergreifende Recherche- und Analyseplattform, die wesentlich auf der in Hessen seit 2017 betriebenen technischen Plattform „hessenDATA“ des Unternehmens Palantir beruht, bereits als geplante Umsetzungsinitiative aufgeführt.

Aus unserer Sicht ist die ablehnende Entscheidung der Bundesinnenministerin auch deshalb nicht nachvollziehbar, weil das zugrundeliegende Ausschreibungsverfahren für VeRA vom BMI nicht nur begleitet, sondern auch vorangetrieben wurde und dafür finanzielle Mittel hinterlegt und in Teilen auch verausgabt wurden.

Das Vorhaben des Bundesinnenministeriums, die Analysefähigkeit der Polizei „in eigener digitaler Kompetenz zu entwickeln“ ist grundsätzlich zu begrüßen, sollte jedoch parallel zur flächendeckenden Nutzung der Bundes-VeRA erfolgen.

Die Entwicklung einer solchen Plattform ohne den Parallelbetrieb der Bundes-VeRA ist in Anbetracht der aktuell zu bearbeitenden Kriminalitätsphänomene und deren Gefahrenlagen fachlich nicht nachvollziehbar.

Sie stellt vor dem Hintergrund, dass die Ausbaustufen des PIAV zu den Deliktsbereichen Geldwäsche, Korruption, Politisch motivierte und Organisierte Kriminalität erst 2024 umgesetzt werden sollen, enorme Risiken dar und hat zur Folge, dass das schnelle Erkennen von Tat- und Täterzusammenhängen durch eine Analyseplattform weiterhin durch Insellösungen erfolgen wird, bei dem die Bundesbehörden sich rausnehmen.

6. Abschließende Betrachtung – Beschlusslage des BDK

Der BDK erachtet die flächendeckende Nutzung von Recherche- und Analysesystemen in Form von Plattformtechnologien, die anwendungsübergreifend auf rechtmäßig erhobene Daten zugreifen, für dringend notwendig. Die Verbesserung der Analysekompetenzen kriminalpolizeilicher Sachbearbeiterinnen und Sachbearbeiter muss insbesondere im Bereich der Bekämpfung der Organisierten Kriminalität, des Terrorismus, aber auch im Zusammenhang mit allen Deliktsformen von sexualisierter Gewalt gegen Kinder sowie dem Erwerb und Besitz von Darstellungen sexualisierter Gewalt gegen Kinder und Jugendliche verbessert werden.

Flankierend müssen, neben der technischen Umsetzung, die Bundesländer die notwendigen Gesetzgebungsverfahren initiieren, um die Nutzung von VeRA in den jeweiligen Polizeigesetzen zu regeln. Hierdurch soll ausgeschlossen werden, dass Verzögerungen in der Nutzung des Systems dadurch entstehen, dass notwendige landesgesetzliche Regelungen zu spät implementiert werden.

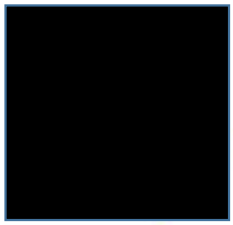
Die in der Vergangenheit vorgetragenen Kritikpunkte zum Unternehmen Palantir Technologies GmbH, sowie die im politischen Raum aufgeworfenen Fragestellungen zur „digitalen Souveränität“ der deutschen Polizei erfordern eine differenzierte Betrachtung. Natürlich sollte die deutsche Polizei ihre Digitale Souveränität im Hinblick auf genutzte IT-Anwendungen sicherstellen.

Allerdings ist, bezogen auf die Nutzung von Analyseplattformen, nicht zu erwarten, dass in annehmbaren Zeiträumen konkurrenzfähige Produkte aus deutscher Produktion auf den Markt kommen werden, selbst wenn sofort gezielt mit der Entwicklung begonnen würde.

Bund Deutscher Kriminalbeamter

Insofern ist die digitale Souveränität der deutschen Polizei eine elementare Zielsetzung, die aber immer unter Berücksichtigung der tatsächlichen Bedarfe kriminalpolizeilicher Sachbearbeiterinnen und Sachbearbeiter und den Interessen der Bevölkerung und der Politik an einer wirksamen Kriminalitätsbekämpfung auch im digitalen Kriminalitätsraum umgesetzt werden sollte.

Aus Sicht der polizeilichen Praxis verursacht jede Verzögerung bei der deutschlandweiten Nutzung von Analyseplattformen erhebliche Erkenntnisdefizite bei den Strafverfolgungsbehörden und setzt uns alle der Gefahr aus, im Wettlauf mit unserem Gegenüber nicht mehr Schritt zu halten und Gefahren für die Bürgerinnen und Bürger nicht oder zu spät zu erkennen.



Dirk Peglow
Bundesvorsitzender

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)

Seiten insgesamt
1/15

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

Seiten insgesamt
15/15

Stellungnahme

Gewerkschaft der Polizei
Bundesvorstand

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)424

Stellungnahme der Gewerkschaft der Polizei (GdP)

zum Antrag der Fraktion CDU/CSU
im Deutschen Bundestag

Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren (BT-Drs. 20/9495)

Berlin, 14.03.2024

Vorbemerkung

Als mit über 205.000 Mitgliedern größte Polizeigewerkschaft begrüßt die Gewerkschaft der Polizei (GdP) das mit dem vorliegenden Antrag zum Ausdruck gebrachte Bestreben, die Handlungsfähigkeit der Strafverfolgungsbehörden weiterhin zu sichern und den polizeilichen Informationsaustausch unter Einsatz moderner Recherche- und Analysetools, namentlich der Software „Bundes-VeRa“, zu verbessern.

Die Erhebung und Nutzung der für polizeiliche Aufgaben relevanten Daten ist für den Erfolg von Polizeiarbeit mit Blick auf Prävention und Strafverfolgung von entscheidender Bedeutung. Die aktuellen Herausforderungen bei der Programmierung entsprechend benötigter Softwarelösungen bestehen unter anderem darin, Auswertetools so zu gestalten, dass Speicherung, Aufbereitung, Analyse, Visualisierung und Ausgabe der Ergebnisse innerhalb einer digitalen Umgebung rechtssicher erfolgen kann. Auswertungen und Analysen von Daten dienen in der Polizeiarbeit dazu, den zuständigen Behörden die notwendigen Informationen zum richtigen Zeitpunkt an der richtigen Stelle aufbereitet zur Verfügung zu Stellen.

Dabei bindet die Erhebung und Nutzung von Daten im polizeilichen Arbeitsalltag erhebliche Ressourcen. Dieser Umstand steht damit in Verbindung, dass wichtige Informationen in der Praxis oft nur isoliert vorliegen und in den vorhandenen Datensystemen nur unter erheblichem zeitlichem sowie personellem Aufwand oder teils überhaupt nicht recherchierbar sind. Die Anzahl der Datenquellen und Systeme, die abgefragt, analysiert und verarbeitet werden können oder müssen, wächst zudem kontinuierlich. Dies bedeutet im Umkehrschluss: Für weitergehende Tätigkeiten, die der Strafverfolgung und Kriminalitätsbekämpfung dienlich sind, geht wichtige Zeit verloren. Vor dem Hintergrund der bedauernswerterweise verbesserungsbedürftigen Personalausstattung der Polizeien von Bund und Ländern ist dies mit erheblichen negativen Konsequenzen verbunden. Dies begründet die Notwendigkeit, dass Strafverfolgungsbehörden sowohl personell gestärkt als auch technisch mit verbesserten und modernen Tools und Rechtsgrundlagen ausgestattet werden müssen. Nur so kann Schwere und Organisierte Kriminalität wirksam und nachhaltig bekämpft werden – und nur so können die Beschäftigten, die die Software anwenden rechtssicher handeln.

Stellungnahme

Zum in Rede stehenden Antrag der CDU/CSU-Fraktion nimmt die GdP wie folgt Stellung:

Zu I.:
Wir halten P20 für das entscheidende Digitalisierungs- und Transformationsvorhaben aller deutschen Sicherheitsbehörden in der Bundesrepublik. Eine Stärkung der Innovation innerhalb des Programms ist elementar, um auch moderneren Ansätzen der Weiterentwicklung der Informationsarchitektur sowie einer übergreifenden Plattformoffenheit mehr Anwendung zu verschaffen.

Die zwingende Notwendigkeit, die Funktionsfähigkeit der Sicherheitsbehörden sicherzustellen, erfordert es einerseits, bestehende Lösungen zunächst weiterhin zu nutzen. Andererseits genügen die existierenden siloartigen und in der Regel nicht kompatiblen Bestandslösungen nicht den Herausforderungen an eine moderne und leistungsfähige IT-Struktur der

Sicherheitsbehörden. Die Digitalisierung der Polizeien in Bund und Ländern als Teil der Organisationsentwicklung erfordert es, auch neue Ansätze im Sinne digitaler Souveränität der deutschen Polizei zuzulassen. Um dieses Ziel zu erreichen, sind die bei den Beschäftigten der Polizeien des Bundes und der Länder vorhandenen IT-Kompetenzen zu stärken, und sind entsprechend Fachkräfte durch eine Steigerung der Attraktivität der Arbeitsbedingungen für Polizeibeschäftigte für ein Arbeiten bei den Sicherheitsbehörden zu begeistern. Dies stellt sicher, dass auch künftig die Nutzung und Verfügbarkeit von Hard- und Software und ihren Weiterentwicklungen durch die Sicherheitsbehörden selbst bestimmt werden können. Dies ist essentiell, um zu gewährleisten, dass eine umfassende Kontrolle über die polizeilichen Daten gewährleistet bleibt. Insofern begrüßen wir, insbesondere mit Blick auf die Notwendigkeit der Sicherstellung der digitalen Souveränität der Sicherheitsbehörden, wenn P20 herstellerunabhängige Entwicklungen betreibt. Zugleich bietet eine Eigenentwicklung sehr viel stärker die Möglichkeit, auf die Bedürfnisse der Beschäftigten, der konkreten Anforderungen der Polizeibehörden und den notwendigen rechtlichen Rahmenbedingungen einzugehen. Vor diesem Hintergrund betonen wir die Notwendigkeit der forcierten Fortführung des laufenden Projektes und der Bereitstellung entsprechend benötigter Haushaltsmittel.

Gerade weil eine herstellerunabhängige (Eigen)Entwicklung auch immer personelle, zeitliche und finanzielle Ressourcen beansprucht, braucht es schnelle effektive entlastende Alternativen. Daher sehen wir zugleich die Notwendigkeit, kurzfristig auch andere, ggf. herstellerabhängige, Lösungen Nutzen zu können.

Bei der Verarbeitung von personenbezogenen Daten werden hohe Hürden festgelegt – weswegen das Bundesverfassungsgericht die Rechtsfigur der „hypothetischen Datenneuerhebung“ geschaffen hat. Auch zum Schutz der Beschäftigten, welche mit „Gotham“ arbeiten würden, muss das Produkt die rechtlichen Rahmenbedingungen (also wie werden personenbezogene Daten verbunden, welche Rechtsgrundlage existieren zur (temporären) Speicherung von Daten, wann werden Daten gelöscht, etc.) berücksichtigen. Dies müsste bei der Anbindung der unterschiedlichen Datentöpfe an „Gotham“ gewährleistet werden. Hierzu wären fein granulierte Konzepte über Zugriffsberechtigungen zu erstellen.

Insbesondere P20 verfolgt bereits im Grundgedanken auch außerhalb der Bundes-VeRa ein ähnliches Ziel. P20 zielt darauf ab, bereits existierende polizeiliche Daten miteinander zu verbinden (über das sog. Datenhaus) und den Beschäftigten bei der Ermittlung starke Unterstützung zu bieten. Insofern müsste dargestellt werden, welche zusätzlichen Anforderungen die Bundes-VeRa abdecken würde, damit keine neuen finanziellen Doppelaufwände anfallen und die Verhältnismäßigkeit gegeben ist.

Aus Sicht der GdP wird mit den in Planung befindlichen Analyse- und Auswerte-Vorhaben bei P20 der grundlegende Beweis angetreten, dass innerhalb von P20 die Expertise existiert um grundsätzlich auch Anforderungen, die „Gotham“ abdecken würde, wie z.B. die Verknüpfung und Visualisierung unterschiedlicher Datentöpfe, zu gewährleisten. Gerade mit Blick darauf, dass ohnehin eine Anbindung bzw. Integration von den bestehenden polizeilichen Systemen erfolgen muss, könnte der Ansatz einer herstellerunabhängigen Entwicklung geeignet sein, um in der Zwischenzeit die notwendigen rechtlichen Rahmenbedingungen zu sichern. Mit einem agilen Ansatz bei der Entwicklung könnten hier auch über Zwischenschritte kurzfristige Teilerfolge

erzielt werden. Die Integration bestehender Datentöpfe verursacht üblicherweise ebenfalls finanzielle und personelle Aufwände. Wie hoch diese bei „Gotham“ ausfallen, lässt sich von unserer Seite aus nicht beziffern. Insofern ist innerhalb von P20 abzuwägen, wie lange die Integration der Bestandssysteme in Gotham dauern würde und welche Aufwände ggü. einer herstellerunabhängigen Entwicklung verbunden sind.

Wir legen besonderen Wert auf gute Arbeitsbedingungen für Beschäftigte in Sicherheitsbehörden. Unklar ist derzeit, ob alle Anforderungen an den Beschäftigtendatenschutz abdeckt sind. Insbesondere Barrierefreiheit gilt es einzuhalten.

Zu II.

1.:
Siehe vorherige Ausführungen.

2.:
Wir erwarten, dass bei einer herstellerunabhängigen Entwicklung, die Kosten nach den gängigen Regeln (modifizierter Königsteiner Schlüssel) des Polizei-IT-Fonds gedeckt werden und zusätzliche Mittel durch den Haushaltsgesetzgeber schnell und unkompliziert zur Verfügung gestellt werden.

3.:
Diese Prüfung muss unserer Ansicht nach in jedem Fall vorgenommen werden – da wir davon ausgehen, dass eine herstellerunabhängige Entwicklung einen sehr ähnlichen Funktionsumfang hätte und dementsprechend die gleichen rechtlichen Anforderungen mit sich bringt. Eine Novellierung von Bundespolizeigesetz und BKA-Gesetz ist aus unserer Sicht ebenso notwendig. Andernfalls wäre zu befürchten, dass aus rechtlichen Gründen stärke Einschränkungen bei Anwendungsfällen notwendig wären.

4.:
Aus unserer Sicht kann die Bundes-VeRa hier zwar große Potentiale bieten, stellt aber nur ein Puzzleteil im Gesamtbild der IT-Infrastruktur der deutschen Polizei dar. Hierzu sehen wir insgesamt im Programm P20 große Potentiale, die derzeit unzureichend ausgeschöpft werden.

5.:
Wir unterstützen das Vorhaben, dass finanzielle und personelle Ressourcen möglichst effektiv und effizient gebündelt werden. Daher sprechen wir uns für das „Einmal-für-alle“ Prinzip aus. Dabei werden einzelne IT-Verfahren federführend von einer Stelle für alle entwickelt. Beim „Einmal-für-Alle-Prinzip“ können IT-Lösungen auch von mehreren verantwortlichen Stellen gemeinsam entwickelt und bereitgestellt werden. Entscheidend ist dabei, dass solche Lösungen oder Verfahren nur „einmal“ entwickelt werden. Gemeinsam entwickelte IT-Verfahren werden den Programmteilnehmern kostenlos zur Verfügung gestellt.

6.:
Analog zu Punkt 4.

7.:
Zustimmung.

8.:
Bisher konnten die Polizeibehörden auch unter großem Einsatz der Polizeibeschäftigten regelmäßige Ermittlungserfolge auch bei der Bekämpfung schwerer Kriminalität erzielen. Bundes-VeRa kann eine Vereinfachung der Arbeit und des Alltags der Polizeibeschäftigten darstellen.

9.:
Wir teilen die geäußerte Sorge um die angespannte Sicherheitslage und erwarten von der Bundesregierung und dem Haushaltsgesetzgeber ein Sondervermögen Innere Sicherheit bereitzustellen, dass angesichts der angesprochenen Lage der Stabilisierung der Sicherheitsbehörden unter den Bedingungen der föderalen Sicherheitsarchitektur in Deutschland dient.