LANDTAG
NIEDERSACHSEN

N i e d e r s c h r i f t

über die 100. - öffentliche - Sitzung

des Ausschusses für Inneres und Sport

am 12. März 2026

Hannover, Landtagsgebäude

Tagesordnung: Seite:

4. **Straftaten im digitalen Raum wirksam und nachhaltig bekämpfen - vorsorgliche Speicherung von IP-Adressen endlich gesetzlich normieren**

   Antrag der Fraktion der CDU - Drs. 19/9900

   (abgesetzt) 71

5. **Freiheitlich-demokratische Grundordnung schützen - Instrumente der wehrhaften Demokratie entschlossen nutzen**

   Antrag der Fraktion der SPD und der Fraktion Bündnis 90/Die Grünen - Drs. 19/9916

   dazu: Eingaben 01300/02/19, 01654/02/19, 01654/02/19-001, 01654/02/19-002, 01742/02/19

   (abgesetzt) 72

Anwesend:

Ausschussmitglieder:

1. Abg. Doris Schröder-Köpf (SPD), Vorsitzende
2. Abg. Deniz Kurku (SPD)
3. Abg. Alexander Saade (SPD)
4. Abg. Julius Schneider (SPD)
5. Abg. Ulrich Watermann (ab TOP 2 v. d. den Abg. Rüdiger Kauroff) (SPD)
6. Abg. Sebastian Zinke (SPD)
7. Abg. Veronika Bode (i. V. des Abg. André Bock) (CDU)
8. Abg. Saskia Buschmann (CDU)
9. Abg. Birgit Butter (CDU)
10. Abg. Lara Evers (CDU)
11. Abg. Alexander Wille (CDU)
12. Abg. Michael Lühmann (GRÜNE)
13. Abg. Nadja Weippert (GRÜNE)
14. Abg. Stephan Bothe (AfD)

Von der Landtagsverwaltung:

Regierungsrat Biela.

Niederschrift:

Regierungsdirektor Dr. Bäse,
Regierungsdirektorin March-Schubert,
Oberregierungsrätin Harmening, Stenografischer Dienst.

Sitzungsdauer: 10:15 Uhr bis 14:56 Uhr.

Außerhalb der Tagesordnung:

Billigung von Niederschriften

Der **Ausschuss** billigt die Niederschriften über die 92., über den öffentlichen Teil der 96., über die 97. und die 99. Sitzung.

***

Tagesordnungspunkt 1:

Unterrichtung durch die Landesregierung zur aktuellen Situation bei der Aufnahme und Unterbringung von Flüchtlingen aus der Ukraine und Asylbewerbern

Unterrichtung

Ltd. MR **Dr. Stomberg** (MI) informiert den Ausschuss über die **aktuellen Zugangszahlen von Asylsuchenden** in Niedersachsen. Im System EASY seien 2026 bisher insgesamt 1 497 Zugänge verzeichnet worden. In der 8. Kalenderwoche (KW) seien 126 Menschen nach Niedersachsen gekommen, in der 9. KW seien 92 gezählt worden, in der 10. KW wiederum 127. In Rücksprache mit dem zuständigen Referat 61 sei ihm mitgeteilt worden, dass sich die Zahlen damit weiterhin auf einem sehr moderaten Niveau bewegten, insbesondere im längerfristigen Vergleich.

Die **Hauptherkunftsländer** der Personen, die Asylerstanträge stellten, seien derzeit sowohl im Bund als auch in Niedersachsen Afghanistan, Syrien und die Türkei. In Niedersachsen folgten dann der Irak und Kolumbien. Diese hätten aktuell Somalia und Russland auf den Plätzen 4 und 5 abgelöst. Im Bund würden diese Plätze von Somalia und dem Irak belegt.

Die Zahl der **Vertriebenen aus der Ukraine**, die seit Kriegsbeginn am 24. Februar 2022 in Niedersachsen angekommen und im System FREE registriert worden seien, summiere sich auf insgesamt 187 376. Derzeit verzeichne Niedersachsen bei der Aufnahme der ukrainischen Kriegsvertriebenen eine leichte Unterquote von 21 Personen. Die Zahl der Ankünfte **russischer Staatsangehöriger** in Niedersachsen liege 2026 bei bisher 24 Personen.

Mit Blick auf **weitere Kriegsgeschehen** sei mitzuteilen, dass seit dem 7. Oktober 2023 327 Palästinenserinnen bzw. Palästinenser sowie vier Israelis in EASY registriert worden seien. Ferner seien seit Beginn der kriegerischen Auseinandersetzungen im Iran am 28. Februar 2026 insgesamt vier Personen von dort nach Niedersachsen eingereist. Es handele sich um geringe Zahlen, die Lage werde jedoch weiter beobachtet.

Derzeit verfüge die Landesaufnahmebehörde Niedersachsen (LAB NI) über 8 802 **Unterbringungsplätze** für Asylsuchende. Mit Stand vom 8. März 2026 seien davon etwa 40 % belegt. Dies bedeute eine Auslastung von rund 50 % an den regulären Standorten und von etwas mehr als 20 % bei den Not- und Behelfsunterkünften. Das Land habe zudem am 28. Januar 2026 mit der Thelen Gruppe einen Mietvertrag für eine Immobilie in Langenhagen abgeschlossen. Der Investor werde die bestehende Immobilie eigenständig zu einer Erstaufnahmeeinrichtung mit 530 Plätzen umbauen. Die Inbetriebnahme sei für das zweite Halbjahr 2027 vorgesehen.

Im Jahr 2025 seien in Niedersachsen insgesamt 1 242 **vollzogene Rückführungen** zu verzeichnen gewesen. Die jüngsten vorliegenden Daten für Januar 2026 wiesen 147 vollzogene Rückführungen aus, davon seien acht Überstellungen nach der Dublin-III-Verordnung. Ferner seien 2 273 Personen 2025 mithilfe des Programms REAG/GARP bzw. Individualhilfen der LAB NI freiwillig ausgereist. Dies entspreche einer Erhöhung von mehr als 60 % im Vergleich zu 2023 und einer

Steigerung um 20 % im Vergleich zu 2024. Im Januar 2026 seien zudem 155 Personen, überwiegend aus Kolumbien, Syrien und der Türkei, mithilfe von REAG/GARP freiwillig ausgereist. Hinzu kämen drei Personen, die über Individualhilfen der LAB NI ausgereist seien.

***

Tagesordnungspunkt 2:

Polizeiarbeit in das Zeitalter der Digitalisierung überführen - verfahrensübergreifende Datenanalysen in Echtzeit ermöglichen

Antrag der Fraktion der CDU - Drs. 19/8214

erste Beratung: 72. Plenarsitzung am 12.09.2025
federführend: AfluS
mitberatend gem. § 27 Abs. 4 Satz 1 i. V. m. § 39 Abs. 3 Satz 1 GO LT: AfHuF

zuletzt beraten: 91. Sitzung am 04.12.2025

Anhörung

Landesbeauftragter für den Datenschutz Niedersachsen

Schriftliche Stellungnahme: Vorlage 7

Anwesend:

- Denis Lehmkemper, Landesdatenschutzbeauftragter
- Dr. Christoph Lahmann, stellvertretender Landesdatenschutzbeauftragter
- Johanna Busche, Referentin Referat 1

LfD **Denis Lehmkemper:** Vielen Dank, dass ich wieder bei Ihnen sein darf. Ich hoffe, dass meine Ausführungen, auch wenn sie vermutlich nicht immer allen gefallen, für Sie hilfreich sein werden.

Das heutige Thema hängt inhaltlich eng mit dem Vortrag, den ich hier in der 98. Sitzung am 26. Februar 2026 zu den Rechtsgrundlagen im Niedersächsischen Polizei- und Ordnungsbehördengesetz (NPOG) gehalten habe, zusammen. In dem heute behandelten Antrag wird erstens die Schaffung einer Rechtsgrundlage im NPOG gefordert, um den Einsatz einer Recherche- und Analysesoftware zu ermöglichen. Zweitens soll sich die Landesregierung parallel mit jenen Ländern abstimmen, die bereits eine solche Recherche- und Analysesoftware des US-amerikanischen Anbieters Palantir nutzen. Drittens sollen die datenschutzrechtlichen Fragestellungen mit dem Landesbeauftragten für den Datenschutz abgestimmt werden.

Zur Forderung, umgehend eine Rechtsgrundlage im NPOG zu schaffen, die den Einsatz einer solchen Analyse- und Recherchesoftware ermöglicht, hatten wir uns bereits vor 14 Tagen ausgetauscht, und ich habe dazu eine Menge gesagt. Noch einmal ganz deutlich: Ich nehme aus der Sicht des Datenschutzes Stellung. Ich bin sehr froh, dass ich nur aus dieser Sicht Stellung nehmen muss; denn die Gesamtabwägung der Fragen, was die Polizei braucht, was im Einsatz sinnvoll ist, aber auch, was datenschutzrechtlich zu beachten ist, obliegt Ihnen. Das ist, glaube ich, keine einfache Abwägung.

Ganz grundsätzlich: Ohne eine entsprechende Rechtsgrundlage ist und wäre der Einsatz einer solchen Software rechtswidrig. Außerdem verschärft sich das Problem - auch das habe ich schon vor 14 Tagen gesagt - in gewisser Weise, wenn man den Funktionsumfang einer solchen

Software mit in Betracht zieht: Wenn KI implementiert wird - in welcher Form auch immer -, hat man gleichzeitig die Vorgaben der KI-Verordnung zu betrachten und zu beachten.

Klar ist: Das Bundesverfassungsgericht hat relativ enge Grenzen für den Einsatz von Analysesoftware in jeder Form gesetzt. Ich hatte bereits gesagt, dass der im Gesetzentwurf enthaltene § 45 a aus unserer Sicht in der vorliegenden Fassung nicht hinreichend ist, wobei es völlig egal ist, welche Software man darunter fassen möchte. Diese Frage muss man näher betrachten. Warum ist das so? Neben personenbezogenen Daten von Verdächtigen hält die Polizei auch eine Vielzahl personenbezogener Daten von Zeugen, Opfern und Unbeteiligten vor. All diese Daten fließen im Zweifelsfall in diese Software ein und werden neu - und anders als bis dahin - miteinander verbunden.

Mit der automatisierten Zusammenführung und Verarbeitung, wie Sie von allen in Rede stehenden Analysetools vorgenommen werden, ändert sich bezüglich der Daten etwas; die Zweckbindung dieser Daten wird aufgehoben. Letztlich werden die Daten durch die Polizei nicht mehr wie bisher vorgangsbezogen, sondern personen- und objektbezogen gespeichert. Außerdem können - so verstehen wir es - auch Daten von Opfern und Zeugen mitverarbeitet werden.

Das führt dazu, dass die polizeiliche Datenverarbeitung einen ganz anderen Charakter bekommt. Bürgerinnen und Bürger können den Eindruck gewinnen, dass die Polizei über sie Akten führt oder - mehr noch - Profile anlegt. Eine solche Datenverarbeitung muss rechtlich sehr sauber abgebildet werden.

Diese Vorgabe ist nicht auf ein bestimmtes Produkt beschränkt, sondern gilt für alle Analysesysteme. Insofern bitte ich, wie ich es schon vor 14 Tagen getan habe, darum, bei der Schaffung einer Rechtsgrundlage besondere Sorgfalt walten zu lassen. Bereits im September 2025 hatten wir dem Innenministerium - und dann auch Ihnen in der Anhörung vor 14 Tagen - eine ausführliche Stellungnahme zur Verfügung gestellt. Wir sind gern bereit, diese Stellungnahme weiter zu unterfüttern und weitere Hinweise zu geben. Wir wollen schlicht helfen, das Ganze datenschutzmäßig sauber abzubilden.

Zu Punkt 2 des Entschließungsantrags - der Forderung, sich mit jenen Ländern ins Benehmen zu setzen, die schon eine Analysesoftware des US-amerikanischen Herstellers Palantir im Einsatz haben -: Aus unserer Sicht muss man sich, bevor man sich mit den anderen Betreibenden zu den dort gesammelten Erfahrungen austauscht, klarmachen, dass nach unserem Wissen die einzelnen Systeme, die auf Palantir beruhen, einen jeweils sehr unterschiedlichen Funktionsumfang aufweisen. Aus unserer Sicht wäre daher anzuraten, zunächst zusammen mit der Landespolizei zu überlegen, welche Funktionen für das eigene System angestrebt werden - also einen Forderungskatalog aufzustellen -, und dann mit einer entsprechenden Marktanalyse zu prüfen, ob für ein solches System verschiedene Anbieter zur Verfügung stehen. Danach ist zu vergleichen, wie gut die ermittelten Anbieter die definierten Anforderungen der niedersächsischen Landespolizei erfüllen.

Vermutlich würde eine solche Marktanalyse dazu führen, dass man auch die Datenschutzaspekte in die Abwägungen einfließen lassen könnte. Dabei geht es um die Fragen, wie die Datenströme verlaufen, wie die Auftragsverarbeitungsverträge (AV-Verträge) gestaltet sind, welche technisch-organisatorischen Maßnahmen erforderlich sind und wie eine Datenschutzfolgeabschätzung aussieht. Auf dieser Grundlage kann überlegt werden, ob man das in dieser Form haben will und ob ein außereuropäischer Anbieter überhaupt in Betracht kommt.

Im Moment kann ich nicht abschätzen, inwieweit die Daten, die über einen außereuropäischen Anbieter verarbeitet werden, tatsächlich in Europa, in Deutschland, in Niedersachsen bleiben. Ich habe da Sorge. Wir konnten das nicht prüfen und haben das nicht geprüft. Um solche Fragen muss man sich aus Datenschutzsicht Gedanken machen. Erst, wenn man genau weiß, was man will, und genau weiß, was Anbieter leisten, wird deutlich, welches System sich eignet. Aus meiner Sicht ist erst dann ein vertiefter Austausch mit den Ländern, die solche Systeme schon in Betrieb haben, sinnvoll.

Einige Hinweise zu den bereits in Betrieb befindlichen Systemen von Palantir, die ich allesamt der Presse entnommen habe - insofern verrate ich hier keine Geheimnisse -: Der Funktionsumfang der bereits eingesetzten Systeme unterscheidet sich, wie schon gesagt, relativ deutlich von Land zu Land. Ein in Bayern laufendes System hat andere Komponenten - gegebenenfalls auch andere Anbindungen an das Internet - als ein in einem anderen Land laufendes System. Aus Baden-Württemberg hört man, dass der Fünf-Jahres-Vertrag mit dem Anbieter ein Volumen von 25 Millionen Euro habe. Das sind immerhin rund 13 000 Euro am Tag. Ich bin mir nicht ganz sicher, ob dafür hier entsprechende Vorkehrungen im Haushalt geschaffen worden sind. Wenn nicht, müsste man sich sicherlich auch darüber Gedanken machen.

Ganz wichtig: Es kommt darauf an, was gebraucht wird. Darüber muss man sich Gedanken machen. Im Zuge dieses Nachdenkens muss man aus meiner Sicht auch die Datenschutzaspekte mit bedenken. Wenn man im Ergebnis keinen europäischen Anbieter findet, der in der Lage ist, den Anforderungskatalog zu erfüllen - das kann ich nicht beurteilen, das weiß ich nicht -, dann muss man sich gleichwohl Gedanken über die Tatsache machen, dass es sich bei dem dann infrage kommenden Anbieter wohl um ein US-amerikanisches Unternehmen handeln wird.

Dann muss man die Risiken, die sich aus der momentanen geopolitischen Situation ergeben - dazu brauche ich sicherlich nicht auszuführen -, genauer im Blick behalten und entsprechende Vorkehrungen treffen. Aus meiner Sicht muss man - allein schon, um die Funktionsfähigkeit der Landespolizei zu gewährleisten - zum Beispiel dafür Sorge tragen, dass das System nicht von anderer Seite abgeschaltet werden kann. Wenn man das alles hinbekommt, mag der Einsatz eines solchen Systems möglich sein.

Aber all das - das will ich sehr deutlich sagen - spricht aus meiner Sicht eher dafür, ein deutsches oder europäisches System auszuwählen - jedenfalls eines, das unter der datenschutzrechtlichen Hoheit der DSGVO und der JI-Richtlinie betrieben wird. Möglicherweise ist dann der Funktionsumfang zunächst nicht ganz so groß, aber das erkauft man sich gegebenenfalls mit einer höheren Stabilität und einer größeren Unabhängigkeit.

Ich habe aber das große Glück, dass nicht ich diese Abwägung treffen muss, sondern Sie dies tun müssen.

Wir haben, wie gesagt, das Palantir-System nicht geprüft. Es ist auch sehr fraglich, ob wir es uns ansehen könnten und dürften. Insofern kann ich nur ganz grundsätzlich sagen: Beschreiben Sie zunächst genau, was die Landespolizei braucht, und gehen Sie damit dann in eine Marktanalyse. Wenn dabei herauskommt, dass europäische Systeme nicht ausreichend leistungsfähig sind, dann erscheint es mir richtig, herauszufinden: Wie lange dauert es, ein solches System aufzubauen? Welche Teile gibt es schon? Wo gibt es Anfänge von Systemen? Wie weit ist das Projekt P20? - Dieses Stichwort wird Ihnen allen etwas sagen. - Kann man damit etwas anfangen? Ich kann das im Moment nicht beantworten. Ich will nur darauf hinweisen, dass die

datenschutzrechtlichen Risiken bei einem europäischen System zumindest aus unserer Sicht erheblich besser beherrschbar wären.

Jetzt komme ich zu dem für mich angenehmsten Teil des Entschließungsantrags, nämlich zu der - dritten - Aufforderung, frühzeitig Kontakt zum Landesdatenschutzbeauftragten aufzunehmen. Darüber freue ich mich selbstverständlich. Ich freue mich auch deshalb darüber, weil vermutlich nicht allen von Ihnen die Antworten, die ich Ihnen heute gebe, gefallen. Es stellt eine erhebliche Herausforderung dar, überhaupt solche Analysesysteme einzuführen.

Wenn ich die Ergebnisse der Innenministerkonferenz dazu richtig verfolgt habe, haben sich die Länder darauf geeinigt, dass diejenigen, die solche Systeme im Moment betreiben, sie weiterbetreiben, aber in nächster Zeit keine weiteren Systeme aufgeschaltet werden. So habe zumindest ich die Verständigung der Innenministerinnen und -minister verstanden. Das scheint mir eine kluge Idee zu sein, weil das Feld sehr bunt ist und wir, ob wir wollen oder nicht, bei dieser Art von Datenverarbeitung, die aus unserer Sicht schon per se hochproblematisch ist, sehr darauf achten müssen, dass wir digitale Souveränität auf Dauer gewährleisten.

Das alles spricht dafür, weiter im engen Austausch zu bleiben, auch zu solch schwierigen Themen. Sie tun das ganz offensiv, und es freut mich, dass ich hier heute vor Ihnen sprechen durfte.

Abg. **Deniz Kurku** (SPD): Herr Lehmkemper, ich will das ganz offen sagen: Ich bin ein Stück weit beruhigt, denn in der vorherigen Anhörung klangen die Aussagen zumindest für mich etwas anders. Vor allen Dingen geht es darum - so verstehe ich Sie -, den Rahmen so eng zu stecken, dass unsere Polizei- und Ordnungsbehörden zwar über ein effizientes System verfügen, aber der Datenschutz und vor allem auch die Freiheit der Menschen garantiert werden können.

Meine Frage: Wie schätzen Sie das Risiko ein, dass sich die genannten Zusagen zum Datenschutz usw. durch ein Update - auch durch ein vorher vertraglich festgelegtes - komplett ändern können? Wirkliche Sicherheit kann es, gerade vor dem Hintergrund des Datenschutzes, eigentlich gar nicht geben; denn es handelt sich um relativ offene und nicht um abgeschlossene Systeme. Wie würden Sie das datenschutztechnisch bewerten?

LfD **Denis Lehmkemper:** Wenn man eine vertragliche Regelung - über AV-Verträge oder Ähnliches - hat, und es werden nachträglich Komponenten aufgeschaltet, die nicht vertragskonform sind, dann - so meine ich grundsätzlich - wird man abschalten müssen. Dazu werden wir sicherlich sehr schnell Einigkeit hier im Raum erzielen; denn wohl niemand wird damit einverstanden sein, wenn Komponenten aufgeschaltet werden, die gesetzlich und vertraglich nicht gedeckt sind. Das kann der Staat nicht wollen!

Aber ich will auch deutlich sagen: So habe ich den Antrag nicht verstanden. Ich habe ihn so verstanden, dass man eine saubere Lösung herbeiführen möchte, auch rechtlich.

Ich habe das - wenn auch in einer geopolitisch etwas anderen Lage - in der sicherlich nicht so extremen, aber doch ähnlichen Diskussion um die Einführung von Microsoft-Produkten gesagt: Bei einem Bäcker, dem ich nicht vertraue, weil er vielleicht kein ordentliches Mehl verbackt, kaufe ich keine Brötchen. - Wie Sie wissen, haben wir bei der Einführung von Teams in der niedersächsischen Landesverwaltung gesagt, dass die damals und jetzt gegebenen Sicherungsmaßnahmen einer Vier mit Versetzung entsprechen - so haben wir es damals formuliert - und wir sie akzeptieren können. Dies würde ich von jedem der Systeme erwarten.

Eine andere Frage ist, ob man das von Anfang an bekommt. Aus datenschutzrechtlicher Sicht rufe ich dazu auf, bitte erst zu prüfen, ob es nicht europäische Systeme gibt, die so etwas besser können.

Aber es bleibt - das will ich ganz deutlich sagen - die Veränderung in der Datenverarbeitung: Mit einem solchen System geht man weg von der Vorgangsdatenverarbeitung hin zu sehr zusammengezogenen Mustern und zu sehr personenbezogenen Datenverarbeitungen. Dieses Problem ergibt sich aber an vielen Stellen, allein schon durch den technischen Fortschritt. Umso wichtiger ist es - da bin ich ganz in der Rolle des Datenschutzbeauftragten -, sauber zu verarbeiten. Ich will also nicht sagen, dass es nicht geht, aber man muss sich darüber klar sein.

Abg. **Birgit Butter** (CDU): Herr Lehmkemper, vielen Dank, dass Sie wieder hier sind. Das zeigt, wie wichtig Sie und Ihre Einschätzung uns sind. So haben wir im Entschließungsantrag ausdrücklich darum gebeten, Ihre Expertise einzubeziehen; denn - da sind wir uns alle hier in diesem Raum einig - wir bewegen uns auf einem hochsensiblen Terrain: im Spannungsverhältnis zwischen der Fähigkeitslücke der Polizei einerseits und dem Datenschutz andererseits.

Ich fand insofern Ihre letzte Einlassung gut. Auch das Bundesverfassungsgericht betont die engen Grenzen; in diesen engen Grenzen ist der Einsatz der Analysesoftware aber zulässig. Wir sind die Gesetzgeber. Wir müssen eine rechtssichere Rechtsgrundlage schaffen. Da wir aber nicht die Weisheit gepachtet haben und Ihre Expertise brauchen, führen wir heute diese Expertenanhörung durch. Insofern sollte vor dem Hintergrund des genannten Spannungsverhältnisses nicht immer wieder gesagt werden: „Dieser Einsatz ist nicht möglich!“, sondern: „Es könnte gehen, wenn ...“ Das Bundesverfassungsgericht legt uns an dieser Stelle keine Steine in den Weg, und auch Sie sagen, dass der Einsatz - mit der gebotenen Sorgfalt! - möglich ist. Dafür bin ich Ihnen sehr dankbar.

Wir müssen uns im Rahmen einer NPOG-Novelle sorgfältig überlegen, welche Rechtsgrundlage wir für ein modernes Polizeigesetz - das war der Anspruch der Innenministerin für die NPOG-Novellierung - brauchen. Insofern habe ich keine konkrete Frage, sondern nur eine Anmerkung, Frau Vorsitzende: Im Rahmen der Anhörung werden wir jetzt unter anderem Vertreter von Palantir und den hessischen Polizeivizepräsidenten hören, aber auch andere Positionen. Wir werden das ganze Spektrum an Meinungen hören, also von absoluter Ablehnung über gemäßigte Positionen bis hin zu absoluter Befürwortung. Insofern wäre es, glaube ich, sinnvoll, wenn wir uns mit Fragen, die sich aus den Beiträgen der Anzuhörenden ergeben, die auf Sie folgen, Herr Lehmkemper, noch einmal an Sie wenden dürften, beispielsweise zu P20 - Herr Polizeivizepräsident Koch wird vielleicht darauf eingehen - und zur Frage sicherer Updates.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Vielen Dank, Frau Butter. So ungefähr hatte auch ich mir das vorgestellt. Sicherlich werden sich auch viele Fragen an die Vertreter von Palantir ergeben, die als Nächste vortragen werden. Auch sollte es möglich sein, auf das eine oder andere später Bezug zu nehmen. Wenn die Anzuhörenden die Möglichkeit haben, auch nach dem eigenen Vortrag an der Sitzung teilzunehmen und sich vielleicht noch ergebende Fragen zu beantworten, würde ich das sehr begrüßen.

Abg. **Stephan Bothe** (AfD): Vorab möchte ich sagen, dass ich es sehr begrüße, dass Palantir heute hier ist. Wir reden über eine ganz bestimmte Software, und insofern sollte der Hersteller auch die Möglichkeit bekommen, sein Produkt zu vertreten, zumal es sogar im Antrag erwähnt wird.

Herr Lehmkemper, vielen Dank für Ihren Vortrag. Sie hatten vor zwei Wochen sehr ausführlich zu einem ähnlichen Thema berichtet. Ich glaube, ich habe Sie damals komplett falsch verstanden. Ich hatte mir notiert - so steht es in meinen Unterlagen -, dass nach dem jetzigen Stand der geplanten NPOG-Änderungen ein Palantir-Einsatz möglich sei. Diesen Satz hatte ich mir aufgeschrieben. Bitte gehen Sie darauf noch einmal ein.

Eine zweite Anmerkung: Sie sprachen davon, dass wir keine US-amerikanische Software mehr verwenden sollen. Ich möchte daran erinnern: Es gibt Microsoft-Anwendungen, iOS, Android. Ich weiß nicht, welche Software Sie in Ihrer Behörde verwenden, aber ich glaube, es würde in Deutschland ziemlich dunkel werden, wenn wir all diese Softwares nicht mehr verwenden würden. Sicherlich kann man von einer veränderten geopolitischen Lage sprechen; das ist Ihr gutes Recht. Allerdings sind die USA und wir immer noch NATO-Partner, also Verbündete, und es gibt überhaupt keinen Grund, das jetzt anders einzuschätzen. Daher frage ich: Haben Sie als Datenschutzbeauftragter explizite Hinweise darauf, dass Palantir beispielsweise Daten aus anderen Bundesländern an US-amerikanische Behörden weitergeleitet hat oder dass Daten aus Bundesländern, wo Palantir bereits genutzt wird, durch Softwareupdates oder andere Maßnahmen abgeflossen sind?

LfD **Denis Lehmkemper:** Zu Ihrer ersten Frage: Ich meine, in der Anhörung gesagt zu haben - jedenfalls wollte ich das sagen, und insofern ist es gut, dass Sie mir die Möglichkeit geben, das klarzustellen -, dass § 45 a NPOG-E die Möglichkeit eröffnet, solche Systeme einzusetzen. Ich meine aber, mich sehr genau daran erinnern zu können, dass ich auf die Unzulänglichkeiten dieser Möglichkeitseröffnung hingewiesen habe. Ich habe auch gesagt, dass diese Norm, wie es sich für Normen gehört, offen ist. Das heißt, darin steht nicht - das wäre wohl auch kaum möglich -: „Der Einsatz von Palantir wird ermöglicht."

Gestatten Sie mir in diesem Zusammenhang eine Randbemerkung; auch das sprach ich eben an. Wir verwenden den Begriff „Palantir" hier wohl meist als Oberbegriff. Nach meiner Recherche, auch bei Datenschutzbeauftragten anderer Länder, werden ganz unterschiedliche Funktionsumfänge unter diesem Oberbegriff gesammelt. Daher stammt mein Vorschlag bzw. meine Bitte, zunächst zu prüfen, was benötigt wird. Auch das, meine ich, habe ich bereits vor zwei Wochen gesagt. Wenn man weiß, was man braucht und haben möchte, kann man gesetzliche Grundlagen viel normenklarer definieren.

Zu Ihrer zweiten Frage nach US-amerikanischer Software: Keine Frage, wir alle haben US-amerikanische Software im Einsatz - ich sogar, das gebe ich freimütig zu, auch privat. Da besteht auf den ersten Blick ein Wertungswiderspruch. Ich bitte aber deutlich darauf zu achten, was die jeweilige Software tut, welche Daten rein theoretisch abfließen und wozu sie genutzt werden können. Wenn man eine ordentliche Betrachtung auch des Datenschutzes in einem Forderungskatalog abbildet, würde sich alles das aus der Datenschutzfolgeabschätzung ergeben. Auf dieser Grundlage kann man - da teile ich Ihre Position - diese Entscheidungen besser treffen.

Ich sehe - wie wohl die meisten hier im Raum - eine geänderte geopolitische Lage, obwohl ich persönlich sehr froh bin, dass die USA unser NATO-Partner sind. Mit einem Blick in Richtung Osten hätte ich mehr Sorgen. Ich sehe die Gefahr, dass wir uns in Bereichen abhängig machen, in denen es sinnvoll wäre, auf mehr digitale Souveränität zu setzen. Wenn es Systeme gäbe, die in Europa produziert und laufen würden und einen ähnlichen Leistungsumfang hätten - das ist die große Frage, die ich nicht beantworten kann -, dann würde ich immer dazu raten, keine Systeme zu nehmen, die außerhalb des DSGVO-Raums entwickelt wurden.

Zu Datenabflüssen oder Datenpannen kann ich nichts sagen. Ich hoffe, dass es bisher keine gegeben hat. Aber daraus zu schließen, dass so etwas nicht passieren wird, scheint mir eine schwierige These. Insofern weiß ich nicht so recht, worauf Sie hinauswollen, aber wir können das gern vertiefen.

Abg. **Saskia Buschmann** (CDU): Herzlichen Dank für die Ausführungen zum Thema Datenschutz und Palantir, Herr Lehmkemper. Der Begriff „Palantir“ wird mittlerweile für Analysesoftwares benutzt wie „Tempo“ für Papiertaschentücher.

Ich halte den Einsatz solcher Systeme für sehr zielführend. Sie haben gesagt, dass man dadurch die Polizei deutlich entlasten kann. Sofern entsprechende europäische Systeme auf dem Markt sind, wollen auch andere Bundesländer gern zu einem solchen System wechseln; zumindest ging das aus den Ausführungen hervor. Meinen Sie, dass die Daten nur mit diesem einen System zu koppeln sind? Oder kann man die Daten auch zu anderen Bereichen überführen?

Ich habe noch eine Frage zum Thema der personen- bzw. vorgangszentrierten Datensammlung. Sie hatten gesagt, dass es diesbezüglich quasi zu einem Wechsel komme. Bislang habe ich das Funktionsprinzip dieser Analysesoftware - ganz gleich, welche man einsetzt - immer so verstanden, dass sie ein Hilfsmittel für die Polizei ist, um Aufgaben technisch zu bewältigen, die bislang händisch erledigt werden müssen. Es müssen also bereits Grundlagen vorliegen, die es gestatten, dass die Polizei Daten zu einer Person zusammenführt. Das heißt, zu diesem Übergang zwischen personen- und vorgangszentrierter Datenverarbeitung kommt es bei der Polizei schon jetzt. Welchen Unterschied sehen Sie in der technischen Anwendung?

LfD **Denis Lehmkemper:** Fangen wir mit dem Unterschied der Datenverknüpfung an. An dieser Stelle geht es um § 45 a des NPOG-Gesetzentwurfs. Wenn diese Regelung tatsächlich so schrankenlos ins Gesetzblatt kommt - wie man in der Verwaltung sagt -, dann können auch Zeugenaussagen, sonstige Daten und Internetrecherchedaten in die Betrachtung mit einfließen.

Das ist, wenn ich auf die Anhörung vor 14 Tagen zurückblicke, damals vielleicht nicht ganz klar geworden: Es geht dabei nicht darum, dass der Polizeivollzugsbeamte in der Polizeidienststelle im Internet recherchiert, ob der Verdächtige auch dort auffällig geworden ist. Dass das passiert und dass das auch richtig und gedeckt ist, ist keine Frage. Es geht vielmehr darum, dass Datenbanken geschaffen werden, die große Teile des Internets durchsuchen und daraus Daten abgreifen, und aus diesen Datenbeständen werden zusammen mit den Ermittlungserkenntnissen neue Erkenntnisse gewonnen. Gerade darin besteht die besondere Qualität dieser Analysesoftware. Das wollen Sie in gewisser Weise - so habe ich Sie verstanden - mit § 45 a erreichen. Dafür muss man prüfen, welche Daten einfließen dürfen. Es muss zum Beispiel geprüft werden, ob sie rechtswidrig im Internet oder falsch sind. All diese Dinge muss man betrachten.

Darin liegt meiner Meinung nach die Veränderung: Daten werden standardisiert vorgehalten - wobei ich nicht von Vorratsdatenspeicherung sprechen möchte -, um sie im Falle eines entsprechenden Bedarfs für die polizeiliche Arbeit verwenden zu können. Das ist etwas anderes als eine Internetrecherche nach einem Verdächtigen. Das hat eine andere Qualität. - Ich hoffe, das ist jetzt deutlich geworden, aber ich befürchte, das ist nicht der Fall.

Abg. **Saskia Buschmann** (CDU): Eine kurze Nachfrage, weil ich das nicht ganz verstehe: Meinen Sie mit „Daten im Internet“ Daten im World Wide Web? Ich habe das bislang immer so verstanden, dass es darum geht, Daten zum Beispiel aus dem polizeilichen Auskunftssystem mit Daten

aus anderen Datenbanken wie den Einwohnermeldedatenbanken zusammenzuführen. Wenn Sie das mit „Internet“ meinen, kann ich Ihnen folgen, aber sonst leider nicht.

LfD **Denis Lehmkemper:** Das ist aber eine Frage der Ausgestaltung der Rechtsgrundlage. Wenn Sie vorgeben, nur die Daten, die ohnehin rechtmäßig erhoben worden sind, anders, schneller - wie auch immer - miteinander in Beziehung zu setzen, dann ist das etwas anderes als das, was auch im Polizeigesetzentwurf angelegt ist, nämlich eine Möglichkeit zur freien elektronischen Recherche im Internet. Wenn Sie das so ausgestalten wollen, dann habe ich an dieser Stelle weit weniger Bauchschmerzen - nicht keine! Aber im Moment ist der Entwurf in dieser Hinsicht aus meiner Sicht noch nicht klar genug.

Abg. **Saskia Buschmann** (CDU): Das bedeutet, dass Ihnen § 45 a noch nicht ausreichend präzise formuliert wurde?

LfD **Denis Lehmkemper:** Ja, die damit auf unserer Seite verbundenen Sorgen ergeben sich auch aus unserer Stellungnahme.

Abg. **Saskia Buschmann** (CDU): Dort müsste also auch geregelt werden, unter welchen Umständen die Analysesoftware überhaupt angewendet werden dürfte?

LfD **Denis Lehmkemper:** Na ja, wenn der Einsatz dann rechtmäßig ist, darf man sie nutzen.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Herr Lehmkemper hatte vor zwei Wochen sogar das Wo thematisiert.

LfD **Denis Lehmkemper:** Sie hatten auch nach den Lock-in-Effekten gefragt, Frau Buschmann. Diese können immer ein Problem sein. Ich kann zurzeit nicht sagen, ob am Ende ein Lock-in-Effekt eintritt. Ich kann aber nur davor warnen, sich zu stark von einem Anbieter abhängig zu machen. - Das ist die Standardwarnung des Datenschutzbeauftragten in allen Belangen. - Irgendwann müssen Sie abwägen, ob man die Risiken, die mit dem Lock-in-Effekt in Bezug auf ein bestimmtes System verbunden sind, eingehen möchte; denn natürlich bestehen diese Lock-in-Effekt-Risiken auch bei jedem anderen System.

Abg. **Michael Lühmann** (GRÜNE): Mich interessiert eine Klarstellung. Wir bewegen uns hier in einem hochsensiblen Bereich. Sie sagten, Teams sei mit der Note 4 gerade noch durchgegangen. Aber jetzt sprechen wir über eine ganz anders gelagerte Software, eine Analysesoftware. Das erfordert eine ganz andere Prüfung: Mit welchen Daten haben wir es zu tun? Es geht noch stärker um die einzelne Person. - In diesem Bereich werden die Noten nach gänzlich anderen Anforderungen vergeben. Im Fall von Palantir starten wir vielleicht mit einer 7 und landen am Ende bei einer 10.

Auch wenn wir anderswo ebenfalls US-amerikanische Software nutzen, reden wir im Fall von Palantir über eine ganz andere Art von Software, auch hinsichtlich der Frage, was sie kann. Die Hinweise zu § 45 a liegen uns vor. Aber selbst, wenn wir zu allen Hinweisen Klärungen finden würden, befänden wir uns in einem sehr schwierigen Bereich, was die Datensouveränität und was die Qualität der Daten, die über eine solche Analyse generiert werden, angeht. Da sind wir quasi im allersensibelsten Kernbereich.

Deswegen lautet Ihr Votum dazu: Vorsicht! - Erstens Vorsicht bei der Gestaltung der Regelung, und zweitens Vorsicht bei der Anwendung. Auch dabei sollten wir Sie quasi immer mit an Bord haben, damit wir gucken können, wie diese Algorithmen wirklich funktionieren und ob beim Einsatz irgendwelche Fehlstrukturen in den Algorithmen festzustellen sind. Auch das wäre zu bedenken. Ein Blick auf die Ergebnisse von Palantir in den USA zeigt nach allem, was wir so mitbekommen, dass es dort einen Bias in dem Algorithmus gibt. Wie wir uns diesem Problem nähern, ist eine weitere Frage.

Abg. **Birgit Butter** (CDU): Ich möchte etwas klarstellen, damit die Diskussion hier nicht in eine falsche Richtung läuft: Uns als CDU-Fraktion ist es wichtig, dass es nicht um mehr Daten geht, sondern um die Zusammenführung und Auswertung bereits rechtskonform von der Polizei erhobener Daten. Dafür brauchen wir in Niedersachsen ein modernes System, und zwar schnell. Das ist der Hintergrund des CDU-Antrags.

LfD **Denis Lehmkemper:** Lassen Sie mich hierzu noch eine Erläuterung geben. Nach allem, was man der Presse entnehmen kann, kommt der bayerische Einsatz von Palantir - er weist mutmaßlich keine Verbindung zum Internet, aber sehr enge Kontrollmöglichkeiten auch für meinen sehr geschätzten bayerischen Kollegen auf - diesen Vorstellungen wohl am nächsten. So vorsichtig möchte ich es formulieren; derzeit kann ich es nicht konkreter fassen.

Palantir Technologies GmbH

Schriftliche Stellungnahme: Vorlage 4

Anwesend:

- Dr. Stefanie Kirschke
- Dr. Josef Korte

Dr. Josef Korte:

Dr. Stefanie Kirschke:

Vors. Abg. **Doris Schröder-Köpf** (SPD): Herzlich willkommen, Frau Dr. Kirschke und Herr Dr. Korte. Herr Dr. Korte leitet für Palantir Technologies die Zusammenarbeit mit den Regierungsbehörden in Deutschland sowie die KI-Strategie im internationalen Regierungsgeschäft. Normalerweise hören wir hier keine Vertreter von Unternehmen an, das ist insofern durchaus ungewöhnlich.

(Abg. Stephan Bothe [AfD]: Normalerweise werden auch keine Unternehmen in Anträgen erwähnt!)

Genau. - Ich darf Sie bitten, vorzutragen.

Dr. Josef Korte: Vielen Dank für die Einladung. Wir begrüßen ausdrücklich die Möglichkeit, hier unsere technischen Perspektiven und Erfahrungen in die Diskussion einzubringen - auch deshalb, weil wir - lassen Sie mich das sagen, weil Sie es eingangs erwähnt

haben - selbstverständlich an den demokratischen Willensbildungs- und Entscheidungsprozess glauben und gern daran mitwirken.

Wir sprechen hier als Vertreter eines Unternehmens, das die im Antrag beschriebene Recherche- und Analyseplattform nicht nur entwickelt, sondern deren Implementierung in vier Bundesländern über mittlerweile fast ein Jahrzehnt begleitet. Durch diese Arbeit sind uns die technischen, rechtlichen und fachlichen Herausforderungen im Zusammenhang mit der Plattform bekannt, und aus dieser Erfahrung möchten wir drei Punkte beitragen, die uns in der Debatte als hilfreich erscheinen.

Erstens. Eine moderne Recherche- und Analyseplattform unterstützt die effiziente Polizeiarbeit und die Einhaltung rechtlicher Vorgaben gleichermaßen. Lassen Sie uns kurz betrachten, wie die Situation heute aussieht. Ermittlerinnen und Ermittler verbringen heute einen erheblichen Teil ihrer Zeit damit, Informationen manuell aus unterschiedlichen polizeilichen Systemen zusammenzutragen: verschiedene Datenbanken, verschiedene Formate, verschiedene Schnittstellen. Bei schweren Kriminalitätsphänomenen entstehen zudem oft Datenmengen, die manuell schlicht einfach nicht mehr zu bewältigen sind. Polizeibeamte benötigen im Ergebnis viel Zeit, um Informationen zu suchen und zu verarbeiten - Zeit, die in akuten Lagen kritisch sein kann oder woanders fehlt.

Wir möchten einen wichtigen Punkt hinzufügen, der in der Debatte oft zu kurz kommt. Wenn Ermittlerinnen und Ermittler heute manuell in verschiedenen Systemen recherchieren, geschieht dies oftmals ohne systemübergreifende Protokollierung und Auditierung, ohne systemübergreifend technisch erzwungene Zugriffsbeschränkungen und ohne systemübergreifend automatisiert durchgesetzte Zweckbindungen oder Löschfristen. Lassen mich dem kurz gegenüberstellen, wie eine moderne Recherche- und Analyseplattform arbeitet. Sie macht im Kern - das ist auch schon erwähnt worden - nichts anderes als das, was Ermittlerinnen und Ermittler auch manuell tun würden. Sie erlaubt es, vorhandene polizeiliche Datenbanken zu durchsuchen, Informationen zu verknüpfen und Zusammenhänge darzustellen - nur eben erheblich schneller, vollständiger und auch nachvollziehbarer. Was aber entscheidend ist: In einer modernen Recherche- und Analyseplattform wird jeder Zugriff protokolliert, jede Berechtigung bis auf den einzelnen Datenpunkt genau konfiguriert und jede Eingriffsschwelle, jede Zweckbindung oder Löschfrist rechtskonform durchgesetzt.

Zusammengefasst bedeutet dies: Effiziente Polizeiarbeit und die Einhaltung rechtlicher Vorgaben sind kein Dilemma, sondern mit Hilfe von Technologie vereinbar. Eine moderne Recherche- und Analyseplattform erhöht nicht nur die Effizienz der Polizeiarbeit erheblich, sie verbessert auch die Einhaltung datenschutzrechtlicher und polizeigesetzlicher Anforderungen und Vorgaben.

Dr. Stefanie Kirschke: Ich darf an dieser Stelle fortfahren.

Zweitens. Eine klare gesetzliche Grundlage ist notwendig und kann auch nach den Vorgaben des Gesetzgebers umgesetzt werden. Dass der Niedersächsische Landtag jetzt im Rahmen der Reform des NPOG eine gesetzliche Grundlage schafft, ist richtig und notwendig; und zwar unabhängig davon, welche Software am Ende tatsächlich zum Einsatz kommt.

Wie Sie alle wissen, hat das Bundesverfassungsgericht im Februar 2023 auch ganz klare Maßstäbe dafür gesetzt. Wir als Technologieunternehmen verstehen diese Anforderungen nicht etwa als Hürde, sondern ganz klar als Gestaltungsauftrag - einen Auftrag, den die Software technisch umsetzen können muss. Konkret heißt das - wie mein Kollege schon gesagt hat -: Die Plattform ermöglicht granulare Zugriffskontrollen für jede einzelne Datenquelle bis auf den Datenpunkt genau. Daten aus eingriffsintensiveren Maßnahmen, wie zum Beispiel der Telekommunikationsüberwachung, können so technisch isoliert werden. Das heißt, sie fließen wirklich nur dann in eine Analyse ein, wenn die gesetzlichen Voraussetzungen dafür erfüllt sind. Vor jeder Analyse legt die Ermittlerin oder der Ermittler die gesetzliche Grundlage fest und damit auch das nutzer- und anlassbezogene zulässige Datenspektrum. Diese Beschränkungen werden in der Software technisch erzwungen. Damit kann ein Ermittler oder eine Ermittlerin nicht auf Daten zugreifen, für die er oder sie keine Berechtigung hat. Und überdies wird selbstverständlich jeder Zugriff vollständig protokolliert - revisionssicher und für die Datenschutzaufsicht nachprüfbar.

Das bedeutet also im Ergebnis, dass eine moderne Analyse- und Rechercheplattform genau darauf ausgelegt ist, die Vorgaben, aber eben auch die Einschränkungen, die Sie als Gesetzgeber machen, verbindlich durchzusetzen.

Drittens. Palantir-Software wird bereits sicher und mit sehr großem Erfolg eingesetzt. Ich möchte jetzt ein wenig auf die Praxis eingehen. In Hessen arbeitet die Polizei mittlerweile seit fast neun Jahren mit unserer Software, in Nordrhein-Westfalen seit sechs Jahren. Bayern hat 2024 den landesweiten Betrieb aufgenommen, und Baden-Württemberg hat im vergangenen Jahr unter Beteiligung des Landesdatenschutzbeauftragten eine gesetzliche Grundlage geschaffen. Dass die Plattform in der Praxis gebraucht wird und auch große Erfolge erzielt, bezweifeln, glaube ich, nicht einmal die Kritiker. Innenminister und Polizeipräsidenten haben wiederholt öffentlich über die Nutzung der Plattform im Rahmen erfolgreicher Ermittlungen - zum Beispiel in der Terrorabwehr, aber auch bei der Aufdeckung eines Missbrauchsrings - berichtet. Auch Polizistinnen und Polizisten berichten von den Vorteilen der Plattform für ihre tägliche Arbeit, und die Polizeigewerkschaften haben sich, wie zuletzt im Anhörungsverfahren in Baden-Württemberg, öffentlich klar für eine Nutzung der Plattform ausgesprochen.

Darauf möchte ich jetzt aber gar nicht so sehr im Detail eingehen, sondern lieber noch eine Frage ansprechen, bei der wir davon ausgehen, dass sie viele von Ihnen zu Recht beschäftigt, und das ist die Frage der Datensouveränität und Betriebssicherheit. Das wurde auch schon erwähnt. Hier ist ganz entscheidend - das möchte ich betonen -, dass die Polizei in Deutschland jederzeit die volle Kontrolle über die Daten und ihre Entscheidungen behält, im Einklang mit den geltenden Gesetzen und Standards. Genau das verstehen wir unter digitaler Souveränität. Deshalb will ich noch einmal ganz klar sagen: Die Plattform läuft On-Premises. Das heißt, sie läuft auf polizeieigener Hardware, in behördlichen Rechenzentren und in polizeieigenen, besonders geschützten Netzwerken. Es gibt keine Internetanbindung. Und noch einmal im Klartext: Die grundlegendsten physischen Sicherheitsparameter - und damit die Datenhoheit und die Betriebssicherheit - liegen vollständig und jederzeit bei der Polizei. Eine Datenexfiltration ist damit technisch und selbstverständlich auch vertraglich ausgeschlossen.

Weil es angesprochen wurde: Selbstverständlich arbeitet unsere Software auch DSGVO-konform. Sonst wäre unsere Arbeit in Europa nicht möglich, sowohl im behördlichen als auch im privatwirtschaftlichen Umfeld.

Wie Sie alle wissen, hat das Fraunhofer-Institut für Sichere Informationstechnologie im Auftrag des Bayerischen Landeskriminalamtes den vollständigen Quellcode unserer Software analysiert. Das Ergebnis war eindeutig: Die IT-Sicherheit und die Datenschutzbelange sind umfassend gewahrt. Daher nochmals: Die Plattform wird bereits seit vielen Jahren in mehreren Bundesländern sicher und mit großem Erfolg eingesetzt.

Ich möchte mit einer kurzen Einordnung schließen. Technologie ist kein Selbstzweck, sondern kann nur auf Grundlage klarer gesetzlicher Regelungen und im Zusammenspiel mit den nutzenden Beamtinnen und Beamten einen Mehrwert für die Polizei und damit für die Sicherheit im Land schaffen. Daher begrüßen wir ausdrücklich die drei im Antrag genannten Forderungen: die Schaffung einer klaren gesetzlichen Grundlage, den Austausch mit den Bundesländern, die bereits Erfahrung gesammelt haben, und die frühzeitige Einbindung des Datenschutzbeauftragten.

Abg. **Deniz Kurku** (SPD): Ich würde gern kurz auf die Behauptung abstellen - das schreiben Sie auch in der schriftlichen Stellungnahme -, dass Palantir keine Daten erhebt, kauft und weiterverkauft. Sie betonen die On-Premises-Architektur. Aus technischer Sicht kann das möglicherweise korrekt sein. Ihre Darstellung - und das kritisiere ich scharf - ist aus meiner Sicht aber unvollständig, es wurden einfach Teile der Wahrheit weggelassen. Die Quellcode-Prüfung durch das Fraunhofer-Institut hat einmalig stattgefunden. Wenn ich richtig informiert bin, war das 2023/2024.

Für mich als Mitglied des Landtages stellt sich folgende Frage: Heutzutage müssen im technischen Bereich bekanntlich bei jeder Kleinigkeit Updates erfolgen, insbesondere aber bei so einem großen System. Muss das Land dann einfach Ihrem Unternehmen vertrauen, dass an dieser Stelle nichts passiert? Sie führen die Prüfung als ein zentrales Argument für unser Vertrauen und als Beleg für Datenschutz an, aber die Ergebnisse sind nicht öffentlich, man kann sie nirgendwo nachlesen. Ich muss sagen, das ist für mich eindeutig zu wenig, um in diesem hochsensiblen Bereich der Polizei- und Ordnungsbehörden, über den wir hier gerade sprechen, mit einem System wie Ihrem zu arbeiten.

Ich möchte auch darauf hinweisen, dass Palantir-Mitarbeiterinnen und -Mitarbeiter laut *SZ*, WDR und NDR in deutschen Polizeidienststellen - so haben es die Recherchen zumindest ergeben - mit Zugriff auf Echtzeitdaten gearbeitet haben. Dieser Punkt wird in der gesamten Stellungnahme mit keinem einzigen Wort erwähnt. Allein das sorgt bei mir, ehrlich gesagt, schon für einen ziemlichen Vertrauensverlust. Das sage ich Ihnen ganz deutlich.

Dr. Josef Korte: Das sind jetzt gleich drei oder vier verschiedene Punkte. Ich versuche, auf alle einzugehen und sie nacheinander abzuarbeiten.

Zunächst einmal ist es tatsächlich ein Missverständnis, dass Daten unser Geschäftsmodell wären. Das sind sie ausdrücklich nicht. Wir verkaufen keine Daten, und deswegen kaufen oder sammeln wir auch keine Daten. Das Gegenteil ist der Fall. Das wäre geschäftsschädigend, denn wir verkaufen Software.

Zu der Frage, wie das sicher aufgespielt werden kann und wie viel Hoheit die Behörden über die eigenen Daten haben: Wir haben es gerade erläutert. Es ist tatsächlich so, dass sämtliche Daten im Besitz der Polizei auf Hardware bzw. auf Servern gespeichert werden, die der Polizei gehören und in behördlichen Rechenzentren entweder von der Polizei selbst oder von entsprechenden Landesdienstleistern betrieben werden, die im gesicherten Netz der Polizei sind. Sämtliche

Tätigkeiten mit diesen Daten finden im gesicherten Netz der Polizei statt. Das heißt, dass es irgendeinen unkontrollierten Zugriff oder gar einen Abfluss von Daten geben könnte, ist technisch ausgeschlossen. Das hat im Übrigen auch das Fraunhofer-Institut festgestellt.

Zu dem Fraunhofer-Gutachten: Ja, das ist tatsächlich VS-NfD eingestuft - schon allein deshalb, weil es sensible Informationen über die Informationsarchitektur bei der Polizei enthält. Zudem berührt es natürlich auch, wenn es um den Quellcode geht, Geschäftsgeheimnisse der Firma Palantir.

Zu Ihrem letzten Punkt - Mitarbeitende der Firma Palantir -: Es ist richtig und auch durchaus üblich, dass bei der Einführung komplexer Software Mitarbeitende beteiligt sind - wir nennen sie Forward Deployed Engineers, aber das gibt es in ähnlicher Form auch bei vielen anderen, übrigens auch bei deutschen Unternehmen - und auch vor Ort in den gesicherten Netzwerken mitarbeiten. Alle Mitarbeitenden, die dort zum Einsatz kommen, sind EU- oder in der Vielzahl deutsche Staatsbürger, sie sind sicherheitsüberprüft - und zwar von jedem einzelnen Auftraggeber, von jeder einzelnen Polizei, mit der wir arbeiten -, und sie arbeiten in der Infrastruktur und in den Netzen der Polizei, wobei ein Abfluss oder eine Exfiltration von Daten, wie wir es eben benannt haben, unmöglich ist. Zudem wird jede Tätigkeit - das ist insoweit hoffentlich auch bei anderen Anbietern normal -, die dort erfolgt, protokolliert und auditiert und kann entsprechend auch von der Polizei nachverfolgt werden.

Um es zusammenzufassen: Wichtig ist, dass die Auftraggeber jederzeit vollständige Hoheit über ihre Daten und vollständige Kontrolle darüber haben, was damit passiert und wer welche Tätigkeiten ausübt.

Abg. **Deniz Kurku** (SPD): Das mit dem „kaufen und verkaufen“ lassen wir mal so stehen. „Erheben“ ist sozusagen genau der Zauber Ihrer Software. Das wird also erfolgen. Es werden Daten erhoben.

Mich interessiert aber ein anderer Punkt. Es ging gerade um den Quellcode. Wäre es, wenn sich - was ich nicht hoffe - in den weiteren Beratungen eine entsprechende Mehrheit finden würde und wir auf das Palantir-System setzen würden, möglich, dass dem Landesdatenschutzbeauftragten der Quellcode und alles Weitere - auch das komplette Audit - zur Verfügung gestellt werden? Es handelt sich bei dem Landesbeauftragten immerhin um eine Vertrauensperson des Landes Niedersachsen.

Dr. Josef Korte: Nein, es ist ein Missverständnis, dass wir in der Software Daten erheben. Die Plattform ist so konzipiert, dass sie es unseren Kunden - in diesem Fall der Polizei - erlaubt, ihre Daten, die sie bereits erhoben haben, rechtskonform zusammenzuführen und rechtskonform zu nutzen, im Rahmen der jeweils landesgesetzlichen und auch bundesgesetzlichen Vorgaben.

Ich habe auch vernommen, dass der Landesdatenschutzbeauftragte sich die Software gern anschauen würde und das gern erklärt bekäme. Selbstverständlich ist er eingeladen, das zu tun.

Abg. **Deniz Kurku** (SPD): Ich meinte das Audit.

Dr. Josef Korte: Für das Audit kann ich das an dieser Stelle nicht zusagen, weil es, wie gesagt, als VS-NfD eingestuft ist. Die Bayerische Polizei hat das durchgeführt. Das müsste also mit der Bayerischen Polizei geklärt werden.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Das würden wir dann gegebenenfalls klären. - Herr Dr. Lahmann möchte gern direkt etwas dazu sagen.

Dr. Christoph Lahmann (LfD): Ich erlaube mir, ganz kurz wenige Sätze dazu zu sagen. Ich möchte Ihren Einwand noch präzisieren: Worin das Problem hier liegt - und ich glaube, das ist auch Ihr Hauptargument -, ist, dass die Sicherheit, die so ein Audit ausstrahlt, sich immer genau auf diejenige Version bezieht, die getestet worden ist. Stellen Sie sich einmal vor, Sie haben einen VW und fragen den TÜV: Besteht mein VW den Crashtest? Der TÜV gibt Ihnen die Antwort: Wir haben schon mal einen VW getestet, der hat das bestanden. - Das ist ungefähr das, was wir im Moment haben.

Wenn wir einbezogen werden würden, würden wir sagen: Gebt uns bitte die Versionsnummer eurer Software. - Unser Votum würde dann für genau diesen einen Versionsstand gelten. Ich würde Sie gern einmal fragen: Welcher Stand wurde getestet, wo stehen Sie heute? Da ist wahrscheinlich sogar ein anderes Hauptrelease dazwischen. Ich wäre da also sehr vorsichtig.

Wenn wir hier Sicherheit haben wollen, müssten wir sagen: Vor jedem Upgrade, vor jedem Sicherheitspatch müsste ein erneuter Rezertifizierungsprozess erfolgen. Insofern ist schon das grundsätzliche Vertrauen in die Software viel wichtiger als dass wir sagen: Wir haben einmal punktuell geguckt, und das war in Bezug auf gewisse Merkmale, die wir auch nicht genau kennen, sauber.

Ich will damit nur sagen: Man sollte vielleicht nicht allzu große Erwartungen an punktuelle Audits richten.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Vielen Dank für diese grundsätzlichen Erläuterungen. Im Geschäftswesen gilt der Grundsatz „Wer zahlt, schafft an“. Das ist hier nicht ganz der Fall.

Abg. **Alexander Saade** (SPD): Üblicherweise sprechen wir hier über gesetzliche Rahmenbedingungen oder darüber, dass wir generell etwas beschaffen wollen. Dass explizit eine Firma zu einer Anhörung eingeladen wird, bei der wir in der Regel Experten zu Wort kommen lassen, ist daher schon eine besondere Situation.

Meine erste Frage lautet deshalb: Würden Sie sich selbst als Experten bezeichnen oder eher als jemanden mit eigenem Geschäftsinteresse, abhängig von Palantir?

Sie haben On-Premise quasi mit digitaler Souveränität gleichgestellt, wenn ich das richtig verstanden habe. Ich bin mir nicht ganz sicher, ob ich dem so folgen kann. Wenn ich das richtig verstehe, braucht es, auch wenn das implementiert ist, weiterhin die Unterstützung von Palantir, von entsprechenden Mitarbeitenden, die dann wahrscheinlich vor Ort Updates auf die Systeme aufspielen. Das Betriebswissen verbleibt also bei Ihnen. Deswegen kann ich dem nicht ganz folgen und würde gern wissen: Sollte Palantir eingeführt werden, welche Rollen bräuchte man in Niedersachsen sowohl für die Einführung als auch für den Betrieb des Ganzen? Kann man überhaupt garantieren, dass, wenn sich die geopolitische Situation ändert - wenn der CEO in Amerika sagt: Jetzt ist Schluss! -, die Systeme weiterlaufen, ohne die Unterstützung von Palantir selbst?

Dr. Josef Korte: Ich würde vorab gern noch ganz kurz zu dem Thema Updates bzw. Upgrades Stellung nehmen. Denn das ist wichtig und steht jetzt im Raum. Sie müssen da selbstverständlich nicht nur uns vertrauen, sondern auch den eigenen Mitarbeitenden bei der Polizei. Jedes Upgrade wird bei der Einspielung bereits dokumentiert und geprüft. Es gibt keine direkte Verbindung zum Internet, sondern es gibt Demilitarisierte Zonen - wenn man das technisch so benennen will -, in denen das entsprechend durch die Polizei geprüft wird. Insofern müssen Sie auch dem technischen Sachverstand der Kolleginnen und Kollegen vertrauen und nicht nur uns.

Dr. Stefanie Kirschke: Zu Ihrer Frage bezüglich der Souveränität: Ganz grundlegend sind wir tatsächlich der Meinung, dass die Souveränität sehr daran zu bemessen ist, dass die Kunden jederzeit und vollständig die Kontrolle über ihre Daten, die Kontrolle über ihre Entscheidungen in der Software und auch die Kontrolle über den Betrieb der Software behalten. Das ist für uns quasi die Definition für digitale Souveränität und einen souveränen Umgang mit den eigenen Daten. Wie gesagt, es geht hier um Daten, die die Polizei rechtmäßig erhoben hat und vorhält. In der Software werden keine Daten neu erhoben, sondern verarbeitet und analysiert.

Ich möchte ebenfalls noch kurz auf die Frage zur Unterstützung durch die Mitarbeiter von Palantir eingehen. Mein Kollege hat es gerade schon gesagt: Ja, besonders in der Implementierungsphase und auch zu sehr speziellen technischen Unterstützungsmaßnahmen sind Palantir-Mitarbeiter beim Kunden tätig, aber immer unter der vollen Aufsicht des Kunden mit speziellen Zugriffsrechten, die dann auch wieder zurückgenommen werden. Das heißt, es besteht kein universeller Zugang für Mitarbeiter.

Ganz prinzipiell - es wurde schon gesagt -: Wir sind ein Softwareunternehmen, wir verkaufen Softwarelizenzen, und wir haben wirtschaftlich kein Interesse daran, dass die Kunden für immer an uns gebunden sind, an unsere Ingenieure. Ganz im Gegenteil: Es ist so, dass wir den Kunden den technischen Betrieb unserer Software in die Hand legen möchten. Wir haben mittlerweile bei allen unseren Polizeikunden in Deutschland - in Hessen, in Bayern - eigene Entwickler, die die Software selbstständig betreiben können, ohne unsere Unterstützung. Das heißt, das Betriebswissen wird tatsächlich von uns an die Mitarbeiter der Polizei, an die Administratoren und Entwickler weitergegeben mit dem Ziel, dass sie die Software betreiben können.

Dr. Josef Korte: Sie haben eingangs unser Expertentum kritisch hinterfragt, wenn ich das richtig verstanden habe. Ich würde für uns in Anspruch nehmen, dass wir technische und fachliche Experten sind. Selbstverständlich sprechen wir hier auch als Unternehmensvertreter. Allerdings benennen wir klar die Möglichkeiten und Grenzen, und die rechtlichen Vorgaben kommen von Ihnen, vom Niedersächsischen Landtag. Sie sagen, was rechtlich zulässig ist, und wir können es technisch umsetzen. So funktioniert aus unserer Sicht das Zusammenspiel.

Abg. **Alexander Saade** (SPD): Zwei meiner Fragen wurden nicht wirklich beantwortet. Ist ein Betrieb ohne Ihren Support, ohne Palantir selbst möglich? Erfolgt das in der Praxis bereits irgendwo in Deutschland? Welche Personen, also welche Rollen bräuchte es von Palantir, um die Software hier in Niedersachsen zu implementieren, und wie wäre deren Status? Wie lange bräuchte man das?

Dr. Josef Korte: Es gibt tatsächlich ein Bundesland, in dem das System komplett ohne irgendeinen betriebsunterstützenden Zugriff oder Ähnliches durch Palantir betrieben wird. Man kann das System also auch ohne unseren direkten Zugriff betreiben.

Zu den Rollen: Dazu braucht es natürlich eine gewisse Art technischer Expertise, also Entwickler und Systemadministratoren. Es braucht eine Handvoll Leute, um das zu betreiben.

Abg. **Michael Lühmann** (GRÜNE): Ich möchte an die Frage anknüpfen, was Ihre Rolle in dieser Anhörung ist. Ich kann Sie gar nicht dafür kritisieren. Das ist feinster Lobbyismus, und Sie machen hier Ihren Job. Ich bin eher irritiert darüber, dass Sie überhaupt zu dieser Anhörung eingeladen wurden. Aber warum sie das für richtig hielten, müssen sich andere fragen.

Ich habe auch einige Fragen an Sie. Wir können über Gesetze alles Mögliche regeln, und dann mag das vielleicht sogar funktionieren. Aber wir reden hier grundsätzlich über Vertrauen, und ich wüsste schon gern, wie wir einer Firma wie der Ihren vertrauen können, wenn Peter Thiel etwa sagt, dass Demokratie und Freiheit nicht mehr so richtig zusammenpassen, dass man Demokratien über Sicherheitsarchitekturen beherrschbar macht. Ich könnte eine ganze Reihe an Zitaten anführen. Meine erste Frage lautet: Wie verhalten Sie sich dazu, dass es eine ganze Menge Menschen gibt, die sagen, das ist im besten Falle rechtsradikal oder schlimmer?

Zweitens. Erklären Sie uns bitte die Funktion und die Arbeit von Palantir im Rahmen der US-amerikanischen ICE-Einsätze und wie Sie das bewerten. Noch einmal: Wir reden hier über Vertrauen.

Drittens. Die Schweizer Armee hat sich sehr eindeutig geäußert. Wir können jetzt gern darüber diskutieren, ob eine Verschlusssache des Fraunhofer-Institutes zu einem Zeitpunkt X mehr Wert hat als eine intensive Analyse der Schweizer Armee. Ich habe jedenfalls großes Vertrauen in die Schweizer Armee. Daran schließt sich die Frage an: Wenn ein Medium darüber berichtet, dass es dort Konflikte gibt, klagt Palantir gegen das Medium. Das passt nicht zu meinem Verständnis, wie wir in Europa über solche Fragen diskutieren. Wie schätzen Sie das ein?

Vors. Abg. **Doris Schröder-Köpf** (SPD): Ich möchte an dieser Stelle etwas in meiner Funktion als Vorsitzende sagen. Diese beiden Herrschaften sind unsere Gäste, und wir behandeln unsere Gäste immer gut und anständig. Ich fände es schön, wenn wir freundlich und sachlich blieben.

Abg. **Michael Lühmann** (GRÜNE): Ich möchte das in Richtung der Anzuhörenden klarstellen. In Ihrer Rolle machen Sie das, was Sie tun müssen, und das ist auch richtig. Es ist keine Kritik an Ihnen, dass Sie hier sind.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Habe ich das falsch verstanden? Dann können wir jetzt auf einem freundlichen Niveau arbeiten.

Dr. Stefanie Kirschke: Ich würde zurückweisen, dass wir als Lobbyisten hier sind. Sicherlich hat Palantir ein wirtschaftliches Interesse am Verkauf seiner Software, aber Herr Dr. Korte hat in den vergangenen fast zehn Jahren die Implementierung dieser Software in mehreren Landespolizeibehörden begleitet. Insofern würde ich nicht von Lobbyismus sprechen, sondern tatsächlich von Expertise. Ich selbst bin im Unternehmen hauptsächlich mit öffentlichen Beschaffungsvorhaben beschäftigt und würde mich auch nicht als Lobbyistin bezeichnen.

Zu Peter Thiel: Das wird in Deutschland sehr oft thematisiert, und wir sind uns auch der Kontroversen bewusst. Allerdings möchte ich ganz klar sagen, dass Peter Thiel seine politischen Aussagen als Privatperson tätigt und nicht im Namen von Palantir. Er hat das Unternehmen im Jahr 2003 mitgegründet, ist seitdem aber nicht mehr im operativen Tagesgeschäft von Palantir tätig, und dementsprechend spiegelt er auch nicht die Ansichten von Palantir wider. Ganz im

Gegenteil ist es so, dass wir im Unternehmen wirklich ganz viele politische Ansichten vereinen, und das sehen wir tatsächlich auch als Stärke. Wir folgen nicht einem Peter Thiel, sondern es gibt eine Vielfalt und eine Debattenkultur, die wir sehr schätzen und fördern.

Zu unserer Arbeit mit ICE: Auch hier verstehe ich das öffentliche Interesse und das Interesse von Ihnen als Abgeordneten. Wir arbeiten mit ICE - mit dem US-Heimatschutzministerium, genauer gesagt - bereits seit 2011 zusammen. Das ist eine sehr lange Zeit, die vier US-Regierungen umspannt - zwei demokratische mit Obama und Biden und die beiden Trump-Regierungen. Das heißt, wir verstehen uns hier als politisch agnostisch und unterstützen wichtige demokratisch legitimierte Institutionen in den USA, aber auch in Europa und Deutschland bei ihrer Arbeit und dabei, ihre Daten rechtskonform zu nutzen.

Sie haben die Berichterstattung zur Schweizer Armee erwähnt. Im Jahr 2024 gab es einen Bericht der Schweizer Armee, wobei wir allerdings ganz klar sagen müssen, dass sich dieser auf eine reine Schreibtischrecherche bezieht. In diesem Bericht sind viele Missverständnisse und Unklarheiten und auch falsche Darstellungen enthalten. Die Schweizer Armee hat uns nie kontaktiert. Wir waren nie bei der Schweizer Armee, um unsere Software prüfen oder evaluieren zu lassen. Es gab nie ein Beschaffungsvorhaben mit der Schweizer Armee, in dessen Rahmen die Schweizer Armee unsere Software hätte evaluieren können. Insofern können wir nichts anderes sagen, als dass darin wirklich viele falsche Aussagen enthalten sind.

Ende vergangenen Jahres hat das schweizerische Magazin *Republik* diesen Bericht zum Anlass genommen, zu berichten. Es ist falsch, dass wir das Magazin auf Schadensersatz verklagt hätten. Es gibt in der Schweiz ein Recht auf Gegendarstellung, und davon möchten wir als Unternehmen Gebrauch machen. Das heißt, es geht hier nicht um eine Klage auf Schadensersatz oder Ähnliches, sondern nur darum, dass wir die Möglichkeit bekommen, unsere Position darzulegen.

Ich hoffe, damit habe ich Ihre Fragen beantwortet.

Abg. **Birgit Butter** (CDU): Vielen Dank, Herr Dr. Korte und Frau Dr. Kirschke. Ich freue mich, dass Sie eingeladen wurden. Das ist richtig und wichtig. Zumindest ist unsere Auffassung, dass man besser miteinander als übereinander sprechen sollte, und hier dreht es sich nun mal um Sie. Sehen Sie es dem Kollegen Lühmann nach: Misstrauen liegt in der DNA der Grünen. Aber das nur am Rande.

Ich möchte gern folgende Fragen an Sie stellen. Ich hatte schon angekündigt, dass ich ein wenig zwischen dem Landesdatenschutzbeauftragten und Ihnen switchen möchte. Der LfD hat in seiner Stellungnahme geschrieben und gerade auch noch einmal gesagt, dass zunächst die Polizei beschreiben soll, was sie braucht, und dann soll es eine Marktanalyse geben - wie lange das dauert, muss man dann schauen. Als einen Kernpunkt hat auch der LfD die Wahrung der digitalen Souveränität genannt. Dazu hat er in seiner schriftlichen Stellungnahme folgende Forderungen aufgestellt:

- Es darf zu keiner ungeprüften Weiterverbreitung von Daten in Drittstaaten kommen, die nicht dem europäischen Rechtsstaatsniveau entsprechen.

- Ein Zugriff auf Daten aus oder der Transfer von Daten in Drittstaaten, deren Rechtsordnung nicht mit dem europäischen Recht vergleichbar ist, muss ausgeschlossen sein.

- Die Datenverarbeitung muss für eine außergerichtliche oder gerichtliche Rechtsdurchsetzung nachvollziehbar und beherrschbar sein.

- Die Software muss langfristig zur Verfügung stehen und verlässlich sein.

- Es muss sichergestellt sein, dass mit der Software eine Umstellung auf geeignetere Systeme möglich ist.

Ich würde gern von Ihnen wissen, ob Palantir das leisten kann.

Dr. Josef Korte: Lassen Sie mich vorwegsagen, dass wir natürlich auch misstrauische Fragen begrüßen. Das gibt uns die Gelegenheit zur Richtigstellung.

Können wir das leisten? - Zu allen fünf Punkten ein klares Ja. Ich gehe auch gern auf die einzelnen Punkte ein.

Zur Weiterverbreitung: Die Daten - wir haben es erläutert - sind in der Hoheit der Polizei. Sie gehören rechtlich der Polizei. Vertraglich, aber auch allein technisch ist ausgeschlossen - und zwar dadurch, dass die wichtigsten Sicherheitsparameter, also die Hardware, die Rechenzentren und die Netze, durch die Polizei kontrolliert werden -, dass die Daten unkontrolliert abgezogen oder weiterverbreitet werden.

Was den Ausschluss eines Datentransfers betrifft, würde ich ähnlich antworten.

Die gerichtliche Auswertbarkeit ist ein spannender Punkt. Ich hatte es im Eingangsstatement kurz erwähnt: Die vollständige und umfassende Protokollierung und Auditierung aller Datenverarbeitungen und auch aller Zugriffe sind ein wichtiges Unterscheidungsmerkmal zu anderen bestehenden Systemen. Unsere Software ist so konzipiert, dass sie genau das leistet und die Nachvollziehbarkeit und die Revisionssicherheit von Tätigkeiten, sowohl in der Datenverarbeitung als auch in der Nutzung der Software, sicherstellt. Das ist ein explizites Merkmal unserer Software, und ich glaube - um als technischer Experte zu sprechen - tatsächlich, dass wir da weltweit führend sind. Insofern: Ja, auch das können wir sicherstellen.

Zur langfristigen Verlässlichkeit: Wir arbeiten jetzt seit acht, neun Jahren mit der Polizei in Deutschland, in zunehmendem Maße mit verschiedenen Bundesländern. Über unsere Verlässlichkeit diesbezüglich habe ich noch keine Beschwerden gehört.

Zur Umstellung auf andere Systeme, falls Palantir eines Tages nicht mehr zur Verfügung stehen sollte, wenn der Vertrag ausläuft, weil eine europäische Lösung verfügbar ist oder aus irgendeinem anderen hypothetischen Grund: Unsere Technologie, unsere Architektur ist offen gestaltet. Wir speichern Daten in gängigen Formaten, wir verwenden gängige offene Programmiersprachen, offene Dateiformate sozusagen, und ein Export dieser Daten und ein Import in andere Systeme ist jederzeit möglich - natürlich im polizeilichen Netz, bevor das jetzt falsch aufgefasst wird. Sie können also die Daten aus der Palantir-Software exportieren und in eine andere Software im polizeilichen Netz importieren und sind als Polizeibehörde jederzeit selbstverständlich in der Hoheit und im Besitz dieser Daten.

Abg. **Saskia Buschmann** (CDU): Ich war gerade etwas irritiert, weil Sie davon gesprochen haben, dass hier Daten erhoben werden. Ich habe das bislang immer so verstanden, dass die Daten durch Ihre Software nur verbunden werden.

Ich habe mir das in Bayern angeschaut und mir erklären lassen, wie das funktioniert, und ich habe es hinterher auch anderen Leuten erklärt, die sagten: Ach so, das ist also wie ein Einfamilienhaus, in dem sieben Räume - Bayern greift auf sieben Datensätze zurück - vorhanden sind. Ich brauche einen Schlüssel, einen Datensatz, und hinterher habe ich die Daten zu dieser einen Person, und diesen Datensatz kann ich dann extrahieren. In Niedersachsen ist es im Moment so, dass wir sieben Reihenhäuser mit jeweils einem einzelnen Datensatz haben, und wir haben möglicherweise keinen Zugangsschlüssel, um in das Haus zu kommen. Der einzelne Polizist hat den Zugangsschlüssel jedenfalls nicht. Meine Frage lautet also: Sie erheben keine Daten, sondern sie verbinden sie nur, richtig?

Ein anderer Punkt: In Bayern wurde mir gesagt, es gibt nichts Vergleichbares - zumindest Stand 2024 -, was das kann, was Sie können. Das ist der jüngste Vertrag, den sie abgeschlossen haben. Ich glaube, sie haben dort auch einen Rahmenvertrag abgeschlossen, dem sich die anderen Bundesländer anschließen können.

Meine letzte Frage betrifft den Zugriff auf Ihre Software oder die Benutzung Ihrer Software. Die kann bei der Polizei jedem einzelnen Polizeibeamten über Rollenverteilung zugeschrieben werden. Das heißt, nicht jeder hat Zugriff auf diese Datenanalyse bzw. auf Ihr System, sondern das ist eben nur dort der Fall, wo die Voraussetzungen vorliegen. Wir als Landtag müssen rechtlich normieren: Wann darf diese Analysesoftware eingesetzt werden und wann nicht? - Ist das richtig?

Dr. Josef Korte: Was Sie sagen, ist richtig: Palantir bzw. die Palantir-Software erhebt keine eigenen Daten, sondern dort werden lediglich die Daten, über die die Polizei ohnehin verfügt, zusammengeführt.

Um die Analogie aus Bayern mit den einzelnen Häusern und den Reihenhäusern aufzunehmen: Tatsächlich kann man es sich so vorstellen, dass die Daten aus den einzelnen Häusern in einem Haus zusammengeführt werden. Die Analogie mit dem Schlüssel würde ich aber zurückweisen. Denn wenn ich als Polizeibeamter für zwei von sieben Häusern keinen Schlüssel habe, habe ich hinterher auch für diese beiden Räume keinen Schlüssel. Wir stellen in der Software durch ein sehr ausdifferenziertes Zugriffskonzept, das implementiert wird, sicher, dass niemand Zugriff auf etwas hätte, auf das er nicht ohnehin aufgrund der Rolle und des Anlasses Zugriff hat. Das ist ganz wichtig.

Zu Ihrer Frage nach dem Zugriffskonzept und der Rollenverteilung: Ja, das ist richtig. Genau so wird es gemacht. Was jemand sehen kann, hängt davon ab, welche Rechte er oder sie hat. Wenn beispielsweise im Bereich Staatsschutz ermittelt wird, ist das breiter aufgestellt als im Bereich schwere Kriminalität. Es hängt aber nicht nur davon ab, sondern es ist auch steuerbar mit Blick auf den Anlass. Da sind wir beim Thema Zweckbindung und anlassbasierte Freischaltung der Daten. Es ist ein großer Unterschied, ob ich in einer akuten Gefahrenlage, beispielsweise aufgrund einer Terrorgefahr, ermittle - dann sehe ich möglicherweise mehr Daten; der Gesetzgeber schreibt letztlich vor, was einschlägig ist -, als wenn ich im Zusammenhang mit einem als niedriger anzusehenden Rechtsgut oder im Rahmen einer als niedriger anzusehenden Gefahr ermittle. Auch das kann über die Plattform bis auf den einzelnen Datenpunkt genau gesteuert werden.

Zu der Frage: Gibt es etwas Vergleichbares? Wir sind in den vergangenen Jahren durch mehrere Ausschreibungen gegangen - nicht nur in Deutschland, aber ich beziehe mich jetzt auf Deutschland -, und das Ergebnis war tatsächlich immer das Gleiche vom Umfang der Leistung her. Übrigens wird bei Ausschreibungen nicht nur die Leistung, sondern auch der Preis bewertet. Beides zusammen ist von den Ausschreibenden offensichtlich so bewertet worden, dass sie Palantir den Zuschlag erteilt haben. Mir persönlich ist nichts bekannt, das einen komplett gleichen Funktionsumfang hätte.

Abg. **Sebastian Zinke** (SPD): Natürlich können Sie als Vertreter eines Unternehmens gar nicht anders, als für dieses Produkt zu werben. Insofern ist es für Sie eine schöne Sache, dass man bundesweit unter Ihrem Namen über Softwareprodukte diskutiert. Das hier ist heute also auch ein bisschen wie eine Werbeveranstaltung für Sie.

Wir sollten als Politik nicht den Eindruck erwecken, als würde die Polizei in Niedersachsen gänzlich ohne Analysesoftware arbeiten. Auch heute schon arbeitet die Polizei in Niedersachsen - wie auch andere Polizeien - mit Analysesoftware. Sie haben jetzt eine neuere, die besondere Komponenten hat. Darüber haben wir hier schon diskutiert.

Palantir ist ein Schlagwort, das im politischen Raum, in der politischen Diskussion - heute bei uns seitens der CDU - als eine Art Wundermittel für die innere Sicherheit in Deutschland gesehen wird. Das ist es nicht. Sie sagen, dass die Bundesländer Hessen, Nordrhein-Westfalen, Bayern und Baden-Württemberg Ihre Software einsetzen. Wenn es sich tatsächlich um ein Wundermittel handeln würde, müssten die Aufklärungsquoten in diesen Bundesländern exorbitant gestiegen sein, seitdem die Software eingesetzt wird. Tatsächlich ist sie aber in Hessen sogar gesunken, in NRW liegt sie bei deutlich unter 60 %. In Niedersachsen beträgt sie über 60 %. Wie erklären Sie, dass die Aufklärungsquoten, seitdem Ihre Software eingesetzt wird, in diesen Bundesländern nicht nach oben, sondern nach unten gegangen sind? Das würde mich interessieren.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Wir haben nachher auch noch die Praktiker aus Hessen hier sitzen.

Dr. Josef Korte: Das wäre tatsächlich auch mein Hinweis gewesen.

Ich stelle jetzt mal eine Mutmaßung in den Raum. Wir befinden uns hier auch ganz maßgeblich im Bereich der Gefahrenabwehr und nicht nur im Bereich der Aufklärung von Straftaten. Wenn es um die Aufklärung von Straftaten geht, müssten wir uns die schwere und schwerste Kriminalität anschauen. Insofern würde ich da tatsächlich auf die Polizei verweisen. Aber ich kann mir vorstellen, woran es liegt. Es geht um den Gefahrenabwehrbereich, und das ist sozusagen ein Präventionsparadox.

Abg. **Nadja Weippert** (GRÜNE): Vielen Dank, Frau Dr. Kirschke und Herr Dr. Korte, dass Sie die Fragen bisher so souverän beantwortet haben. Tatsächlich habe ich aber, wie alle von Rot-Grün, Bauchschmerzen, wenn es um Ihre Software geht. Ich bin absolut gegen sie. Das sage ich geradeheraus vorweg. Deshalb gehe ich auch davon aus, dass wir sie hier in Niedersachsen wahrscheinlich nicht einführen werden, weil Rot-Grün sich in diesem Punkt sehr einig ist.

Ich möchte aber trotzdem noch ein paar Fragen stellen, weil ich heute die Möglichkeit dazu habe. Ihr Unternehmen wurde, soweit ich weiß, wahrscheinlich 2003 gegründet, und mittlerweile befinden wir uns im Jahr 2026. Zum Vergleich: Das erste iPhone wurde 2007 vorgestellt; es ist ein bisschen später auf den Markt gekommen, aber das ist trotzdem eine krasse

Entwicklung. Ich kann mir kaum vorstellen, dass in den Polizeibehörden nicht mit Fernwartung gearbeitet wird, sondern immer noch Menschen dort hingehen und Sachen einspielen. Auch die ID-Modelle von VW werden beispielsweise über Fernwartung betreut, Patches und Updates werden automatisch eingespielt. Da setzt sich niemand hin und schiebt einen Stick ein, um das zu aktualisieren. Das kommt mir für so ein modernes Unternehmen wie Ihres doch sehr komisch vor. Vielleicht erläutern Sie das noch einmal genauer.

Die Frage ist nämlich: Wie können wir sicherstellen, dass wirklich nur solche Sachen ins System kommen, die unserem Staat bzw. den Polizeibehörden helfen? Wir alle wissen, dass wir uns in einer massiven hybriden Bedrohungslage befinden. Wir sind nicht mehr im Jahr 2003. Palantir ist im Grunde als Reaktion auf die Anschläge vom 11. September gegründet worden, aber wir sind jetzt in einer ganz anderen Situation. Die Weltlage hat sich verändert; wir haben es gerade schon vom Landesdatenschutzbeauftragten gehört. Nichts ist mehr so, wie es war.

Mein Kollege Herr Lühmann hat bereits die ICE-Raids angesprochen. Ich möchte auch darauf eingehen. Dort arbeiten Sie auch mit anderen Anbietern zusammen, zum Beispiel mit Paragon. Solange demokratische Regierungen an der Macht sind, die die Freiheit und die Grundrechte schützen wollen, kann das vielleicht noch funktionieren. Wir machen hier aber ein Gesetz für die Zukunft, und wir wollen vorausschauende Regelungen, gerade auch für unsere Polizei und die Sicherheitsbehörden. Insofern stellt sich die Frage: Wie ist es, wenn andere Programme dazukommen? Wie könnten diese das gegebenenfalls ausnutzen?

Ein ehemaliger Palantir-Mitarbeiter hat gesagt: Es deckt den gesamten Verlauf der Abschiebung von Einzelpersonen ab, von der Identifizierung und Überwachung bis hin zur Verhaftung. - Das bezieht sich auf Paragon in Kombination mit Palantir bei den ICE-Raids.

Meine Fragen lauten also: Wie möchten Sie das machen, und wie funktioniert das Einspielen der Software?

Im Mai 2025 ist von 13 ehemaligen Palantir-Mitarbeitenden ein offener Brief verfasst worden. Darin heißt es:

> „Tech-Firmen wie Palantir tragen dazu bei, autoritäre Strukturen unter dem Deckmantel einer von Oligarchen geführten Revolution zu normalisieren. Das müssen wir stoppen.“

Wie verhalten Sie sich dazu? - Wer tiefer einsteigen möchte: Gestern Abend gab es im ZDF wieder eine Reportage zu Ihrem Unternehmen.

Abschließend möchte ich auf die Klage, die gerade beim Bundesverfassungsgericht anhängig ist, zu sprechen kommen - eine Kontrollklage, wenn ich das richtig sehe. Die Gesellschaft für Freiheitsrechte (GFF) hat Verfassungsbeschwerde gegen die Möglichkeit polizeilicher KI-Überwachung in Bayern erhoben, und zwar unter anderem mit Blick auf Artikel 61 a des Bayerischen Polizeiaufgabengesetzes, der der Polizei ein sogenanntes Data Mining erlaubt. Dort wertet ein Programm auf Basis der Überwachungssoftware Gotham von Palantir - ich glaube, jeder kennt Batman und weiß, was sich hinter Gotham City verbirgt - riesige Datenmengen aus und stellt Verbindungen her - und zwar auch zu Personen, die nicht im Zusammenhang mit Straftaten stehen. Es gehen schließlich auch Menschen zur Polizei, die Opfer oder Zeuginnen und Zeugen einer Straftat geworden sind. Wer eine Strafanzeige stellt, wird also auch von der Software erfasst. Und genau da liegen der Fehler und die Herausforderung: Wir können nicht einfach Daten von Unschuldigen sammeln. Das darf nicht passieren! Wie gesagt, wir müssen in Europa nicht nur

Souveränität mit Blick auf Bereiche wie Energie etc. herstellen, sondern insbesondere auch mit Blick auf die digitale Infrastruktur, gerade in Zeiten hybrider Bedrohungen.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Ich gebe Ihnen gleich die Möglichkeit zu antworten, möchte zuvor aber darauf hinweisen, dass wir eine Stunde hinter dem Zeitplan liegen. Vier Wortmeldungen liegen noch vor. Danach würde ich gern fortschreiten und den nächsten Anzuhörenden aufrufen.

Dr. Josef Korte: Ich beginne mit dem Updateprozess. Selbstverständlich kommt keiner mehr mit einem Stick vorbei, sondern das läuft über einen Updateserver, und dieser spielt das dann an eine Demilitarisierte Zone. Ich hatte das bereits dargestellt: Es handelt sich dabei um einen Rechner, der sozusagen zwischen dem Netz der Polizei und dem freien Internet hängt. Dort werden Updates gescreent, und dort werden sie auch bewertet. Updates sind immer auch dokumentiert und können entsprechend ausgewertet werden. Die technischen und fachlichen Experten der Polizei haben also durchaus die Möglichkeit, sich das entsprechend anzuschauen, bevor es eingespielt wird - und das tun sie auch, sie nehmen das sehr ernst. Das ist der normale Gang der Dinge für jede Art von Software, die in gesicherten Netzen betrieben wird, sei es bei der Polizei, im Verteidigungsbereich oder Ähnliches.

Sie machen ein Gesetz für die Zukunft, das ist richtig. An dieser Stelle sei uns gestattet, darauf hinzuweisen: Wir wollen die Polizei dazu befähigen, die Daten, die bereits vorhanden sind, rechtskonform und effizient zu nutzen, und selbstverständlich soll sich die Konfiguration der Software genau an dem orientieren, was der Gesetzgeber vorgibt. Genau das tun wir in allen vier Bundesländern, in denen die Software genutzt wird. Zuletzt wurde in Baden-Württemberg die Rechtsgrundlage geschaffen, und jetzt, im Implementierungsprozess, orientiert sich die genaue Konfiguration der Software selbstverständlich exakt an dem, was die Rechtsgrundlage - und übrigens auch der Datenschutzbeauftragte - vorgibt. Da ich selbst in diesen Prozess involviert bin, kann ich das guten Gewissens so unterstreichen.

Zum Thema Überwachungsstaat und Massendatenbank - das implizieren Sie ja -: Jemand, der gegen Grundrechte verstoßen oder Daten missbräuchlich verwenden wollen würde, wäre schlecht damit beraten, Palantir-Software dafür einzusetzen. Wir haben es dargestellt: vollständige und revisionssichere Protokollierungen, Zugriffskontrollen, Zweckbestimmungen - automatisiert wird alles so durchgesetzt, wie es der Gesetzgeber vorsieht. Das sind also die denkbar schlechtesten Voraussetzungen, um mit diesen Daten Missbrauch zu begehen. Jedenfalls ist das meine Einschätzung. Insofern würde ich das zurückweisen.

Zum Sammeln der Daten bzw. zu dem Punkt, dass auch Daten von Zeugen und anderen Beteiligten erfasst werden, die damit nichts zu tun haben: Dazu sind die datenpunktgenaue Steuerung der Zugriffsrechte und auch die anlassgenaue Steuerung der Zugriffsrechte implementiert. Insofern können Zeugendaten, wenn das so vorgesehen ist, selbstverständlich von Recherchen ausgeschlossen werden. Das ist alles möglich. Sie als Gesetzgeber machen die Vorgaben, wie es sein soll, und wenn das so gewollt ist, fließen selbstverständlich keine Zeugendaten ein. Die können technisch isoliert werden.

Dr. Stefanie Kirschke: Zu den Löschfristen: Es gibt für unterschiedliche Daten natürlich auch unterschiedliche Löschfristen. Auch diese sind gesetzlich vorgegeben. Die Polizei muss das entsprechend umsetzen, und das kann auch technisch in unserer Software umgesetzt werden. Das heißt, Zeugendaten werden dann auch entsprechend gelöscht. Das ist ganz klar.

Ich möchte im Folgenden noch auf die übrigen Punkte eingehen. Sie hatten die ICE-Problematik in den USA und die Rolle unserer Software angesprochen. Wie gesagt, besteht unsere Zusammenarbeit mit dem US-Heimatschutzministerium schon seit sehr langer Zeit. Sie begann unter der damaligen demokratischen Obama-Regierung. Ja, die Behörde nutzt unsere Software, um ihre Daten rechtssicher, rechtskonform und besser zu nutzen und um den Zugriff revisionssicher zu auditieren. Ich möchte in diesem Zusammenhang aber um Verständnis bitten, dass es hier in diesem Gremium um die deutsche Polizeiarbeit geht. Ich persönlich habe nicht alle Einzelheiten zu unserer Arbeit in den USA zur Verfügung und kann dazu jetzt auch keine detaillierten Aussagen machen. Wir können gern, wenn Sie dies wünschen, eine schriftliche Stellungnahme nachreichen.

Sie hatten die Kontrollklage der GFF in Bayern wegen der KI-Überwachung angesprochen. Dazu möchte ich ganz klar sagen, dass diese Klage nicht unsere Software oder Palantir als Technologieunternehmen betrifft. Auch hier ist im Prinzip der bayerische Gesetzgeber derjenige, der sich darum kümmern muss. Ganz klar ist aber, dass die Software, wie sie in Bayern von der Polizei eingesetzt wird, keine KI enthält - auch kein „Data Mining“. Das ist nicht der Fall.

Abg. **Deniz Kurku** (SPD): Ich muss ich an dieser Stelle nachhaken. Ihre Aussage war jetzt auf das „Data Mining“ bezogen, aber ich hatte am Anfang eine andere Frage gestellt - das haben Sie bei der Vielzahl an Fragen vielleicht einfach vergessen -: Ich möchte noch einmal auf die Recherchen des NDR und anderer Medien abstellen, wonach in deutschen Polizeidienststellen Palantir-Mitarbeiterinnen und -Mitarbeiter mit Zugriff auf Echtzeitdaten gearbeitet haben. Könnten Sie dazu noch etwas sagen?

Ich habe noch zwei weitere Fragen. Zum einen geht es um die selbstlernende KI im laufenden Betrieb. Sie schreiben:

> „Sollten künftig, mit entsprechender gesetzlicher Grundlage, KI-gestützte Analysemethoden eingesetzt werden, lässt sich in der Plattform auch dies konfigurativ abbilden…“

Da bin ich mehr als hellhörig geworden, das sage ich Ihnen ganz klar. Denn es ist schon so, dass man jetzt eine Rechtsgrundlage schafft, die dann aber mit Blick auf die Funktionen schrittweise ausgeweitet werden kann, und ich mache mir riesengroße Sorgen, dass diese Rechtsgrundlage dann für eine weitaus weitreichendere Datenverarbeitung genutzt wird. Wenn ich vor diesem Hintergrund sehe, dass in Bayern das System mit VeRA - ich nenne es mal „Palantir light“ - auch schon weit unterhalb der eigentlich ursprünglich angedachten Eingriffsschwelle eingesetzt wurde - Stichwort „Eigentums- und Vermögensdelikte“ usw. -, sträuben sich mir wirklich die Nackenhaare.

Ein anderer Punkt, Stichwort „Vergabeargument“. Sie schreiben - das klingt fast schon wie ein Sachzwang -:

> „Ein bestehender Rahmenvertrag ermöglicht eine Beschaffung ohne erneutes Ausschreibungsverfahren.“

Als Kommunalpolitiker und Landtagsabgeordneter ist das für mich höchst problematisch, weil wir hier von hochsensiblen Daten sprechen, und da müssen wir als Niedersächsischer Landtag, glaube ich, ganz klar eine Souveränitätsargumentation dagegenhalten. Wir können nicht sagen: Wir machen das einmal, und dann ist alles gut, und Palantir regelt das dann für die nächsten Jahrhunderte. - Ich würde Sie bitten, auch dazu kurz etwas zu sagen.

Ein Punkt, der mir extrem wichtig ist, ist die Auseinandersetzung mit dem US Cloud Act. Der sagt, kurz gesagt, dass US-Strafverfolgungsbehörden über IT-Unternehmen auch im Ausland Zugriff auf alle Daten haben. Ich finde - das geht auch in Richtung der von mir geschätzten CDU-Fraktion -, das müsste eigentlich schon ausreichen. Was sagen Sie dazu? Sie hatten es eben schon angerissen. Aus meiner Sicht müsste es am Ende eine rechtsgutachtliche Prüfung geben, ob US-Behörden über eine Muttergesellschaft oder über andere ein Recht haben, auf unsere Quellcodes oder Betriebsdaten usw. zuzugreifen. Dazu hätte ich gern eine Einschätzung von Ihnen, denn das finde ich mehr als beachtlich. Das muss nicht im Rahmen dieser Anhörung sein, das können Sie auch gern schriftlich beantworten.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Ich finde, es ist ein guter Vorschlag, dass Sie ein paar Informationen nachreichen; denn wir sind jetzt mehr als eine Stunde hinter dem Zeitplan.

Dr. Josef Korte: Über das große Interesse freuen wir uns natürlich.

Ich fange mit den Mitarbeitenden an. Ja, es ist richtig: Im Rahmen der Implementierung arbeiten Mitarbeitende am System in den Netzen der Polizei. Ich habe eben dargestellt, wie die Mitarbeitenden überprüft sind, wie sie auch verpflichtet sind und dass sie eben in der Infrastruktur der Polizei arbeiten und ein Datenabfluss oder Ähnliches, was vielleicht unterstellt wird, eben nicht möglich ist.

Zur selbstlernenden KI und der Frage, wie sie eingesetzt wird: Grundsätzlich können Sie an die Plattform auch KI-Modelle anschließen, wenn Sie das wollen. Sie müssen es aber nicht. Das regelt sozusagen der Gesetzgeber. Wenn Sie sagen, das soll komplett ohne KI betrieben werden, dann kann es komplett ohne KI betrieben werden. Das greift auch, wenn Sie sagen, dass das zum Beispiel nur mit einem europäischen KI-Modell betrieben werden darf. Wir liefern im Übrigen selbst keine KI-Modelle, sondern wir haben sozusagen eine Modellschnittstelle, an die Sie jedes Modell anschließen können. Das heißt, wenn Sie in der Zukunft ein von der Polizei oder von einem europäischen Anbieter entwickeltes KI-Modell haben, das Sie als Gesetzgeber gern einsetzen würden, dann könnten Sie dies tun. Das wird aber aktuell im Rahmen von VeRA nicht gemacht. Wie gesagt, die Entscheidung liegt bei Ihnen als Gesetzgeber und entsprechend bei der Polizei.

Zum Thema US Cloud Act: Selbstverständlich ist es vertraglich ausgeschlossen, dass wir Daten abfließen lassen oder weitergeben. Ich habe es eben schon gesagt: Wir hätten daran gar kein Interesse. Auch rechtlich ist es ausgeschlossen, denn unsere Kunden sind die Besitzer der Daten, und unsere Kunden haben die volle Kontrolle über die Daten. Schlussendlich ist es auch technisch ausgeschlossen, schon allein aufgrund der Infrastruktur, die ich gerade erläutert habe: polizeiliche Hardware, polizeiliches Rechenzentrum, polizeiliches Netz. Selbst wenn wir wollten, könnten wir nichts abfließen lassen oder einer Cloud-Act-Anfrage nachkommen. Lassen Sie mich noch einmal ganz klar sein: Es gab bislang keinerlei diesbezügliche Anfrage aus dem Cloud Act, und wenn eine käme, dann wäre auch genau das unsere Antwort - rechtlich und technisch unmöglich.

Dr. Stefanie Kirschke: Zur Ausschreibung: Sie hatten den bestehenden Rahmenvertrag erwähnt, den das Landeskriminalamt Bayern abgeschlossen hat. Das war nicht unsere Idee, so wurde die Ausschreibung veröffentlicht, und ich bin mir sicher, das wurde vorher mit den Ländern auch so abgestimmt. Bayern agiert als Primärauftraggeber, und alle weiteren Bundesländer oder die Polizeibehörden der Bundesländer und auch zum Beispiel das BKA, also auch Bundesbehörden,

agieren als Sekundärauftraggeber. Das war ein EU-weites Ausschreibungsverfahren, an dem wir teilgenommen haben und das sich über ein ganzes Jahr mit Vertragsverhandlungen hingezogen hat. Daraus ist dann dieser Rahmenvertrag entstanden.

Wir haben das also nicht in unsere Stellungnahme geschrieben, damit es so klingt, als ob wir das einzige Unternehmen wären, das das machen kann. Das war das Ergebnis dieses EU-weiten Ausschreibungsverfahrens. Es gab wirklich sehr intensive Prüfungen, Evaluierungen und Verhandlungen, und am Ende haben wir den Zuschlag bekommen. Dieser Rahmenvertrag erlaubt den anderen Landespolizeibehörden, mit Standard-EV-BIT-Verträgen unsere Software zu nutzen. Es handelt sich also um Standardverträge, die nicht wir aufsetzen, sondern im Rahmen des Rahmenvertrages gibt es Musterverträge, und diese werden dann genutzt.

Abg. **Stephan Bothe** (AfD): Sehr geehrte Frau Dr. Kirschke, Herr Dr. Korte, vielen Dank, dass Sie heute hier sind. Ich glaube, das ist eine sehr wichtige Anhörung, denn man redet bereits seit längerer Zeit in diesem Landtag über Sie. Es ist schön, dass man jetzt auch einmal mit Ihnen sprechen kann.

Ich möchte daran erinnern, dass Palantir auch in der Ukraine eingesetzt wird, zur Abwehr von Drohnenangriffen. Es wird in Israel im militärischen Bereich eingesetzt, auch zur Abwehr von Angriffen. Man kann also sagen, dass es in der Sicherheitsarchitektur in NATO-Staaten ein ganz wichtiger Faktor ist.

Nur eine kurze Frage: Sie sind in vielen Ländern aktiv, auch in Deutschland, und zwar in mehreren Bundesländern. Gab es zu irgendeinem Zeitpunkt eine Datenschutzpanne, oder gab es einen Vorwurf von Ihren Auftraggebern, dass Daten abgeflossen sind? Gab es irgendwelche Verfahren? Ist Ihnen da etwas bekannt?

Dr. Josef Korte: Die Antwort ist klar: Die gibt es nicht, und wenn es sie gäbe, wäre uns das wahrscheinlich auch bekannt. Insofern: nein.

Abg. **Alexander Saade** (SPD): Ich interessiere mich für den Praxisbetrieb. Ich kenne das aus der Ermittlungsarbeit: Wenn man am Ende den Bericht verfasst, schreibt man genau auf, wie man zu einer Schlussfolgerung gekommen ist. Daher meine Frage: Lässt sich komplett nachvollziehen, wie die Software auf das Ergebnis gekommen ist? Wie wird das dokumentiert, und wie kann man das als Kunde nachvollziehen?

Dr. Josef Korte: Das ist eine sehr gute Frage, und das ist tatsächlich eines der Themen, über die wir gern sprechen möchten.

Es ist nicht so, dass die Software ermittelt, sondern das tut immer noch die Beamtin oder der Beamte. Die Software ermöglicht es aber über die entsprechenden Datentöpfe, auf die man Zugriff hat, schnell und effizient zu recherchieren, die Daten miteinander zu verknüpfen und entsprechend darzustellen - zum Beispiel ein Netzwerkdiagramm mit einer organisierten Kriminalität oder Ähnliches. Das ist insofern nachvollziehbar, als dass Sie zu jedem Datenpunkt, den Sie in die Analyse einbeziehen - also bis auf den einzelnen Datenpunkt genau -, feststellen können: Aus welchem System kommt er, in welchem Kontext wurde er erhoben, und welche Zugriffsrechte liegen auf diesem Datenpunkt? Wo kommt er her, wo geht er hin, wer darf ihn sehen? Sie können lückenlos zurückverfolgen, woher das kommt, und insofern ist das dokumentiert. Die Entscheidung, was daraus am Ende geschlossen wird - ob es der Verdächtige in einem Fall ist

oder nicht -, obliegt in jedem Fall dem Polizeibeamten oder der Polizeibeamtin. Da macht das System insofern keine Vorgabe, keinen Vorschlag oder Ähnliches.

Abg. **Michael Lühmann** (GRÜNE): Erstens. Ich halte Lobbyismus gar nicht für problematisch. Ich finde bloß wichtig, dass er transparent ist. Ansonsten ist es vollkommen okay, dass man das macht, auch in parlamentarischen Debatten und im parlamentarischen Umfeld.

Zweitens. Misstrauen ist konstitutiv für eine Demokratie. Das kann man einfach so festhalten. Ich finde das völlig unproblematisch. Wir haben eine Kontrollfunktion, und die funktioniert auch über Misstrauen.

Ich habe zwei Fragen. Eine davon haben Sie schon beantwortet. Ich komme da aber trotzdem nicht mit. Sie können ausschließen, dass es einen US-Zugriff gibt, auch auf Grundlage US-amerikanischen Rechts? Können Sie definitiv ausschließen, dass es mit einer existierenden Rechtsgrundlage trotzdem keinen Zugriff geben kann und wird - obwohl ja einer der Kritikpunkte ist, dass man es kann? Dann haben wir hier eine Rechtsgrundlage, die das auch ermöglicht. Und Sie garantieren uns hier, dass das nie stattfinden wird? Sie können für die US-Administration sprechen? Das ist die erste Frage.

Die zweite Frage lautet: Können Sie garantieren, wenn wir hier ein System einführen, das sich nicht mal eben migrieren lässt - wir haben auch noch ein paar andere Gutachten gelesen, wonach das stark beeinträchtigt wird -, dass Palantir nicht aufgrund von US-Exportbestimmungen abgeschaltet wird, dass nicht eines schönen Tages eine US-Administration beschließt: Das ist sicherheitsrelevante Software, die darf nicht mehr exportiert werden? Können Sie garantieren, dass das so bleibt, dass diese Rechtsgrundlage niemals herangezogen wird und dass weder Donald Trump noch andere US-Präsidenten jemals davon Gebrauch machen können, um uns das System abzuschalten?

Vors. Abg. **Doris Schröder-Köpf** (SPD): Das ist eine wirklich sehr schwer zu beantwortende Frage.

Dr. Stefanie Kirschke: Ich denke, wir können sie sehr gut beantworten. Noch einmal zu dem Cloud Act - Herr Dr. Korte hat schon darauf hingewiesen -: Wir sprechen nicht für die US-Regierung. Wir sind ein US-amerikanisches Unternehmen, das ist richtig, aber der Cloud Act - das will ich auch betonen - gilt für alle Unternehmen, die unter diese US-Gerichtsbarkeit fallen; auch für deutsche oder europäische Unternehmen, die in den USA tätig sind. Das betrifft also nicht nur Palantir.

Der große Unterschied, den wir hier machen müssen - das haben wir schon versucht, klarzustellen -, ist diese grundlegende Trennung zwischen Datenhoheit und Eigentümer der Daten auf der einen und Softwareunternehmen als Auftragsverarbeiter auf der anderen Seite. Das sind rechtliche Begriffe, und es ist bei uns eben so, dass wir in allen unseren Kundenbeziehungen - nicht nur in Deutschland, sondern weltweit - als Auftragsverarbeiter fungieren. Wir haben keinen Zugriff auf die Daten. Wir verkaufen, kaufen und erheben keine Daten - das haben wir jetzt mehrfach dargestellt -, und vor diesem Hintergrund können wir auch keine Daten an eine US-Regierung weitergeben, falls es eine Anfrage gäbe. Das ist schlicht und einfach - Herr Dr. Korte hat es schon ausgeführt - technisch und vertraglich nicht möglich, weil die Daten der deutschen Polizei gehören und nicht uns. Wir haben keinen Zugriff.

Die Mitarbeiter - das haben wir auch schon gehört - haben unter Kontrolle und Aufsicht des Kunden für technische Unterstützung in den gesicherten Netzwerken und Rechenzentren der Polizei für ganz gewisse Zeitpunkte und ganz klar begrenzte Aufgaben Zugang - mehr nicht, und es fließen keine Daten ab.

Ich kann Ihnen nicht garantieren, dass es nie eine Anfrage geben wird. Wir können klar sagen, dass es noch nie eine Anfrage gegeben hat. Sollte es eine Anfrage geben, würden wir das entsprechend prüfen und genau mit den Argumenten, die ich Ihnen gerade genannt habe, beantworten. Wir sind Datenverarbeiter und besitzen die Daten nicht.

Dr. Josef Korte: Um das zusammenzufassen: Es ist rechtlich und technisch nicht möglich, im Rahmen des Cloud Acts Daten abfließen zu lassen.

Zum Thema Migration: Da steht der Begriff „Kill-Switch“ im Raum bzw. die Frage, ob irgendwie der Zugriff blockiert werden könnte, wenn eine entsprechende politische Ansage kommt. Ich glaube, das ist ein Szenario, das weit über Palantir hinaus Konsequenzen hätte; wir sind ja nicht die einzige US-amerikanische Firma. Aber wir nehmen diese Sorge natürlich ernst. Deshalb der Hinweis: Wir haben unsere Verträge mit der deutschen Entität bei deutschen Kunden nach deutschem Recht, und die Software wird, wie schon mehrfach erläutert, durch die Polizei betrieben, und alle Daten befinden sich auf Hardware der Polizei, im Rechenzentrum der Polizei und in Netzen der Polizei. Im allerschlimmsten Fall, wenn es nicht mehr möglich wäre, mit Upgrades zu versorgen oder Ähnliches, könnten die Daten aus dem System exportiert und in ein - wie auch immer geartetes - souveränes System überführt werden. Insofern sehe ich nicht die Gefahr eines „Kill-Switches“ oder ähnlicher Szenarien.

Abg. **Sebastian Zinke** (SPD): Wie bewerten Sie Ihre gerade gemachten Ausführungen und die von Ihnen ausgesprochene Garantie vor dem Hintergrund, dass wir auch andere US-amerikanische Dienste nutzen, bei denen wir die Garantie haben, dass bestimmte Kommunikationsinhalte Ende-zu-Ende-verschlüsselt sind, bei denen wir als Sicherheitsbehörden - weder der Verfassungsschutz noch andere Nachrichtendienste noch die Polizei - keinen Zugriff auf diese Daten haben, wir aber in entsprechenden Fällen durch US-Behörden Hinweise bekommen, die aus solch einer verschlüsselten Kommunikation stammen? Vor einigen Jahren haben wir auch offenbart bekommen, dass diese Dienste nicht nur unsere Kommunikation mitlesen und entschlüsseln können, sondern dass auch Regierungsmitglieder bis hin zum Bundeskanzler oder zur Bundeskanzlerin, also Regierungsinterna, über diese Programme US-amerikanischer Unternehmen abgehört werden, obwohl es dort ebenfalls diese Garantien gibt, die Sie gerade ausgesprochen haben.

Dr. Josef Korte: Ich glaube, der entscheidende Unterschied liegt im technischen Setup. Wir reden hier wahrscheinlich von Cloud-Services, wahrscheinlich auch von Services, die wir nicht nur in europäischen Clouds und ähnlichen Touchpoints haben. Ich kann nur spekulieren.

Bei der Polizei und bei allen unseren deutschen Polizeikunden reden wir von On-Premise-Lösungen, die in geschützter Hardware und in geschützten Netzwerken der Polizei betrieben werden. Also wenn Sie unterstellen würden, dass amerikanische Dienste darauf Zugriff hätten, dann gäbe es sicherlich noch ein ganz anderes Problem als Palantir. Aber das will ich jetzt einmal ausschließen. Insofern ist das technische Setup hier grundsätzlich anders als das Setup bei den von Ihnen beschriebenen Szenarien.

Deutsche Polizeigewerkschaft - Landesverband Niedersachsen

Schriftliche Stellungnahme: Vorlage 6

Anwesend:

- Christian-Tobias Gerlach, stellvertretender Landesvorsitzender

Christian-Tobias Gerlach:

Christian-Tobias Gerlach: Zunächst möchte ich mich bedanken, dass ich heute hier im Namen der Deutschen Polizeigewerkschaft (DPolG) zu Ihnen sprechen darf. Denn das ist ein sehr wichtiges Thema, das auch den Kolleginnen und Kollegen in der Praxis sehr viel bedeutet.

Unsere schriftliche Stellungnahme liegt Ihnen vor, sodass ich mich heute auf drei Punkte konzentrieren möchte: die praktischen Herausforderungen der Polizeiarbeit im digitalen Zeitalter, die Funktionsweise und vor allen Dingen den konkreten Nutzen solcher Systeme für die Gefahrenabwehr und die Strafverfolgung. Da ich grundsätzlich Praktiker bin, werde ich versuchen, immer auch ein paar praktische Beispiele mit anzuführen, weil ich denke, dass das dann plastischer und auch besser greifbar ist.

Vorwegstellen möchte ich: Die Polizei hat heute in vielen Fällen kein Erkenntnisproblem, sondern wir haben als Polizei in vielen Bereichen eher das strukturelle Problem, wie wir die Masse an Daten, die wir bekommen, vernünftig auswerten können. Wir haben unser Vorgangsbearbeitungssystem, wir haben verschiedene Einwohnermeldedaten, wir haben polizeiliche Informationssysteme, die teilweise sogar auf Bundes- oder Europaebene laufen, wir haben Telekommunikationsauswertungen, Erkenntnisse aus verschiedenen Ermittlungsverfahren und zunehmend auch - das darf man nicht vergessen - digitale Spuren, die zum einen aus dem Internet kommen, zum anderen aber auch zugeliefert werden. Wenn wir uns die Infrastrukturlandschaft oder die IT-Infrastruktur angucken, stellen wir fest, dass das ganz viele verschiedene Systeme sind. Wir haben also kein System, in dem alle Daten vorhanden sind - das ist schon in den bisherigen Ausführungen deutlich geworden -, sondern wir haben, um das Bild von Frau Buschmann zu bemühen, sozusagen verschiedene Räume, und als Ermittler muss ich immer überlegen: In welchen Raum möchte ich denn jetzt eigentlich gerade, und wo könnten für mich relevante Informationen liegen?

Das Ganze ist historisch gewachsen und dementsprechend in Teilen auch unterschiedlich aufgebaut und nur im begrenzten Umfang miteinander verknüpft. Die Folge ist: Als Ermittler muss ich das Ganze manuell rekonstruieren. Ich muss mir überlegen: Wie könnte es gewesen sein? Ich hatte die Gelegenheit, in Den Haag bei Europol zu arbeiten. Das war zu der Zeit, als der Anschlag auf Charlie Hebdo stattfand, und das war für mich sehr eindrucksvoll. Denn Europol hatte schon vorher sozusagen verschiedene Container, aber auch immer nur basierend auf dem, was zugeliefert wurde, und wenn man dann sieht, wie nach so einem tragischen Ereignis sehr viele Menschen plötzlich Daten stückchenweise zusammensuchen müssen, um überhaupt zu einem großen Ergebnis zu kommen, dann weiß man, wie viel Zeit dabei unter Umständen verloren geht. Dabei ist die Zeit gerade bei gefahrenabwehrenden Maßnahmen oder bei strafrechtlichen Ermittlungen, die gefahrenabwehrrechtliche Maßnahmen nach sich ziehen, sehr kostbar.

Ein weiteres Beispiel für Massendaten: Im Bereich der häuslichen Gewalt - das ist politisch immer noch eines der Top-Themen, und zwar zu Recht - werden Chatverläufe angeliefert. Wenn diese 190 Seiten umfassen, brauchen die Ermittlerinnen und Ermittler durchaus eine gewisse Zeit, um sie zu lesen, zu verstehen und die Zusammenhänge zu erfassen. Es ist schon beachtlich, wie viel Zeit das kostet.

Zur Funktionsweise der Software: Im Kern geht es hier für uns um die Datenintegration, denn das ist eine der Funktionsweisen, mit der diese Software arbeitet. Die Kunst ist es - und das ist uns als DPolG sehr wichtig -, diese ganzen Quellen vernünftig zusammenzuführen. Wir haben in unserer schriftlichen Stellungnahme auch etwas dazu gesagt. Wichtig ist natürlich, dass wir die Datenqualität bereits vor Einführung einer solchen Software überprüfen und versuchen, diese Zusammenführung überhaupt möglich zu machen. Denn ganz so einfach ist das aktuell nicht. Eine Software kann natürlich nur dann gut sein, wenn auch die Datenqualität gut ist. Das kann man nicht alles der Software überlassen, sondern da müssen wir nachschauen.

Richtig ist aber - das ist auch schon in den bisherigen Ausführungen deutlich geworden -, dass wir nicht unbedingt Daten nutzen, die uns noch nicht vorliegen, sondern wir sprechen in erster Linie von Daten, die auf Basis bestimmter rechtlicher Grundlagen bereits erhoben sind und uns als Polizei vorliegen - nur eben in unterschiedlichen Zimmern bzw. Containern, um bei diesen Bildern zu bleiben. Ich glaube, wir müssen an dieser Stelle aufsatteln und diese Zimmer begehbar machen.

Ein weiterer Punkt ist die Datenverknüpfung. Bei Ermittlungsverfahren habe ich in den Ermittlungsakten vielleicht häufiger dieselbe Telefonnummer, wiederkehrende Fahrzeugkennzeichen, Adressen oder Kontaktpersonen. Es geht hier um die mögliche Beziehung zwischen Datensätzen bzw. darum, diese zusammenzuführen. Vorhin wurde schon zu Recht gesagt: Es ist nicht so, dass wir gar nichts haben. Aus meiner Zeit als Ermittler kann ich sagen: Früher hatten wir mit SAFIR - jetzt gibt es eine neue Version - ein System, das im Prinzip genau das gemacht hat; aber eben auch nur dann, wenn wir die Daten auch überführt haben. Es gab also keine automatische Schnittstelle, keine Datenüberleitung von unserem Vorgangsbearbeitungssystem in SAFIR, sodass wir sofort ein Objektdatennetz - so ein Spinnennetz, wer mit wem, wann, wie gesprochen hat - zur Verfügung hatten, sondern man musste dem System sagen: Diese Daten packst du bitte da rein! - Das heißt, wenn ich als Ermittler keinen Anhaltspunkt für ein SAFIR-Verfahren hatte, wäre das am Ende nie dabei herausgekommen, auch wenn diese Daten vorgelegen hätten. An dieser Stelle müssen wir ansetzen.

Im Bereich Wohnungseinbruchdiebstähle haben wir sehr häufig gesagt: Ich habe Personen, die durch die Analysten aber vielleicht erst später überprüft werden. Dadurch verliere ich Zeit. - Im konkreten Fall wusste ich am Ende, wer es war, wusste aber auch, dass ich diesen Personen so nicht mehr habhaft werden kann. Der Faktor Zeit ist also beim Erkennen von solchen Zusammenhängen unendlich wichtig, weil daraus am Ende auch ermittlungsrelevante Schlüsse gezogen werden können.

Ein weiterer Punkt ist die Analyse und Mustererkennung von solchen Softwares. Ich hatte vorhin als Beispiel den Bereich der häuslichen Gewalt genannt. Das kann ich auch auf andere Bereiche übertragen. Ich muss als Ermittler diese Datenmengen lesen, muss sie verknüpfen, muss sie verstehen und dann auch noch erkennen: Hier haben wir ein Muster. - Das ist schon eine große Herausforderung. Wir sprechen unter Umständen über Kleinstdaten wie eine Telefonnummer,

wo ich erkennen muss: Die habe ich schon mal gesehen. - Das ist nicht unmöglich, aber es ist doch eher ein Glücksgriff bzw. dem Zufall geschuldet, dass ich darauf komme.

Das System kann auch die Verbindungen zwischen verschiedenen Ermittlungsverfahren erkennen. Ich bin kein Strafrechtler, sondern ein einfacher Beamter, aber auch ich habe gelernt, dass in einem Strafverfahren eine Konnektionsprüfung erfolgen sollte. Die Ermittlungsbehörden sind eigentlich gehalten, zu prüfen, ob es einen Zusammenhang zwischen verschiedenen Strafverfahren gibt, und dabei hilft eine solche Software ungemein - wie auch immer sie am Ende heißen mag. Ich hatte SAFIR angesprochen. Wenn ich diese Beziehungsgeflechte visualisiere, mache ich sie einfacher greifbar. Ich habe dann im Prinzip ein Spinnennetz, anhand dessen ich sehen kann: Der mit dem, die mit dem oder die mit der. - Das habe ich dann vor Augen, wodurch es für mich als Ermittler sehr viel einfacher ist, das Ganze zu verknüpfen und weitere Ermittlungsschritte zu generieren.

Zum praktischen Nutzen für die Polizeiarbeit: Der praktische Nutzen solcher Systeme zeigt sich besonders bei ganz bestimmten Einsatzfeldern. Ein Beispiel ist die Gefährdungsanalyse bei potenziellen Gewalttätern. Hier ist es wichtig, dass vorhandene Informationen aus verschiedenen Quellen schnell zusammengeführt werden können, um eine möglichst fundierte Lageeinschätzung treffen zu können. Das gilt unter anderem bei Extremismus, Terrorismus, der organisierten Kriminalität, aber auch der Cyberkriminalität und der sexualisierten Gewalt gegen Kinder, denn gerade hier sprechen wir häufig von Netzwerken, von komplexen Beziehungsstrukturen, die wir ohne technische Unterstützung nur sehr aufwendig rekonstruieren können. Das heißt, die Analyseplattformen - egal, wie sie am Ende heißen - können uns helfen, Zusammenhänge schnell zu erkennen, Ermittlungen effizienter zu strukturieren und Gefährdungslagen früher einzuschätzen. Welche Bundesländer - auch das ist nicht ganz unerheblich - solche Analyseplattformen schon nutzen, wurde bereits ausgiebig thematisiert.

Ich betone an dieser Stelle: Wir sind ergebnisoffen. Es muss nicht die Firma Palantir mit dem Programm Gotham sein. Für uns ist an dieser Stelle aber auch sehr wichtig zu betonen, dass wir eine solche Software einfach brauchen. Die vorhandenen Lösungen reichen nicht aus. Wir müssen natürlich auch sehen, dass eine gewisse Kompatibilität mit anderen Bundesländern gegeben ist. Mit Verlaub, am Ende ist es, was die Arbeit betrifft, in Niedersachsen genauso wie in Bayern, in Baden-Württemberg, in Hessen oder in Nordrhein-Westfalen.

Ich bin kein Verfassungsrechtler, aber wir müssen uns darüber im Klaren sein, dass der Einsatz solcher Systeme klare gesetzliche Grundlagen erfordert - diese schaffen wir mit dem NPOG - und dass das Bundesverfassungsgericht in seinem Urteil aus 2003 sehr deutlich gemacht hat, wo die Grenzen sind und welche verfassungsrechtlichen Anforderungen an eine solche Software gestellt werden. Da geht es um Zweckbindung, Eingriffsschwellen, Transparenz und datenschutzrechtliche Sicherungen. Ich glaube, Herr Lehmkemper hat dazu gerade schon sehr ausführlich ausgeführt.

Aus praktischer Sicht möchte ich einen Punkt ganz besonders hervorheben, nämlich dass der Erfolg dieser Analyseplattform maßgeblich auch von der Datenqualität abhängt. Anders formuliert: Eine Analyseplattform ist immer nur so gut wie die Datenbasis, auf der sie arbeitet. Ich glaube, wir sind schon sehr gut in Niedersachsen. Auch das habe ich bei Europol gelernt. Wir sind eines der wenigen Bundesländer, die zu dieser Zeit sehr kompatibel waren. Insofern stehen wir schon sehr gut da. Aber wir sollten uns im Vorhinein über die Kompatibilität der

Datenstrukturen, über klare Schnittstellen und konsistente Datenpflege Gedanken machen. Wir brauchen natürlich auch eine funktionierende IT-Infrastruktur, die das Ganze entsprechend unterstützt.

Aus gewerkschaftlicher Sicht ist es uns, wie gesagt, am Ende egal, wie das Produkt heißt. Wir brauchen es aber im Prinzip besser gestern als morgen oder in sieben Jahren, wenn wir eine deutsche oder europäische Lösung kreiert haben. Denn der Schuh drückt. In der Zeit, als ich in Den Haag gearbeitet habe - das war 2015 -, hätten wir uns eine Software gewünscht, die so etwas leisten kann.

Entscheidend ist, dass wir als Polizei über funktionsfähige, rechtssichere und technisch zuverlässige Werkzeuge verfügen. Am Ende ist es zweitrangig, wer es liefert, aber wir brauchen es genau in dieser Art und Weise. Langfristig begrüßen wir das Programm P20. Da geht es bekanntlich um eine bundesweite Datenharmonisierung. Das können wir nur unterstützen und halten daran fest. Aber solange kurzfristig keine vergleichbare Alternative vorhanden ist, muss man sich vielleicht auch dazu durchringen, sich einfach am Marktführer zu orientieren.

Zum Schluss möchte ich noch einmal sagen: Die Polizei hat kein Erkenntnisproblem, sie hat zunehmend ein Strukturproblem bei der Auswertung vorhandener Daten. Wenn wir wollen, dass die Polizei höchste digitale Leistungsfähigkeit zeigt, dann müssen wir auch die Voraussetzungen dafür schaffen. Ich könnte auch sagen: Wenn man weiterhin in der Champions League spielen möchte, dann darf man nicht mit Schuhen aus der Kreisklasse spielen.

Abg. **Birgit Butter** (CDU): Vielen Dank, Herr Gerlach, für die Ausführungen aus der Sicht eines Praktikers, der im Rahmen der Gefahrenabwehr Hilfsmittel und Werkzeuge an die Hand bekommen muss, um den vorhandenen Datenschatz zu heben.

Sie sagten zu Beginn Ihrer Ausführungen: „Es ist nicht so, dass wir gar nichts haben." Das klang auf der anderen Seite manchmal ein bisschen durch. Ich will Frau Dr. Sowa nicht vorgreifen, aber in ihrer schriftlichen Stellungnahme drückt sie das besonders deutlich aus:

> „Es stellt sich zudem die Frage, welchen konkreten Mehrwert eine verfahrensübergreifende Datenanalyse in Echtzeit - gegebenenfalls unter Einsatz von Künstlicher Intelligenz - gegenüber bestehenden IT-gestützten, vorgabenbezogenen und statistisch fundierten Verfahren bietet, die auf nachvollziehbaren Modellen beruhen und die Freiheits- und Persönlichkeitsrechte jedenfalls auf der Analyseebene wahren."

Da möchte ich gern von Ihnen als Praktiker wissen: Wie wichtig ist ein modernes Analysesystem?

Christian-Tobias Gerlach: Ein modernes Datenanalysesystem ist sehr wichtig. Damit wäre die Frage grundsätzlich beantwortet. Ich glaube, ich habe versucht, darzulegen, wie komplex das Ganze mittlerweile ist. Gerade, wenn wir von Gefahren sprechen, bringt es nichts, wenn ich in zwei Wochen weiß, dass theoretisch in drei Minuten etwas passiert. Ein Echtzeit-Datenanalysesystem ist eben etwas komplett anderes als das, was wir aktuell zur Verfügung haben.

Abg. **Saskia Buschmann** (CDU): Herzlichen Dank, Herr Gerlach, für die Ausführungen aus der Praxis. Auch ich komme aus der Praxis, und wir wollen etwas für die Praxis tun. Insofern frage ich Sie - das hat uns Herr Lehmkemper eingangs mehr oder weniger mit auf den Weg gegeben -: Welche Daten müssen erhoben bzw. verknüpft oder gespeichert werden, damit die Polizei damit gut arbeiten kann?

Sie haben etwas zum Thema P20 gesagt. Wie weit sind wir mit der Datenharmonisierung? Wie ist der Stand der Dinge? „P20“ klingt ja danach, dass es 2020 so weit abgeschlossen hätte sein sollen, insbesondere wenn man weiß, dass es 2015 oder 2016 angeschoben wurde.

Eine dritte Frage, zum Thema SAFIR: Sie haben gesagt, dass die SAFIR-Datenbank nur mit den Daten arbeitet, die vorher eingepflegt worden sind - die von NIVADIS dorthin überführt wurden -, und diese in dem Netz darstellt. Andere Daten als die aus NIVADIS waren im SAFIR-Datennetz nicht vorhanden. Ist das richtig?

Christian-Tobias Gerlach: Ich beginne mit der letzten Frage. Nach meiner Kenntnis sind nur die Daten, von denen wir gesagt haben, dass sie überführt werden sollen, überführt worden. Aber ich muss überlegen, ob ich dazu im Detail tatsächlich viel sagen kann.

Viel wichtiger ist, glaube ich, die Frage, von welchen Daten wir sprechen. Polizeilicherseits ist es natürlich schwer zu sagen, welche Daten wir am Ende erheben müssen. Alles ist ein Datum. Auch bei Beweismitteln können Daten enthalten sein. Um die Datennetze überhaupt abbilden zu können, sprechen wir natürlich von personenbezogenen Daten, die wir rechtmäßig erheben - über Telefonnummern, Adressen, Kontaktpersonen oder Ähnliches. Am Ende wird durch so eine Software erkannt, dass Person A mit Person B möglicherweise häufigeren Kontakt hat - je nachdem, was ich zuliefere. Bei bestimmten Straftaten können wir zum Beispiel auch Telekommunikationsdaten erheben. Das heißt, es werden Unmengen an Daten zugeliefert, bei denen ich händisch analysieren muss, welche Telefonnummer mit welcher anderen Telefonnummer im Kontext steht. Ich glaube, die Antwort auf die Frage, welche Art von Daten erhoben werden muss, lautet: Das ist sehr mannigfaltig. Es kommt immer auf den konkreten Anlass an.

Die Frage nach P20 kann ich nicht beantworten, da ich dort weder gewerkschaftlich noch polizeilich Berührungspunkte habe.

Abg. **Sebastian Zinke** (SPD): Vielen Dank, dass Sie noch einmal ganz ausdrücklich gesagt haben, dass die Polizei Niedersachsen - anders als der Eindruck, der hier vielleicht erzeugt werden sollte - durchaus Datenanalysetools hat. Sie haben SAFIR erwähnt. Ich weiß, dass wir zum Beispiel eine große Welle von Wohnungseinbrüchen darüber bearbeitet haben und auch Ermittlungserfolge hatten und dieses Phänomen am Ende des Tages zurückgedrängt haben. Auch dafür wurde das Instrument eingesetzt - nicht nur für organisierte Kriminalität, wofür man es hauptsächlich eingesetzt hat. Wir haben so etwas in Benutzung, aber ich glaube, wir sind uns alle miteinander einig, dass die Polizei bei zunehmender Datenflut Instrumente an die Hand bekommen muss, um mit diesen Daten Ermittlungen tätigen zu können, aber auch, um im Rahmen der Gefahrenabwehr zügig arbeiten zu können.

Die Bedenken, die es gibt - datenschutzrechtlicher Art etc. -, sind hier bereits geäußert worden. Meine Frage lautet: Sie sagen nicht, dass man dieses System, das hier heute im Vordergrund steht, anschaffen soll, sondern dass man der Polizei Instrumente an die Hand geben soll, mit denen diese Dinge zügig erledigt werden können, damit mit diesen Datenmengen umgegangen werden kann? So habe ich Sie verstanden. Vielleicht können Sie das bestätigen.

Sie haben auch gesagt: Man muss die Daten - beispielsweise bei SAFIR - händisch eingeben. Verstehe ich Sie richtig, dass Sie sich im Grunde wünschen, dass man das nicht mehr machen muss,

sondern dass es dann doch KI-basiert ist und man als Mitarbeiter der Polizei Niedersachsen vom System aufgezeigt bekommt, wenn irgendetwas passiert oder irgendeine Verknüpfung festgestellt worden ist?

Christian-Tobias Gerlach: Ich beginne mit dem Ende: Was ich mir wünschen würde, spielt zum Glück nicht unbedingt eine Rolle. Dazu möchte ich auch gar nichts sagen. Mit „händisch eingeben“ meinte ich: Als Ermittler muss ich festlegen, welche Daten in das andere System transportiert werden. Es ist also nicht so, dass dort alles automatisch hineinläuft, sondern ich muss sagen: Ich möchte in einem bestimmten Vorgang bestimmte Daten aus dem Zimmer A in das Zimmer B bringen. Und das macht es natürlich kompliziert. Wenn das Ganze automatisiert wäre, wäre es ein Stück weit einfacher - erheblich sogar.

(Abg. Sebastian Zinke [SPD]: Das ist also anlassbezogen?)

Genau, es muss anlassbezogen erfolgen.

(Abg. Sebastian Zinke [SPD]: Und Sie hätten das gern automatisiert?)

Ich hätte das gern automatisiert, wir hätten das gern ein Stück weit automatisiert, weil wir zum aktuellen Zeitpunkt einen Anlass bräuchten, im Sinne von: Ich habe eine Idee, ich mache ein Umfangsverfahren auf, ich nehme diese Daten und lege sie dort hinein. Dann sage ich: Zeige mir bitte, wo die Telefonnummern, die Kennzeichen, die Personen aufgetreten sind! - Das bedeutet, wenn ich im Vorweg überhaupt nicht erkenne, dass wir so ein Verfahren haben, das relativ groß ist - gerade im Bereich der Strukturermittlungen der organisierten Kriminalität beispielsweise -, dann würden diese Daten niemals zusammengeführt werden, weil sie dann tatsächlich in ihrem Zimmer und dort wahrscheinlich in einem Schrank in verschiedenen Schubladen liegen würden. - Ich versuche, dieses Bild jetzt weiter zu benutzen und auszuschmücken. - Sie würden dort liegen, und niemand würde wissen, dass sie eigentlich reichen, um ein neues Haus zu bauen.

Polizeipräsidium Frankfurt am Main

Schriftliche Stellungnahme: Vorlage 5

Anwesend:

- Polizeivizepräsident Bodo Koc, ehemaliger Chief Digital Officer der hessischen Polizei
- Juliane Stieg, Verantwortliche HessenDATA am Innovation Hub 110

Bodo Koch: Kurz zu meiner Person: Ich bin Polizeivizepräsident im Polizeipräsidium Frankfurt am Main, war vorher als Chief Digital Officer der hessischen Polizei für die Digitalisierung in Hessen verantwortlich und habe 2016 als Projektleiter die auf Gotham von Palantir basierende Software HessenDATA in Hessen eingeführt. Juliane Stieg ist die Verantwortliche für das Team, das die Analyseplattform konfiguriert und Datenpipelines und solche Dinge unter seiner Kontrolle hat. Wir freuen uns sehr über die Einladung nach Niedersachsen und nehmen gern zu dem Antrag Stellung.

Ich möchte zunächst den fachlichen Aspekt nach vorn stellen, weil darüber bereits diskutiert wurde. Wir haben in Hessen nicht nur sehr viele fachliche Erfahrungen gesammelt, sondern auch

das Thema Recht ein Stück weit gestaltet, weil wir die Ersten waren, die diese Norm geschaffen haben. Fachlich ist, glaube ich, besonders wichtig zu betonen: Wir haben es mit globaler und digitaler Kriminalität zu tun, und wir sehen Phänomene, bei denen wir einen deutlichen Zuwachs an Daten haben. Eine Fokussierung auf das Themenfeld Kinderpornografie führt in Hessen dazu, dass wir im forensischen Bereich Daten im Petabyte-Umfang haben. Das ist eine sehr stark wachsende Datenquelle.

Ein weiteres Beispiel sind die Kryptohandys im Bereich der schweren und organisierten Kriminalität. Da wurden verschiedene Systeme geknackt, und die Chatverläufe wurden auch den Polizei- und Sicherheitsbehörden zur Verfügung gestellt. Wir reden hier über Millionen von Chatverläufen in wenigen Verfahren. Ich glaube, sehr viele polizeiliche Maßnahmen, die im Kontext von Rauschgift- und organisierter Kriminalität getroffen werden, beruhen auf genau solchen Datenmengen. Das Thema Cyberkriminalität - hybride Bedrohungen sind eben angesprochen worden - spielt ebenfalls eine sehr große Rolle.

Das heißt, es gibt einen massiven Zuwachs an Daten, und mit diesem müssen wir professionell umgehen. Deshalb ist es wichtig, dass wir die Daten in der polizeilichen Hoheit haben und vernünftig darauf gucken können.

Ich möchte an dieser Stelle bereits sagen, dass das Thema Datenschutz bei uns von Beginn an wichtig war. Die Rechtsgrundlage haben wir mit unserem Datenschutzbeauftragten in Hessen abgestimmt und in den Landtag gebracht.

Zur Lage in Hessen und dazu, warum wir das System 2016 eingeführt haben: Zu dieser Zeit gab es in Europa multiple Anschlagsszenarien. Es gab die Anschläge auf Charlie Hebdo - das wurde bereits angesprochen - und das Bataclan-Theater in Paris, es gab Terroranschläge in Belgien, und in Berlin hat Anis Amri den Anschlag auf den Weihnachtsmarkt begangen. Bei Amri gab es beispielsweise massive Bezüge zur Rauschgiftszene und der salafistischen Szene, die leider Gottes erst im Nachhinein festgestellt wurden. Wir haben uns dann im Innenministerium die Frage gestellt: Hätten wir diese Zusammenhänge erkannt?

Der ehrliche Befund lautete: Wir hätten es nicht erkannt. Das hat damit zu tun, dass unsere Systeme im Grunde siloartig organisiert sind. Das bedeutet, wenn wir beispielsweise Vorgangsdaten haben, wird sozusagen dieser Topf aufgemacht und geguckt: Haben wir Erkenntnisse zu dieser Person? Das wird in diesem Datentopf abgefragt, und es ist tatsächlich so - das gilt für alle Länder, die nicht über eine solche Software verfügen -, dass das teilweise händisch aufgeschrieben wird. Die Information wird analog erfasst, und es werden Abfragen in weiteren Datentöpfen gemacht. Ich habe gerade erwähnt, wie datenintensiv Polizeiarbeit heutzutage ist und dass unsere Ermittlerinnen und Ermittler insofern nicht mehr in der Lage sind, Zusammenhänge analog bzw. in Papierform zu erfassen. Das ist im Grunde die große Schwachstelle.

Im Kontext mit P20 - damit war ich auch jahrelang befasst - ist zu sagen: Dort sind sehr viele Befunde erhoben worden, aber nach unserem Verständnis ist zu wenig in der Umsetzung passiert. Es ist elementar wichtig, diese Daten in ein gemeinsames Bild zu bringen. Wenn man nicht in der Lage ist, sie zusammenzuführen und insgesamt in den Blick zu nehmen, fehlt in den Ermittlungen unter anderem die Geschwindigkeit. Ich möchte betonen: Wir reden über Gefahrenabwehr, und bei der Gefahrenabwehr ist es wichtig, schnell handeln zu können, um eine Gefahr abzuwehren. Das ist elementar. Deswegen betreffen die Rechtsgrundlagen im Schwerpunkt die Gefahrenabwehr. Bei Missbrauchsfällen geht es darum, einen vorhandenen laufenden

Missbrauch zu verhindern. Das ist der Schwerpunkt in der Gefahrenabwehr. Natürlich ist das immer eine doppelfunktionale Maßnahme. Das heißt, die Information wird dann auch für die Strafverfolgung genutzt.

Wir haben also die Fähigkeitslücke gesehen, und wir haben sie geschlossen, indem wir es ermöglicht haben, diese verschiedene Datentöpfe miteinander zu verbinden. Dabei ist wichtig zu betonen: Wir haben eine Rechtsgrundlage geschaffen, die die Weiterverarbeitung der Daten ermöglicht. Die Daten, die wir rechtmäßig erhoben haben, dürfen wir mit dieser Weiterverarbeitungsnorm weiterverwenden - nicht mehr und nicht weniger. Wenn wir darüber politisch diskutieren, ist für die Frage, wie viele Daten die Polizei hat, die Erhebungsnorm entscheidend. Das muss man klar sagen. Das ist kein Thema für die Debatte über eine Analyseplattform. Bei den Rechtsgrundlagen, die in den Ländern geschaffen wurden, geht es um die Frage: Dürfen wir die polizeilich rechtmäßig erhobenen Daten mit einer solchen Analyseplattform weiterverarbeiten?

Ich saß mehrere Jahre im Verwaltungsrat von P20 und durfte mitbekommen, wie die Polizeien aller Länder und des Bundes gesagt haben - nicht auf ein bestimmtes Softwareunternehmen bezogen -: Wir brauchen die Fähigkeiten einer Analyseplattform. - Das ist ein sehr tief getragener Konsens zwischen den Polizeien der Länder und des Bundes, und auf höchster Ebene - Holger Münch koordiniert das Ganze - wurde mit den Landespolizeipräsidentinnen und -präsidenten dazu ein Beschluss gefasst.

Was die Umsetzung betrifft, ist zu P20 noch abschließend zu sagen: Der Rahmenvertrag, der gerade schon angesprochen wurde, ist unter Federführung des BMI mit Bayern gemacht worden, mit dem Ziel, dort abzurufen. Es gab dann unterschiedliche politische Positionen, die dazu geführt haben, dass nicht abgerufen wurde. Der Rahmenvertrag ist also nicht auf Grundlage einer Idee von Palantir entstanden, sondern aus dem tief getragenen Wunsch heraus: Wir brauchen eine Analyseplattform. - Dabei geht es nicht um ein Unternehmen, sondern es wurden Fähigkeiten bzw. polizeilich-fachliche Anforderungen aufgeschrieben, und diese wurden umgesetzt.

Deshalb ist mir auch wichtig, in Richtung Datenschutz zu betonen, dass es aus unserer Sicht fachlich nicht sinnvoll wäre, zu sagen: Wir schreiben noch einmal auf, was wir schon wissen. - Wir kennen die notwendigen Fähigkeiten, um eine solche Analyseplattform auszuschreiben. Die Ausschreibung ist bereits erfolgt, und der Zuschlag ist seitens Bayern der Firma Palantir erteilt worden. Der Rahmenvertrag ist vom Bund bisher nicht abgerufen worden, aber er ist so verhandelt worden, dass er abrufbar wäre. Das ist die Ausgangssituation.

Wie gesagt, im Moment gibt es eine Fähigkeitslücke, und das sagen wir auch nach außen sehr klar. Das bedeutet, dass einige Länder Daten noch händisch aufschreiben müssen und versuchen müssen, diese analog zu verknüpfen, und das sehen wir als sehr großes Problem an. Wir haben viele Beispiele für sehr gute Erfahrungen mit der Software. Wenn wir die Daten verknüpfen, sind wir sehr schnell, und wir können Tat- und Täterzusammenhänge sehr relevant erkennen.

Ich möchte Ihnen drei Beispiele nennen. Das erste betrifft Massendaten, die wir im Jahr 2018 von einer amerikanischen Sicherheitsbehörde zur Verfügung gestellt bekommen haben. Dabei handelte es sich um Social-Media-Daten, und zwar im PDF-Format. Stellen Sie sich ein PDF-Dokument mit 3 000 bis 6 000 Seiten vor, in dem uns das Leben einer Person in einem sozialen Netzwerk zur Verfügung gestellt wird. Es waren riesige Datenmengen, die ausgedruckt unzählige Aktenordner gefüllt hätten, und zwar allein aus einem Verfahren. Es ging dabei um die

Verschleierung von Aktivitäten im Bereich der organisierten Kriminalität bzw. des Terrorismus. Acht Accounts wurden überwacht, und deren Inhalte wurden uns zur Verfügung gestellt. Wir wussten, dass es den Verdacht gab, dass der damalige Präsident Trump umgebracht werden sollte. Das Ganze betraf Eschwege im Norden von Hessen. Da hat man zunächst ein Stück weit geschmunzelt und sich gefragt: Kann das überhaupt passieren?

Wir haben das aber ernst genommen, und wir waren unter Nutzung der Analysesoftware in der Lage, innerhalb eines Wochenendes relevante Stellen in diesen Daten, in diesen acht Accounts zu detektieren, und wussten dann: Hier geht es um Vorbereitungshandlungen, hier geht es um Schlagwörter wie „Waffe“ oder „Bombe“. Wir konnten daraufhin einen Durchsuchungsbeschluss erwirken, haben am Montag durchsucht und haben einen 19-jährigen Mann festgenommen. Dieser hatte eine Handgranate in seiner Wohnung, er hatte mit dem IS kommuniziert, und das Anschlagsschreiben war bereits vorbereitet. Das wäre dann live gegangen. Auch wenn es nicht realistisch war, den amerikanischen Präsidenten umzubringen: Der junge Mann hat eingeräumt, dass er einen Anschlag begehen wollte, und wir haben das mit hoher Geschwindigkeit durch eine schnelle Auswertung der Daten verhindern können. Das war der relevanteste Fall, bei dem wir mithilfe der Software offensichtlich einen Anschlag verhindert haben.

Ein zweites Beispiel. Mithilfe von HessenDATA gab es im Bereich der schweren organisierten Kriminalität - bei Europol redet man von Organized Crime Groups; das betrifft Geldautomaten-Sprengungen und andere Phänomene - mehrmals Ermittlungserfolge. Daran sehen wir, dass wir Zusammenhänge herstellen können, wodurch wir in der Lage sind, Gefahren abzuwehren und Täter festzunehmen.

Dritter Punkt: pädophile Netzwerke. Leider haben wir Kinderpornografie früher viel zu sehr täterbezogen bekämpft. Wir bekämpfen das in Hessen massiv, und zwar vor allem mit dem Ansatz, uns die Netzwerke anzugucken. In einem Fall hatten wir einen Bezug von Nordrhein-Westfalen nach Kassel, und wir waren in der Lage, mit der Software einen Kinderpornoring auf Mallorca aufzudecken, indem wir die Daten von zwei Bundesländern eingespielt haben. Es ging dabei um Datenpunkte. Zwei unterschiedliche Devices, also Mobilfunkgeräte, waren im gleichen WLAN auf Mallorca eingebucht. Diese vermeintliche Kleinigkeit haben wir in den Daten gefunden, und das hat dazu geführt, dass wir feststellen konnten, dass sich diese Personen in einer Finca, die sie angemietet hatten, Kinder haben zuführen lassen und dort dauerhaft Missbrauch begangen haben.

Insgesamt sehen wir es als eine dringende fachliche Notwendigkeit, die Zusammenhänge herzustellen. Denn es ist der Kernauftrag der Polizei, Gefahren abzuwehren. Wir müssen nicht auf ein einzelnes Verfahren gucken, sondern es geht darum - ich gehe jetzt noch einmal zurück in Richtung Anis Amri und Terrorkriminalität -, zu schauen, wo es Bezüge zwischen Terrorgruppierungen gibt, und zwar auch länderübergreifend. Denn wir reden über internationale Kriminalitätsphänomene. Wer in die Daten zur organisierten Kriminalität (OK) schaut, der sieht, dass es sich um ein vernetztes bzw. arbeitsteiliges Handeln von OK-Gruppierungen handelt, die weltweit agieren, und in diesem Kontext erklärt sich auch, warum wir Analyseplattformen brauchen. Es ist kriminalistisch unstrittig, dass wir sonst keine Chance mehr haben.

Um die Freiheit der Menschen zu schützen, ist es natürlich hochrelevant, dass wir vernünftig damit umgehen. Dafür haben wir ein Rollen- und Rechtekonzept; das ist bereits angesprochen worden. Das heißt, wir sind in der Lage, dezidiert zu sagen, wer welche Daten sehen darf. Ich vereinfache das mal: Haben wir zum Beispiel 2 000 Nutzer, können davon rund 20 in den ganz

großen Topf, also auf alle Details, sehen. Dann wird entsprechend abgestuft, wer welche Daten sehen darf. Die Technologie ermöglicht uns „Privacy by Design“. Auch der Zweckbindungsgrundsatz spielt dabei eine Rolle. Wenn wir nur in einen Datentopf gucken dürfen, wird die Polizei keine Tat- und Täterzusammenhänge erkennen können. Wir müssen uns das in Gänze anschauen, weil wir komplexe und abgeschottete Täterstrukturen haben. Mit Blick auf den Datenschutz müssen wir dafür sorgen, dass nachvollziehbar protokolliert wird, wer welche Abfrage gemacht hat, und wir müssen klar gegen Missbrauch vorgehen.

In der HessenDATA-Software gibt es eine Maske, wo die Ermittlerinnen und Ermittler eintragen sollen, warum sie die Plattform nutzen. Wir nennen das Zugriffskontrolle. In der Diskussion wird oft die Frage gestellt, ob unbeteiligte Bürger in den Fokus rücken. Ich hatte in meiner Heimatstadt Marburg einen Verkehrsunfall, mir ist einer von hinten in den Wagen gefahren. Da bin ich im polizeilichen Vorgang ein Unfallteilnehmer, ich bin Teil dieser Daten. Wenn das jemand abfragt, weil er sich aus irgendeinem Grund für mich interessiert, ist das eine rechtswidrige Abfrage. Zugriffskontrolle bedeutet: Wir dürfen Zielpersonen abfragen, wenn wir Gefahren abwehren wollen oder wenn wir einen Verdacht haben. Nur diese Namen dürfen wir in die Maske eingeben. Das geben unsere Ermittler und Ermittlerinnen an, und dann dokumentiert diese Plattform exakt, welche Ermittlungsschritte gemacht werden. Wenn wir einen Missbrauchsverdacht haben, gucken wir uns an: Welche Rechtsgrundlage wurde angegeben, und was wurde tatsächlich durchgeführt?

Zum Themenfeld Informationssicherheit und Datenschutz sowie zu den Diskussionen, die darüber geführt wurden: Das Team von Juliane Stieg verantwortet komplett die Datenintegration mit eigenem, von uns geschulten Personal. Die Hardware ist Hardware der hessischen Polizei, die Server stehen in der Hessischen Zentrale für Datenverarbeitung. Zum On-Premise-Prinzip ist gerade schon ausgeführt worden. Zu der Frage, warum an dieser Stelle nicht der Cloud Act greift: Weil auf unsere Infrastruktur, die wir komplett kontrollieren, niemand zugreifen kann - auch nicht Palantir. Das ist unsere Infrastruktur. Ich bin kein Jurist, aber das Gesetz sieht vor, dass amerikanische Firmen verpflichtet werden könnten. Wir sind aber keine amerikanische Firma, und es ist unsere Hardware, es sind unsere Daten, und die kontrollieren wir. Wenn wir nur an einem Tag in den vergangenen acht Jahren das Gefühl gehabt hätten, dass da irgendetwas passiert, würde die hessische Polizei nicht mehr mit Palantir zusammenarbeiten.

Auch in Vergabeverfahren werden Zuverlässigkeiten geprüft. Es sind bestimmte Dinge im Zusammenhang mit dem Fraunhofer-Institut angesprochen worden. Die Updates werden von uns intensiv kontrolliert. Wir haben intensive Sicherheitsmaßnahmen eingebaut, um einen Abfluss von Daten zu verhindern. Das muss man ganz klar sagen. Im operativen Geschäft gibt es dafür keine Anhaltspunkte, sondern es ist eine sehr gute, vertrauensvolle Zusammenarbeit. Wir sind aber bei der Ausrichtung der Maßnahmen davon ausgegangen, dass es auch anders sein könnte. Über die Maßnahmen, die man getroffen hat, redet man in der IT aber nicht im Detail - denn dann würde man seine Konzepte komplett offenlegen.

Um das zusammenzufassen: Die Frage, ob man im digitalen Zeitalter Datenanalysen in Echtzeit und Analyseplattformen braucht, können wir nur bejahen. Es ist unstrittig, dass man das braucht. Wir nutzen die Systeme der Firma Palantir in der Form, wie wir sie einsetzen, wegen der großen Fähigkeitslücke, die im Moment vorhanden ist. Eben wurde auch die Innenministerkonferenz erwähnt und gesagt, dass grundsätzlich Einvernehmen bezüglich der Stärkung der digitalen Souveränität hergestellt wurde. Unser hessischer Minister hat aber auch gesagt: Solange wir noch nicht dort sind, wo wir hinwollen, müssen wir, um die Freiheit und den Schutz der

Bevölkerung, der Bürgerinnen und Bürger Deutschlands zu garantieren, die Fähigkeiten haben, um in der Lage zu sein, Gefahren und Tat-Täter-Zusammenhänge schnell zu erkennen, um Anschläge oder herausragende Gefahrenlagen zu verhindern.

Abg. **Deniz Kurku** (SPD): Vielen Dank für Ihre Darstellung, Herr Koch. Soweit ich weiß, gibt es in Hessen rund 15 000 Abfragen pro Jahr über diese Software. Da kann man schon von einem Masseneinsatz sprechen. Das Bundesverfassungsgericht hat aber ausdrücklich verboten, dass das als Regelmaßnahme genutzt wird. Sehen Sie das auch kritisch? In Hessen ist das ja längst Realität.

Wir haben zudem gehört, dass man - zumindest hypothetisch - das System für die Sicherheits- und Ordnungsbehörden sozusagen mit einem einzigen Knopfdruck abschalten könnte. Wenn die Polizei die Software in so vielen Fällen nutzt, handelt es sich durchaus um ein maßgebliches Instrument im polizeilichen Alltag. Wie schätzen Sie vor diesem Hintergrund diese Gefahr ein?

Ich komme zu meiner letzten Frage. In Hessen gab es zu dem Thema, über das wir hier sprechen, einen parlamentarischen Untersuchungsausschuss. Denn am Ende hat ein Vergabeverfahren ohne Teilnehmerwettbewerb stattgefunden. Wir müssen das hier nicht ausführlich diskutieren. Ich würde einfach nur gern wissen: Was haben Sie als Quintessenz daraus gezogen? Was würde man heute vielleicht anders machen?

Bodo Koch: Zu den 15 000 Abfragen: Die rechtliche Grundlage ist § 25 a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung. Danach dürfen wir die automatisierte Datenanalyse bei schweren Straftaten, im Bereich der organisierten und der Staatsschutzkriminalität nutzen. Wie die polizeiliche Kriminalstatistik zeigt, gibt es durchaus sehr viele Straftaten, die in diesen Bereich fallen. Wir haben ungefähr 25 000 Mitarbeiterinnen und Mitarbeiter, und insgesamt setzen, wie gesagt, 2 000 Beamte die Software ein, und zwar entsprechend der gesetzlichen Vorgaben.

Wir haben auch alles umgesetzt, was uns vom Bundesverfassungsgericht - ich durfte uns dort mit vertreten - aufgetragen wurde. Im Übrigen hat uns das Bundesverfassungsgericht - das möchte ich betonen - nur wenige kleine Hausaufgaben gegeben. Der Kernpunkt war im Grunde die mangelnde Bestimmtheit der gesetzlichen Befugnisse und nicht die Anzahl der Abfragen. Wir hatten den Einsatz von HessenDATA in riesigen Dokumenten geregelt - das waren mehrere Aktenordner voller Regelungen -, und große Teile davon haben wir in eine Verwaltungsvorschrift und ins Gesetz übernommen - allerdings nicht allzu detailliert, um dynamisch auf Veränderungen reagieren zu können. Das haben wir entsprechend geändert. Wir haben also einen klaren gesetzlichen Rahmen, in dem wir das System nutzen.

Zu Frage 2: Wir schätzen es als extrem unrealistisch ein, dass das System auf Knopfdruck abgeschaltet werden könnte. Wir arbeiten jetzt im neunten Jahr mit Palantir zusammen, und im operativen Geschäft - wir schauen nicht auf mögliche Anteilseigner - ist die Zusammenarbeit sehr gut und vertrauensvoll. Wenn dieser sehr hypothetische Fall aber tatsächlich eintreten würde, hätten wir den sogenannten Stack trotzdem komplett unter Kontrolle, weil die Software bei uns läuft. Ich will ehrlich sein: Wenn man irgendwann kein Update mehr bekommt, ist das natürlich nicht optimal. Aber das ist für uns ein sehr kleines Risiko. In der Diskussion geht es auch erst einmal darum, ob man die Fähigkeit hat oder nicht.

Zu Ihrer Frage zum Untersuchungsausschuss - auch dort durfte ich mich äußern -: Ich hatte noch nicht erwähnt, dass wir zu diesem Zeitpunkt neben der internationalen Terrorlage auch eine konkrete Gefährdungslage in Hessen hatten. Es gab eine Gruppierung bzw. eine Terrorzelle, die im Rhein-Main-Gebiet agierte, und wir hatten eine Besondere Aufbauorganisation eingesetzt. Vor diesem Hintergrund haben wir gesagt: Wir brauchen eine marktfertige Software.

Das Vergaberecht sieht in solchen Fällen das Konstrukt der zeitlich dringlichen Vergabe vor. Wenn beispielsweise die Bundeswehr kurzfristig aus zwingenden Gründen eine ganz bestimmte Waffe braucht, kann sie vom regulären Vergabeverfahren abweichen und diese Waffe direkt beschaffen. Eine saubere Ausschreibung muss in solchen Fällen aber nachgeholt werden. Wir haben auch zeitlich dringlich beschafft, haben die Palantir-Software eingeführt und gleichzeitig ein Vergabeverfahren eröffnet. Nach sechs Monaten hat die Firma Palantir dann auch in dem Vergabeverfahren den Zuschlag bekommen. In Nordrhein-Westfalen und Bayern wurde trotz vieler Bemühungen - deutsche Firmen haben gesagt, sie könnten das auch - auch die zweite bzw. dritte Ausschreibung von Palantir gewonnen.

Der Untersuchungsausschuss hat also letztlich klar gezeigt, dass wir bei der Vergabe nach Recht und Gesetz gearbeitet haben.

Abg. **Saskia Buschmann** (CDU): Herzlichen Dank, Herr Koch. Sie hatten sich zu den Rahmenverträgen eingelassen. Wir leben in einer sehr komplexen Welt, und es wäre schon zielführend, wenn man deutschlandweit dasselbe System nutzen würde, um die gleich Art von Daten zu erhalten. Wie sehen Sie das?

Bodo Koch: Ich habe eben deutlich gemacht, dass wir bei P20 einen sehr großen fachlichen Konsens im Hinblick auf die Nutzung einer Analyseplattform hatten. Der Konsens kommt aus einer sehr starken fachlichen Haltung. Es geht darum, nationale und internationale Kriminalität zu bekämpfen und eine Plattform zu haben, über die man übergreifend Informationen austauschen kann. In den Ländern, die jetzt schon die Software nutzen, gibt es immer wieder übergreifende Datenaustausche, und wir sehen, wie gut das funktioniert. Wir sehen, dass wir - unabhängig von einem konkreten Anbieter - eine Plattform mit unterschiedlichen Mandanten brauchen, in die die entsprechenden Rechtsgrundlagen integriert sind und über die man sehr einfach Daten austauschen kann. Das würde die Kriminalitätsbekämpfung erheblich verbessern. Und ja, wir brauchen an dieser Stelle eine nationale Lösung.

Abg. **Birgit Butter** (CDU): Vielen Dank, Herr Koch und Frau Stieg, für Ihr Kommen und Ihre Ausführungen. Diese sind besonders wichtig, denn Sie sind die Praktiker, die schon mit diesem Tool arbeiten und Erfahrung gesammelt haben.

Ich danke Ihnen sehr herzlich, dass Sie noch einmal ausdrücklich zur Zweckbindung, zur Zugriffskontrolle Stellung genommen haben - auch, um hier sozusagen gewisse Verteufelungen ein wenig einzudämmen. Von einigen - auch von Anzuhörenden, die nach Ihnen an der Reihe sind - wird die steile These vertreten, dass Bayern, Hessen und Nordrhein-Westfalen an dieser Stelle verfassungswidrig unterwegs sind, und es wird angeführt, dass es im Moment Klageverfahren gibt. Man muss immer auch gucken, aus welcher Ecke die Klagen kommen und ob die Kläger denn zufrieden wären, wenn es eine europäische Lösung gäbe. Denn diese haben grundsätzlich etwas gegen Datenerhebungen.

Wenn ich Sie richtig verstanden habe, war es die fehlende Bestimmtheit der Regelungen, die vom Bundesverfassungsgericht moniert wurde, und an dieser Stelle haben Sie nachjustiert. Ist das richtig?

Sie haben auf die Notwendigkeit zur Neuausrichtung der Informationsarchitektur bei der Polizei des Bundes und der Länder im Jahr 2016 hingewiesen - Stichwort „Saarbrücker Agenda“ - und darauf, dass sich alle einig waren, dass etwas getan werden muss. Das ist zehn Jahre her. Sie haben sich 2017 in Hessen auf den Weg gemacht und gute Erfahrungen gesammelt, aber wir hier in Niedersachsen sind noch nicht weitergekommen. Es wird immer auf P20 verwiesen und gesagt: Das wird möglicherweise eine Lösung sein. - Können Sie kurz erklären, was P20 ist und wie weit P20 ist?

Bodo Koch: Zur ersten Frage: Die Bestimmtheit der Regelungen war tatsächlich das Hauptthema. Das Gericht hat uns gefragt: Warum haben Sie das nicht in das Gesetz oder in die Verwaltungsvorschrift geschrieben? Das wurde uns sehr stark mitgegeben. Denn wir konnte auf alle Fragen antworten und sagen: Wir haben Konzept 1, Konzept 2 und Konzept 3. - Früher waren Gesetze, glaube ich, nicht so detailliert ausformuliert. Das ist an dieser Stelle aber aufgrund des Eingriffes, der hier vorgenommen wird, nötig. Durch die verschiedenen Datentöpfe haben wir eine deutlich größere Eingriffstiefe. Deswegen haben wir Dinge, die wir an anderer Stelle aufgeschrieben hatten, zum einen etwas länger im Gesetz ausgeführt, zum anderen haben wir das aber insbesondere auch über eine Verwaltungsvorschrift gemacht, die transparent nach außen veröffentlicht wird, um den Bürgerinnen und Bürgern sagen zu können: Das ist das, was wir mit dieser Software machen. Das war der Hauptgrund, und seit dieser Zeit haben wir die Analyseplattform im Einsatz.

Zu P20: Alle Polizeien der Länder und des Bundes haben sich hier zusammengetan. Das ist praktisch das Digitalisierungsvorhaben unter Federführung des BMI. Tatsächlich gibt es schon sehr viele Befunde zur Analyse; die Anforderungen sind bereits mehrfach aufgeschrieben worden. Der Ansatz war, das Bayern vorausgeht bzw. die Federführung übernimmt. Als Bayern die Ausschreibung gemacht hat, war das System bereits in Hessen und Nordrhein-Westfalen im Einsatz. Bayern ist aber wieder ergebnisoffen in das Verfahren gegangen, weil alle dachten: Vielleicht hat sich der Markt in Deutschland und Europa verändert.

Aber auch als die Bayern gemeinsam mit dem BMI ausgeschrieben haben, kam am Ende nur ein Anbieter heraus, und das war die Firma Palantir. Dieser Anbieter hat dann von Bayern den Zuschlag bekommen, nicht aber von den anderen Beteiligten. Ich würde sagen, obwohl es einen fachlichen Konsens gab, war im Verwaltungsrat politisch keine Einigung möglich, und somit ist das nicht abgerufen worden. Der aktuelle Stand von P20 ist, dass man am Datenhaus arbeitet, um die Daten zusammenzubringen. Diesen Grundgedanken trägt Hessen auch mit. Das wird aber nicht dazu führen, dass die Fähigkeitslücke in der nötigen Geschwindigkeit geschlossen werden kann.

Abg. **Alexander Saade** (SPD): Ich habe eine Frage zur Ausschreibung, speziell in Bayern. Soweit mir bekannt ist, waren die Anforderungen in der Ausschreibung so definiert, dass Bayern verlangt hat, dass es ein System sein muss, das in der Praxis bereits läuft. Das wäre für mich vergleichbar mit dem Fall, dass man Funkstreifenwagen haben möchte und in der Ausschreibung sagt: Der Hersteller ist egal, vorn müssen die Wagen aber einen Daimler-Stern haben. - Ungefähr

so wirkt das auf mich. Können Sie darauf einmal genauer eingehen und vielleicht auch sagen, aufgrund welcher Marktanalyse Sie zu dem Ergebnis kommen, dass es kein vergleichbares System auf dem Markt gibt?

Was mich vor allem interessiert, ist, ob HessenDATA die Möglichkeit sieht, auf ein anderes System zu wechseln bzw. ob der Datenexport auch direkt für andere Systeme genutzt werden kann. Welche Kosten wären damit gegebenenfalls verbunden? Oder ist man jetzt sozusagen an ein bestimmtes System gekettet?

Bodo Koch: Zum Thema Marktfähigkeit: Wir verfolgen die Aussagen in der Presse natürlich auch sehr intensiv, und an der einen oder anderen Stelle wundern wir uns schon. Wir hatten eine Situation - Terroranschläge in Frankreich und Belgien, eine Terrorzelle in Hessen -, in der wir eine marktfertige Lösung brauchten, und wir hatten mit Blick auf die Fähigkeitslücke, um es deutlich zu sagen, keine Lust, drei bis fünf Jahre lang eine Analyseplattform zu entwickeln. Das ist die Aussage. Man kann darüber gern schreiben, aber man sollte dann auch sagen, was die Idee dahinter war.

In einer Situation, in der man schon sehr lange diskutiert, bedeutet Marktfähigkeit: Wir wollen eine schnelle Lösung. Ich bin jetzt, wie gesagt, bei der damaligen Situation und dem Stand von Hessen, und marktfähig war für uns eine wesentliche Herausforderung. Um es klar zu sagen: Das ist nicht vergleichbar damit, dass am Ende ein Daimler dabei herauskommt, sondern das bedeutet, dass sich selbst Jahre später deutsche bzw. europäische Firmen - dafür werben wir auch immer - so aufstellen können, dass sie, wenn sie marktfähig sind, wieder im Wettbewerb stehen. Wir würden uns freuen, wenn wir so eine Stärkung der digitalen Souveränität hinbekommen.

Abg. **Alexander Saade** (SPD): Ich habe mit meiner Frage nicht auf Hessen abgezielt - da waren die Bedingungen sicherlich anders -, sondern auf Bayern, wo es auch eine Ausschreibung gab. Dort wurde explizit auf ein System abgestellt, das schon in der praktischen Nutzung ist. Da ging es nicht einmal um Marktfähigkeit.

Bodo Koch: Ich würde trotzdem klar dagegenhalten, dass damit nicht ein bestimmter Anbieter gemeint war, sondern es bei diesen Lagen immer darum geht, dass wir diese Fähigkeiten dringend brauchen. Es gibt einen gewissen Handlungsdruck, weil es sich um Phänomene handelt, die die Sicherheit der Bürgerinnen und Bürger am ehesten beeinträchtigen. Ich glaube, man muss das schon in diesem Kontext sehen. Ich würde sagen, dass das auch in Bayern so gemeint war.

Zum Thema Marktanalyse - ich würde insofern nur für Hessen sprechen -: Wir hatten eine zeitlich dringliche Beschaffung. Wir wussten, einer kann es, und den haben wir bezuschlagt. In einem solchen Fall gibt es vorab keine klassische Marktanalyse, sondern wir haben eine europaweite Ausschreibung gemacht und die Anforderungen benannt. Das Verfahren hat sechs bis acht Monate gedauert, und am Ende kam tatsächlich die Firma Palantir dabei heraus.

Zum Datenexport: Das sind unsere Daten, sie liegen auf unseren Servern. Wir hören immer wieder von einem Lock-in-Effekt. Wir können Ihnen das aber gern vor Ort zeigen: Wir nehmen die Daten, holen sie heraus und spielen sie in ein anderes System ein. So einfach ist das. Wir machen das jetzt seit acht Jahren und wundern uns, dass das immer wieder anders in der Presse steht. Die Wahrheit ist, dass wir die Datenhoheit haben und sie hingeben können, wo wir wollen.

Abg. **Saskia Buschmann** (CDU): Noch eine praktische Frage: Wenn wir in Deutschland einen Terroranschlag haben - Sie haben Anis Amri und Ähnliches angesprochen -, wird man auch fragen, welche Daten vorliegen. Welchen zeitlichen Vorteil erreichen Sie durch die Auswertung mit einer Analysesoftware im Vergleich zur händischen Auswertung? Können Sie die Wege einer analogen Auswertung ein bisschen näher beschreiben?

Bodo Koch: Ich kann den Stand in Hessen vor HessenDATA beschreiben. Daran wird vielleicht die Fähigkeitslücke deutlich bzw. was in Ländern, die keine solche Plattform nutzen, passiert.

Vor HessenDATA kommt ein Fernschreiben zu Anis Amri: Wir haben Erkenntnisse, dass in Berlin ein Terroranschlag war. - Es werden die Gruppierung und Informationen zu der Person aufgelistet. Das funktioniert über Fernschreiben. Das heißt, das geht zu jedem LKA, und von dort aus wird zentral in den Ländern gesteuert: Welche Informationen habt ihr zur Person Anis Amri und einer bestimmten Gruppierung, zu Kontaktpersonen etc.?

Vor HessenDATA wurden solche Fernschreiben in Hessen in alle entsprechenden Bereiche weitergeleitet. Sie gingen in die Silos der Präsidien, teilweise noch in Untersilos, und es wurde versucht, das wieder zusammenzuführen. Das LKA hat dann Tage später - möglicherweise dauert es noch länger, wenn man in Massendaten gucken muss - gesagt: Es kommt etwas zurück. - Vom LKA in Wiesbaden wäre das dann wieder nach Berlin gegangen, und das BKA wäre entsprechend beteiligt worden. Das war der Weg vor HessenDATA. Das heißt, wir hatten Datensilos in den Polizeipräsidien, die nicht miteinander kompatibel waren.

Seit der Einführung von HessenDATA sind alle Daten so angebunden, dass mit *einem* Zugriff auf *eine* Analyseplattform gefragt wird: Sind Anis Amri und die fünf oder acht Kontaktpersonen plus zwei Fahrzeuge in Hessen bekannt? Und dann können wir innerhalb von ungefähr fünf Minuten, nachdem wir nach dem Vier-Augen-Prinzip noch einmal darauf geschaut haben, sagen: Wir haben Informationen. Oder: Wir haben keine Informationen. - In all diesen Lagen ist das hochrelevant. Und das gilt wieder unabhängig vom Anbieter.

Wir haben mit dem Bayerischen LKA gesprochen, mit Blick auf den Terroranschlag in München auf ein jüdisches Objekt. Da ging es ebenfalls um eine Situation, in der man den Namen eines möglichen Tatverdächtigen eingeben kann, um sofort handeln und sagen zu können: Ich kann in das Umfeld hinein ermitteln und in Fahndungsmaßnahmen gehen.

Der Anschlag auf den Weihnachtsmarkt in Magdeburg ist ein etwas anderer Fall. Dort handelte es sich um eine Amokfahrt. Aber auch dann stellt sich die Frage: Was wissen wir zu der Person? Das betrifft den Bereich Staatsschutz und ist ebenfalls ein relevanter Aspekt. Unsere Gefährder stehen auf einer Beobachtungsliste, und wenn eine neue Information bzw. eine neue Straftat hinzukommt, läuft bei den jeweils Zuständigen eine Nachricht auf: Zu dem Gefährder gibt es einen neuen relevanten Sachverhalt. Schau dir das bitte an! - Das schafft Sicherheit für die Bürgerinnen und Bürger, und das ist über eine solche Plattform möglich.

Das sind die Vorteile. Man ist im übergreifenden Informationsaustausch nicht nur sprechfähig, sondern man hat fachlich sofort Anknüpfungspunkte, um gefahrenabwehrende Ermittlungen durchzuführen.

AG KRITIS

Schriftliche Stellungnahme: Vorlage 2

Anwesend:

- Manuel Atug, Gründer und Sprecher

Manuel Atug: Lassen Sie mich vorab sagen: Auch wir von der AG KRITIS finden es ziemlich verstörend, dass im Hohen Haus der Anbieter der gewünschten Software als offensichtlicher Befürworter an der Anhörung teilnimmt, während andere Anbieter nicht an der Diskussion beteiligt werden. Unabhängigkeit sieht ein bisschen anders aus. Das finden auch wir seltsam.

Unser generelles Selbstverständnis ist: Polizeien sollen natürlich digitalisieren können, und, ja, es gibt dafür Lösungsmöglichkeiten - aber nicht durch Palantir oder sogenannte alternative Lösungen aus Europa oder Deutschland. Darauf komme ich gleich zu sprechen.

Zur Anmerkung von Palantir, es gebe große Erfolge, die noch nicht einmal die Kritiker bezweifelten, möchte ich klar und unaufgeregt anmerken: Gucken Sie gerne mal aus der eigenen Blase heraus! Dann werden diese Fake News in der realen Welt aufgeklärt. Die AG KRITIS kennt keine wissenschaftliche und unabhängige kriminologische Evaluierung dazu. Wir haben vorhin viele anekdotische Beispiele gehört, aber das sind eben nur Anekdoten und Beispiele und keine strukturierte Form der Erfassung von Verhältnismäßigkeit.

Wie Palantir funktioniert und warum europäische Alternativen aus unserer Sicht ebenfalls offensichtlich verfassungswidrig sind, möchte ich im Folgenden kurz erklären.

Der Einsatz einer Software wie Palantir oder vergleichbarer Alternativen, die ontologische Datenmodelle nutzen, ist aus einem einfachen Grund offensichtlich verfassungswidrig: Sie ist „Rasterfahndung by Design und Default“. Das ist die Logik hinter ontologischen Modellen. Zur Nutzung müssen Mitarbeitende - beispielsweise von Palantir - sogenannte Data Pipelines bauen; das haben wir vorhin gehört. Diese Data Pipelines lesen aus den bestehenden Polizeidatenbanken kontinuierlich alle Informationen aus und speisen diese strukturiert in Palantir als Datenbasis ein. Daten in diesen polizeilichen Datenbanken wurden allerdings mit Zweckbindungen erhoben - beispielsweise Zeugendaten und Aussagen - und dürfen nicht ohne Weiteres anderweitig genutzt oder zweckentfremdet missbraucht werden.

Auch die hypothetische Datenneuerhebung wäre in diesem Kontext noch erwähnenswert und relevant, wurde aber in der Debatte ebenfalls komplett ignoriert.

Die kontinuierlich-strukturierte Einspeisung von Daten in Palantir stellt also eine „Rasterfahndung by Design und Default“ dar. Die Zweckbindung der Daten muss vor der Einspeisung in die Data Pipelines von Palantir eigentlich durch Kennzeichnung der Daten sichergestellt werden. Daher ist eine Klassifizierung der Daten in allen polizeilichen Datenbanken der Strafverfolgungsbehörden *vor* einem solchen Softwareeinsatz vorzunehmen, und nur verfassungsrechtlich legitimierte Daten dürfen dann in eine automatische Datenanalyse und ein Recherchesystem überführt werden. Das ist hier an manchen Stellen nicht der Fall. Dies muss also gesetzlich und auch technisch sichergestellt werden; andernfalls bleibt ein offensichtlich verfassungswidriger Zustand erhalten, selbst bei Einsatz von alternativen Lösungen.

Die Data Pipelines werden nicht von den Strafverfolgungsbehörden selbst „gebaut“, sondern von Mitarbeitenden von Palantir entwickelt. Wir haben ja gerade von den Forward Deployed Engineers gehört, die dann vor Ort eingesetzt werden. Dadurch haben diese Palantir Mitarbeitenden Zugriff auf die Verarbeitungslogik und auch auf die Daten selbst. Das kann man technisch nicht verhindern, und es wurde auch bestätigt, dass das nicht verhindert wird. Sie haben also immer einen Zugriff auf die Daten, auch wenn er streng kontrolliert wird - das ist das Problem.

Palantir nutzt also, wie erwähnt, Ontologie, um die Daten der Strafverfolgungsbehörden mittels Data Pipelines kontinuierlich in die eigene Datenbasis zu integrieren. Ontologie als technische Basis ist ein formales Bedeutungsmodell, das definiert, wie Daten in den jeweiligen Landespolizeien verstanden, verknüpft und im Operativen nutzbar gemacht werden. Das heißt, Palantir beschreibt alle Eigenschaften, Merkmale und Beziehungen der Daten zueinander einheitlich und strukturiert sie als gemeinsame Bedeutungswelt in einem zentralen System. Das ist keine Superdatenbank oder ein System nach dem Motto: „Da kann man mal Recherchen machen“. Da wird ein digitaler Zwilling einer Strafverfolgungsbehörde geschaffen, der alle Daten, alle Prozesse, alle Regeln und alle Nutzerinteraktionen in einem einheitlichen Modell strukturiert, zentral zusammenführt und maschinell verarbeitet, durchsucht und logisch verknüpft. Das sind keine Kleinigkeiten!

Ich habe ein Beispiel mitgebracht. Es wird ein Mensch als semantisches Objekt dargestellt und angelegt und gesagt: Das ist ein Mensch. Dem werden dann Merkmale wie Name, Geburtsdatum usw. zugeordnet, aber auch Handynummern, Adressen und andere Elemente. Zu diesen Merkmalen gehören auch Tätowierungen, Narben, Fotos, Videos und Fallaktennummern. Darüber hinaus gibt es zum Beispiel auch Fahrzeuge, die wiederum jeweils ein Objekt darstellen, und diesen kann man dann die Merkmale Kennzeichen, Marke, Farbe, Seriennummer etc. zuordnen. Bei Handys kann man die Nummern mit allen Kommunikationen und Kommunikationspartner*innen dieser Nummer und alle Daten aus IMSI-Catcher-Überwachungen, Standorte durch stille SMS oder Bewegungsdaten durch Zeitstempel bei Standorten ermitteln.

Die USA - ICE - kaufen von Data Brokern Milliarden von Datensätzen für Standorte, speisen sie in Palantir auch als Data Pipeline ein und kommen damit fast zu einer Echtzeitüberwachung, wo sich bestimmte Personen aufhalten. All das kann man da einspeisen; das ist super easy implementierbar. Darüber hinaus werden auch Fingerabdrücke, Lichtbilder, Fallakten der Ermittler mit den Berichten, die Sammlung einzelner polizeilicher Vorgänge wie die Aufnahme eines Verkehrsunfalls und digitale Asservate all diesen Objekten zugeordnet. Das kann man in Palantir sehr einfach strukturieren. Die Ermittler*innen können auch Daten aus dem Internet, also auch aus sozialen Medien, einspeisen und analysieren; das wurde uns gerade bestätigt. Das betrifft nicht nur Social-Media- oder Telekommunikationsdaten, sondern beispielsweise auch Daten von Einwohnermeldeämtern oder aus Waffenregistern. Alles kann man per Data Pipeline einbinden, zuordnen oder manuell einspeisen, wenn man möchte, und wenn man bereits über Daten verfügt, kann man diese importieren, wenn man keine automatisierte Data Pipeline hat. Das haben wir vorhin gehört: Das können die 3 000 bis 6 000 PDF-Seiten pro Fall sein oder die Datenbestände im Petabyte-Bereich bei Massendaten.

Das alles ist also als Beziehungsgeflecht dieser Objekte und Merkmale in Palantir vorhanden und wird dann visualisiert und ist umgehend verfügbar. Die Analyse kann innerhalb von fünf Minuten erfolgen - das wurde gerade gesagt - und umfasst alle Daten aus allen Datenbanken, die in Palantir eingespeist werden, auch wenn diese verfassungsmäßig nicht von der Strafverfolgungsbehörde hätten verarbeitet werden dürfen. Faktisch ist damit eine Rasterfahndung standardmäßig

implementiert und die Zweckbindung rein technisch aufgehoben - und das kann man nicht verhindern, denn das ist der Sinn und Zweck von einem ontologischen Modell. Das heißt, das verfassungsmäßige Trennungsgebot wird unterwandert und aufgehoben.

Aufgrund dieser Beziehungsgeflechte im ontologischen Datenmodell basierende und datengetriebene Entscheidungen und Prozesse von den Strafverfolgungsbehörden verändern sogar die Arbeitsweise der Polizei und machen sie und ihre hoheitlichen Aufgaben vollständig abhängig von einem externen System und Anbieter - namens Palantir. NRW und Bayern haben öffentlich bereits mehrfach ihre totale Abhängigkeit von Palantir kommuniziert und machen auch gar kein Geheimnis daraus.

Eine kurze Aufklärung zum Thema „KI in Palantir“ - denn es wird gesagt, das gebe es aktuell nicht, aber die Debatten darüber finden zurzeit statt -: Für den zukünftigen Einsatz von KI sind alle Palantir-Plattformen darauf ausgelegt, KI-Modelle und Machine-Learning-Funktionen nahtlos einzubinden - das wurde schon bestätigt -, um Analysen und automatische Fallentscheidungen oder Triggerpunkte zu realisieren. Das heißt, irgendwo taucht eine Nummer auf, und dann wird etwas automatisiert gemacht. So wird Palantir beispielsweise mit KI-Integration bei ICE in den USA oder beim Targeting, also bei der Zielauswahl, von Israel in Gaza genutzt. Das ist Sinn und Zweck dieser Funktion, und das ist irgendwie auch der Zweck eines Ermittlers oder einer Ermittlerin - das ist die Logik dahinter.

Die Ontologie spielt im Zusammenhang mit KI, wenn sie in Palantir eingeführt wird, eine Schlüsselrolle. Denn qualitativ hochwertige Daten sind immer die Grundlage für ein gutes maschinelles Lernen. Das ist durch die Data Pipelines und die Ontologie sichergestellt. Der sogenannte Artificial Intelligence Platform Pipeline Builder von Palantir soll die gesamten Large-Language-Model-Funktionen in die Data Pipelines und in die Analyse von Palantir integrieren. Das Ontologiesystem verbindet dann die Daten mit KI-Modellen und -Prozessen und erlaubt dann, Aktionen direkt an ein Objekt zu verknüpfen. Das heißt, damit wird KI-basierte Automatisierung, sogenannte Decision Automation, möglich.

Eine Vorstellung der Wirksamkeit bekommt man, wenn man zum Einsatz von Palantir durch ICE in den USA recherchiert. Das ist ein wirkmächtiges System. Damit kann auch das umstrittene Predictive Policing ermöglicht werden, das das LAPD genutzt und wieder abgeschafft hat, das Europol teilweise genutzt und auch wieder abgeschafft hat. So ist der Funktionsumfang von KI darin zu verstehen.

Ich will noch kurz zu einer Lösungsmöglichkeit ausführen. Die Lösung ist nicht, Palantir oder eine Alternative zu nutzen, sondern das P20-Datenhaus aufzubauen und mit einer funktionierenden Suchfunktion auszustatten. Das gibt es nämlich - Stand heute - immer noch nicht. Die Ankündigung liegt nun auch schon mehr als zehn Jahre zurück. Dafür wäre es notwendig, dass alle Bundesländer für jeden einzelnen Datenpunkt dann auch die jeweilige Rechtsgrundlage, die Speicherung und Verarbeitung erlaubt, mit abzulegen. Mit einer solchen Kennzeichnung der Daten erreicht man die Zweckbindung. Damit kann man dann eine konforme Softwarelösung bauen, die gäbe es dann mit P20.

Statt also viel Geld in bürgerrechtsverachtende Spionagesoftware aus dem Haus Palantir zu investieren, wäre es daher zielführender, P20 endlich zu priorisieren und umzusetzen, die Kennzeichnung aller polizeilichen Daten vorzunehmen und auf die Zweckbindung zu achten. Das wäre wirklich funktional. Das macht dann nicht Palantir für sich in seiner eigenen Intelligenz - das ist

proprietär und kann man nicht exportieren -, sondern dann hätte die Polizei diese digitale Souveränität in ihrer eigenen Hoheit. - Mehr Details dazu in der Stellungnahme.

Palantir ist, das muss man verstehen, nicht nur eine Software, sondern eine Machtinfrastruktur. Sie mag den Sicherheitsbehörden als effizientes Ermittlungswerkzeug dienen, aber in einem anderen - beispielsweise politischen - Kontext kann sie schnell zum Instrument systematischer Überwachung und Verfolgung werden. Wir sollten aus der Historie gelernt haben, dass das durchaus ein Punkt ist, den man in der Risikoabwägung betrachten muss.

Aktuelle Beispiele aus den USA verdeutlichen, wie datengetriebene Analyseplattformen mit Einsatz von Palantir bei ICE in migrations- und sicherheitspolitischen Kontexten eingesetzt wird. Der Zweck solcher Machtinfrastruktur ist nicht statisch, er verschiebt sich mit politischen Rahmenbedingungen in einem Kontextwechsel. Wer diese Risiken relativiert, verkennt die politische Dimension digitaler Sicherheitsarchitekturen, denn Infrastrukturen für Sicherheit sind immer auch Infrastrukturen für Macht - und Macht verlangt demokratische Kontrolle, bevor sie installiert wird. Und die können wir durch eine solche Struktur der Basis schlicht nicht gewährleisten. Mit P20 wäre das aber möglich.

So viel erst einmal zum Beginn. Ich könnte noch über viele andere Dinge berichten, die hier anders oder interessant diskutiert wurden, gehe jetzt aber gerne auf Ihre Fragen ein.

Abg. **Saskia Buschmann** (CDU): Herzlichen Dank, Herr Atug. Ich bin Polizeibeamtin, und ich bin ein bisschen darüber irritiert, dass Sie sagen, zu jedem Objekt, das in den Datenbanken der Polizei vorliegt, werden auch Dinge wie Tattoos und alles mögliche Weitere gespeichert. Dafür bräuchte die Polizei schon gewisse Rechtsgrundlagen, und die Daten, die bei der Polizei gespeichert sind, sind rechtmäßig erhoben worden. Das heißt, wenn Daten zu Tattoos vorhanden sind, dann wird auch eine andere Rechtsgrundlage als eine einfache lediglich für die Identitätsfeststellung vorgelegen haben. Erst dann wird das auch gespeichert. Ich hätte gerne von Ihnen eine Klarstellung, ob solche Angaben wirklich bei jeder Person vorhanden sind.

Sie haben gesagt, es werde ein digitaler Zwilling der Datenbank der Polizei erstellt. Zeitgleich sprechen Sie aber auch von Data Pipelines, über die quasi die Daten von den einzelnen Datenbanken abgegriffen werden, also zum Beispiel aus einer Einwohnermeldedatei oder aus einer Waffenregisterdatei, wenn man so etwas dort mit einbinden würde - was ja, wie Sie gesagt haben, durchaus möglich ist. Das heißt, die Daten werden dann nicht eins zu eins importiert, sondern sie bestehen weiterhin bei den Stellen, die die Daten rechtmäßig erhoben und gespeichert haben?

Manuel Atug: Auch wenn ich kein Jurist bin: Die Daten in einer Einwohnermeldedatenbank oder in einer der insgesamt 200 bestehenden Polizeidatenbanken und -dateien sind natürlich rechtmäßig erhoben. Für diese Daten gibt es eine Zweckbindung. Der ursprüngliche Sinn und Zweck zum Beispiel einer Sportdatenbank ist, Hooligans zu registrieren, und der einer psychologischen Datenbank ist es, psychologisch auffällige Menschen zu erfassen. Der entscheidende Punkt ist nicht, etwas an diesem Original zu verändern. Diese ursprüngliche Datensammlung ist ja mit der Zweckbindung auf einer entsprechenden Rechtsgrundlage aufgesetzt worden.

Wenn man aber diese Daten über eine Data Pipeline in Palantir integriert und über das ontologische Modell strukturiert, dann werden diese Zweckbindung und Trennung aufgehoben, weil alle Angaben in einem Datentopf zusammengepackt wurden. Ich meine, war der Kollege aus

Frankfurt, der von einem „Datentopf“ sprach, und zwei oder drei Leute in Hessen haben Zugriff auf den gesamten Datentopf. Diese Art von Zugriff ist nicht das, was das Trennungsgebot vorsieht.

Zwar können in einer Software superfeine Rechte- und Rollenmodelle eingebaut werden; alles machbar! Sie können auch sagen, dass die Leute von Palantir niemals an die Daten herankommen. Aber wir haben aus den Aussagen von Edward Snowden, Chelsea Manning und Thomas Drake aus den USA gelernt, dass selbst NSA, CIA und FBI nicht in der Lage waren, ihre Daten vor einer Exfiltration zu schützen. Ich halte es für vermessen, zu sagen, dass das technisch nicht möglich ist. Auf der logischen Ebene gibt es, wenn ein Mensch Zugriff auf die Daten hat, immer einen Weg, diese abzugreifen.

Fairerweise muss ich sagen, dass ich heute neu gelernt habe, dass die Daten über eine Demilitarisierte Zone, also über ein separates System angeliefert und dann in die internen Systeme der Polizei eingespeist werden. Ich bin tatsächlich von einem Offline-Transfer über sogenannte AirGap-Übermittlungen ausgegangen. Auch diese Art von Kommunikationsbeziehungen, die bei Systemen im Internet bestehen, sind natürlich fehleranfällig; denn ein Quellcode ist immer anfällig und kann auch missbraucht werden. Es gibt Sicherheitslücken. Selbst die Abhörschnittstellen - Stichwort „Lawful Interception“ - von Telekommunikationskonzernen in den USA waren nicht hinreichend geschützt, und die Chinesen haben alle Daten abgegriffen. Insofern ist die Problemlage immer vorhanden und darf niemals heruntergespielt werden, nach dem Motto: „Na ja, das ist ja unrealistisch“, oder: „Wir warten auf den GAU, bis dann mal was passiert ist.“ Auch das wurde vorhin in diesem Kontext diskutiert: Gab es jemals Abgriffe? - Nein, gab es nicht. - Na gut, dann können wir weitermachen, bis es knallt! - Das ist, glaube ich, nicht die richtige Strategie.

Die Rechtsgrundlage ist also bei der ursprünglichen Aufnahme von Angaben - zum Beispiel einer Tätowierung - in eine Datenbank vorhanden. Wenn alles in Palantir eingespeist ist, übernimmt dieses System für sich selbst die Aufgabe, in den Data Pipelines diese Rechtsgrundlagen und Zweckbindungen zuzuordnen. Die Polizeibehörden haben dieses Wissen dann aber immer noch nicht. P20 war genau dafür gedacht, dieses Wissen bei den Polizeibehörden in die Datenbanken einzubauen, um die rechtskonforme digitale Verwendung sicherzustellen. Das ist die Kritik daran.

Abg. **Michael Lühmann** (GRÜNE): Vielen Dank, Herr Atug. Ich habe eine grundsätzliche Verständnisfrage. Wir haben in der Anhörung zu der Rechtsgrundlage, die wir überhaupt erst einmal schaffen müssen, gehört: So etwas wie Superdatenbanken möchte die CDU nicht schaffen. Das ist europarechtlich auch gar nicht möglich. Jetzt sagen Sie aber, dass wir hier nicht über Superdatenbanken sprechen, sondern über Ontologie, also eigentlich über etwas noch Heftigeres. Bitte erklären Sie mir das mit der Ontologie näher: Worüber reden wir hier? Wir müssen uns im Klaren darüber sein, was wir schaffen, wenn eine solche Software genutzt werden soll, und wo die Konflikte liegen.

Manuel Atug: Auch beim Einsatz einer Superdatenbank würden die Daten in einem Datenformat abgespeichert, auf die man dann mit verschiedenen Suchanfragen zugreift. Im Gegensatz dazu die Ontologie: Wohl jeder kennt die Wikipedia. In der Wikipedia ist Ontologie implementiert, denn sie weist eine semantische Struktur auf. Das heißt, wenn ein Objekt - ein Wikipedia-Artikel - als Mensch klassifiziert wird, dann kann man auf diese Weise sozusagen alle Menschen aufrufen. Wenn es heißt, dass diese Person aus der Stadt X kommt, dann kann man die Stadt X

aufrufen, und automatisch wird angezeigt, welche bekannten Menschen mit einer Verbindung zur Stadt X im öffentlichen Leben stehen.

Derartige Daten werden nicht händisch in ein System gefriemelt, sondern die Ergebnisse werden durch diese ontologische Struktur automatisch in den entsprechenden Datensätzen angezeigt. Hinter der Wikipedia steht also keine Superdatenbank, sondern es werden Objekte angelegt - zum Beispiel ein Mensch, der Michael Lühmann heißt, eine Person des öffentlichen Lebens ist und bestimmte Merkmale aufweist. An dieses Objekt kann man dann ein Geburtsdatum und alles mögliche Andere heften und auf dieser Grundlage auf Knopfdruck beispielsweise erfahren, wer an diesem Tag oder in diesem Monat oder in diesem Jahr oder *genau* an diesem Tag in diesem Monat in diesem Jahr ebenfalls Geburtstag hat.

Dieses Beziehungsgeflecht und die Struktur der Daten miteinander sind auf einer abstrakten Ebene sozusagen die Metadatenverbindung und die logische Verknüpfung, die Sichtweise auf Daten. Wenn man einfach nur Daten nebeneinanderstelle, kann man zum Beispiel erkennen, dass es dabei oft um Telefone geht. Dann kann man mühselig manuell raussuchen, ob sich diese zum Tatzeitpunkt in der Nähe zu einem bestimmten Ort befanden. Aber mit der Skalierung dieser Ontologie und der Nutzung von Massendaten, die in solchen Systemen genutzt werden - wir reden ja von Petabytes und von rund 15 000 Anfragen pro Jahr; ICE kauft zum Beispiel von Data Brokern Milliarden von Datensätzen -, hat man natürlich eine strukturierte und sehr skalierfähige Massenüberwachungsfunktion für eine Rasterfahndung.

Ein Beispiel: Als Ermittler möchte ich wissen, wo eine bestimmte Telefonnummer überall vorkam. Ich kann sie durch die Decision Automation sogar triggern lassen, indem ich vorgebe: Wenn diese Nummer jemals vorkommt, soll mir das angezeigt werden. Und dann kommt diese Nummer auch zum Vorschein, wenn sie beispielsweise im Rahmen einer Zeugenaussage vorkam, wenn sie im Rahmen einer Quellen-TKÜ oder TKÜ-Überwachung vorkam, wenn sie durch andere Dienste bereitgestellt wird usw. Aber auch alle Beziehungsgeflechte dieser Telefonnummer zu den anderen Nummern sind dann bekannt, weil diese Struktur dann gegeben ist. Außerdem kann ich als Ermittler dann automatisch das Beziehungsgeflecht dieser Nummer zu allen anderen Menschen, Fahrzeugen, Standorten etc. strukturieren; man kann das auch nicht verhindern, man kann ja nur die Rechte beschränken.

Wenn man dann eine KI eingeführt hat, kann man dieses automatisierte System - so wie die ICE in den USA - zusätzlich mit dem Produkt Gaia von Palantir, einer Geolokationsdatenbank, anreichern. Man kann sich auf einer stufenlos zoombaren Karte - einer Weltkarte, einer Karte nur von den USA, oder noch kleinräumiger - den wahrscheinlichen Standort einer Nummer oder einer Person aufgrund der Beziehungsdaten oder der Standortdaten, die man frei im Netz finden oder kaufen kann, anzeigen lassen. Standortdaten ergeben sich beispielsweise oft aus Fotos, wo sie als Metadaten enthalten sind. Wenn man ein Foto mit dem Handy macht, wird meist die Geolokation in das Bild eingespeist.

Es handelt sich also nicht um eine Superdatenbank, sondern um ein Beziehungsgeflecht der Daten. Je mehr Daten man einspeist, desto genauer kann man die Täter finden oder eine Struktur analysieren. Durch diese Grundfunktion steigert Palantir vollautomatisch den Bedarf an Daten: Man fängt also klein an, man braucht dann aber immer mehr. Erst möchte man zusätzlich KI, dann irgendwann Gaia, und dann möchte man vielleicht öffentliche Daten einspeisen, etwa aus Social Media. In den USA werden auch Clearview-Daten - das Unternehmen ist für die Gesichtserkennung bekannt -, also Milliarden von Bildern von Menschen, mit eingespeist. Man

kann dann natürlich auch sehr einfach Videoüberwachungsdaten einspeisen und abfragen, wo eine Person war.

Das heißt: Eine Möglichkeit zur lückenlosen Kontrolle und Massenüberwachung aller Menschen ist strukturiert in diesem System und dieser Ontologie gegeben. Das ist die Machtinfrastruktur, auf die ich mich an dieser Stelle berufe. Dieses System kann man nicht nach dem Motto „Na ja, es wird schon gutgehen!“ beschränken. Ich unterstelle keinem Ermittler und keiner Ermittlerin - um Gottes Willen! -, dass sie im rechtsfreien Raum agieren. Natürlich halten die sich überwiegend an Recht und Ordnung. Es gibt aber auch Einzelne, die es eben nicht tun.

Eine solche missbräuchliche Nutzung sehen wir sehen immer wieder. Hessen wird dazu als Paradebeispiel angeführt. Dort wurden Daten zu Helene Fischer 80-mal abgerufen, obwohl es dafür keine erkennungsdienstliche Behandlung als Grundlage gab. Man konnte leider nicht feststellen, wer das war. Auch über Palantir und andere Systeme wurden schon Abfragen durchgeführt, zu denen es dann hieß: Das können wir nicht genau nachvollziehen, denn die Abfrage lief über einen Shared Account von mehreren Ermittler*innen, und deshalb können wir nicht sagen, wer es war.

Es gab in Hessen aber auch schon Fälle, bei denen die Abfrage auf einen Account zurückverfolgt werden konnte. Aber da hieß es dann: Ich habe leider mein Passwort hier auf dem Post-it neben dem Rechner liegen gehabt, das war dann vielleicht ein Kollege oder Kollegin. - Auch da wusste man nicht, wer es war.

Die ganze Protokollierung bringt also nichts, wenn so etwas nicht *wirklich* unabhängig und permanent sichergestellt wird. Unabhängige Kontrollen wären dann durch LfD & Co. möglich - theoretisch. In der Praxis heißt es aber von den LfD selbst, sie hätten das System nicht analysiert. Teilweise können sie auch nicht genug technische Expertise aufbringen oder haben nicht genug Ressourcen, um eine unabhängige Kontrolle durchführen zu können. In einer solchen Situation muss man dann auf „Hoffentlich geht’s gut!“ vertrauen.

Eine letzte Anmerkung, die auch Hessen betrifft: Wir alle erinnern uns an den rechtsradikalen Terrorakt in Hanau. Auch da hätte ein System wie das von Palantir nicht geholfen. Die angegriffenen Leute haben die Notrufnummer angerufen, aber nur fünf sind durchgekommen. Der Rest hat ein Besetzzeichen gehört. Hinterher kam raus: In Hessen ist die Notrufnummer schon seit Jahren chronisch unterbesetzt. - Schade! Einer der Anrufer wurde dann erschossen; er hatte vergeblich versucht, dort anzurufen.

Auch eine Notrufnummer ist Notfallgefahrenabwehr. Man kann nicht alles mit Software und Technik lösen, sondern man muss auch prüfen, wie man grundsätzlich über solche Strukturen nachdenkt und wie man Defizite abstellt. Das Geld dutzendfach in Millionenhöhe einem Unternehmen zu geben und zu sagen, dass die Zweckbindung, die Struktur, die Abläufe von diesem dann im eigenen System organisiert werden, ist sicherlich nicht die Lösung. Ja, die Daten können exportiert werden - aber wem nützen diese Daten, wenn man die Ontologie und die Zweckbindung nicht kennt? Diese Angaben lassen sich nicht exportieren, sie müssten auf Grundlage von P20 in einem eigenen System aufgebaut werden. Dann hat man eine nachhaltige Lösung, dann ist das System sogar digital souverän, und dann wird auch Vertrauen bei der Bevölkerung in eine vernünftige Digitalisierung der Strafverfolgungsbehörden aufgebaut.

Bodo Koch: Herr Atug, ich würde gerne ein paar Punkte klarstellen.

Erstens. Den schrecklichen Anschlag in Hanau in diesen Zusammenhang zu stellen, halte ich nicht für fair und gut.

Zweitens. Das ist keine Rasterfahndung. Vielmehr - das ist im Grunde auch gesagt worden - handelt es sich um eine eigene Norm in den entsprechenden Gesetzen. Somit kann man diese Behauptung einfach nicht aufstellen.

Drittens. Die Rechtsgrundlage, über die jetzt hier diskutiert wird und die der in Hessen zumindest ähnelt, sieht nach unserem Verständnis ja gerade vor, dass verschiedene Datenquellen miteinander in Bezug gesetzt werden. Deswegen finde ich Ihre Aussagen einfach nicht klar genug, sondern es ist ja gerade die Idee, eine automatisierte Datenanalyse über verschiedene Datentöpfe hinweg zu ermöglichen. Solche Auswertungen zu ermöglichen, wird, glaube ich, auch hier sehr grundsätzlich diskutiert.

Viertens. Das Thema Vollautomatik gibt es bei uns nicht, sondern es stellt sich immer die Frage, was entsprechend wie abgerufen wird.

Fünftens. Zur Klarstellung: In das System sollen nur Daten einfließen, die rechtmäßig nach den Landesgesetzen - auch nach dem, was jetzt hier ausgehandelt wird - erfasst worden sind. Das kann man nicht auf die Software beziehen, sondern wir haben in Hessen in der Software das umgesetzt, was wir rechtlich dürfen, was in § 25 a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung steht und was uns das Bundesverfassungsgericht mitgegeben hat. Somit ist das rechtskonform, und ich bitte darum, dass das auch als rechtskonform angesehen wird.

Manuel Atug: Ich hatte eingangs erklärt, dass ich kein Jurist bin und auch keine juristische Bewertung abgebe. Wenn ich sage, dass ein System technisch eine „Rasterfahndung by Design and Default“ ist, dann beziehe ich mich als Sachverständiger im technischen Bereich auf die technische Grundfunktion und möchte hier keine rechtliche Bewertung abgeben. Das hatte ich nicht vor. Sie können das rechtlich dekorieren, wie Sie wollen - technisch bleibt es das, was es ist.

Dieselbe Diskussion gibt es zu Staatstrojanern. Dazu heißt es, dass diese Software auf ein Handy zugreift, aber sie darf dann nicht auf eine beliebige vergangene Kommunikation zugreifen, sondern nur auf die Teile der Kommunikation, für die das von der Rechtsprechung zugelassen ist. Dazu weisen wir darauf hin, dass das technisch nicht möglich ist: Entweder hat man Zugriff auf die Kommunikation - und damit auch auf die Historie -, oder man hat ihn nicht. Es wird also eine rechtliche Unterscheidung vorgenommen, die technisch gar nicht möglich ist, die einfach, wenn man sich das unter technischen Aspekten anguckt, Quatsch ist. Mit diesem technischen Defizit in der realen Rechtsprechung leben wir. - Das besteht nun einmal auch in der Rasterfahndung.

Zum Thema „vollautomatisch“: Ich habe nicht behauptet, dass die Vollautomatisierung in Deutschland schon vorhanden ist - aber beispielsweise in Israel. Dort hat man schon vor Jahren mit Lavender eine KI-automatisierte Erkennung von Targets - also das, was Palantir auch immer bewirbt: Target Detection und AI Kill Chain - erreicht. In Israel hieß es, man könne ohne KI 50 „Terroristen“ pro Tag ermitteln, mit KI und Automatisierung seien es aber 5 500 pro Tag. Allerdings hat man dabei unterschlagen, dass man damit einen Kollateralschaden von bis zu 23 Unschuldigen pro erwischtem „Terroristen“ in Kauf nimmt, was völkerrechtlich zumindest schwer bedenklich ist. Aber das scheint Netanyahu nicht zu interessieren; er hat ja auch ein Aushungern der Bevölkerung zugelassen, was völkerrechtlich auch nicht legal ist.

(Zuruf: Bleiben Sie bitte sachlich!)

- Ich versuche, sachlich zu erklären, warum eine Vollautomatisierung in Palantir möglich ist und was man damit nach einem politischen Kontextwechsel alles machen kann.

Sie sagen, dass es keine Vollautomatisierung gibt. Sie müssten aber eigentlich sagen, dass es sie *noch* nicht gibt. Den politischen Kontextwechsel hat es vielleicht auch noch nicht gegeben. Aber wenn es irgendwann vielleicht beides gibt - und wir reden schon vom nächsten Schritt, nämlich der Einführung von KI bei Palantir -, dann sehen wir eine Entwicklung in eine Richtung. Davor wollen wir rechtzeitig warnen. Die Frage ist: Wie gehen wir damit um?

Wir haben dafür mit P20 eine Lösung. Sie klingt langweilig und doof. Es gibt Fähigkeitslücken, das stimmt. Es gäbe auch erhebliche Defizite, wenn man Parallelisierung einführt, weil man inzwischen so sehr von Palantir und dieser Fähigkeitslückenfüllung abhängig ist. Das macht die Situation - wie in einem Abwärtsstrudel - einfach immer nur schlimmer. Wir versuchen einfach nur, davor zu warnen, weil wir sagen: Kritische Infrastruktur ist schützenswert, die Daseinsvorsorge und auch die Sicherheit der Bevölkerung sind wichtig. Es gibt den Kritis-Sektor Staat und Verwaltung, wozu auch die Gefahrenabwehr gehört. Wir sehen die Risiken, dass das zukünftig nicht gewährleistet wird, wenn diese Kontextwechsel oder Problemlagen eintreten. Wir möchten auch nicht überspitzen oder was auch immer, sondern das sind bereits existierende Fakten. Darüber müssen wir reden dürfen.

Abg. **Birgit Butter** (CDU): Vielen Dank, Frau Vorsitzende, dass Sie Herrn Koch noch einmal haben zu Wort kommen lassen. Denn hinter mir regte sich schon Widerspruch zu den Ausführungen von Herrn Atug.

Herr Atug, Sie haben Ihren Beitrag mit Hinweisen auf „Fake News“ und „Anekdoten“ angefangen und gesagt, dass es die Erfolge möglicherweise nicht gibt. Ihre Stellungnahme enthält Stichworte wie „Scheinbehauptung“, „Mysterium“ und „bürgerrechtsverachtende Spionagesoftware“. Ich glaube, da sollte man ein bisschen abrüsten und sachlich werden.

Gerade zu P20 habe ich eben dem Polizeivizepräsidenten Koch die Frage gestellt, wie der Stand der Dinge ist und ob das wirklich eine greifbare Lösung ist. Ich habe Ihre Stellungnahme gelesen und deswegen den Ball nach Hessen gespielt und gefragt, was P20 ist und wie weit P20 ist. Das hilft uns insofern nicht weiter.

Sie haben angemerkt, dass hier Palantir mit am Tisch sitzt. Rot-Grün, wir alle hätten die Möglichkeit gehabt, zu sagen, wen wir noch hätten einladen sollen. Aber bis jetzt habe ich noch von keinem Experten gehört, dass es einen anderen Anbieter gäbe, der so weit ist wie Palantir und den wir hier hätten einladen können.

Vors. Abg. **Doris Schröder-Köpf** (SPD): Grundsätzlich ist es bei der Benennung von Anzuhörenden so, dass jede Fraktion ihre Vorschläge unterbreitet. Es ist jeder Seite unbenommen, ihre Vorschläge zu machen. Herr Atug gilt als Experte. Ich selber kann es nicht beurteilen. Ich glaube jetzt einfach mal, was ich da lese. Ich kann es aber auf keiner Seite im Kern beurteilen. Wir respektieren und honorieren also, dass Sie hier sind und sich so lange geduldet haben.

Abg. **Saskia Buschmann** (CDU): Ich habe eine ganz einfache Frage, die Sie mit Ja oder Nein beantworten können. Wenn ich Sie richtig verstanden habe, sehen Sie die Lösung zur Schließung der Fähigkeitslücke lediglich im P20-Datenhaus und nicht in irgendeiner externen Software - ob sie jetzt Palantir oder wie auch immer heißt -? Für Sie gibt es also lediglich die Lösung P20?

Manuel Atug: Wenn wir digitale Strafverfolgung verfassungskonform, nachhaltig und digital korrekt umsetzen wollen, ja.

Abg. **Alexander Saade** (SPD): Herr Atug, vielen Dank für Ihre Ausführungen; ich halte es durchaus für wichtig, dass man in diesem Kontext skizziert, was alles möglich ist. Ich glaube, das ist wirklich wahnsinnig wichtig.

Meine Frage geht aber in eine andere Richtung, nämlich auch in die Richtung P20-Datenhaus. Welche Ressourcen sind Ihrer Meinung als IT-Experte nach notwendig? Wie schnell könnte man ein wirklich tragfähiges, funktionierendes System auf Bundesebene umsetzen? Welche politischen Vorarbeiten wären dazu vielleicht auch notwendig?

Manuel Atug: Ich mache es kurz: Man braucht den politischen Willen.

Abg. **Michael Lühmann** (GRÜNE): Ja, der politische Wille war lange nicht gegeben, und das bedauern wir. Die dadurch entstandene Lücke ist dann durch Palantir gefüllt worden, weil im Bund offenkundig kein Konsens bestand, am P20-Datenhaus weiterzubauen.

Sie sagten, es gibt in diesem Konzept noch ein paar Fähigkeitslücken. Wie kann man diese schließen? Wo liegt da die Herausforderung? Auch das sollten wir ein bisschen mitdenken: Wie bekommt man das, was noch fehlt, eingewoben? Gibt es auch dafür Möglichkeiten? Oder sollte man Schritt für Schritt anfangen und dann gucken, wie man das auflöst?

Manuel Atug: Da ist es wohl zu einem Missverständnis gekommen. Ich wollte nicht sagen, dass es in P20 Fähigkeitslücken gibt. Vielmehr ist P20 aktuell überhaupt nicht so aufgebaut, dass man es nutzen kann. Die - mit Verlaub - popelige Suchfunktion, die da irgendwie implementiert ist, kann man keinem Ermittler und keiner Ermittlerin antun. Das bringt nichts. Das ist ineffizient und führt zu gar nichts.

Was man braucht, ist der politische Wille, P20 wirklich zu einem Datenhaus aufzubauen und darin dann die Daten zu kennzeichnen und auf diese Weise die Rechtskonformität sozusagen anzuflanschen, sodass die Zweckbindung sozusagen eigenständig realisieren werden kann. Dann steht auch ein gemeinsames Datenformat zur Verfügung, und dann kann man auch auf die Daten anderer Bundesländer zugreifen; die Kooperation mit zwei anderen Bundesländern wurde vorhin angesprochen.

Noch einmal: Uns geht es nicht darum, die Digitalisierung der Polizeibehörden zu verhindern. Wir als AG KRITIS begrüßen das explizit. Allerdings hätten wir gern eine sinnvolle Digitalisierung. Wenn die Fähigkeiten in fremde Hände gegeben werden, die erlösmaximiert getrieben sind und vielleicht auch andere Machtverhältnisse anders missbrauchen können, ist das aber nicht sinnvoll. Und das hatten wir nun mal mit IBM/Hollerith-Maschinen. Das hatten wir mit einer Datenbank mit Daten zu allen - fast eine Million - Juden in den Niederlanden, die so geschützt werden sollten. Aber die Nazis haben Zugriff auf diese Daten bekommen. Dann war diese Datenbank die Todesliste, die abgearbeitet wurde. Das sind aus der Vergangenheit bekannte konkrete Kontextwechsel, die kein Palantir, kein Zugriffsrecht und nichts Sonstiges verhindern können.

Was wir aber machen können, ist, in P20 eine Suchfunktion einzubauen, so wie es ursprünglich gedacht war. Dann kann man diese Daten sinnvoll und rechtskonform verarbeiten - und das mit Effizienz, sodass Ermittler*innen nicht leiden, wenn sie ein System benutzen, und nicht irgendwie den süßen Nektar einer verbotenen Frucht „Palantir“ nutzen. Vielmehr können sie mit einem solchen sinnvollen digitalen Konstrukt wirklich arbeiten, und zwar verfassungskonform und mit dem Vertrauen der Bevölkerung. Mehr wollen wir gar nicht.

Gesellschaft für Informatik e. V.

Schriftliche Stellungnahme: Vorlage 3

Anwesend:

- Dr. Aleksandra Sowa, Präsidiumsmitglied

Dr. Aleksandra Sowa: Ich bedanke mich für die Einladung als Sachverständige und nehme zu dem Antrag der Fraktion der CDU vom September 2025 wie folgt Stellung:

Ich teile die Sorge vor negativen Auswirkungen, die unvollständige oder lückenhafte Ergebnisse aus Datenrecherchen und -analysen mit herkömmlichen Mitteln haben können, wenn es darum geht, Gefährdungslagen frühzeitig zu erkennen oder Straftaten, etwa Kinderpornografie, Cyberangriffe oder Terroranschläge, zu verhindern. Ebenso ist zu begrüßen, dass Regierungen, Regulierungsbehörden oder Parlamente - nationale wie auch regionale - Zeit und Ressourcen in den Schutz und die Sicherheit der Bürgerinnen und Bürger investieren.

Daher möchte ich zuerst Bezug auf die Digitalpolitik der deutschen Bundesregierung nehmen und noch einmal das Stichwort aufgreifen, das heute in der Diskussion schon ein paar Mal gefallen ist, konkret zum Umgang mit dem Thema digitale Souveränität, das mir im Kontext genau dieses Antrags sehr relevant erscheint. Im Koalitionsvertrag zwischen CDU, CSU und SPD heißt es: „Unsere Digitalpolitik ist ausgerichtet auf Souveränität, Innovation und gesellschaftlichen Fortschritt.“ Und weiter: „Digitalpolitik ist Machtpolitik.“ Dieser Satz insinuiert auch, dass mit der Digitalpolitik Machtbissbrauch möglich ist.

Die Bundesregierung setzt bei der digitalen Souveränität auf das Prinzip „Wirtschaft first“. Der Staat soll zum Ankerkunden für die digitale Wirtschaft werden und vorrangig private IT-Dienstleister zur Stärkung der digitalen Souveränität nutzen. Das betrifft insbesondere auch den Verteidigungs- und Sicherheitsbereich. Dies führe ich aus, um die allgemeinen Rahmenbedingungen für den Einsatz von Systemen zu verfahrensübergreifenden Datenanalysen oder ganz einfach zum Einsatz von Analysesoftware im Rahmen von Gefahrenabwehr und Straftatenverhütung durch die Polizei in Deutschland zu skizzieren.

Angesichts dieser klaren Zielsetzung auf der Bundesebene stellt sich die Frage, ob den Vorgaben des vorliegenden Antrags durch den Einsatz von Palantir-basierten Systemen entsprochen werden kann. Lassen Sie mich bitte erklären,

- warum ich der Auffassung bin, dass dem nicht so ist,
- was gegen den Einsatz spricht und

- was notwendig wäre, um vergleichbare digitale souveräne Lösungen künftig überhaupt in Betracht zu ziehen.

Ich möchte meine Ergänzungen entlang folgender vier Fragen strukturieren. Sie werden auch hören, dass diese an einigen Stellen mit den Empfehlungen des Landesdatenschutzbeauftragten harmonieren.

Erste Frage: Sind verfahrensübergreifende Datenanalysen in Echtzeit, gegebenenfalls unter Einsatz von KI, tatsächlich wirksamer oder effizienter als herkömmliche Verfahren?

Um diese Frage zu beantworten, ist es essenziell, zu konkretisieren, was mit schweren Straftaten, die verhindert werden sollen, gemeint ist. Die Bereiche, in denen die Polizei in Deutschland Palantir- bzw. Gotham-basierte Systeme einsetzen soll, sind bislang nicht hinreichend klar definiert.

So wurde diese Analysesoftware zum Beispiel in Hessen anfangs nicht nur bei schwerer oder organisierter Kriminalität und bei Terrorismus eingesetzt, sondern auch zur Aufklärung von Einbrüchen. Heute haben wir außerdem gehört, dass sie auch zur Aufklärung von Geldautomatensprengungen eingesetzt wurde. Dafür werden sogar die Daten von Unfallzeugen ausgewertet, wie mein Kollege Manuel Atug gerade erläutert hat. In Bayern wird VeRA offenbar nicht nur bei schweren Verbrechen eingesetzt.

Daher lautet meine Empfehlung, direkt im Gesetz ausdrücklich und präzise zu definieren, bei welchen schweren Straftaten diese Analysesoftware eingesetzt werden darf. Zudem bedarf es klarer technisch-organisatorischer Kontrollen - nicht nur demokratischer, sondern tatsächlich gelebter Kontrollen -, um sicherzustellen, dass der Einsatz tatsächlich auf diese schweren Straftaten beschränkt bleibt, verbunden mit einer wirksamen Aufsicht für diesen Bereich - im Sinne des Dürrenmatt‘schen Satzes: „Die Herrschenden müssen überwacht werden, nicht die Beherrschten.“

Zweite Frage: Welchen messbaren Nutzen und welche Risiken sind mit dem Einsatz spezifischer Technologien wie Palantir bzw. Gotham verbunden?

Ein effektives Monitoring ist zwingend geboten, um die Zweckmäßigkeit, Ordnungsmäßigkeit und Wirksamkeit des Einsatzes einer verfahrensübergreifenden Recherche- und Analysesoftware zu prüfen. Dieses sollte eine vorgelagerte Analyse zur Notwendigkeit, Wirksamkeit und Effizienz der bestehenden Befugnisse - nicht nur auf den Einsatz von bisherigen Technologien beschränkt - umfassen und auf einer gesetzlich verankerten Evaluierungspflicht basieren. So wurde zum Beispiel kürzlich der Mangel an einer solchen Evaluation vom Bundesrechnungshof im Zusammenhang mit der Umsetzung der Cybersicherheitsstrategie des Bundes moniert. Prüfer kritisierten in ihrem Bericht unter anderem die fehlende Erfassung des Ist-Zustandes, was aus ihrer Sicht als Ausgangspunkt für eine klare Definition des zu erreichenden Soll-Zustandes notwendig sei. Dadurch seien eine operative wie strategische Steuerung und Kontrolle nicht möglich, sagten die Prüfer. Die Evaluierung muss insbesondere die Effizienz und Effektivität des Gesetzes überprüfen und auf vorab definierten, messbaren Kriterien beruhen.

In Würdigung der Empfehlung des Bundesrechnungshofes zur Cybersicherheit lautet daher meine Empfehlung: Verankerung einer verpflichtenden Evaluierung im Gesetz zum Zwecke eines strategischen und operativen fortlaufenden Controllings - Stichwort „Continuous Auditing“ - der Zielerreichung. Ergänzend sollte eine Analyse zur Wirksamkeit bisheriger Ermittlungsinstru-

mente sowie der bestehenden Befugnisse der Sicherheitsbehörden - die Ist-Erhebung, ob diese überhaupt schon genutzt und vollumfänglich eingesetzt werden - erfolgen, um eine präzise Zieldefinition zu ermöglichen. Das Ziel einer solchen Maßnahme, um es mit Montesquieu auszudrücken: „Wenn es nicht notwendig ist, ein Gesetz zu machen, dann ist es notwendig, kein Gesetz zu machen."

Dritte Frage: Welche Alternativen bestehen, und wie fällt deren jeweilige Nutzen-Risiko-Bilanz aus? Denn im Antrag wird von „alternativlos" gesprochen. Zusatzfrage: Gibt es andere Technologien, Methoden oder Systeme, die das angestrebte Ziel erreichen oder das Problem eventuell sogar besser adressieren, ohne dass diese massive Eingriffe in die Freiheiten und Grundrechte der Bürgerinnen und Bürger bedeuten?

Tatsächlich waren leistungsfähige Datenanalysen bereits im analogen Raum möglich und dank der Entwicklung statistischer Methoden zur Identifikation von Abweichungen oder Unregelmäßigkeiten effektiv praktisch einsetzbar, etwa im Bereich der analytischen Forensik, der Wirtschaftsprüfung, der internen Revision sowie bei der Bekämpfung von Wirtschaftskriminalität oder White-Collar Crime. Die IT hat manuelle Auswertungen erheblich beschleunigt, erleichtert und systematisiert, etwa durch den Einsatz regelbasierter Revisionssoftware. Ein Beispiel ist die Analyse großer Zahlenreihen im Transaktionsbereich zur Identifikation von Auffälligkeiten, Abweichungen und Unregelmäßigkeiten, die Hinweise auf mögliche Manipulationen liefern können. Diese Methode basiert auf dem Benfordschen Gesetz.

Ich führe ein Beispiel aus dem Bereich der forensischen Analyse an, weil wir dort vier verfahrensbasierte IT-Systeme und Softwareverfahren etabliert haben und weiterentwickeln, um mit Prüfungen oder durch Tests ihre Funktionalität, Sicherheit und die Einhaltung der geltenden Normen und Gesetze - auch des Datenschutzes - zu gewährleisten. Ab dem Jahr 2027 greifen darüber hinaus in Deutschland Vorgaben aus dem europäischen Cyber Resilience Act, die „Security by Design" zum verpflichtenden Element von Produkten und Systemen bzw. in der Softwareentwicklung machen. Zur Definition und Operationalisierung eines gemeinsamen Privacy-and-Security-by-Design-Verfahrens tragen wir als Fachgruppe PET (Privacy Enhancing Technologies) bei der Gesellschaft für Informatik bei. Das BSI ist federführend verantwortlich als Aufsichtsbehörde.

„Der menschlichen Kunst der Täuschung sind Grenzen gezogen", pflegte Sherlock Holmes zu sagen. Bei einer Analysesoftware wie Palantir verhält es sich anders. Es besteht erhebliche Unklarheit darüber, wie sie konkret funktioniert, welche Verarbeitungsschritte sie vornimmt und welche Datenbestände in welcher Form einbezogen werden. Teilweise entsteht auch der Eindruck, dass selbst Hersteller und Entwickler die Funktionsweise des Systems nicht vollständig transparent darlegen können oder wollen. Hinzu kommt, dass erprobte Methoden zur Prüfung oder zum Testen von KI-Systemen erst konzipiert und entwickelt werden müssen.

Daher lautet meine Empfehlung, im Rahmen einer Studie den Einsatz bestehender Software und Systeme zu erproben bzw. die Entwicklung einer solchen, basierend auf validierten wissenschaftlichen Methoden zur Aufdeckung von Abweichungen oder Unregelmäßigkeiten, zu fördern. Außerdem sollten eine Zentralisierung der Datenerfassung, eine unverschlüsselte oder nicht anonymisierte Datenhaltung, die Weitergabe von Daten an Dritte ohne klare Zweckbindung sowie die Einräumung von Zugriffsrechten an Dritte explizit ausgeschlossen werden.

Zuletzt die vierte Frage: Welche potenziellen Schäden für Sicherheit, Privatsphäre und demokratische Rechte könnten entstehen?

Befugnisse für Sicherheitsbehörden, die mit gravierenden Eingriffen in Freiheitsrechte und Grundrechte der Bürgerinnen und Bürger verbunden sind, erfordern zugleich flankierende Maßnahmen zum Schutz dieser Rechte. Hierzu zählen insbesondere - in Europa ist das der Schwerpunkt - informationelle Selbstbestimmung und - in den USA - der Schutz vor unrechtmäßiger Überwachung zum Beispiel durch den Staat. Die mit erweiterten Analyse- und Überwachungsbefugnissen einhergehenden Machtasymmetrien auszugleichen, ist Pflicht des Staates.

Wie eine solche Balance gelingen kann, zeigen die Strategien der US-Regierung zu Privacy Enhancing Technologies und ihrer Erforschung. Gerade in den vergangenen Jahren wurden zwei derartige Strategien novelliert, aktualisiert, neu aufgelegt, so die National Privacy Research Strategy, mit der das Ziel verfolgt wird, strategische Prioritäten für die Datenschutzforschung festzulegen, und zwar sowohl für staatlich finanzierte als auch für industriegetriebene Forschung. Die gezielte Förderung von PET eröffnet die Möglichkeit, datenbasierte Technologien einschließlich künstlicher Intelligenz nutzbar zu machen, ohne dabei den Schutz der Privatsphäre strukturell zu schwächen.

So ergibt sich auch die Empfehlung: Angesichts des erheblichen Überwachungspotenzials, das mit automatisierter Datenanalyse einhergeht, besteht auch in Deutschland und Europa dringender Handlungsbedarf, Forschung und Entwicklung im Bereich PET - dazu gehören neben Pseudonymisierung und Anonymisierung auch Verschlüsselung, Kryptografie - strategisch zu stärken, und zwar entsprechend der im Koalitionsvertrag formulierten Zielsetzung: „Wir fördern die breite Anwendung von Privacy Enhancing Technologies.“

Mein Fazit: Unter technischen IT-Gesichtspunkten werden die im Antrag unterbreiteten Vorschläge den in sie gesetzten Hoffnungen und Erwartungen noch nicht gerecht. Das erklärte Ziel größerer Cyber- und IT-Sicherheit wird durch eine US-amerikanische Entwicklung nicht gewährleistet. Aus gutem Grund hat daher die gewiss nicht der Zurückhaltung bei der Kriminalitätsbekämpfung verdächtige Schweiz Palantir eine eindeutige Absage erteilt, denn den Eidgenossen von Politik bis Polizei und Armee sind nach Medienberichten die Risiken des Einsatzes zu groß. Eventuell wäre daher vor weiteren Entscheidungen eine parlamentarische Reise in die Alpenrepublik empfehlenswert.

An dieser Stelle verweise ich für weitere Details auf meine schriftliche Stellungnahme und bedanke mich für Ihre Aufmerksamkeit. Ich freue mich auf Ihre Fragen, natürlich auch im Nachgang zu dieser Anhörung, wenn die Zeit jetzt nicht ausreicht.

Abg. **Birgit Butter** (CDU): Frau Dr. Sowa, herzlichen Dank für Ihren Vortrag.

Sie haben mehrfach das Stichwort „Cybersicherheit“ angesprochen. Ich möchte außerdem den Hinweis auf die erheblichen Kosten für die Software - es war von 25 Millionen Euro die Rede - aufgreifen. Das Innenministerium hat im Januar 30 Millionen Euro für das Schutzschirmprojekt Aegis zur Abwehr von Cyberbedrohungen in die Hand genommen, das ein KI- und - im Gegensatz zu Palantir - Cloud-gestütztes Verfahren ist. Auch diese Anwendung stammt von einem US-amerikanischen Unternehmen, nämlich Palo Alto Networks. Es soll in Land, Hochschulen und Kommunen genutzt werden, also in jedem kleinsten Teil unseres Landes.

Das Innenministerium hat in diesem Zusammenhang auch zur Frage der digitalen Souveränität Stellung genommen: Diese habe in Ermangelung europäischer Alternativen durch die Anbieterqualität ihre Grenzen. Deswegen habe sich das Land für das weltweit führende Firewall-Anbieterunternehmen aus Kalifornien entschieden.

Auch bei diesem Projekt können Daten aus dem Landesnetz ins Ausland abfließen, zum Beispiel in die Analysecloud von Palo Alto Networks. Wird da nicht eine gewisse Doppelmoral sichtbar? Die eine Software kann eingesetzt werden - auch für viel Geld - und die andere nicht?

Dr. Aleksandra Sowa: Vielen Dank für diese Frage, die etwas anspricht, was durchaus bezeichnend ist. Während wir hier über Ihren Antrag und auch über die Modernisierung des Polizeigesetzes in Niedersachsen diskutieren, arbeiten wir von der Gesellschaft für Informatik an einer Stellungnahme zum Entwurf eines neuen Cyberabwehrgesetzes. Dazu waren wir in der vergangenen Woche neben zehn anderen Organisationen und Institutionen gefragt worden, welche Probleme, welche Kritik oder welche zu lobenden Punkte bei diesem Gesetzentwurf gesehen werden. Dabei handelt es sich um ein Artikelgesetz, das sowohl das BSI- als auch das BKA-Gesetz betrifft; ich glaube, auch das Verfassungsschutzgesetz, aber da bin ich mir nicht sicher. Dabei wird gerade über die Erweiterung von Befugnissen diskutiert, die genau solche Beauftragungen ermöglichen sollen, während diese Aufträge bereits vergeben werden. Das ist eine auch für uns sehr schwierige Situation, weil wir oft vor praktisch schon vollendete Tatsachen gestellt werden.

Das gleiche Thema, das Sie gerade genannt haben - Cybersicherheit mit einem Firewall-System -, haben wir auch mit Microsoft; denn Landesregierungen beauftragen US-amerikanische Unternehmen oder nutzen die Cloud-Lösungen US-amerikanischer Tech-Unternehmen.

Ich verstehe, dass es im Moment keine Alternativen gibt. Ich verstehe auch, dass Europa mit dem Versuch, Systeme wie eine Cloud-Lösung unter Gaia-X auf die Beine zu stellen, nicht erfolgreich war. Die Frage ist, warum wir nicht erfolgreich waren. Können wir das nicht besser machen? Können wir das genauso, wie es uns die US-Amerikaner zeigen, aber in Bezug auf unsere eigene Bevölkerung? Wir dürfen uns nicht darauf verlassen, dass zum Beispiel neue Forschungen und die Entwicklung von Schutzmaßnahmen den Bürgerinnen und Bürgern angesichts dieser neuen Systeme mehr Rechte verschaffen. Wir dürfen uns nicht täuschen, dass die Forschungsprogramme der USA auf ihre eigenen Bürger abzielen und nicht zum Beispiel auf Bürger in Europa oder in Deutschland. Deshalb müssen wir zum Ausgleich noch unsere eigenen Schutzmaßnahmen finden.

In der Forschungsstrategie gerade zu PET, aus der ich zitiert habe, steht auch ein sehr markanter Satz. Den sollte man sich vielleicht vor Augen halten, um sich klarzumachen, dass wir derzeit gar nicht so schlecht aufgestellt sind, wie wir manchmal vermuten, wenn man die Forschung nicht genau verfolgt. Dort heißt es, dass sich die USA der Tatsache bewusst sind, dass die Forschung im Bereich Kryptografie hauptsächlich außerhalb der USA stattfindet.

Die Wissenschaft und die Forschung sind in Deutschland weiter, was die Möglichkeiten des Einsatzes von Schutzmaßnahmen für Bürgerinnen und Bürger angeht, um ihre Daten anonym zu halten, gerade bei solchen Auswertungen oder wenn sie zum Beispiel unverschlüsselt in einer Cloud liegen. Eigentlich sollte es uns möglich sein, so etwas zu verhindern. Das wäre ein erster Schritt. Wir sind ziemlich weit fortgeschritten.

Die Frage ist nur: Können gerade die Regierungen und die Parlamente diese Forschung so weit unterstützen, dass sie zu Produkten führt, die dann den Bürgerinnen und Bürgern tatsächlich zur Verfügung stehen? Dabei geht es zum Beispiel um eine Ende-zu-Ende-Verschlüsselung für jeden, ohne dass man sich zum Beispiel identifizieren muss, um eine Anonymisierung oder sogar um die anonyme Nutzung bestimmter Dienste. Können Regierungen und Parlamente das ermöglichen? So könnte eine gewisse Balance hergestellt werden.

Aber ich gebe Ihnen recht: Im Moment werden wir mit Entscheidungen zugunsten US-amerikanischer Firmen überschüttet, und die Frage ist, wie man darauf reagieren kann. Langfristig wären tatsächliche digitale Souveränität und auch Forschung und Entwicklung meine Antwort.

Abg. **Michael Lühmann** (GRÜNE): Vielen Dank, Frau Dr. Sowa. Ich habe eine konkrete Nachfrage zu dem Komplex der PET einerseits und der Möglichkeit andererseits, vorhandene Daten doch irgendwie vergleichen zu können, indem man eine Art von Rauschen darüberlegt, sodass man eben nicht alles komplett zuordnen kann. Auf diese Weise könnte der datenschutzrechtlichen Problematik vielleicht begegnet werden.

Wir sehen durchaus die Notwendigkeit, dass man Daten zu gewissen Zwecken zusammenführen und ansehen können muss, weil die Polizei die bekannten Herausforderungen hat. Wir sehen gleichzeitig, dass man zum Beispiel zum Training von KI-Modellen Daten benötigt. In diesem Bereich wird intensiv diskutiert, wie man bei personenbezogenen Daten vorgeht; sie müssten eigentlich anonymisiert oder pseudonymisiert werden. Dazu kommt aber immer wieder der Hinweis, das sei ein unverhältnismäßig großer Aufwand, und deswegen könne man das dann doch nicht machen. Meine Frage: Was ist in diesem Bereich möglich? Ich meine - ich bin Laie - dazu das Stichwort „Rauschen“ gelesen zu haben. Vielleich können Sie erläutern, was das bedeutet, was möglich ist und welche Herausforderungen dabei noch bestehen.

Dr. Aleksandra Sowa: Sie sprechen Differential Privacy an, zu der in Deutschland sehr intensiv geforscht wird. Bislang hat diese Methode Rechenkapazitäten sehr stark beansprucht, weshalb sie nur sehr selten Anwendung fand. Gerade auf mobilen Geräten liefen diese Verfahren nicht gerade schnell.

Mittlerweile besteht das Problem, dass die Rechenkapazitäten dafür nicht ausreichen, immer weniger. Bei der Forschung zu Differential Privacy liegt Deutschland - auch zum Beispiel in Göttingen wird dazu geforscht - ziemlich weit vorn. Interessant ist, wie die Firmen damit umgehen. In den USA gibt es einen sehr starken Bereich der industriegetriebenen Forschung. Mit den gleichen Methoden, mit denen sich Bürgerinnen und Bürger zum Beispiel vor Übergriffen oder einem Überinteresse des Staates oder von Wirtschaftsunternehmen schützen können, schützen zum Beispiel Unternehmen wie Apple die Kundendaten. Dieses Unternehmen hat sich sehr früh dafür entschieden, Differential Privacy einzusetzen, um die Kundendaten für den Fall zu schützen, dass zum Beispiel die US-Regierung oder eine der Institutionen Einblick in die Daten der Kunden nehmen möchte. Dort hatte man also entschieden, dass die hardwareseitige Verschlüsselung nicht ausreicht; denn sie kann offenbar gebrochen werden. Die Frage war also: Welches Instrument können wir unseren Kunden an die Hand geben, das verhindert, dass ihre Daten ausgelesen werden?

Dieses Verfahren anonymisiert die Daten. Das bedeutet, wir nutzen sowohl die Hardware als auch die Software nicht anonym, sondern geben unsere Daten, und diese werden dann später anonymisiert, sprich: durch dieses Verfahren unkenntlich gemacht. Das ist eine Art von Schutz,

durch den es vielen Institutionen - auch der Polizei usw. - nicht möglich ist, auf die Originaldaten zuzugreifen.

Eine zweite Firma, die gerade an diesem Verfahren forscht, ist Google in Deutschland. Wir werden in der nächsten Zeit einen PET-Talk organisieren, eine Austauschveranstaltung, um sich online aus erster Hard über neue Entwicklungen, gerade zu PET, informieren zu können. Wir stehen in Kontakt mit Google, damit sie uns aus Hamburg ihre Methode vorstellen. In den USA ist das offenbar schon längere Zeit im Gespräch. Aber auch in Deutschland nimmt man den Schutz der personenbezogenen, aber auch aller anderen sensitiven Daten sehr ernst. Und Google als Cloud-Betreiber kann diese Verfahren dann nicht nur für mobile Verfahren bzw. Geräte, sondern auch bei vielen anderen Lösungen anbieten. Ob man dafür bezahlen muss, werden wir abwarten müssen, ebenso bezüglich der Frage, wie gut und schnell das funktioniert.

Ob es Privacy dann nur für diejenigen gibt, die es sich leisten können, ist ein anderes Thema. Es handelt sich um privatwirtschaftliche Unternehmen. Wir dürfen also nicht erwarten, dass das alles einfach so für jeden verfügbar sein wird. Deshalb ist die Rolle des Staates, der Parlamente und auch der Forschung so wichtig, damit diese Verfahren gestützt und dann vielleicht später auch in der breiten Masse verfügbar sind.

Abg. **Nadja Weippert** (GRÜNE): Vielen Dank, Frau Dr. Sowa. Die Diskussion lief nun in unterschiedliche Richtungen. Das eine ist die Datenanalysesoftware, das andere der Abwehrschirm. Ich möchte das einmal einordnen.

Die erste Firewall mit einer benutzerfreundlichen Oberfläche, die überhaupt entwickelt worden ist, stammt von gateProtect in Buchholz in der Nordheide. Dieses Unternehmen war Anfang der 2000er-Jahre Vorreiter, ist dann aber in anderen Firmen aufgegangen. Es wurde quasi verkauft. Auch das ist ein Punkt: Wenn andere Unternehmen solche Pioniere quasi aufkaufen oder mit ihnen fusionieren, dann wird die Technologie dort weiterentwickelt. So steckt ein Kern der ursprünglichen Software von gateProtect wohl immer noch in vielen Firewalls.

Wir hören immer wieder von Fusionen. Wir sollten uns nicht von den USA abhängig machen. Insofern müssen wir aus meiner Sicht bestrebt sein, europäische Lösungen im Sinne europäischer Souveränität zu finden, um einen Schutz für die Verwaltung, für die Kommunen und auch für andere Bereiche sicherzustellen.

Ich finde die Vermischung an dieser Stelle aber sehr unglücklich, denn das eine ist das Thema Palantir bzw. Analysesoftware - das betrifft einen Abfluss von Daten -, und das andere Thema ist der Schutz von Daten. Das wollte ich einordnen, weil es mich stört, wenn wir über jedes Stöckchen springen, das uns hingehalten wird. Wir müssen tatsächlich bei allem souverän sein. Alle in irgendeiner Art und Weise bestehenden Abhängigkeiten müssen beendet werden. Das fängt, wie gesagt, bei der Energie an und endet im digitalen Raum. Aber vielleicht können Sie eine generelle Einschätzung geben, welche Aussichten es für europäische Lösungen gibt.

Dr. Aleksandra Sowa: Ich teile Ihre Auffassung, dass es jetzt vielleicht ein wenig zu spät ist, um bestimmte Lösungen zu entwickeln. Wir hätten viel früher daran arbeiten sollen. So war, meine ich, in den beiden jüngsten Koalitionsverträgen auf Bundesebene vom Grundrecht auf Ende-zu-Ende-Verschlüsselung die Rede. Darin war die Sicherheit sozusagen als Super-Grundrecht genannt, aber auch die Ende-zu-Ende-Verschlüsselung, also für jeden verfügbare Kryptografie, damit sich jeder schützen kann.

Dieser Ansatz, verknüpft mit dem Prinzip der Datenminimierung aus der Datenschutz-Grundverordnung, wäre bereits eine gute Basis, um sich heute weniger Sorgen über den Einsatz von Analysesoftware oder insbesondere sogar den Einsatz von KI-gestützten Analyse- und Auswertungssystemen machen zu müssen. Denn heute - so habe ich es zum Beispiel dem Statement von Herrn Gerlach von der DPolG entnommen - besteht das Problem, dass man wirklich unglaublich viele Daten angesammelt hat. Insofern sind auch die Daten ein gewisser Teil des Problems. Als mündiger Bürger fragt man sich natürlich, warum die Polizei so viele Daten braucht: Warum hat man in so vielen unterschiedlichen Datenbanken unterschiedliche Datensätze erfasst? Das bringt mich wieder zum Prinzip der Datenminimierung.

Ich gebe Ihnen dazu ein aktuelles Beispiel, das zeigt, wie exorbitant groß die Masse an Daten geworden ist, die durch unterschiedliche Institutionen zu verschiedenen Zwecken, die man nicht immer nachvollziehen kann, gesammelt werden: Ein Bekannter von mir musste für irgendeinen Amtsvorgang seine Meldebescheinigung vorlegen. Er hörte von der Beamtin, dass diese Meldebescheinigung nicht aktuell sei. Aber er war nicht umgezogen, und sein Name hatte sich auch nicht geändert. Also ging er ins Rathaus zur Meldestelle, um sich eine neue Bescheinigung ausstellen zu lassen; denn, so dachte er, sie war vielleicht zu alt. Er wollte auch nicht diskutieren; denn man ist dem Ganzen auch ein bisschen ausgeliefert und darauf angewiesen, dass ein Vorgang bearbeitet wird. Bei der Meldestelle wurde ihm gesagt, er habe doch zwischenzeitlich geheiratet. Damit sei seine alte Meldebescheinigung nicht aktuell.

In diesem Moment frage ich mich als zertifizierte Datenschutzauditorin: Wozu braucht man für eine Meldebescheinigung eine Statusangabe, ob man ledig, verheiratet oder verwitwet ist? Diese Frage hätte man sich eigentlich schon stellen müssen, als man dieses Verfahren definiert hat. Wozu braucht man überhaupt so viele Daten? Das Prinzip der Datenminimierung wurde in diesem Fall bereits bei der Definition des Verfahrens nicht eingehalten. Ich bin mir ziemlich sicher, dass das eine neue Entwicklung der vergangenen Jahre ist. Als die Verfahren und Prozesse neu definiert worden sind, sind viele neue Datenabfragen hinzugekommen. Jetzt steht man vor einem großen Datenschatz und fragt sich: Was könnte man damit anfangen? Dann kommt man schnell zu der Antwort: Lass uns doch eine Software aufsetzen, und die schaut - vielleicht auch mit KI -, ob sie etwas findet!

Ich meine das nicht abwertend, aber ich plädiere für eine verfahrensbasierte Software, bei der man vorgibt, welche Daten oder Datenbanken man zur Verfügung hat und was man finden will. Die Grundlage für diese Abfrage müssen nicht immer statistische Verfahren oder wissenschaftliche Ansätze und Methoden sein, sondern es können auch die Kenntnisse und Erfahrungen der Ermittler sein, die wissen, welche Indikatoren zum Beispiel darauf hindeuten, dass jemand einen Terroranschlag oder einen Cyberangriff beabsichtigen könnte. Man benötigt dafür aber validierte Merkmale und Indikatoren. Dann kann man eine solche Suche innerhalb von wenigen Sekunden durchführen. Denn aufgrund der heute zur Verfügung stehenden hohen Rechenkapazitäten ist es mit jeder Software - nicht nur mit KI-basierter Software - praktisch möglich, in wenigen Sekunden oder Minuten ein Ergebnis aus verschiedenen Datenbanken zu erhalten.

cyberintelligence.institute

Schriftliche Stellungnahme: Vorlage 8

Per Videokonferenztechnik zugeschaltet:

- Dr. Michael Littger, Strategiedirektor und Mitglied der Geschäftsleitung

Dr. Michael Littger: Vielen Dank für die Einladung an das cyberIntelligence.institute zur Stellungnahme als Sachverständiger.

Der Entschließungsantrag der CDU-Fraktion identifiziert auch aus unserer Sicht ein ganz reales und dringendes Problem. Die niedersächsische Polizei benötigt selbstverständlich moderne und leistungsfähige Werkzeuge zur Datenanalyse. Die vorgeschlagene Lösung allerdings, die Einführung der Palantir-Software, ist aus Gründen der digitalen Souveränität, des Datenschutzes und der langfristigen strategischen Ausrichtung der deutschen Sicherheitsarchitektur erheblich problematisch und wird von uns sehr kritisch gesehen.

Dafür gibt es drei Gründe, die ausführlich in unserer schriftlichen Stellungnahme dargelegt sind.

Erstens. Die Nutzung von Palatir würde Niedersachsen bzw. Deutschland in einem Kernbereich staatlicher Souveränität von einem US-amerikanischen Unternehmen abhängig machen. Die Möglichkeit eines erzwungenen Technologieentzugs durch US-Exportkontrollmechanismen, die es tatsächlich gibt, der Einsatz von Wartungspersonal eines US-Unternehmens in hochsensiblen Bereichen und die prinzipielle Möglichkeit nachrichtendienstlicher Zugriffe unter US-Recht stellen Risiken dar, die durch technische Maßnahmen allein nicht eliminiert werden können. Das halte ich für sehr wichtig. Die begrenzte Aussagekraft der Analyse des Fraunhofer-Instituts, die wir uns angeschaut haben, vermag diese Bedenken auch nicht auszuräumen, zumal sie die aus sicherheitspolitischer Sicht existenzielle Frage der Datenverfügbarkeit im Falle eines Technologieentzuges überhaupt nicht adressiert.

Zweiter Grund: Die Einführung von Palatir als vermeintliche Übergangslösung, als die sie oft bezeichnet wird, würde aus unserer Sicht den sehr schwierigen Aufbau souveräner europäischer Alternativen faktisch unmöglich machen; denn sie verschließt den relevanten Markt und absorbiert die notwendige Nachfrage für die Entwicklung solcher Produkte hier in Deutschland und andernorts in Europa. Aus unserer Sicht ist es eine Frage der politischen Priorisierung, ob man den Weg des geringsten Widerstandes jetzt wählt, also eine verfügbare US-Software-Lösung einführt, oder ob man die deutlich anspruchsvollere, aber mögliche und langfristig einzig verantwortbare Strategie verfolgt, eigene Fähigkeiten aufzubauen.

Die aktuelle geopolitische Lage, in der die Zuverlässigkeit transatlantischer Partnerschaften nicht mehr als selbstverständlich gelten kann und in der technologische Souveränität offensichtlich zum entscheidenden Faktor staatlicher Handlungssouveränität geworden ist, spricht aus unserer Sicht eindeutig für die zweite Option. Es wäre fahrlässig, die innere Sicherheit unseres Landes auf eine Technologie zu gründen, deren Verfügbarkeit von den außenpolitischen Entscheidungen eines einzelnen Drittstaates abhängt.

Niedersachsen sollte sich daher auf Bundesebene dafür einsetzen, dass die Mittel, die für Lizenzgebühren und den Betrieb einer Palantir-Infrastruktur aufgewendet werden müssten, stattdessen in die Entwicklung einer europäischen, souveränen Lösung investiert werden. Die Kosten für

den Betrieb von Palantir sind übrigens in den bereits nutzenden Bundesländern erheblich und stellen langfristig eine finanzielle Belastung dar, die in keinem angemessenen Verhältnis zu dem steht, was mit denselben Mitteln an eigener Entwicklungskapazität und eigener Kontrolle, auch Kostenkontrolle, hätte aufgebaut werden können. Jeder Euro, der in eine Abhängigkeit vom Ausland fließt - in dem Fall in eine Abhängigkeit von den USA -, fehlt für den Aufbau eigener Kompetenzen. Das ist, glaube ich, ganz generell ein Thema.

Der richtige Weg besteht aus unserer Sicht deshalb darin, die Schaffung einer verfassungskonformen Rechtsgrundlage - auch darüber sprechen wir in dem Gutachten - für die automatisierte Datenanalyse umgehend voranzutreiben und gleichzeitig die Entwicklung einer souveränen, modularen und offenen Analyseplattform als gesamtgesellschaftliche Aufgabe in Angriff zu nehmen. Ja, das erfordert politischen Willen, erhebliche Investitionen, eine enge Zusammenarbeit zwischen Bund, Ländern und Forschungseinrichtungen sowie der europäischen IT-Wirtschaft. In der Übergangszeit sind die vorhandenen polizeilichen IT-Systeme gezielt zu ertüchtigen. Das ist möglich und beispielsweise durch Open-Source-Komponenten zu ergänzen.

Drittes und letztes Argument für die sehr kritische Haltung unsererseits: Die Sicherheit der Bürgerinnen und Bürger und die Wahrung ihrer Grundrechte sind keine Gegensätze, sondern zwei Seiten derselben Medaille. Eine moderne polizeiliche Datenanalyse muss natürlich beiden Ansprüchen gerecht werden. Das kann sie nur auf der Grundlage einer technologischen Souveränität, algorithmischer Transparenz und wirksamer demokratischer Kontrolle. Niedersachsen hat die Gelegenheit, hier eine verantwortungsvolle Vorreiterrolle einzunehmen und einen Weg zu beschreiten, der nachhaltig zukunftsfähig ist, anstatt einer kurzfristigen, aber strategisch fragwürdigen Lösung zu folgen.

Die Debatte über den Entschließungsantrag der CDU sollte deshalb zum Ausgangspunkt einer breiten und grundlegenden Auseinandersetzung mit der Frage werden, wie Deutschland seine digitale Souveränität im Bereich der inneren Sicherheit dauerhaft sicher stärken kann, nicht durch Abhängigkeit, sondern durch Eigenständigkeit.

Abg. **Saskia Buschmann** (CDU): Auch Ihnen herzlichen Dank für Ihre Worte an uns. Sie sagten, wir sollten die Mittel nutzen, um eine eigene Entwicklung voranzubringen. Welcher zeitliche Horizont schwebt Ihnen dabei vor? Wie lange dauert es, bis wir auf der Grundlage eigener bzw. europäischer Entwicklungen ein System mit derselben Leistungsfähigkeit haben, die Palantir derzeit hat?

Dr. Michael Littger: Hier eine zeitliche Vorgabe festzulegen, wäre nicht seriös. Ich glaube, der erste Schritt ist die politische Entscheidung, das zu wollen und möglicherweise auch ein Zieldatum dahinterzusetzen. Der zweite Schritt ist dann, die Pferde loszuschicken. Parallel sollten die Systeme mit den bestehenden Möglichkeiten vernetzt werden. Es gibt ja schon Möglichkeiten, damit loszulegen. Außerdem stehen Fähigkeiten über Forschungsprogramme zur Verfügung. Es gibt sehr gute Kapazitäten in den deutschen Forschungseinrichtungen, das Fraunhofer-Institut und weitere mehr. Das haben wir in der Stellungnahme näher dargestellt.

Das Problem ist bislang: Es gibt die Initiative zu dieser politischen Entscheidung nicht. Und wenn man sie nicht auf den Weg bringt, wird sie auch nicht kommen. Insofern wäre die Antwort unter den aktuellen Bedingungen: gar nicht. Aber wir würden uns wünschen, dass das in einem vertretbaren Zeitraum passiert.

Abg. **Michael Lühmann** (GRÜNE): Vielen Dank, auch für das Plädoyer, dass man erst einmal anfängt, die Lücken zu schließen, und nicht jetzt einen Marktteilnehmer aus den USA holt und dann alle vorhandenen Initiativen erstickt werden. Das nehmen wir mit, ebenso wie das Plädoyer, dass man sich politisch dazu entschließen muss.

Meine Frage bezieht sich auf das Stichwort „Misstrauen“; Frau Butter sprach es schon an. Sie sagten gerade, eine demokratische Kontrolle hielten Sie für sehr wichtig. Hier gibt es den „Ausschuss zur Kontrolle besonderer polizeilicher Datenerhebungen“. Dort werden wir informiert. Sie plädieren - so verstehe ich Sie - dafür, dass man zumindest für einen gewissen Zeitraum - oder dauerhaft? - diese Einsatzmöglichkeiten auf der Grundlage einer entsprechenden gesetzlichen Regelung kontrolliert?

Dr. Michael Littger: Die parlamentarische und datenschutzrechtliche Kontrolle ist auf jeden Fall essenziell, und sie wäre unter den momentanen Voraussetzungen wohl nicht gewährleistet. Datenschutz ist bekanntlich keine Momentaufgabe, wie heute gesagt wurde, sondern eine Daueraufgabe. Da aber bislang die Transparenz, die erforderlich wäre, um eine effektive Kontrolle zu gewährleisten, überhaupt nicht gewährleistet ist, muss man fragen, wie diese genau ermöglicht werden sollte. Selbstverständlich ist es Ihr gutes Recht als Parlament und als Auftraggeber - in letzter Instanz - genau zu wissen, was dort in welcher Form eingespielt wird.

***

Tagesordnungspunkt 3:

Rückführungsmanagement optimieren - Sekundärmigrationszentren in Niedersachsen umgehend einrichten

Antrag der Fraktion der CDU - Drs. 19/9257

erste Beratung: 82. Plenarsitzung am 18.12.2025
federführend: AfluS
mitberatend gem. § 27 Abs. 4 Satz 1 i. V. m. § 39 Abs. 3 Satz 1 GO LT: AfHuF

zuletzt beraten: 93. Sitzung am 15.01.2026

Der **Ausschuss** setzt diesen Punkt aus Zeitgründen von der Tagesordnung ab.

***

Tagesordnungspunkt 4:

Straftaten im digitalen Raum wirksam und nachhaltig bekämpfen - vorsorgliche Speicherung von IP-Adressen endlich gesetzlich normieren

Antrag der Fraktion der CDU - Drs. 19/9900

erste Beratung: 87. Plenarsitzung am 04.03.2026
AfluS

Der **Ausschuss** setzt diesen Punkt aus Zeitgründen von der Tagesordnung ab.

***

Tagesordnungspunkt 5:

Freiheitlich-demokratische Grundordnung schützen - Instrumente der wehrhaften Demokratie entschlossen nutzen

Antrag der Fraktion der SPD und der Fraktion Bündnis 90/Die Grünen - Drs. 19/9916

erste Beratung: 88. Plenarsitzung am 05.03.2026
federführend: AfluS
mitberatend: AfRuV

dazu: Eingaben 01300/02/19, 01654/02/19, 01654/02/19-001, 01654/02/19-002, 01742/02/19

Der **Ausschuss** setzt diesen Punkt aus Zeitgründen von der Tagesordnung ab.

***