Landtag von Baden-Württemberg **Drucksache 17 / 9670**

17. Wahlperiode

Beschlussempfehlung und Bericht

des Ausschusses des Inneren, für Digitalisierung und Kommunen

zu dem Gesetzentwurf der Landesregierung – Drucksache 17/9478

Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften

Beschlussempfehlung

Der Landtag wolle beschließen,

1. dem Gesetzentwurf der Landesregierung – Drucksache 17/9478 – zuzustimmen;

2. den Antrag der Abg. Julia Goll u. a. FDP/DVP und Stellungnahme des Ministeriums des Inneren, für Digitalisierung und Kommunen – Palantir Gotham – Risiken und Alternativen – Drucksache 17/9382 – für erledigt zu erklären.

22.10.2025

Die Berichterstatterin:	Der Vorsitzende:
Petra Häffner	Ulli Hockenberger

Bericht

Der Ausschuss des Inneren, für Digitalisierung und Kommunen hat den Gesetzentwurf der Landesregierung – Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften – Drucksache 17/9478 in seiner 44. Sitzung, die als gemischte Sitzung mit Videokonferenz stattfand, am 22. Oktober 2025 beraten. In die Beratung miteinbezogen wurde außerdem der Antrag der Abgeordneten Julia Goll u. a. FDP/DVP und die Stellungnahme des Ministeriums des Inneren, für Digitalisierung und Kommunen – Palantir Gotham – Risiken und Alternativen – Drucksache 17/9382.

Vor der Ausschussberatung des Gesetzentwurfs hat der Ausschuss nach § 50a Absatz 3 der Geschäftsordnung eine öffentliche Anhörung zu diesem Gesetzentwurf in öffentlicher Sitzung durchgeführt (*Anlage*).

Eine Abgeordnete der Fraktion der FDP/DVP fragt, ob seitens des Innenministeriums im Nachgang zur soeben durchgeführten Anhörung bereits eine erste Einschätzung zu einem möglichen Nachbesserungsbedarf gegeben werden könne.

Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente

Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.

Zum Antrag Drucksache 17/9382 und hier konkret zur Stellungnahme zu den Ziffern 4, 5, 6 und 8 interessiere sie, wie weit die dort dargestellten Kooperationen bereits seien, in welcher Form später eine Vergabe funktionieren könne und welche Modalitäten bei einer europaweiten Ausschreibung zu beachten seien.

Ein Abgeordneter der Fraktion der SPD schließt sich dieser Frage an und bittet zudem um eine zeitliche Größenordnung, bis wann dann die Einsatzfähigkeit der Software gegeben wäre.

Der Minister des Inneren, für Digitalisierung und Kommunen erklärt eingangs, nach seinem Eindruck habe keiner der soeben angehörten Sachverständigen die Software Palantir generell abgelehnt; vielmehr sei übereinstimmend die Überzeugung geäußert worden, dass die Polizei ein solches Instrument brauche oder es ihr jedenfalls zuzubilligen sei. Insofern habe es auch keine fundamentale Kritik am Gesetzentwurf gegeben; Kritik sei lediglich an bestimmten Details geübt worden. Hierzu sei ihm wichtig zu betonen, dass, da beim geplanten Einsatz von Palantir in Baden-Württemberg keine künstliche Intelligenz zur Anwendung komme, auch nicht die Gefahr bestehe – anders als von manchen Referenten dargelegt –, dass das System halluziniere.

Er versichert, die im Rahmen der Anhörung gegebenen Anregungen gründlich prüfen zu wollen.

Zu der Entwicklungskooperation mit Airbus Defence and Space sowie der Digitalsparte der Schwarz Gruppe legt er dar, die Rahmenbedingungen für eine solche Zusammenarbeit würden derzeit geprüft, was auch die Frage der vergaberechtlichen Gegebenheiten umfasse. Grundsätzlich müsse sichergestellt werden, dass eine solche Partnerschaft innerhalb einer Entwicklungskooperation einer späteren Nutzung dieser Software durch die Sicherheitsbehörden nicht entgegenstehen würde.

Unmittelbar nach Abschluss der rechtlichen Prüfungen könnten die entsprechenden Gespräche mit den betreffenden Stakeholdern aufgenommen werden.

Die Dauer eines solchen Ausschreibungsverfahrens veranschlage er auf circa ein Jahr.

Die Abgeordnete der Fraktion der FDP/DVP kündigt namens ihrer Fraktion für die folgende Abstimmung über den Gesetzentwurf Drucksache 17/9478 Enthaltung an und erklärt, dem Anliegen, dass die Sicherheitsbehörden geeignete Softwarelösungen für eine verbesserte Datenanalyse erhielten, stehe die FDP/DVP-Fraktion grundsätzlich positiv gegenüber; jedoch solle zunächst eruiert werden, inwiefern sich aus den Stellungnahmen im Rahmen der Anhörung bis zur zweiten Lesung noch Änderungsbedarfe ergäben.

> Der Gesetzentwurf der Landesregierung – Drucksache 17/9478 – wird mehrheitlich angenommen.
>
> Der Ausschuss beschließt zudem als Empfehlung an das Plenum ohne förmliche Abstimmung, den Antrag Drucksache 17/9382 für erledigt zu erklären.

3.11.2025

Häffner

Anlage

Anhörung zu dem

Gesetzentwurf der Landesregierung
– Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften
– Drucksache 17/9478

Vorsitzender Ulli Hockenberger: Meine sehr geehrten Damen und Herren! Ich darf Sie alle auch im Namen meiner Stellvertreterin, Kollegin Schwarz, recht herzlich begrüßen. Ich darf insbesondere Herrn Minister Strobl, Herrn Staatssekretär Blenke, Frau Landespolizeipräsidentin Dr. Hinz, Herrn Landespolizeidirektor Schneider und Frau Landeskriminaldirektorin Zarges begrüßen. Ich begrüße die Vertreterinnen und Vertreter der Ministerien, ich begrüße insbesondere die Pressevertreter und die Bürgerinnen und Bürger, die uns per Livestream zugeschaltet sind.

Ich rufe nun auf

Öffentliche Anhörung zu dem

Gesetzentwurf der Landesregierung
– Gesetz zur Einführung einer automatisierten Datenanalyse und zur Änderung weiterer polizeirechtlicher Vorschriften
– Drucksache 17/9478

Ich darf die Referenten begrüßen, die ich dann auch im Detail jeweils noch vorstellen werde.

Mit Ihrem Einverständnis darf ich unseren ersten Referenten, Herrn Polizeipräsident Thomas Berger, aufrufen. – Herr Berger, Sie haben das Wort. Schön, dass Sie da sind.

Herr Berger: Vielen Dank. – Herr Vorsitzender, meine Damen und Herren Abgeordneten, Herr Minister, Herr Staatssekretär! Für mein fünfminütiges Eingangsstatement habe ich mir echt überlegt: Was sage ich denn in fünf Minuten zu diesem Thema?

Als Erstes möchte ich sagen, dass ich es insgesamt gut finde, dass das, was wir hier machen, überhaupt stattfindet. Das unterscheidet uns vielleicht von anderen Staaten: Exekutivbefugnisse, die man in unsere Hände legen will, müssen jederzeit durchleuchtet, diskutiert und rechtsstaatlich behandelt werden. Jetzt bin ich froh, dass eine solche Anhörung überhaupt stattfindet. Das ist mir sehr wichtig, weil ich in keinem anderen System die Verantwortung für so etwas tragen möchte; und für meine Kollegen gilt – ich denke, da spreche ich für alle – das Gleiche.

Als ich die Liste der Experten – es ist ja eine Expertenanhörung; und da sind wirklich hochkarätige Experten eingeladen – gesehen habe, habe ich mich gefragt: Was ist denn meine Expertise? Ich bin weder ein hochdekorierter Jurist noch bin ich ein IT-Sachverständiger. Was macht mich denn für diese Runde zum Experten? Dann habe ich das diskutiert, und mir wurde klar: Ich bin vielleicht Experte in der Übernahme von Verantwortung, und zwar verantworte ich ständig Dinge, die ich am Ende des Tages einsetze, und das schon seit 34 Jahren. Deswegen denke ich, dass das Thema Verantwortung heute auch eine große Rolle spielt, nämlich mit der Zielrichtung: Können wir verantworten, was wir da tun, und mit welchen Maßnahmen und unter welchen Maßgaben können wir diese Verantwortung tragen? Ich bin in persona hier, und ich stehe in persona für diese Verantwortung.

Das Zweite – das möchte ich noch einwerfen –: Technologie hat immer das Potenzial, Schaden zuzufügen. Die Polizei, die Bundeswehr, aber auch die Dienste, wir nutzen Technologie, die potenziell in der Lage ist, Menschen zu schaden. Ich nenne beispielhaft die Waffentechnologie: Unsere Waffen unterscheiden sich kaum von den Waffen, die irgendwo sonst in der Welt gegen Menschen eingesetzt wer-

den. Was uns unterscheidet, ist, in welchem Kontext wir diese Dinge nutzen – nämlich in einem föderalen, gewaltengeteilten Kontext. Dabei ist nicht die Sache an sich wichtig – die Sache selbst ist gefahrengeneigt; das ist so –, sondern es stellt sich vielmehr die Frage: In welchem Kontext setzen wir die Dinge ein? Ich hoffe, dass wir heute im Rahmen der Diskussion noch einmal auf dieses Thema kommen: In welchem Kontext wollen wir denn diese Mittel einsetzen?

Und es geht nicht darum, hier eine bestimmte Software einzusetzen, sondern es geht darum: Bekommen wir die Befugnisse, diese Befähigungslücke zu schließen? Ich kann Ihnen sagen: Wir müssen diese Befähigungslücke schließen; denn die Befähigungslücke, die wir vorfinden, hat die Gegnerschaft, die gegen uns und gegen die Bürger arbeitet, nie. Die haben nie eine Befähigungslücke, sondern die gehen mit der Zeit. Wir müssen in der Lage sein, die Menschen mit den Mitteln der Zeit in all ihren Lebensbereichen zu beschützen, und zwar so, dass sie die Sicherheit als selbstverständlich empfinden.

Ich hoffe, dass wir heute im Rahmen der Diskussion dieses Thema „Können wir das verantworten?“ gemeinsam besprechen werden. Ich kann Ihnen eines sagen: Ich werde das verantworten. Ich habe mir das gut überlegt. Ich habe meine Führungscrew mitgebracht; sie wird das verantworten. Wir werden die Verantwortung für den Einsatz einer solchen Software – egal, welche es sein wird – übernehmen, auf der Grundlage des Gesetzes, das wir dringend brauchen und das hoffentlich im November verabschiedet wird.

Vorsitzender Ulli Hockenberger: Vielen Dank, Herr Präsident Berger. – Ich würde dann Herrn Professor Dr. Michael Waidner vom Fraunhofer-Institut für Sichere Informationstechnologie aufrufen, der uns per Video zugeschaltet ist. – Herr Professor Waidner, Sie haben das Wort.

Herr Dr. Waidner: Vielen Dank. – Meine Damen und Herren! Erst einmal herzlichen Dank für die Einladung zu dieser Anhörung. Ich entschuldige mich, dass ich nicht vor Ort anwesend sein kann. Ich kommentiere aus Sicht der IT; ich bin der IT-Sachverständige hier.

Der Gesetzentwurf ist aus meiner Sicht vorbehaltlos zu begrüßen – das vorweg. Moderne Datenanalysewerkzeuge mit oder ohne KI sind in allen Bereichen unverzichtbar geworden. Für die Polizeiarbeit bedeuten sie einen doppelten Gewinn – Herr Berger hat das gerade schon angedeutet –: Quantitativ kann weniger Personal mehr Daten sichten; qualitativ werden existierende Datenberge überhaupt erst vollständig auswertbar. Ohne Automatisierung ist dies praktisch nicht mehr möglich.

Entscheidend ist: Wir sprechen von einem Werkzeug für Polizeibeamte und nicht von einer Wunderwaffe, die ihre Arbeit übernimmt. Solche Werkzeuge haben kein Eigenleben, sie suchen sich nicht selbstständig ihre Daten irgendwo im Netz, sie denken sich auch nicht selbst irgendwelche Klassifikations- und Koordinationsregeln aus. Der Gesetzgeber definiert mit diesem Gesetzentwurf einen abstrakten Rahmen, und die Polizei als Betreiber muss ebendiesen Rahmen für konkrete Datenquellen im Zuge des Rechts regeln und in Vorgaben für die erlaubten Abfragen übersetzen. Wie wir gerade gehört haben, ist die Verantwortung bei der Polizei.

Jedes Experiment birgt Risiken, es gibt dafür aber bewährte Lösungsansätze: Illegale Abfragen können durch Protokollierung, Überwachung und Anomalieerkennung identifiziert werden. Der Gesetzentwurf enthält bereits entsprechende Vorgaben; moderne Systeme unterstützen dies technisch.

Algorithmen-Bias bleibt ein berechtigtes Thema: Während heutige Abfragen vorwiegend regelbasiert und nicht KI-basiert erfolgen, wird maschinelles Lernen künftig eine größere Rolle spielen. Das Entscheidende: Verantwortung und Prüfung liegen immer und vollständig beim Menschen. Das System trifft keine Entscheidungen; es stellt nur Daten bereit und muss im Sinne der KI-Verordnung – also des EU AI Act – transparent machen, wie diese entstanden sind.

Das Risiko durch externe Angriffe wird minimiert, indem die Systeme in isolierten, abgeschotteten Rechenzentren der Polizei betrieben werden – nicht in der Cloud,

nicht im Ausland. Technisch und organisatorisch wird sichergestellt, dass Daten nur hinein, nicht aber hinaus fließen. Updates erfolgen über Datenträger oder sogenannte Datendioden – ohne einen Rückkanal für Telemetriedaten oder einen Wartungszugang. Mein Institut hat die Palantir-Software im Auftrag des bayerischen LKA analysiert und kann bestätigen: Ein sicherer Betrieb in dieser Form ist möglich, ein Datenabfluss ist damit ausgeschlossen, weshalb auch die Befürchtungen bezüglich des US CLOUD Act gegenstandslos werden.

Verfügbarkeitsprobleme durch Schwachstellen oder verzögerte Updates sind das verbleibende Risiko. Hier entscheiden das IT-Management des Betreibers, die Professionalität des Herstellers und dessen langfristige Zuverlässigkeit – ein kritisches Auswahlkriterium bei der Plattformwahl.

Zur Frage der Herkunft der Alternativen: Das Land beabsichtigt ja, als Plattform das Produkt „Gotham“ von Palantir zu nutzen. Dazu muss man wissen: Palantir ist seit 2003 technologischer Marktführer in diesem Bereich und hat in umfassendes Domänenwissen investiert. Die USA-Ansässigkeit bedeutet potenzielle Einflussmöglichkeiten durch die US-Regierung – das aber gilt genauso für jeden anderen US-Konzern von Microsoft bis hin zu Lockheed Martin, die mit Produkten wie Windows und F-35 eigentlich noch zentralere Positionen in der Sicherheitsarchitektur Deutschlands einnehmen. Das ist kein zu übersehendes Risiko, bleibt aber eine politische Entscheidung.

Dass sich manche Kritik weniger an den politischen Rahmenbedingungen entzündet als vielmehr an den Gründerpersonen und deren politischen Ansichten, halte ich für nicht besonders zielführend. Man vergleiche die Debatte hier mit der Haltung gegenüber ähnlich gelagerten Produkten anderer US-Hersteller, etwa dem i2 Analyst’s Notebook, das häufig eingesetzt wird, das bis letztes Jahr von IBM angeboten wurde – niemand stört sich daran.

Ja, es gibt auch europäische Alternativen, beispielsweise ArgonOS aus Frankreich. Palantir gilt aber im Vergleich als überlegen. Mit viel Geld und festen Abnahmezusagen wäre es sicherlich möglich, den Vorsprung aufzuholen. Ob das sinnvoll wäre, ist angesichts knapper Kassen und der Vielzahl an Abhängigkeiten von US-Technologien im Sicherheitsbereich allerdings sehr fraglich. Wir müssen mehr in unsere digitale Souveränität investieren, dabei eben klug vorgehen und dort investieren, wo es sich am meisten lohnt – also dort, wo wir eine reale Chance auf Führerschaft in einem strategisch und ökonomisch wichtigen Technologiebereich haben.

Fazit: Der Gesetzentwurf schafft einen angemessenen Rahmen. Ich denke, die Wahl, die das Land hier praktisch getroffen hat – „Gotham“ von Palantir –, ist eine technisch gute und aus IT-Sicherheitssicht handhabbare Wahl. – Vielen Dank.

Vorsitzender Ulli Hockenberger: Vielen Dank, Herr Professor Waidner. – Ich darf dann als nächsten Experten Herrn Professor Dr. Johann Justus Vasel von der Heinrich-Heine-Universität Düsseldorf aufrufen und auch ihn per Video begrüßen. – Herr Professor Vasel, wenn Sie uns hören, dann hätten Sie jetzt das Wort.

Herr Dr. Vasel: Herzlichen Dank. – Zunächst: Ganz herzlichen Dank für die Einladung; ich fühle mich sehr geehrt. Vielen Dank an den Ausschuss und dessen Vorsitzenden für diese Möglichkeit der Stellungnahme.

Ich möchte mich zunächst meinen beiden Vorrednern anschließen, zunächst dem Präsidenten Thomas Berger, der von einer Befähigungslücke sprach, die ich auch attestieren möchte und die hier mit einem, wie ich finde, sehr gelungenen und sinnvollen Vorschlag geschlossen werden soll. Zudem möchte mich meinem Vorredner Herrn Kollegen Professor Waidner anschließen: Ich glaube, er hat eindrucksvoll die Vorzüge digitaler Analyseinstrumente für die Polizeiarbeit aufgezeigt. Dies ist eine conditio sine qua non, und wenn der Staat seiner Fundamentalaufgabe, Sicherheit und Freiheit zu gewährleisten, gerecht werden will, dann muss er entsprechend auch mit Instrumenten der Gegenwart ausgestattet werden.

Dafür schaffen Sie hier die Gesetzesgrundlage, und schon das ist aus rechtswissenschaftlicher Perspektive begrüßenswert; denn wir wissen, dass diese Software,

von der eben schon die Rede war, in mehreren Bundesländern bereits eingesetzt worden ist und seit vielen Jahren eingesetzt wird – zum Teil auch ohne eine ausreichende, jedenfalls aus verfassungsrechtlicher Perspektive ausreichende Legitimationsgrundlage. Der Gesetzentwurf, den wir in Ihrem Bundesland vorliegen haben, ist, wie ich finde, in der Tat überwiegend sehr gelungen.

Ich darf, obwohl das vielleicht bekannt ist, ganz kurz die Normenstruktur des neuen § 47a noch mal rekapitulieren oder ins Gedächtnis rufen: Absatz 1 legt die Eingriffsbefugnisse fest, Absatz 2 die Grenzen des Eingriffs, Absatz 3 legt fest, welche Datenbestände einbezogen werden können. In Absatz 4 werden technisch-organisatorische Vorkehrungen getroffen; diese beinhalten insbesondere ein Rechte- und Rollenkonzept sowie ein Konzept zur Datenkategorisierung etc. Die Absätze 5 und 6 betreffen ebenfalls eine Vertiefung der organisationsrechtlichen Dinge. Absatz 7 normiert ein Anordnungserfordernis und Absatz 8 die Mitwirkung des Landesbeauftragten für den Datenschutz in dieser Hinsicht.

Das ist sicherlich eine komplexe, gerade aber im Rechtsvergleich mit den anderen mittlerweile existenten Grundlagen dann doch noch relativ kompakte Norm. Ich kann sagen, dass die maßgebliche Rechtsprechung, nämlich das Bundesverfassungsgerichtsurteil von Februar 2023, das auf über 50 Seiten ausbuchstabiert hat, was die verfassungsrechtlichen Anforderungen an automatisierte Datenanalyse sein müssen, sehr wohl reflektiert worden ist. Der Gesetzgeber hat hier gut, sauber und gründlich gearbeitet. Er hat aber auch bestimmte Lehren aus den Normen der anderen Bundesländer – soweit vorhanden – gezogen; das ist in Bayern der Fall, und es ist in Hessen der Fall – wobei dort der erste Normansatz für verfassungswidrig erklärt und dann noch einmal novelliert worden ist –, ebenso in Hamburg, in Nordrhein-Westfalen und in Rheinland-Pfalz. Wenn man ein bisschen rechtsvergleichend über Ihren Entwurf schaut und dabei auch die Rechtsprechung des Bundesverfassungsgerichts reflektiert, dann möchte ich fünf Positiva nennen und vielleicht auch einige Punkte ansprechen, an denen man noch nachbessern könnte, wenn man wollte, um vielleicht einem „Angriff“ aus Karlsruhe auf dieser Grundlage entgegenzuwirken oder dessen Wahrscheinlichkeiten zu mindern.

Zu den Positiva: Die Entscheidung ist von Menschen zu treffen, insofern ist auch eine manuelle Auslösung erforderlich. Das ist eigentlich eine Selbstverständlichkeit – das wurde schon gesagt –, hilft aber gerade auch dabei, der Furcht in breiten Teilen der Bevölkerung entgegenzuwirken. Gut, dass das hier expliziert worden ist.

Es ist auch sehr lobenswert, dass diskriminierende Algorithmenrisiken im Normtext aufgegriffen worden sind.

Was ich als drittes Positivum nennen möchte, ist, dass das Schutzgüterkonzept abgestuft ist. Viertens: Es ist keine direkte Anbindung an Internetdienste erfolgt; auch das ist sicherlich sehr begrüßenswert.

Abschließend hebe ich noch positiv hervor, dass in dem Normtext eine Unterscheidung, ein Differenzierungskonzept nach Verurteilten, Beschuldigten, Verdächtigen oder sonstigen Anlasspersonen abgebildet worden ist. Insofern ist es, wie gesagt, ein reflektierter Entwurf, den Sie vorgelegt haben und zu dem ich nur gratulieren kann.

Gleichwohl kann man natürlich aus den anderen Normen auch noch ein bisschen lernen, und zwar in beiderlei Richtungen. Zum einen könnte man sich z. B. an der bayerischen Norm – § 61a des Bayerischen Polizeiaufgabengesetzes – orientieren und überlegen, ob man den Schutz bestimmter Dinge noch mal explizit hervorheben will, etwa in Bezug auf die Gefahren für Anlagen kritischer Infrastruktur – da gibt es natürlich große Bedrohungsszenarien – oder für bestimmte Kulturgüter von überragender Bedeutung, ebenso wie auf Umweltschäden – das ist in § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung normiert worden. – Darüber könnte man jedenfalls nachdenken.

Ich denke, man könnte in der Norm auch noch modifizierend aufführen, dass der Datenschutzbeauftragte nicht nur – wie es in Absatz 8 heißt – bei „wesentlicher Änderung“ angehört werden muss, sondern möglicherweise auch ein Recht hat oder dafür vorgesehen ist, stichprobenartig den Einsatz der Software und des Systems zu kontrollieren. Das haben andere Gesetzesnormen aufgegriffen, und das

mag als verfahrensrechtliche Sicherung auch gewissen verfassungsrechtlichen Bedenken entgegentreten.

Manche der Gesetze oder Legitimationsgrundlagen in anderen Bundesländern sehen auch vor, dass man explizit anführt, dass die Beamtinnen und Beamten vom Polizeidienst geschult werden sollen. Ob das jetzt unbedingt Gesetzesdignität erlangen muss, ist die Frage – das kann man vielleicht auch an die Verwaltung delegieren –, mag aber auch unter Wesentlichkeitsgesichtspunkten verfassungsrechtlichen Bedenken schon expressiv entgegenwirken. Insofern sei angeregt, dass man darüber noch mal nachdenken könnte.

So weit von mir. Ich finde, das ist ein überwiegend sehr gelungener Gesetzesvorschlag. – Vielen Dank.

Vorsitzender Ulli Hockenberger: Vielen Dank, Herr Professor Vasel. – Wir kommen dann zum nächsten Referenten. Ich darf den Präsidenten des Anwalts-Verbands Baden-Württemberg im Deutschen Anwaltverein, Herrn Professor Dr. Kothe, begrüßen. – Herr Professor Kothe, Sie haben das Wort.

Herr Dr. Kothe: Vielen Dank. – Herr Vorsitzender, meine Damen und Herren! Ich danke Ihnen, dass ich hier und heute für den Anwaltsverband zu der geplanten Änderung des Landespolizeigesetzes sprechen darf. In der Annahme, dass Ihnen unsere Stellungnahme vom 19. August bekannt ist, kann und muss ich mich hier kurzfassen.

Herr Berger sprach zu Recht von einer Befähigungslücke, die geschlossen werden muss; da werden Sie von uns keinen Widerspruch hören – nur zu der Art und Weise des Vorgehens. Gestatten Sie mir, dazu eine Parallele zu ziehen: Wenn sich eine Gemeinde einem Investor gegenüber vertraglich verpflichtet, für ihn quasi mundgerecht einen Bebauungsplan aufzustellen und zu beschließen, damit dieser seine Investition verwirklichen kann, dann ist seit 60 Jahren in der Rechtsprechung geklärt, dass dieser Bebauungsplan unwirksam ist. Wir haben hier eine ähnliche Situation. Wir und die Bürger sind gespannt, wie der Landtag damit umgehen wird.

Auch wenn gesagt wurde, es gehe ja nicht um eine bestimmte Software, ist schon bekannt, dass die Software „Gotham“ des Unternehmens Palantir bereits beschafft ist – mit einer Laufzeit von fünf Jahren. Wir kennen den Vertrag nicht; ich nehme an, die wenigsten von Ihnen kennen den Vertrag. Wir wissen also nicht, was dort geregelt ist und wie abgesichert ist, dass keine Daten abfließen. Die Ursprungsversion ist geprüft worden – das sei unbestritten –, aber es gibt keine Software, die fünf Jahre ohne Updates läuft. Wie das bei den Updates funktionieren wird, wissen wir schlicht und ergreifend nicht.

Ich weiß auch nicht, ob deutsches oder US-amerikanisches Recht vereinbart wurde. Einer meiner Vorredner sprach eben den US CLOUD Act an, der doch durchaus Anwendung finden kann; denn danach sind US-amerikanische Firmen verpflichtet, die Daten, die sie erheben oder die sie verarbeiten – egal, ob in den USA oder außerhalb der USA, egal, ob die Personen dort wohnen oder nicht –, auf Anforderung an die US-Regierung weiterzuleiten. Dagegen gibt es zwar ein Widerspruchsrecht, aber nur, wenn der betreffende Staat eine Vereinbarung mit der US-Regierung geschlossen hat. Soweit wir das wissen, hat das bislang nur Großbritannien gemacht.

Dementsprechend gibt es von unserer Seite durchaus Befürchtungen, die auch darin gründen, dass eine Abhängigkeit von diesem Softwarehersteller entstehen könnte. Wenn es denn diese Software sein soll – wovon ich ausgehe –, dann sollten Sie sich gleichzeitig aber auch nach Alternativen umsehen und investieren, damit Sie in fünf Jahren wirklich eine Alternative zur Verfügung haben und die Zusammenarbeit mit Palantir nicht allein aus einem Mangel an Alternativen fortsetzen müssen.

Zur Sache selbst. Am Gesetzentwurf und am Vorgehen fällt auf: Normalerweise wird ein Pflichtenheft anhand von rechtlichen Vorgaben, wie etwas umgesetzt werden soll, formuliert. Wir haben innerhalb der Polizei eine besondere Struktur: Welche Dienststellen verwalten welche Daten usw., usf.? Wir haben eine technische Vorgabe durch die Software; soll heißen: Hier kommt der Gesetzentwurf – der

eigentlich das Pflichtenheft sein sollte – nach der technischen Situation, nach der technischen Klärung. Und das ist nicht unbedingt glücklich. Verstärkt wird das Ganze dadurch, dass künstliche Intelligenz eingesetzt werden soll.

Ich sage Ihnen nichts Neues, wenn ich sage, dass das Recht auf informationelle Selbstbestimmung nur auf gesetzlicher Grundlage eingeschränkt werden darf. Die Regelung muss verhältnismäßig sein; die Voraussetzung und der Umfang der Beschränkung müssen sich daraus klar und erkennbar für den Bürger ergeben.

Das heißt, mit Blick auf die Wesentlichkeitstheorie, den Bestimmtheitsgrundsatz und die Normenklarheit ist es bedenklich, dass hier die Bestimmung der in der Analyse einzuspeisenden Inhalte nicht an den grundgesetzlich geschützten Inhalten – das heißt, den Informationen der natürlichen Personen – ausgerichtet ist, sondern daran, wie die polizeilichen Arbeitssysteme strukturiert sind. Damit fällt nicht der Gesetzgeber – also Sie – eine klare Entscheidung darüber, welche Informationen über welche und wie viele Personen wie verarbeitet werden dürfen. Das weckt Bedenken an der ganzen Konzeption, die die Verantwortung weitestgehend der Exekutive überträgt.

Soll heißen: Die Erlaubnis zum Einsatz künstlicher Intelligenz bei der Datenanalyse muss unseres Erachtens durch eine klare Definition der Zwecke und Ziele durch den Gesetzgeber, also durch Sie, begrenzt werden. Es muss geregelt werden, wer denn offensichtlich unbeteiligt ist. Die Daten offensichtlich Unbeteiligter sollen nur bei Vorgangsdaten gesperrt werden. Die Unbeteiligten sind aber auch bei Fällen und anderen Dingen beteiligt – da muss ich nur an meinen Berufsstand denken. Gerade diejenigen, die Sie mit dieser Software ausfiltern wollen, sind häufig anwaltlich vertreten. Sind wir beteiligt, oder sind wir unbeteiligt? Sind wir im System drin oder nicht? – Diese Fragen stellen sich.

Zur Abmilderung der Eingriffsintensität und zur Überprüfung der Datenanalyse sollte schon vom Gesetzgeber klargestellt werden, wie die tatbestandlichen Voraussetzungen für die Benachrichtigungspflicht bei weiteren Maßnahmen – die im Gesetzentwurf relativ pauschal genannt werden – geregelt sind.

Letzter Punkt: In dem geplanten Gesetz wird – nicht unüblich, aber trotzdem immer wieder zu bedenken – vielfach mit unbestimmten Rechtsbegriffen gearbeitet, was z. B. die „Sachen von bedeutendem Wert“ oder „schwere Straftaten“ angeht. Wenn ich all dies in Kombination damit nehme, dass die Anordnungsbefugnis auf den Polizeiführer vom Dienst delegiert werden kann, dann ist das offen gestanden zu vage. Da sollte also nachgearbeitet werden. Es sollte zumindest in der Begründung nachgearbeitet werden, unter welchen Voraussetzungen diese Dinge geschehen dürfen. – Vielen Dank.

Vorsitzender Ulli Hockenberger: Vielen Dank, Herr Professor Kothe. – Ich darf zu Beginn der Fragerunde einen Hinweis geben: Professor Vasel muss uns um 14:45 Uhr aus dringenden terminlichen Gründen verlassen. Das hat er mir heute Morgen mitgeteilt, und wir wollen das natürlich gewährleisten. Ich würde Sie deshalb bitten, sich zunächst auf die Fragen an ihn zu konzentrieren.

Gibt es direkt Fragen an Herrn Professor Vasel? – Frau Goll, bitte.

Abg. Julia Goll FDP/DVP: Vielen Dank. – Ich mache es auch kurz und schnell – vielen Dank an alle für die Stellungnahmen –: Herr Professor Vasel, ich habe an Sie eine ganz konkrete Frage. Sie haben einige Nachbesserungen erwähnt, die man machen könnte. Können Sie bitte noch einmal klarstellen, welche Nachbesserungen Sie aus rechtlicher Hinsicht für unbedingt erforderlich halten und welche Sie – ich sage es bewusst in Anführungszeichen – nur für sinnvoll erachten? Danke schön.

Vorsitzender Ulli Hockenberger: Gibt es weitere Fragen an ihn? – Das ist erkennbar nicht der Fall. – Herr Professor Vasel, bitte.

Herr Dr. Vasel: Ganz herzlichen Dank für die Frage und die Gelegenheit, dazu noch einmal Stellung zu nehmen. Es kommt natürlich auf die Perspektive an: Wenn Sie das Ziel haben, Ihren eigenen und auch den formulierten Ansprüchen gerecht zu werden, dann mag es einiges geben, was da noch einzufügen ist. Wenn Sie nur – in Anführungsstrichen – Karlsruher Vorgaben befriedigen wollen, ist das ein etwas anderer Maßstab – wobei auch der ungewiss ist. Denn einerseits haben wir dieses Grundlagenurteil – von manchen auch als Palantir-Entscheidung bezeichnet – aus dem Februar 2023 vorliegen, was relativ umfangreich ist, was natürlich anschließt an über 40 Jahre Rechtsprechung im Bereich der informationellen Selbstbestimmung und des Sicherheitsverfassungsrechts. Auf der anderen Seite hat auch diese Entscheidung gewisse Dinge offen gelassen.

Eine Sache hat sie aber ganz deutlich gemacht – und da geht sie über die bisherige Rechtsprechung hinaus –, nämlich, dass das Bundesverfassungsgericht geneigt ist, automatisierten Datenanalysen – jedenfalls, wenn sie auch möglicherweise KI-basiert sind – ein spezifisches Eingriffsgewicht zuzusprechen, zuzuschreiben. Dieses spezifische Eingriffsgewicht muss abgesenkt werden, entweder indem man die Eingriffsschwellen höher setzt oder eben eine andere Form von Eingriffsgewichtsabsenkung vornimmt. Im Wesentlichen – das kann man sagen – geht es darum, dass man entweder die Datenherkunft beschränkt oder die Methoden beschränkt. Eine Methodenbeschränkung ist, wenn ich das in Ihrem Gesetzentwurf richtig sehe, nicht vorgesehen. Das finde ich aus technischen Gründen und aufgrund der Dynamik der technischen Entwicklung auch zutreffend und richtig, dass sich der Gesetzgeber da nicht zu sehr den Innovationen verschließt. Aber das heißt, wenn Sie in der Methode keine Begrenzung vornehmen, müssen Sie möglicherweise – aus Karlsruher Perspektive – eine Begrenzung in den Datenplattformen, die angeschlossen werden, oder bei den Daten, die eingespeist werden, vornehmen.

Ich sage das deshalb bewusst vorsichtig, weil das Bundesverfassungsgericht in seinem Grundsatzurteil aus dem Jahr 2023 sehr viele „Je-desto"-Formeln" und Möglichkeiten aufgezeigt hat, wie man diese Eingriffsgewichtsabsenkung vornehmen kann. Insofern obliegt es Ihnen und dem Gesetzgeber, das auszuwählen. Aber, wie gesagt, entweder man müsste die Datenbestände, die man anschließen darf, beschränken oder die Methoden. Ob Sie eine Präferenz für eine dieser Richtungen haben, weiß ich nicht. Die Maßstäbe, die das Bundesverfassungsgericht in der Hinsicht anlegt, sind insofern für beide Richtungen auch noch nicht ganz klar, für die man sich entscheiden kann.

Ihnen ist vermutlich bekannt, dass, soweit ich weiß, auch gegen alle anderen Normen Verfassungsbeschwerden in Karlsruhe anhängig sind, also gegen die Norm in Nordrhein-Westfalen, gegen die Norm in Bayern und auch gegen die novellierte Norm in Hessen. All diese Verfassungsbeschwerden geben natürlich, wenn man sie in ihrem Umfang analysiert, Aufschluss darüber, was da moniert werden kann oder moniert worden ist. Insofern würde ich sagen: Wenn Sie sich auf die sichere Seite stellen wollen, dann wäre möglicherweise eine Aussage zur künstlichen Intelligenz, die benutzt werden kann, Karlsruher Bedenken entgegenwirkend, oder eine noch konkretere Benennung und Begrenzung der Datensilos, die angeschlossen werden können. Das ist aber natürlich kein ganz leichtes Terrain, das in einem Gesetzentwurf sinnvoll und, wie gesagt, entwicklungsoffen zu formulieren.

Vorsitzender Ulli Hockenberger: Vielen Dank, Herr Professor Vasel. Ich sehe dann keine weiteren Fragen an Sie. – Dann hatten sich zunächst der Kollege Seimer und dann der Kollege Gehring gemeldet. – Herr Kollege Seimer, bitte.

Abg. Peter Seimer GRÜNE: Sehr geehrter Herr Vorsitzender, sehr geehrte Kolleginnen und Kollegen, sehr geehrte Gäste! Vielen Dank für die interessanten Ausführungen. Ich möchte noch mal den Blick auf die technische Ebene, den Datenabfluss und das Datenabflussrisiko werfen. Zunächst habe ich die Bitte, ob Sie noch einmal erläutern und klarstellen können, worin sich das Polizeinetz – das CNP-ON – vom herkömmlichen Internet, von der Cloud-Infrastruktur etc. unterscheidet.

Herr Professor Dr. Waidner, Sie haben in Ihrer Stellungnahme sehr deutlich gesagt, dass es technisch ausgeschlossen sei, dass Daten abfließen. So gelte zwar der US CLOUD Act – da Palantir ein amerikanisches Unternehmen ist –, dieser könne aber aufgrund des technischen Ausschlusses, dass Daten abfließen können,

de facto nicht greifen. So ähnlich ist dies seitens des Innenministeriums auch in der Stellungnahme zu dem von Kollegen Binder im August eingereichten Antrag Drucksache 17/9329 formuliert worden; ein Zugriff durch ausländische Stellen sei ausgeschlossen. Ich habe die große Bitte, das noch einmal klarzustellen bzw. auf einer technischen Ebene zu erklären, warum Sie solche Aussagen treffen können.

Abg. Christian Gehring CDU: Geschätzte Kolleginnen und Kollegen! Zunächst möchte ich mich für die Anhörung, die ich richtig und wichtig finde, und für die Statements bedanken. Ich habe jetzt ein, zwei Stichpunkte aufgeschrieben. Professor Dr. Waidner hat gesagt: „Technisch sicher, einwandfrei“. Professor Dr. Vasel hat gesagt: „Sehr gelungener Gesetzentwurf“. Ich habe den Eindruck, dass wir das nicht nur in der Politik und für die Polizei diskutieren, wir bekommen auch mit, dass sich die Privatwirtschaft bezüglich einer Software bei Palantir bedient. Da wollte ich fragen, ob Ihnen bekannt ist, welche Unternehmen aus der Privatwirtschaft ebenfalls eine Software von Palantir beschafft haben und ob es da die gleichen Überprüfungen gab. Denn ich kann mir nicht vorstellen, dass ein großer Industriekonzern sich einfach auf die Aussagen von Palantir verlässt, sondern dies auch hat prüfen lassen.

Abg. Sascha Binder SPD: Herzlichen Dank an die Dame und die Herren, die uns heute Rede und Antwort stehen. Zunächst einmal: Herr Präsident Berger, herzlichen Dank, dass Sie auch das Parlament so in den Mittelpunkt gestellt und gesagt haben, dass Sie, die Polizei in Baden-Württemberg, auch aufgrund dieser Anhörung und des Parlamentsverfahrens gern für diese Demokratie arbeiten. Ich habe mir bei diesen Ausführungen die Frage gestellt: Welche Rolle hat denn das Parlament bei der Beauftragung von Palantir gespielt, zu einem Zeitpunkt, zu dem dieses Parlament noch keinerlei Rechtsgrundlage für diese Möglichkeit hatte? Hat es überhaupt eine Rolle gespielt, oder ist man davon ausgegangen, dass, wenn diese Software bestellt wird – die man ohne Rechtsgrundlage gar nicht einsetzen kann –, das Parlament auf jeden Fall folgt – oder vielleicht auch leichter folgt, wenn man Ausgaben tätigt, die sonst gar nicht zu einem Nutzen kommen?

Im Anschluss habe ich noch die Frage, wie viel Geld das Land Stand heute für diese Software ausgegeben hat – ohne sie bis zum heutigen Tag nutzen zu können.

Eine weitere Frage: Es wurde gesagt – ich glaube, Herr Professor Dr. Waidner hat es angesprochen –, dass es auch noch andere Software aus Frankreich und, ich glaube, aus Polen gibt. Können Sie mir erklären, was mit dieser Software nicht funktioniert in Bezug auf das, wozu wir Ihnen heute eine Rechtsgrundlage geben sollen, was aber mit der Software von Palantir geht, und an welcher Stelle Sie aufgrund dieser Rechtsgrundlage – nämlich dem Gesetzentwurf der Landesregierung – mit der Software anderer Anbieter etwas nicht so umsetzen können?

Professor Dr. Waidner, Sie haben sich schon sehr klar und deutlich ausgedrückt – da gab es ja kaum ein Zaudern –, was die Frage der Sicherheit dieser Software betrifft. Meine Frage geht in die Zukunft: Die Landesregierung sagt, Palantir sei nur eine Übergangssoftware, eine Übergangstechnologie, und man wolle auch die Möglichkeiten der Vertragsverlängerung nicht nutzen, sondern in fünf Jahren unmittelbar auf eine andere Software wechseln – die es Stand heute nach Ihren eigenen Aussagen noch gar nicht gibt. Sie haben auch von erheblichen finanziellen Mitteln gesprochen. Sie sind ja sehr klar in Ihren Aussagen, deshalb hoffe ich auch auf eine klare Aussage zu meiner Frage: Wenn wir in fünf Jahren eine neue Software für die Polizei haben wollen – für die diese Rechtsgrundlage ja die Möglichkeiten schafft –, wie viele finanzielle Mittel sind dafür notwendig? Und wie lange, meinen Sie, dauert es, eine neue Software so zu implementieren, dass es beim Übergang zu dieser Software keinen Qualitätsverlust, aber auch keine Hinderungen im polizeilichen Ablauf gibt? Nach der Gesetzesgrundlage ist ja der gesamte Polizeivollzug von dieser Software betroffen. Vielleicht können Sie uns ganz grob sagen, was eine solche Umstellung in ihrer finanziellen und zeitlichen Dimension bedeutet.

Abg. Julia Goll FDP/DVP: Jetzt habe ich noch Fragen an die anderen Sachverständigen. Auch Ihnen natürlich vielen Dank.

Herr Berger, ich wäre Ihnen dankbar, wenn Sie noch einmal herausstellen könnten, wo Sie genau die Befähigungslücke sehen. Ist das nur eine Frage von – in Anführungsstrichen – Man- bzw. Womanpower? Das Bild ist ja gern verwendet worden, dass die Software oder die Möglichkeit der automatisierten Datenanalyse einfach viele, viele Polizeibeamte ersetzt, die man ansonsten an vorhandene Akten setzen würde. Geht es also tatsächlich nur um die Frage, wo Sie eine Befähigungslücke sehen, oder geht diese Lücke, die Sie beschreiben, noch darüber hinaus?

Die weiteren Fragen sind vielfach schon gestellt worden. Herr Professor Kothe, an Sie habe ich noch eine Nachfrage. Vorab darf ich sagen, dass ich viele der Kritikpunkte, die Sie zum Ablauf – „Was wurde zuerst geregelt, und was kam später?“ – angesprochen haben, teile und auch nachvollziehen kann. Allerdings – und dazu haben Sie sich auch geäußert – befinden wir uns nicht in einem Gesetzgebungsprozess zur Software von Palantir, sondern dazu, im Polizeigesetz die rechtliche Möglichkeit zu schaffen, automatisierte Datenanalyse zuzulassen. Jetzt hat sich Herr Professor Vasel vor allem dazu geäußert, was er an dem Gesetzentwurf gut findet und inwieweit seiner Meinung nach die Anforderungen, die das Bundesverfassungsgericht gestellt hat, erfüllt sind. Können Sie sich dem denn annähern? Jetzt sollen Sie mir kein Gutachten über das Gutachten von Professor Vasel geben, sondern vielmehr eine Aussage darüber, ob Sie seine Meinung teilen, dass der Gesetzentwurf diese Anforderungen doch sehr weitgehend erfüllt.

Sie haben konkrete Dinge genannt, auf die ich auch gern noch mal eingehe. Unbestimmte Rechtsbegriffe: Ja, Sie sagen es selbst, die haben wir immer im Gesetz, da werden wir wohl nicht herauskommen. Sehr konkret waren Sie bei der Delegation auf Polizeiführer, die Sie offenkundig kritisieren.

Dann komme ich zu Ihrer Kritik, man bräuchte eine klarere Bestimmung zu beteiligten und unbeteiligten Personen: Wenn man in das Gesetz einmal hineingeht, dann wäre meine Frage: Haben Sie da konkrete Anmerkungen, wo man etwas nachbessern müsste? Beziehen Sie sich möglicherweise auf den Absatz 4 des neuen § 47a, in dem von einer Verwaltungsvorschrift die Rede ist, die vieles Weitergehende regeln sollte? Sind Sie möglicherweise der Meinung, dass das, was dort für die Verwaltungsvorschrift vorgesehen ist, ansonsten ins Gesetz hinein müsste? Oder – auch diese Möglichkeit besteht natürlich – sind Sie der Meinung, dass man ein solches Gesetz überhaupt gar nicht weitgehend rechtssicher hinbekommen kann?

Vorsitzender Ulli Hockenberger: Vielen Dank. – Ich habe jetzt Fragen an Herrn Präsident Berger, Professor Waidner und Professor Kothe notiert. In dieser Reihenfolge würde ich Ihnen jetzt gern das Wort erteilen. – Herr Präsident Berger, bitte.

Herr Berger: Ich hoffe, ich habe alles mitnotiert – falls nicht, grätschen Sie bitte gleich rein, damit ich alle Ihre Fragen beantworten kann.

Zum Thema Datenaustausch: Das machen wir in Deutschland schon seit sehr vielen Jahrzehnten. Man hat sich also mit dem Thema „Wie tauschen Behörden in Deutschland Daten über die Ländergrenzen aus, und wie machen wir diese Daten sicher?“ schon sehr lange beschäftigt. Das ist jetzt keine Debatte, die aus diesem Diskussionshintergrund kommt, sondern es ist eigentlich eine Standardanwendung, die wir dort machen; der Verbund tauscht schon seit Jahrzehnten Daten mit dem Bundeskriminalamt aus.

Damals hat man sich überlegt: Wie machen wir es sicher? Wir haben in der IT-Sicherheit vier Komponenten – wir kommen vielleicht noch einmal darauf zu sprechen –: Die eine ist der Rechenzentrumsbetrieb, die zweite ist die Übertragung der Daten, die dritte ist natürlich die Software, die wir dort betreiben, und die vierte ist der Faktor Mensch. Auf die dritte Komponente möchte ich auf der Basis Ihrer Frage jetzt nicht eingehen, Herr Seimer, weil Sie ja ganz explizit nach den Netzen gefragt haben.

Man löst das Problem dadurch, dass man für die Polizei ein Fernmeldesondernetz eingerichtet hat. Das heißt, die Polizei konnte ganz normal telefonieren, ohne dass man das öffentliche Netz benutzt, und zwar, indem man einfach deutschlandweit neben das normale Netz eine zweite Leitung gelegt hat. Deswegen hat jede Polizeidienststelle und jeder Apparat eine zweite Nummer.

Übertragen auf die IT ist das natürlich auch so. Das CNP-ON ist ein vom BKA als Zentraldienststelle zur Verfügung gestelltes Netz. Da haben wir – so nennt sich das – drei Konzentratoren, drei Netzübergänge in Baden-Württemberg; da haben wir ein bisschen nachgebessert. Wir verteilen die Daten auf dem CNP-ON, das heißt, auf der unteren Netzebene, und wenn wir andere Netze nutzen, dann haben wir eine Verschlüsselungstechnologie, die auch über den Q-Day hinaus – ich weiß nicht, ob das ein Begriff ist – in der Lage ist, quantenspezifizierte Hackerangriffe abzuwehren.

Es gibt Standards, die macht das BKA, und zwar für alle vier Bereiche, also nicht nur für das Netz. Das heißt, wir übertragen die Daten entweder im eigenen Netz – im CNP-ON – oder in einem speziell geschützten Netz mit ganz, ganz hohen Sicherheitsstandards. Das betreiben wir schon seit Jahrzehnten, und mir ist kein Fall bekannt – und es gibt Kollegen, die länger bei der Polizei sind als ich –, bei dem man über den Netzbetrieb Datenabfluss innerhalb der Polizei aus einem solchen Grund hatte. Damals hat man also ein relativ teures Verfahren gewählt, und das betreiben wir auch heute noch. Das wird irgendwann Diskussionen geben, Herr Seimer, weil es wirklich sehr teuer ist, so ein eigenes Netz zu betreiben.

Aber die Diskussionen haben wir nicht nur hier, sondern auch im Digitalfunk. Da haben wir – ich sage es jetzt einfach mal – einen eigenen Mobilfunk. Da gibt es natürlich immer die Diskussion: Ist es uns das wert, dass wir quasi ein eigener Mobilfunkbetreiber sind? Diese Diskussion kann man führen, aber das ist eine politische, eine finanzpolitische Diskussion, die man führen muss. – Ich hoffe, die Frage ist so weit beantwortet.

Herr Abg. Binder, Sie haben als Thema die Reihenfolge von Palantir und Gesetzgebungsverfahren angesprochen. Ich bin nicht Teil des Gesetzgebungsverfahrens, und ich bin auch nicht dabei, wenn es darum geht, wie weit sich die Regierungsfraktionen auf manche Dinge einigen. Da muss ich Sie einfach bitten, Verständnis zu haben; das weiß ich nicht. Aber klar war: Man hat sich darauf geeinigt, dass die Polizei diese Befähigung braucht, und hat dafür im Zuge der Haushaltsberatungen 2024 für den Doppelhaushalt 2025/2026 erhebliche Mittel eingebracht. Ich sage es mal so: Auf kommunaler Ebene ist es nicht unüblich, dass die Exekutive arbeitet, bevor die Legislative – die Gemeinderäte – z. B. Bebauungspläne beschließt. Ich war 17 Jahre lang Stadtrat. Die Exekutive – die Verwaltung – hat sehr oft schon vorbereitende Maßnahmen getroffen, bevor es dann der Gemeinderat beschlossen hat. – Das soll aber keine Entschuldigung sein.

Vielmehr war klar: Wir hatten da eine Ermessungsproblematik, und zwar lag die einfach darin, dass Ende März 2026 – so ist das vertraglich geregelt – die Kosten für diese Software um 100 % gestiegen wären. Das heißt, das war ein Kostenrisiko von fast 25 Millionen € für den Fall, dass wir diesen Zeitpunkt überschreiten. Dann stellte sich natürlich die Ermessensfrage: Ist diese politische Willensbildung mit dem Risiko, das wir auf der Kostenseite haben, in Einklang zu bringen? Da ist dann die Entscheidung gefallen, dass wir im Prinzip das Kostenrisiko nicht eingehen sollen. Deswegen ist dieser Vertrag zustande gekommen.

Ich sage es mal so: Es geht ja nicht um den Vertrag, sondern es ging ja darum: Sollen wir diese Fähigkeit bekommen oder nicht? Ich bin mir sehr sicher, wir werden noch andere Softwarelösungen in diesem Segment haben, die auf dieser Gesetzesgrundlage fußen, die jetzt gemacht wird. – So viel zum Thema Reihenfolge.

Es ist, Herr Binder, kein Geld an die Firma Palantir geflossen. Wenn es darum geht, was diese insgesamt bereits gekostet hat: Natürlich haben wir vorbereitende Maßnahmen getroffen – Personalkosten bei der Polizei, Personalkosten bei der bayerischen Polizei; es gibt Workshops usw. Aber es ist noch kein Geld an die Firma Palantir überwiesen worden. Im Vertrag steht: ab Betriebsfähigkeit – und die Betriebsfähigkeit ist nicht eingetreten.

Die dritte Frage war, wenn ich es richtig verstanden habe: Was macht die Palantir-Software im Vergleich zu anderen Softwarelösungen so besonders? Warum ist sie besonders gut oder besser? Da gibt es mannigfaltige Themenstellungen – im Prinzip bin ich ja nur der Techniker –, bei denen es darum geht, welche fachlichen Lösungen die Software der Kriminalpolizei – in dem Fall dem Landeskriminalamt

– bietet. Man muss wissen: In der Software ist polizeiliches Erfahrungswissen aus mehreren Dekaden enthalten. Das heißt, die haben diese Software ganz speziell für die Polizei entwickelt. Andere Anbieter haben Software in anderen Segmenten, die sind aber aus der Fachlichkeit anders geprägt. Sie haben ein französisches Unternehmen angesprochen; das kommt aus dem Defense-Bereich. Dessen Fokus war es, Datenanalyse für Militäraufgaben zu machen – das ist halt nicht das Gleiche. Da muss man in der Fachlichkeit abgrenzen. Es ist halt etwas anderes, ob die Schwarz Gruppe ihre Warenströme oder ihre Supply Chains neu ordnet und dafür eine Auswertesoftware einsetzt, oder ob eine Software speziell für die Fachlichkeit – in dem Fall für die Sicherheitsbehörden – da ist.

Da muss man einfach sagen – noch mal: ich bin kein Vertreter von irgendeiner Software; ich kann das nur neutral sagen –: Es ist einfach so, dass die Fachleute, die diese Software nutzen sollen – nicht ich, sondern die Kriminalisten –, sagen: Sie bietet uns immense Vorteile im Bereich der Forensik, also im Bereich der Einbindung von Beweismitteln innerhalb dieses Verfahrens, im Bereich der Darstellung und im Bereich der Datenmigration.

Es geht ja darum: Wie fähig ist die Software, aus verschiedenen Daten ein Portfolio herzustellen, das am Ende des Tages auswertbar ist? Da haben die Fachleute – übrigens bundesweit; das ist jetzt keine Idee aus Baden-Württemberg gewesen; wir sind da nicht allein unterwegs, und die bayerischen Kollegen kommen auch ziemlich ausgeschlafen in die Arbeit – festgelegt, dass im Prinzip diese Fachlichkeit durch die Firma Palantir am besten ist. Deswegen haben die bayerischen Kollegen im Auftrag aller Länder, im Auftrag der damaligen Bundesinnenministerin diesen Vertrag ausgehandelt und unterschrieben; und wir haben aus diesem Vertrag abgerufen. Das heißt, der Grundvertrag – der Rahmenvertrag mit Bayern – ist geschlossen. Wir haben aus diesem Vertrag nun einen sogenannten EVB-IT-Vertrag abgerufen. – Herr Binder, passt das so weit? – Okay.

Frau Goll, Sie haben mich gebeten, die Befähigungslücke genauer zu beschreiben. Die Befähigungslücke hat zwei Elemente: Das eine ist die qualitative Lücke; die haben Sie nicht angesprochen, sondern nur die quantitative. Ich habe die Krawallnacht geführt, und wir haben damals das Beweisportal geöffnet. Das heißt, die Menschen konnten die Videos, die sie bei YouTube eingestellt haben, uns zur Verfügung stellen – Massendaten. Es war ein wahnsinniger Aufwand, diese Massendaten später auch beweisverwertbar und gerichtsverwertbar Tätern zuzuordnen. Sie waren ja selbst Richterin – es ist wirklich ganz schwierig, die Beweiskette so herzustellen, dass wir im Prinzip eine lückenlose Beweisführung machen können. Das ist der quantitative Ansatz. Die Befähigung kann man mit viel, viel Man- und Womanpower decken.

Aber es gibt auch einen qualitativen Aspekt: Menschen werden müde, Menschen müssen nach zwölf Stunden Pause machen, Menschen können nicht 24/7 arbeiten. Das ist genau der Punkt, wo uns die Automation hilft. Die Technik – der Roboter und auch die Technologie – wird nicht müde, und sie liefert eine Auswertequalität rund um die Uhr. Es gilt nicht die Landesarbeitszeitverordnung; es gilt das alles nicht, was wir berücksichtigen müssten, wenn das Menschen machen. Deswegen haben wir die Befähigungslücke auf der einen Seite natürlich in der Auswertung.

Die Lücke, die wir beschreiben, ist nicht allein eine polizeispezifische Lücke. Die hat jeder, der mit Endautomatisierung unterwegs ist: Der Faktor Mensch ist wichtig beim Thema Entscheidungen. Aber hier reden wir darüber, Befähigungen von Entscheidungen herzustellen. Bei der Erstellung, beim Enhancement – „Wie können wir Entscheidungen gut machen?“ – ist halt die Automation momentan einfach das Mittel der Wahl, um Entscheidungen herbeizuführen, die dann durch den Menschen – und zwar ausgeschlafen – –Wenn ich von der KI, die 25 Stunden am Stück gearbeitet hat, einen Vorschlag erhalte, kann ich – ausgeschlafen – diese Ergebnisse nehmen und daraufhin meine Polizeientscheidungen treffen. – Das sind die zwei Lücken. Ich könnte noch mehr ins Detail gehen, aber das ist im Prinzip schlagwortartig das, was wir als Befähigungslücke bezeichnen, quantitativ wie qualitativ. – Ich hoffe, ich habe Ihre Frage damit einigermaßen beantwortet.

Herr Dr. Waidner: Ich versuche es in einer einigermaßen logischen Reihenfolge zu beantworten. Die Frage von Herrn Gehring, wer diese Software noch verwendet, kann ich nicht beantworten. Ich bin kein Berater von Palantir oder sonst irgendwas; ich habe da also keine tieferen Einsichten. Man kann lesen, dass Palantir ungefähr die Hälfte seines Umsatzes mit kommerziellen Unternehmen macht. Neben „Gotham“ haben sie auch noch ein Produkt, das sich „Foundry“ nennt – das ist so was Ähnliches für die Wirtschaft. Aber welche Unternehmen auf eine Software von Palantir zurückgreifen und wie diese ihre Qualitätssicherung machen, kann ich bei bestem Willen nicht sagen. Bei manchen weiß ich, dass sie „Foundry“ einsetzen; mehr kann ich dazu aber nicht sagen.

Es ist vielleicht interessant, wenn man sich mal kurz klarmacht, wie groß Palantir eigentlich ist. Palantir hat einen Jahresumsatz – das habe ich gerade nachgeschaut – zwischen 2 und 3 Milliarden US-Dollar. Sie sind nicht so groß wie SAP, aber deutlich größer als die Software AG – das frühere zweite große deutsche Unternehmen im IT-Bereich.

Für die anderen Fragen muss man wissen, was Herr Berger wahrscheinlich macht, wenn er irgendeine Software in dem Gebiet kauft und einsetzt. Wenn man das Wort „Software“ hört, dann stellt man sich typischerweise so etwas vor wie Windows, Microsoft Office oder Microsoft 365. Aber die Datenanalysesoftwareprodukte von Palantir, ArgonOS oder DataWalk usw. funktionieren ganz anders. Typischerweise ist es so: Im Sicherheitsbereich kommen die nicht als irgendein Cloudservice, den man sich herunterlädt oder so, sondern es gibt eine Packliste mit sehr viel Hardware – das sind ein paar Decks voll mit Servern. Dort wird diese Software einmal draufgespielt, und dann wird sie isoliert in einem Rechenzentrum – in diesem Fall im Rechenzentrum der Polizei – betrieben.

Wenn man diese Software nun betreiben möchte, besteht ein großer Teil des Projekts darin, dass man die Daten, die man hat, überhaupt in diese Software hineinbekommt. Ein großer Teil des Projekts, das Ihre Polizei durchführen muss, besteht darin, dass man die Datenquellen beschreibt; ganz viele von denen sind unstrukturiert. Das sind nicht irgendwelche Datenbanken oder XML-Files, sondern das sind beispielsweise Protokolle oder Mitschriften – also unstrukturierte Daten, die man mit etwas übersetzen muss. Firmen wie Palantir, aber auch ein paar andere haben dabei sehr viel Erfahrung, wie das in bestimmten Domänen aussieht, was also das Vokabular der Polizei ist und wie die typischen Vorgänge der Ermittlungsbehörden aussehen. Das wird alles beschrieben. Das nennt man Ontologie und Verfahrungsbeschreibung. Dafür muss man alles aufbereiten. Das verursacht sehr viel Aufwand und kostet Geld – Herr Berger kann vielleicht sagen, wie viel Aufwand und Geld das ist; ich kann es nicht. Das ist wirklich der große Aufwand, wenn man in ein solches System einsteigt.

Wenn man jetzt in fünf Jahren auf ein anderes System umsteigen wollte, braucht man in gewisser Weise gerade dasselbe noch einmal für das andere System. Es wird aber aller Wahrscheinlichkeit sehr viel günstiger werden, da sich zumindest die Polizei schon einmal diese ganze Arbeit gemacht hat. Man muss es dann wir von dem einen System auf das andere System umziehen; das ist immer noch sehr viel Arbeit – wer jemals z. B. eine SAP-Migrierung mitgemacht hat, weiß, wovon ich spreche –, aber es ist dann nicht mehr ganz so viel. Wie viel Geld das wäre – da müsste ich dann wieder an Herrn Berger verweisen.

Jetzt gab es öfter, auch von Herrn Kothe, den Hinweis auf den US CLOUD Act und wie das sein kann. Das kann schon so sein, wie ich es gesagt habe. Typischerweise werden solche Systeme in einem Rechenzentrum betrieben. Das Rechenzentrum hängt zwar im Netz der Polizei, weil die Polizei ja Zugriff auf das System haben und Anfragen stellen will; das Kernsystem ist aber getrennt. Die Daten kommen nicht über irgendwelche Verbindungen etwa aus dem Internet, sondern werden – typischerweise für solche Systeme – sozusagen von Hand migriert. Es gibt eine Datenbank, die kopiert man einmal rüber und dann regelmäßig wieder; dann wird diese eingelesen und in das große System des jeweiligen Anbieters überführt. Das läuft aber alles im Rechenzentrum der Polizei.

Jedes System, auch dieses, braucht Updates. Das ist immer die große Frage, und die Hersteller haben es auch ganz gern, wenn sie hin und wieder in das System

schauen können und sehen, was dort passiert. Bei so einem Datenanalysesystem für die Polizei macht man das nicht; es gibt beispielsweise keine Telemetriezugänge oder so etwas in der Art. Wenn es eine Wartung gibt, dann macht das der Betreiber typischerweise selbst. Man hat auch nicht einen Fernzugang für den Hersteller, sondern man geht als Betreiber, als Polizei, hin und macht das alles. Die Updates, die man braucht, werden regelmäßig eingespielt – entweder ganz altmodisch über beispielsweise DVDs oder CDs; häufiger gibt es Geräte, die man Datendioden nennt. Diese sind technisch so konstruiert, dass Daten nur von außen nach innen gehen, nicht von innen nach außen – das ist tatsächlich technisch. Eine Datendiode muss man sich so vorstellen: Auf der einen Seite – außen – gibt es einen Sender, der Lichtsignale aussendet. Auf der anderen Seite gibt es einen Sensor, der die Lichtsignale entgegennimmt. In die Gegenrichtung gibt es aber nichts; deswegen kann auch keine Information in die andere Richtung fließen. In diesem Sinn kann man wirklich sagen: Wenn das Polizeinetz sicher ist, dann fließen definitiv keine Informationen nach außen, wenn man das so aufsetzt. – Wie die Polizei Baden-Württemberg das jetzt aufsetzt, weiß ich natürlich nicht.

Der letzte Punkt ist – ganz technisch gesehen –: Wenn der Hersteller auf die Idee kommt, nicht mehr weitermachen zu wollen, wenn er in Konkurs geht, verkauft wird, oder wenn uns z. B. ein Hersteller in den USA einfach nicht mehr mag, und es dann keine Updates mehr gibt, dann haben wir natürlich früher oder später ein Problem. Ohne Updates sollte man solche Systeme nicht weiterlaufen lassen. Aber das ist das einzige technische Problem – das man bei solchen Systemen eigentlich immer hat.

Dass keine Daten herausfließen können, kann man tatsächlich technisch absichern. Dazu muss natürlich das Polizeinetz insgesamt sicher sein; das wiederum muss es aber sowieso sein. Wenn das nämlich nicht sicher ist, dann haben Sie ein größeres Problem als das, dass der Hersteller auf irgendein System zugreifen kann. – Ich glaube, dass ich damit die Fragen beantwortet habe, wenn nicht, müssen Sie mich erinnern.

Herr Dr. Kothe: Ich habe es so gesehen relativ einfach, weil ich nur Ihre Frage beantworten muss, Frau Goll. Sie hatten so schön formuliert, ob ich mich der Auffassung von Herrn Vasel annähern könnte. – Annähern? Ja, kein Problem. Der Punkt ist der: Das Bundesverfassungsgericht sagt, im Gesetz selbst ist zu regeln, welche Datenbestände einbezogen werden. Genau da könnte man bei diesem Gesetzentwurf durchaus noch nachbessern – wenn ich mir z. B. den § 47a anschaue, dann betrifft das die von mir angesprochenen unbestimmten Rechtsbegriffe. Ein einfaches Beispiel: wenn dies zur Abwehr einer Gefahr für Leib und Leben usw. erforderlich sei. Auch jede Wirtshausschlägerei ist eine Gefahr für Leib und Leben. Das kann also nicht gemeint sein – hoffe ich zumindest. Aber hier sind eben unbestimmte Rechtsbegriffe drin. Oder die „Sachen von bedeutendem Wert“, die geschützt werden sollen: Welche sind das? Sind das nur Infrastruktureinrichtungen, die wichtig sind, die geschützt werden sollen? Es steht weder im Gesetzentwurf noch in der Begründung. – Wir hatten eine ähnliche Diskussion schon bei früheren Änderungen des Landespolizeigesetzes.

Das Nächste, was wir hier haben, ist „Straftat von erheblicher Bedeutung“ – die sind auch nicht definiert. Welche Straftat ist von erheblicher Bedeutung? Das könnte ich zumindest in der Begründung einschränken, indem ich sage: Es muss ein bestimmtes Strafmaß darauf stehen, wenn denn diese Straftat verwirklicht wird. Auch das haben wir hier nicht.

Insofern: Ja, ich kann mich ihm annähern. Es wäre interessant gewesen, wenn er auch noch die Negativpunkte hätte schildern können, wozu er aus Zeitgründen nicht mehr gekommen ist; das hätte mich dann auch interessiert. – Aber zu den unbestimmten Rechtsbegriffen, die hier sind: Ich habe keine Probleme damit, wenn die Voraussetzungen dafür definiert sind, dass auch der Polizeiführer vom Dienst eine solche Anordnung treffen kann. Aber diese Voraussetzungen sind dank eben dieser unbestimmten Rechtsbegriffe aus meiner Sicht nicht eindeutig festgelegt.

Außerdem: Vieles in einer Verwaltungsvorschrift zu regeln, halte ich für bedenklich. Wenn, dann sollte so was bitte in einer Rechtsverordnung geregelt werden. Natürlich kann der Gesetzgeber das auf den Verordnungsgeber delegieren – keine

Frage –, aber doch bitte nicht in einer Verwaltungsvorschrift. Selbst wenn sie veröffentlicht wird – sie ist und bleibt ein Verwaltungsinternum.

Zu den Updates hat Herr Waidner gerade etwas gesagt: – Gut, das mag so sein. „Die Worte hör´ ich wohl, allein mir fehlt der Glaube“ – wenn ich das so sagen darf.

Was mich auch noch stört: Natürlich steht im Gesetzentwurf – da Sie mich nach einem konkreten Beispiel fragten –, es sollten diskriminierende Algorithmen ausgeschlossen werden. Wie wird das gewährleistet? Dazu habe ich keine Antwort gefunden, weder im Gesetzentwurf noch in der Begründung. Auch auf die Gefahr hin, dass mir Herr Berger dafür vielleicht böse ist: Wenn ich an die Anhörung zur elektronischen Fußfessel denke, bei der wir uns auch über die personellen Mittel und die Möglichkeiten der Polizei in diesem Zusammenhang unterhalten haben, dann frage ich mich, wie das gewährleistet werden soll. – Ich denke, damit habe ich Ihre Frage beantwortet.

Vorsitzender Ulli Hockenberger: Herr Berger ist nicht in der Lage, in einer öffentlichen Anhörung böse mit Ihnen zu werden. Da müssen Sie sich keine Sorgen machen.

(Herr Berger: Auch sonst nicht!)

Es hat sich noch der Kollege Karrais gemeldet.

Abg. Daniel Karrais FDP/DVP: Vielen Dank an die Sachverständigen. Ich habe präzisierende Nachfragen, und zwar zunächst an Herrn Polizeipräsident Berger: Sie hatten das Beispiel mit der Krawallnacht angeführt und dass man da natürlich eine schnellere Auswertung erreichen kann. Auf der Grundlage dieser Schilderungen: Welche Daten werden denn da genutzt? Nach meinem Verständnis waren das immer „Eh da“-Daten – sprich: Daten, die die Polizei schon hat, und nicht irgendwelche zusätzlichen Daten, die durch den Einsatz von Palantir oder irgendeiner anderen Software beschafft werden. In der öffentlichen Diskussion wird manchmal der Eindruck erweckt, dass dann irgendwelche Social-Media-Geschichten automatisiert ausgewertet oder sonstige Verzeichnisse, die sonst irgendwo beim Staat sind, durchforstet werden. Dazu können Sie sicherlich etwas sagen.

Hierzu auch die Frage an Herrn Professor Kothe: Sehen Sie in dem Gesetzentwurf die Möglichkeit, dass Onlinedurchsuchungen durchgeführt werden können, oder sehen Sie dies nicht?

Ich bin schon einigermaßen erstaunt über Ihre Einschätzung, Herr Professor Kothe, bezüglich der technischen Sicherstellung der Sicherheit. Ich gehe davon aus, Sie haben einen sehr hohen juristischen Sachverstand; ich bin mir aber unsicher, ob Sie mit „Die Worte hör´ ich wohl, allein mir fehlt der Glaube“ eine fundierte Bewertung der tatsächlichen technischen Sicherheitslage darstellen können. Vielleicht können Sie das auch noch mal richtigstellen; ich finde das zumindest mal fragwürdig.

Die Ausführungen von Herrn Professor Waidner habe ich so verstanden – das können Sie vielleicht mit einem kurzen „Ja“ oder „Nein“ oder gegebenenfalls mit einer kurzen Begründung, warum nicht, beantworten –, dass im Regelfall – das wird ja technisch von Fachleuten durchgeführt – ein Datenabfluss auch nach Updates deshalb ausgeschlossen ist, weil es in einem separaten Netz stattfindet und weil bei solchen Updates dies der Betreiber, also die Polizei, selbst durchführt und diese Updates entweder über DVDs, die nur in eine Richtung ausgelesen werden können, oder eben über diese Diodentechnik aufgespielt werden, bei der auch nur in eine Richtung kommuniziert werden kann. Wenn Sie das noch einmal kurz bestätigen, wäre ich Ihnen sehr dankbar.

Abg. Sascha Binder SPD: Zunächst einmal: Professor Dr. Waidner, eine Frage ist noch offen, und zwar die Frage, ob Sie davon ausgehen – unabhängig davon, ob Sie beziffern können, was das an Entwicklung kostet, unabhängig davon, ob Sie uns darstellen können, wie lange die Implementierung der Software dauert –, dass es innerhalb von fünf Jahren überhaupt möglich ist, eine Software zu kreieren, die

den gleichen Standard hat wie die Software, die Palantir anbietet. Darauf haben Sie bisher noch nicht geantwortet.

Herr Präsident Berger, wir haben jetzt unterschiedliche Begrifflichkeiten zu dem Vertrag vorliegen. In dem von mir gestellten Antrag Drucksache 17/9329 hat die Landesregierung von der „Bereitstellung der Software“ gesprochen. Sie haben jetzt von der „Betriebsfähigkeit“ gesprochen. Für mich stellt sich die Frage: Wenn Sie die nächsten fünf Jahre keine Rechtsgrundlage haben, um diese Software einzusetzen, heißt das dann, dass diese Software nicht betriebsfähig ist und damit der Vertrag nicht in Gang gesetzt wird? Oder reicht es, wenn Palantir die Software bereitstellt – ohne dass sie funktionieren soll –, und dann wird trotzdem Geld abgebucht? Denn wenn es nur um die Betriebsfähigkeit ginge, käme der Vertrag, solange Sie die Betriebsfähigkeit nicht herstellen, ja nicht ins Laufen, und Sie müssten kein Geld zahlen, und der Gesetzgeber könnte noch einmal frei entscheiden, was er jetzt tut. Das wäre ja eine Möglichkeit; nur sind wir bislang von anderen Begrifflichkeiten und von einer anderen Vertragslage ausgegangen.

Dann habe ich noch eine Frage zu dem Thema „Wie seriös ist Palantir, welche Rolle hat Palantir?“. Sie haben es vorhin gesagt: Wir haben mehrere Dimensionen – die Dimension „Mensch“ haben wir ja auch noch. Die Frage ist: Wie gehen Sie denn mit Mitarbeiterinnen und Mitarbeitern von Palantir um? Darf da jeder an diesen Server? Laut der Stellungnahme zu meinem Antrag – ich habe es nicht mehr ganz im Kopf, deshalb kann ich es nicht mehr wörtlich zitieren – sei es normalerweise nicht üblich, dass Mitarbeiter von Palantir unbeaufsichtigte Zutrittsmöglichkeiten in das Rechenzentrum haben. Wenn man sich die Dokumentationen – Sie verweisen immer auf andere Bundesländer – dazu anschaut, dann sitzen dort verdammt viele Leute von Palantir an den Polizeiservern. Was sagen Sie dazu? Welche Sicherheitsvorkehrungen treffen Sie bei der Dimension Mensch?

Und zuletzt: Neben der Verheißung, dass es in fünf Jahren eine andere Software gibt, gibt es eine noch weitere Verheißung, nämlich dass das Parlamentarische Kontrollgremium für den Verfassungsschutz weitere Kompetenzen erlangen soll. Was glauben Sie, wie viele Maßnahmen Sie dem Parlamentarischen Kontrollgremium vierteljährlich vorlegen können und in welcher Tiefe dieses Ihre einzelnen Analysen überprüfen kann?

Abg. Peter Seimer GRÜNE: Ich hätte noch einmal die Nachfrage an Sie, Herr Berger, weil Sie vorhin das Netz sehr detailliert beschrieben haben – dafür danke ich Ihnen –: Können Sie noch einmal darstellen, ob die „Gotham“-Daten ausschließlich über das CNP-ON laufen oder auch über diese Verschlüsselungen, bei denen Sie gesagt haben, die wären ebenfalls quantensicher?

Abg. Daniel Karrais FDP/DVP: Ich habe eine Frage vergessen – Entschuldigung –, und zwar an Herrn Professor Kothe. Sie hatten in Ihrem Eingangsstatement kritisiert, dass man ja nicht so genau wisse, welche Daten von wem wie oft von wie vielen Menschen gesammelt bzw. ausgewertet werden. Jetzt habe ich in meiner Funktion als Gesetzgeber ein bisschen das Problem, dass ich das beispielsweise beim Landesamt für Verfassungsschutz auch nicht so genau weiß. Die können bestimmte Maßnahmen ergreifen – alles natürlich im Rahmen der Gesetzeslage –, aber auch da habe ich ja keine Quantifizierung dessen, was gemacht wird. Würden Sie dann sagen, dass das Verfassungsschutzgesetz ein schlechtes Gesetz ist?

Herr Berger: Es waren jetzt doch eine Vielzahl an Fragen. Ich hoffe, dass ich das alles auf die Reihe bekomme.

Herr Karrais, wir erheben keine neuen Daten, sondern wir machen die Daten, die wir haben, auswertbarer. Ich sage Ihnen ein Beispiel – Sie haben es bezogen auf die Krawallnacht –: Das Delikt, das im Raum stand, war schwerer Landfriedensbruch. Schwerer Landfriedensbruch hat bestimmte Tatbestandsvoraussetzungen, die das gegenseitige Mitwirken, z. B. in einer Gruppe, beinhalten. Herauszufinden, ob diese Gruppe z. B. bereits vor diesem Tag in Gemeintäterschaft oder in Abhängigkeit Straftaten begangen hat, hilft uns natürlich nachher in der Beweisführung.

Die Herausforderung besteht darin, all diese Tatbestandsmerkmale aus der Masse an Daten, die wir bereits haben – keine Datenerfassung –, mit den Ermittlungser-

kenntnissen in Einklang zu bringen, als Ergänzung. Da ist es halt so: Wir haben auf der einen Seite ein Auswerteproblem. Damit hat Palantir hat nichts zu tun; die Auswertung von Videodaten hat mit Palantir zunächst mal nichts zu tun, sondern die Verknüpfung dieser Ermittlungserkenntnisse mit dem Bestand, den wir haben, im Ermittlungsverfahren, um sie dann der Justiz zu übergeben, das ist der Mehrwert, den wir haben – im Bestand, also nicht neu, sondern im Bestand.

Auf die Krawallnacht bezogen: Wir haben die Personen über Auswertungen festgestellt und müssen dann das Delikt des schweren Landfriedensbruchs nachweisen. Da hilft es uns natürlich, wenn wir diese Daten, die im Bestand sind – z. B. über Vortaten –, im Prinzip schnell ermitteln können. In Bayern etwa gab es diesen Anschlag, wo relativ schnell klar war, über die Auswertung durch Palantir der Bestandsdaten, dass es mit großer Wahrscheinlichkeit ein Einzeltäter ist und nicht ein Gruppierungsdelikt.

Herr Binder, zur Rechtsgrundlage – Polizeigesetz –: Es gibt verschiedene Rechtsgrundlagen zum Einsetzen von Auswertesoftware. Wenn morgen der Bund in der Strafprozessordnung die Möglichkeit schafft, dann müssen wir auch in der Lage sein, das zu tun. Wir reden jetzt hier vom Polizeigesetz Baden-Württemberg, aber es gibt natürlich auch noch andere gesetzliche Grundlagen, die uns irgendwann – vielleicht aus einem Bundesgesetz heraus – die Möglichkeit geben, Daten zu erheben. Da wäre es gut, wenn der Gesetzgeber diese geschaffen hat, damit wir nicht Jahre brauchen, um die auch anzuwenden. Das heißt, die Fähigkeit zu haben, ist wichtig; denn was nützt mir das beste Gesetz, wenn ich danach nicht fähig bin, es umzusetzen? – Das ist die Sichtweise darauf.

„Betrieb“ bedeutet: Die Firma Palantir hat alles getan, um den Betrieb zu machen; um das geht es. Sonst könnte ich – im Prinzip ist es ja wie beim Bau – die Bezahlung des Baus so lange hinauszögern, bis ich keinen Fehler mehr finde. – Nein, Betriebsfähigkeit heißt, dass Palantir nachweislich alles getan hat, dass wir es betreiben könnten. Falls ich mich da missverständlich ausgedrückt habe, dann tut es mir leid; das war nicht mein Ziel.

„Faktor Mensch“ – das ist eine Frage, die trifft uns alle, die wir hier in Führungsverantwortung sind. Wie können wir sicherstellen, dass Leute, die wir in den Staatsdienst übernehmen oder die für uns arbeiten, am Ende des Tages nicht schädlich sind? Wir haben die gängigen Methoden: Es gibt Geheimschutzvorschriften, was diese Menschen machen müssen. Es gibt Sicherheitsüberprüfungen. Da gibt es verschiedene Stufen: Wir verlangen die Sicherheitsüberprüfungsstufe 2 für die Mitarbeiter, die dort drin sind. In dem Fall ist es so: Wir versuchen, die Personen, die bei uns hineinwollen – da wir unser Rechenzentrum in Hessen betreiben, ist es das hessische Überprüfungsmodell; das ist aber das gleiche Modell wie in Baden-Württemberg –, behördlich zu prüfen. Das bezieht sich z. B. auf den kriminalistischen Background dieser Personen, aber auch auf andere Dinge, die sie angreifbar machen, Schulden oder anderes. – Also: Die müssen SÜ-überprüft sein.

Wenn Sie mich heute fragen: „Können Sie das ausschließen?“, dann sage ich Ihnen: Nein. Keiner von uns – Sie sind Führungskraft, ich bin Führungskraft – kann ausschließen, dass sich Mitarbeiter oder andere Personen inkriminieren lassen und Dinge tun, an denen wir zwar nicht schuld sind, für die wir aber immer die Verantwortung tragen. Das heißt, Mitarbeiter tun Dinge – –

Abg. Sascha Binder SPD: Nur dass Sie mich da richtig verstehen: Mir ging es nicht um Ihre Mitarbeiter, sondern um die Mitarbeiter von Palantir.

Herr Berger: Das ist genau das Gleiche. Wenn wir Leute in unsere Organisation reinholen, dann müssen die die gleichen Standards erfüllen wie unsere eigenen Leute – das ist die Grundidee. Da haben wir relativ hohe Sicherheitsstandards, was diese Themen angeht. Ich hoffe jetzt einfach, dass das so ist. Aber ich bin auch ganz ehrlich: Wenn Dienste Schwachstellen von Menschen finden und ausnutzen können, dann gibt es da keine hundertprozentige Sicherheit – und das wahrscheinlich nirgends.

Dann wurde noch die Frage nach der PKG-Tiefe gestellt, also wie tief das gehen soll. Ich kenne das PKG noch aus einer Vorverwendung. Das ist ein sehr selbstbe-

wusstes Gremium, das die Tiefe seiner Durchsetzung selbst bestimmt; damals war das jedenfalls so. In dem Gremium haben die Gremiumsmitglieder auch deutlich gesagt, was sie wissen wollen. Ich kann mich nicht erinnern – aus der Zeit, als ich noch im Ministerium war –, dass man den PKG-Kollegen keine Auskunft gegeben hätte. Das wüsste ich nicht. Das PKG kann so tief fragen, wie sie es für notwendig halten, und wir werden antworten.

Herr Binder – seien Sie mir nicht böse –, die Frage „Wie viele Fälle werden das sein?“ ist eine spekulative Frage. Ich hoffe, gar keiner. Am liebsten wäre mir, wir könnten berichten, wir hätten keinen einzigen Fall gehabt. Ich kann es Ihnen aber nicht sagen; das ist rein spekulativ.

Zum Thema Polizeigesetz möchte ich eine Anmerkung machen, und zwar als einer, der das Polizeigesetz weder entworfen noch geschrieben oder dort Paragrafen eingefügt hat: Im Polizeigesetz ist das Rechtssystem so, dass wir Spezialnormen haben, aber auch Generalnormen. Das, was Sie sagen, Herr Professor Kothe, fällt u. a. in den Bereich des § 5 – Verhältnismäßigkeit. Die ist nämlich immer zu prüfen, und zwar bei allen Eingriffsmaßnahmen. Bei einer Kneipenschlägerei, die jetzt vielleicht die objektiven Tatbestandsmerkmale erfüllen würde, gibt es immer noch den Grundsatz der Verhältnismäßigkeit und des Mindesteingriffs, der ebenfalls zu berücksichtigen ist. Deswegen ist die Prüfung zweigeteilt: spezialnormmäßig, aber auch die Generalnorm ist zu überprüfen.

Zur Befähigungslücke habe ich Frau Goll geantwortet. – Herr Binder, ich hatte mir hierzu auch Ihren Namen noch notiert. – Okay.

Vorsitzender Ulli Hockenberger: Herr Binder ist so selbstbewusst: Wenn etwas vergessen wird, fragt er selbst nach.

(Heiterkeit – Zuruf des Abg. Peter Seimer GRÜNE)

– Jetzt langsam. Wir machen erst die Antwortrunde fertig, dann geht es weiter. – Herr Professor Waidner, bitte.

(Abg. Peter Seimer GRÜNE: Meine Frage noch!)

– Direkt dazu? – Ah, bitte.

Herr Berger: Herr Seimer, die Netze – Entschuldigung! Die Netze müssen die Qualitätsstandards des BKA erfüllen. Wenn wir die nicht bekommen, dann ist der Teufel los; das kann ich Ihnen sagen – da gibt es dann richtig viele Scherereien. Da gibt es nämlich auch die Monitoringteams, die genau das überprüfen. Ich sage es jetzt mal so: Wir versuchen, das Ganze über das CNP-ON abzubilden. Wenn das mengenmäßig nicht geht, müssen wir andere Wege nehmen über kryptierte Leitungen – spezielle einzelne Leitungen der Telekom –, die dann die gleichen Standards haben wie das CNP-ON.

Als das CNP-ON geboren wurde, Herr Seimer, da war die IT noch ein bisschen anders. Es ist natürlich schon so, dass der limitierende Faktor auch die Übertragungskapazitäten sind. Das ist ein bisschen wie beim Streaming daheim: Früher bin ich mit 20 Mbit/s ganz gut zurechtgekommen, heute geht das nicht mehr. Deswegen kann ich es nicht ausschließen, dass wir beides nutzen. Aber ich kann Ihnen sagen: Alles ist nach den gleichen Sicherheitsstandards abgesichert.

Herr Dr. Waidner: Herr Karrais wollte auch noch ein Nicken oder ein „Ja“ haben. Das kann ich beherzt sagen.

Ich will noch einmal kurz sagen: Kann man das physikalisch trennen? Ich kann nur sagen: Die Polizei kann ein System so betreiben, dass das System – das von Palantir oder welches auch immer – physikalisch getrennt ist und dass definitiv keine Daten über diese Ecke herausfließen und in die USA wandern oder in der Hoheit von Palantir oder wem auch immer sind. Dementsprechend greift auch der US CLOUD Act nicht, weil da nichts ist, auf das er angewandt werden könnte. Das ist eine physikalische Aussage, die man, glaube ich, schlecht hinterfragen kann. – Die anderen, logischeren Sachen hat Herr Berger gerade genannt.

Herr Binder, ich hatte die Frage tatsächlich überhört. In fünf Jahren eine Alternative zu Palantir neu zu entwickeln ist mit hinreichend viel Geld machbar; das ist gar keine Frage. Ich hatte vorhin kurz gesagt, wie groß Palantir ist – das hatte ich auch mit dem Hintergedanken gesagt, dass man sich einfach mal vorstellt, wie viel Aufwand das ist. Das ist sicherlich ein Betrag, der kein kleiner zweistelliger Millionenbetrag ist, sondern eher größer ausfällt.

Man kann sich natürlich überlegen, das ganz neu zu implementieren. Das Unternehmen secunet – das ist das größte deutsche Sicherheitsunternehmen für digitale Produkte – hatte vor, ich glaube, zwei Jahren einmal angekündigt, sie würden das tun, und haben es dann abgebrochen, weil sie keine öffentliche Zusage hatten, dass das Skript auch verwendet wird. Dieser Markt ist wirklich klein – es gibt jetzt nicht so viele Polizeibehörden auf der Welt. Niemand geht freiwillig in diesen Markt hinein, wenn er sich nicht sicher ist, dass er kommerziell auch Erfolg hat.

Es gibt natürlich existierende Produkte aus Frankreich, es gibt ein polnisch-amerikanisches Unternehmen und noch ein paar andere. Die kenne ich nicht so gut. Die könnte man vielleicht aufbauen und auf deren Grundlage dann etwas machen. Wie viel das kostet, weiß ich nicht. Aber wir reden da wirklich von größeren Millionenbeträgen – deutlich mehr, als die Polizei in Deutschland z. B. für die Software von Palantir jährlich investieren muss. Das sind schon große Beträge, die man in die Hand nehmen müsste.

Vorsitzender Ulli Hockenberger: Vielen Dank, Herr Professor Waidner. – Jetzt waren noch Sie gefragt, Herr Professor Kothe. Ich glaube, „Die Worte hör´ ich wohl, allein mir fehlt der Glaube“ war das Intro.

Herr Dr. Kothe: Das war die Provokation, die ich eben untergebracht habe und auf die Sie auch prompt reagiert haben.

(Zuruf des Abg. Daniel Karrais FDP/DVP)

Wenn es denn so ist – wie uns gerade eben noch einmal erklärt wurde –, dass es ein physikalisch abgetrenntes System ist, dann ist das sicherlich richtig. Wir haben eben aber auch gehört, dass in anderen Behörden durchaus Mitarbeiter von Palantir tätig sind, um die Updates aufzuspielen. Deswegen hatte ich mir erlaubt, das so provokativ zu formulieren. Wenn es denn anders gesichert ist, sei´s drum.

Ich war außerdem noch mal provokativ, als ich das Beispiel mit der Kneipenschlägerei brachte. Natürlich haben Sie recht, Herr Berger, dass es einen Verhältnismäßigkeitsgrundsatz gibt, der immer zu beachten ist – keine Frage. Aber es war nur eines der Beispiele aus dem Katalog, der für diese Datenerhebung, Datenverknüpfung möglich sein soll – womit ich noch einmal auf das rekurrieren wollte, was ich vorhin sagte: dass mir eben jegliche Eingrenzungen für die „Sachen von bedeutendem Wert“ und „Straftaten von erheblicher Bedeutung“ fehlen.

Deswegen hatte ich jetzt ganz bewusst provokativ dieses Beispiel gebracht. Natürlich kann ich es mir lebhaft vorstellen: Dann sitzt am Sonntagnachmittag – Gefahr im Vollzug – der Polizeiführer vom Dienst da und fragt sich, ob es jetzt im Rahmen der Verhältnismäßigkeit ist, eine bestimmte Maßnahme anzuordnen – und das ohne jegliche Handhabe, die ihm das Gesetz oder die Begründung vorgibt. Allein die Verhältnismäßigkeit – es ist ein weites Feld. Dass das Probleme geben wird und geben kann: Ich glaube nicht, dass Sie mir da widersprechen werden.

Sie hatten noch nach den Online-Durchsuchungen gefragt, Herr Karrais. Wenn Sie mit Online-Durchsuchungen meinen, dass das System beispielsweise Social-Media-Accounts durchsuchen könnte, dann muss ich Ihnen sagen: Nein, das sehe ich in diesem Zusammenhang nicht. Aber: Was ist denn mit landesfremden Daten gemeint, die durchaus mit erhoben und untersucht werden können? Dafür habe ich auch keine Begründung gefunden.

Dann haben wir gerade diese Krawallnacht angesprochen und dabei die Videoaufnahmen erwähnt, die dort zur Verfügung gestellt wurden. Sind das dann Asservaten, die auch durchsucht werden können? Dann habe ich zwar keine Online-Durchsuchung in dem Sinne, dass ich jetzt aktiv von hier aus auf Social-Media-Accounts

zugreife, aber ich habe Vorgangsdaten, die vorhanden sind und die ich auswerten kann. Ist es das, was ich will? – Sie sehen es: Ich missgönne der Polizei dieses Instrument nicht. Ich meine nur, man muss es rechtstaatlich an den entsprechenden Stellen eingrenzen.

Das führt uns auch zu Ihrer letzten Frage. Über das Landesverfassungsschutzgesetz haben wir an anderer Stelle schon diskutiert. Der Punkt ist, dass man die Befugnisse – insbesondere dann, wenn es um den Einsatz von KI geht – durch eine ausreichend oder hinreichend konkrete Bestimmung von Zweck und Zielen eingrenzen muss. Denn wir wissen alle, dass KI auch halluziniert. Es müssen meines Erachtens Grenzen eingezogen werden, damit der Polizeibeamte, der entscheidet – völlig egal, ob es jetzt an der obersten Führungsebene ist oder der Polizeiführer vom Dienst, der entscheiden muss –, weiß, bis wohin er gehen kann oder was seine Ermächtigungsgrundlage auslöst und was nicht. Das ist gemeint.

Herr Berger: Weil das Thema KI gerade noch einmal aufkam und Sie das mehrfach betont haben, muss ich klarstellen, dass in der Software von Palantir – so, wie wir sie nutzen werden – keine KI enthalten ist. Das, was wir nutzen, ist keine künstliche Intelligenz. Wir nutzen jetzt nicht irgendeine Form von künstlicher Intelligenz – weil das jetzt immer wieder aufgekommen ist. Das ist keine KI, und wir nutzen auch keine KI. Der Schritt zur Nutzung der KI hat natürlich noch höhere Problemstellungen, da ich, wenn ich die KI nutze, zwangsläufig auch andere Infrastrukturmaßnahmen benötige, über die wir heute noch gar nicht gesprochen haben. Das, was wir nutzen wollen, ist das Produkt „Gotham“ von Palantir, und das hat keine KI-Komponente enthalten. Das ist wichtig.

Das Zweite ist – das ist mir noch mal wichtig zu betonen, weil das mit dem „Polizeiführer vom Dienst“ angesprochen wurde –: Der Polizeiführer vom Dienst kann den polizeilichen Schusswaffengebrauch anordnen – so wie jeder Kollege draußen auch. Das sind Maßnahmen, die auch nach dem Verhältnismäßigkeitsgrundsatz getroffen werden, die von der Eingriffstiefe her ein bisschen intensiver sind als eine Auswertung, die wir über eine Software tätigen. Das heißt, beim Schusswaffengebrauch trauen wir es den Polizisten zu, dass sie diesen nach den Regelungen korrekt umsetzen, und bei der Auswertung von Software sagen wir dann dem Polizeiführer vom Dienst, dafür sei er nicht ausreichend gerüstet? – Das sage ich mal so, um Ihnen ein bisschen entgegenzukommen und um das abzuwägen. Ich habe vorhin gesagt: „Ich bin Verantwortungsexperte.“ Ich vertraue meinen Polizeiführern vom Dienst zu 100 %, dass sie jede Nacht diese Entscheidungen korrekt treffen.

Herr Dr. Kothe: Darauf würde ich gern erwidern. Natürlich kann der Polizeiführer vom Dienst, wie jeder andere auch, den Schusswaffengebrauch anordnen. Aber da liegt auf der Hand, welche Rechtsgüter betroffen sind. Meines Erachtens sollte das bei dem Einsatz hier deutlicher hervorgehoben werden. – Das ist der Punkt, auf den ich zu sprechen kommen wollte. – Dann hatten Sie gerade auch noch einen Satz gebracht, auf den ich etwas sagen wollte, aber – –

(Unruhe)

Vorsitzender Ulli Hockenberger: Einen Moment, bitte. – Wir haben hier eine Anhöung, die auch Zuhören voraussetzt. Das ist noch mal ein Appell an alle Beteiligten hier. Ich denke, dass die Fragen im Großen und Ganzen beantwortet worden sind. Der Dialog zwischen Ihnen, Herr Kothe, und Herrn Berger findet mit Sicherheit eine fruchtbare Fortsetzung nach der Anhörung. Die Fragen sind aber, soweit ich das sehe, alle beantwortet. Das versetzt mich in die Lage, Ihnen allen zu danken – insbesondere den Experten, die dabei waren, und den Abgeordneten für die Fragen und die Diskussion.

Ich schließe damit die öffentliche Anhörung. Ich unterbreche kurz. Wir setzen die nicht öffentliche Sitzung fort, sobald der Livestream beendet ist.