CYBERINTELLIGENCE .Institute

cyberintelligence.institute // Friedrich-Ebert-Anlage 49 // 60308 Frankfurt a.M.

Frau
Hanna Naber MdL
Präsidentin des Niedersächsischen Landtags
Hannah-Arendt-Platz 1
30159 Hannover

cyberintelligence.institute GmbH
MesseTurm // Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

Prof. Dr. Dennis-Kenji Kipker
Research Director & Founder
Dennis.Kipker@cyberintelligence.institute

Per E-Mail: joerg.biela@lt.niedersachsen.de

Frankfurt a.M., 09.03.2026

Betreff: **Stellungnahme zum Entschließungsantrag der CDU-Fraktion „Polizeiarbeit in das Zeitalter der Digitalisierung überführen – verfahrensübergreifende Datenanalysen in Echtzeit ermöglichen“ (Drucksache 19/8214)**
Eine kritische Abwägung zur Einführung der Datenanalysesoftware Palantir in Niedersachsen unter besonderer Berücksichtigung der digitalen Souveränität

Berufener Sachverständiger:
Prof. Dr. Dennis-Kenji Kipker, Forschungsdirektor und Gründer cyberintelligence.institute

Sehr geehrte Frau Präsidentin,

ich bedanke mich für die Möglichkeit zur fachlichen Stellungnahme des benannten Entschließungsantrags im Rahmen der nachfolgenden Ausführungen:

I. Einleitung und Gegenstand der Stellungnahme

Der Entschließungsantrag der CDU-Fraktion im Niedersächsischen Landtag (Drucksache 19/8214) greift ein zweifellos drängend aktuelles Thema auf: die Notwendigkeit, die polizeiliche Arbeit in Niedersachsen mit modernen Analyse- und Recherchewerkzeugen auszustatten, um der stetig wachsenden Datenflut Herr zu werden. Dass die Polizei vor erheblichen Herausforderungen steht, wenn es darum geht, heterogene Datenmengen aus unterschiedlichen Verfahren und Systemen effizient zusammenzuführen und auszuwerten, ist dabei unbestritten. Die zunehmende Komplexität organisierter Kriminalität, die Bekämpfung von Cyberkriminalität und die Prävention terroristischer Bedrohungslagen machen leistungsfähige Datenanalysewerkzeuge erforderlich. In diesem Punkt ist dem Antrag ausdrücklich zuzustimmen.

Allerdings wirft der Antrag mit seiner Forderung, konkret die Software des US-amerikanischen Unternehmens Palantir Technologies einzuführen, fundamentale Fragen auf, die einer

differenzierten und kritischen Betrachtung bedürfen. Die vorliegende Stellungnahme setzt sich mit den Chancen, aber auch den erheblichen Risiken und strukturellen Problemen auseinander, die mit der Nutzung von Palantir verbunden sind. Ein besonderer Schwerpunkt liegt dabei auf der Frage der digitalen Souveränität, also der Fähigkeit, als Staat die eigene innere Sicherheit eigenständig und unabhängig von Drittstaaten gewährleisten zu können.

II. Die Ausgangslage: Berechtigter Modernisierungsbedarf der polizeilichen Datenanalyse

Die im Antrag geschilderte Problemlage ist real und verdient ernsthafte Beachtung. Die Polizei in Niedersachsen arbeitet mit einer Vielzahl von Datenbanken, die historisch gewachsen und technisch heterogen sind. Eine verfahrensübergreifende Recherche, bei der Informationen aus unterschiedlichen Systemen in Echtzeit zusammengeführt und analysiert werden können, ist mit den herkömmlichen Mitteln kaum noch leistbar. Dies betrifft insbesondere die Erstellung von Gefährderanalysen bei kriminalistisch auffälligen Personen, die Bekämpfung extremistischer Netzwerke und die Aufklärung komplexer Kriminalitätsphänomene wie Kindesmissbrauch im digitalen Raum.

Die Forderung nach einer entsprechenden Rechtsgrundlage im Niedersächsischen Polizei- und Ordnungsbehördengesetz ist vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts vom 16. Februar 2023 ebenfalls nachvollziehbar und überfällig. Ohne eine spezielle gesetzliche Ermächtigungsgrundlage ist der Einsatz automatisierter Datenanalysesysteme verfassungsrechtlich nicht zulässig. Insoweit ist die gesetzgeberische Initiative, unabhängig von der konkreten Softwarefrage, grundsätzlich zu begrüßen. Gleichwohl darf die Dringlichkeit der technischen Modernisierung nicht dazu führen, dass fundamentale Fragen der staatlichen Souveränität und des Datenschutzes nachrangig behandelt werden.

III. Palantir: Funktionsweise und Einsatz in anderen Bundesländern

Der Antrag verweist auf die erfolgreiche Nutzung der Palantir-Software in Hessen, Nordrhein-Westfalen und Bayern. In Hessen wird die Plattform seit 2017 unter dem Namen „Hessendata“ betrieben und kommt jährlich nach Angaben der Landesregierung rund 15.000 Mal zum Einsatz. Nordrhein-Westfalen nutzt seit 2022 die „DAR“ genannte Variante, Bayern hat den Vollbetrieb im August 2024 aufgenommen, und auch Baden-Württemberg hat beschlossen, die Software einzuführen. Die Ermittlungserfolge, die dem Einsatz der Software zugeschrieben werden, sind durchaus bemerkenswert und reichen von der Verhinderung von Anschlägen bis zur Aufklärung von Fällen sexuellen Kindesmissbrauchs.

Die grundsätzliche Leistungsfähigkeit der Palantir-Plattform soll hier nicht in Abrede gestellt werden. Die Software ermöglicht eine intelligente Verknüpfung und Analyse großer Datenmengen aus

verschiedenen Quellen und ist in der Lage, bisher unerkannte Zusammenhänge sichtbar zu machen. Die entscheidende Frage ist jedoch nicht, ob die Software technisch leistungsfähig ist, sondern ob ihre Nutzung angesichts der damit verbundenen strategischen Risiken und Abhängigkeiten der richtige Weg für Niedersachsen und für Deutschland insgesamt ist.

IV. Digitale Souveränität als zentrales Kriterium staatlicher Sicherheitsarchitektur

Die gravierendste Problematik des Entschließungsantrags liegt in der Frage der digitalen Souveränität. Wer Palantir zur Grundlage polizeilicher Datenanalyse macht, begibt sich in eine strukturelle Abhängigkeit von einem privatwirtschaftlichen Unternehmen eines Drittstaates – und zwar in einem Bereich, der zum innersten Kern staatlicher Souveränität gehört: der inneren Sicherheit. Diese Dimension wird im Antrag zwar nicht ignoriert, aber systematisch unterschätzt.

Es sei daran erinnert, dass Palantir Technologies nicht ein beliebiges Technologieunternehmen ist, sondern ein Unternehmen, das historisch eng mit den US-amerikanischen Nachrichtendiensten und dem Verteidigungsministerium verbunden ist. Die Firma wurde mit maßgeblicher finanzieller Beteiligung der CIA-nahen Risikokapitalgesellschaft „In-Q-Tel“ gegründet und erzielt bis heute einen erheblichen Teil seines Umsatzes mit Aufträgen US-amerikanischer Sicherheits- und Nachrichtendienste. Diese enge Verflechtung mit dem US-amerikanischen Sicherheitsapparat ist kein Makel, sondern gehört zum Geschäftsmodell des Unternehmens. Für europäische Sicherheitsbehörden bedeutet sie jedoch, dass sie eine Technologie einsetzen, deren Entwicklung von Anfang an auf die Bedürfnisse und unter dem Einfluss eines fremden Sicherheitsapparats ausgerichtet war und ist.

Die Abhängigkeit von Palantir beschränkt sich keineswegs auf den bloßen Lizenzerwerb einer Software. Vielmehr handelt es sich um eine tiefgreifende strukturelle Verflechtung. Die Software muss kontinuierlich gewartet, aktualisiert und an die spezifischen Anforderungen der jeweiligen Sicherheitsbehörde angepasst werden. Hierfür ist nach wie vor US-amerikanische Expertise unverzichtbar. In der Praxis bedeutet dies, dass Mitarbeiterinnen und Mitarbeiter, die unmittelbar von einem US-amerikanischen Hersteller zur Verfügung gestellt werden, in sensiblen Bereichen deutscher Sicherheitsbehörden tätig sind. Sie haben dabei notwendigerweise Zugang zu hochsensiblen Systemen und sind in laufende operative Prozesse eingebunden. Dies stellt eine grundlegende Schwachstelle dar, die weit über die reine Frage der Datensicherheit im technischen Sinne hinausgeht.

Die Vorstellung, dass Wartungspersonal eines ausländischen Unternehmens in den IT-Systemen deutscher Sicherheitsbehörden arbeitet und dabei potenziell Einblick in operative Ermittlungsdaten, Gefährderprofile und nachrichtendienstliche Erkenntnisse erhält, sollte aus sicherheitspolitischer Perspektive Anlass zu größter Besorgnis geben. Es geht dabei nicht zwingend um den Vorwurf einer

gezielten Spionage, sondern um die prinzipielle Möglichkeit des Zugriffs durch einen Drittstaat, der eigenen nationalen Interessen folgt und eigenen Rechtsordnungen unterliegt. US-amerikanische Unternehmen unterliegen der Jurisdiktion der Vereinigten Staaten, einschließlich nachrichtendienstlicher Zugriffsbefugnisse, die in Gesetzen wie dem CLOUD Act oder dem Foreign Intelligence Surveillance Act (FISA) verankert sind.

Besonders bedenklich ist in diesem Zusammenhang auch die Frage der Sicherheitsüberprüfung des eingesetzten Wartungspersonals. Während deutsche Sicherheitsbehörden über etablierte Verfahren zur Überprüfung der Zuverlässigkeit eigener Mitarbeiterinnen und Mitarbeiter verfügen, ist die Möglichkeit, ausländische Servicetechniker in vergleichbarer Tiefe zu überprüfen, naturbedingt begrenzt. Es entsteht eine paradoxe Situation: Um die innere Sicherheit zu gewährleisten, müssen deutsche Behörden externen Personen Zugang zu sensiblen Systemen gewähren, über deren Loyalität und Zuverlässigkeit sie keine vergleichbare Kontrolle haben wie bei eigenem Personal. Dieser strukturelle Widerspruch lässt sich durch vertragliche Vereinbarungen oder Geheimhaltungsabkommen nur teilweise auflösen, da die tatsächliche Durchsetzbarkeit solcher Vereinbarungen gegenüber einem Unternehmen, das primär der US-amerikanischen Rechtsordnung unterliegt, im Ernstfall fraglich ist.

V. Die begrenzte Aussagekraft der Fraunhofer-Analyse

Der Antrag verweist auf eine Untersuchung des Fraunhofer-Instituts, die ergeben habe, dass die Software „ohne Sicherheitsbedenken benutzt werden kann“ und ein nicht autorisierter Datenabfluss an Dritte ausgeschlossen werden könne. Diese Darstellung bedarf einer wesentlichen Relativierung. Die Methodik und die vollständigen Ergebnisse der Fraunhofer-Analyse sind nicht öffentlich zugänglich. Es handelt sich um eine nicht umfassend offengelegte Studie, deren Prüftiefe, Prüfumfang und zugrunde liegende Annahmen von unabhängiger Seite nicht vollständig nachvollzogen werden können. Eine sicherheitspolitische Entscheidung von dieser Tragweite auf eine Studie zu stützen, deren Methode und Ergebnisse nicht vollständig transparent sind, ist aus wissenschaftlicher und politischer Sicht problematisch.

Entscheidend ist zudem, dass die Frage des Datenabflusses nur eine von mehreren sicherheitsrelevanten Dimensionen darstellt. Selbst wenn man die Vertraulichkeit der Daten als hinreichend gesichert ansehen wollte – was bei proprietärer Software eines ausländischen Anbieters grundsätzlich schwer mit letzter Sicherheit zu gewährleisten ist –, bleibt die mindestens ebenso kritische Frage der Datenverfügbarkeit unbeantwortet. Was geschieht, wenn Palantir als Technologieträger in Deutschland nicht mehr zur Verfügung steht? Dies ist keineswegs ein abstraktes Szenario: Die Vereinigten Staaten verfügen über ein elaboriertes System nationaler Exportkontrollbeschränkungen, mit dem der Export sicherheitsrelevanter Technologien jederzeit eingeschränkt oder untersagt werden kann. Im Falle geopolitischer Spannungen oder veränderter

politischer Prioritäten in Washington könnten deutsche Sicherheitsbehörden buchstäblich über Nacht von einer Schlüsseltechnologie abgeschnitten werden, auf die sie sich operativ verlassen.

Die jüngere Vergangenheit hat eindrucksvoll gezeigt, wie schnell sich geopolitische Konstellationen verschieben können und wie bereitwillig die Vereinigten Staaten technologische Abhängigkeiten als Druckmittel einsetzen. Die Erfahrungen im Bereich der Halbleiter-Exportkontrollen gegenüber China oder der Umgang mit europäischen Verbündeten in Handels- und Technologiefragen illustrieren, dass technologische Souveränität kein abstraktes Konzept ist, sondern eine ganz reale sicherheitspolitische Notwendigkeit darstellt.

Es kommt hinzu, dass die Fraunhofer-Analyse in erster Linie die technische Frage des Datenabflusses im engeren Sinne adressiert hat. Die weitergehende Frage, inwieweit die Software selbst als nachrichtendienstliches Instrument instrumentalisiert werden könnte – etwa durch verdeckte Funktionen in zukünftigen Updates oder durch die gezielte Manipulation von Analyseergebnissen –, lässt sich bei proprietärer Software ohne vollständige Quellcodeoffenlegung prinzipiell nicht abschließend beantworten. Eine einmalige Prüfung zu einem bestimmten Zeitpunkt kann keine dauerhafte Gewähr für die Integrität einer Software bieten, die regelmäßig aktualisiert wird und deren Weiterentwicklung außerhalb der Kontrolle der nutzenden Behörden liegt. Jedes Software-Update müsste erneut einer umfassenden Sicherheitsprüfung unterzogen werden, was in der Praxis kaum realisierbar ist, ohne den laufenden Betrieb erheblich zu beeinträchtigen.

VI. Das Paradoxon der Übergangslösung: Warum Palantir den Aufbau eigener Fähigkeiten verhindert

Der Antrag greift den auch aus Baden-Württemberg bekannten Ansatz auf, Palantir als „Übergangslösung“ zu nutzen, bis deutsche oder europäische Unternehmen vergleichbare Software anbieten können. Diese Argumentation klingt auf den ersten Blick pragmatisch und lösungsorientiert. Bei näherer Betrachtung erweist sie sich jedoch als in sich widersprüchlich, denn die Einführung von Palantir als vermeintliche Übergangslösung steht dem Aufbau nativer digitaler Souveränität diametral entgegen.

Der Antrag selbst benennt das Problem mit bemerkenswerter Offenheit, zieht daraus aber die falschen Schlüsse. Er stellt fest, dass deutsche oder europäische Unternehmen ohne eine Anschubfinanzierung durch Sicherheitsbehörden von sich aus keine vergleichbare Software entwickeln werden, „zumal völlig ungewiss ist, ob diese Produkte tatsächlich von den Sicherheitsbehörden geordert und eingesetzt werden.“ Genau hier liegt der Kern des Problems: Wenn die Sicherheitsbehörden der großen Flächenländer sich nacheinander für Palantir entscheiden, wird der Markt für deutsche und europäische Alternativprodukte faktisch geschlossen,

bevor er sich überhaupt öffnen kann. Kein europäisches Unternehmen wird die erheblichen Investitionen in die Entwicklung einer konkurrenzfähigen Analyseplattform tätigen, wenn die potenziellen Kunden – die deutschen Sicherheitsbehörden – bereits an einen US-amerikanischen Anbieter gebunden sind.

Die Erfahrung zeigt, dass „Übergangslösungen" in der IT-Beschaffung eine ausgeprägte Tendenz zur Verstetigung haben. Sind Systeme einmal eingeführt, Mitarbeiterinnen und Mitarbeiter geschult und Arbeitsprozesse auf die spezifische Plattform angepasst, wird ein Wechsel mit jedem Jahr kostspieliger und unwahrscheinlicher. Die Einführung von Palantir wäre daher mit hoher Wahrscheinlichkeit keine vorübergehende Brückenlösung, sondern eine langfristige strategische Festlegung, die den Aufbau souveräner europäischer Alternativen nicht nur nicht fördert, sondern aktiv behindert.

Dieser sogenannte „Vendor-Lock-in-Effekt" ist aus zahlreichen IT-Beschaffungsprojekten der öffentlichen Verwaltung wohlbekannt. Sobald die Datenstrukturen, Schnittstellen und Arbeitsabläufe einer Organisation auf ein bestimmtes Produkt zugeschnitten sind, entstehen Wechselkosten, die den Umstieg auf ein alternatives System ökonomisch und organisatorisch prohibitiv werden lassen. Im Falle von Palantir wären diese Wechselkosten besonders hoch, da die Plattform nicht lediglich ein Werkzeug unter vielen darstellt, sondern als zentrale Infrastrukturkomponente in die gesamte polizeiliche Datenverarbeitung eingebunden würde. Ein späterer Umstieg würde nicht nur die Migration großer Datenbestände erfordern, sondern auch die vollständige Umschulung des Personals und die Neugestaltung etablierter Arbeitsprozesse. Die politische Bereitschaft, diese Kosten zu tragen, dürfte im Zeitverlauf drastisch sinken, zumal ein funktionierendes System politisch nur schwer gegen ein noch zu entwickelndes Alternativsystem ausgetauscht werden kann.

VII. Bürgerrechte und Datenschutz: Die verfassungsrechtliche Dimension

Neben der Frage der digitalen Souveränität wirft der Einsatz einer leistungsfähigen Datenanalysesoftware erhebliche bürgerrechtliche und datenschutzrechtliche Fragen auf, die unabhängig vom konkreten Hersteller bestehen. Das Bundesverfassungsgericht hat in seinem grundlegenden Urteil vom 16. Februar 2023 enge Grenzen für die automatisierte Datenanalyse gezogen. Die bloße Schaffung einer Rechtsgrundlage genügt nicht; diese muss den verfassungsrechtlichen Anforderungen an Bestimmtheit, Verhältnismäßigkeit und effektive Kontrolle genügen.

Die Möglichkeit, große Datenmengen in Echtzeit zu verknüpfen und auszuwerten, birgt das systemimmanente Risiko einer umfassenden Profilbildung, die über den konkreten Ermittlungsanlass hinausgeht. Gerade bei der prädiktiven Analyse – also dem Versuch, aus

vorhandenen Daten künftige Gefährdungslagen vorherzusagen – bestehen erhebliche Risiken für unbescholtene Bürgerinnen und Bürger, die aufgrund statistischer Korrelationen in den Fokus polizeilicher Aufmerksamkeit geraten können, ohne dass ein konkreter Verdacht gegen sie vorliegt. Eine Rechtsgrundlage muss daher nicht nur den Einsatz der Software als solchen regeln, sondern auch wirksame Schutzmechanismen gegen eine überschießende Datenverarbeitung und klare Löschfristen vorsehen.

Hinzu kommt die Problematik der algorithmischen Transparenz. Bei proprietärer Software eines ausländischen Anbieters ist die vollständige Nachvollziehbarkeit der Analysealgorithmen in der Regel nicht gewährleistet. Dies erschwert nicht nur die gerichtliche Überprüfung im Einzelfall, sondern auch die parlamentarische und datenschutzrechtliche Kontrolle. Der im Antrag vorgesehene frühzeitige Austausch mit dem Landesbeauftragten für Datenschutz ist zwar richtig, greift aber zu kurz, wenn die Kontrollinstanzen die Funktionsweise der Software mangels Zugang zum Quellcode nicht vollständig durchdringen und überprüfen können.

Darüber hinaus muss die gesellschaftliche Debatte über die Grenzen polizeilicher Datenanalyse stärker geführt werden. Die technischen Möglichkeiten der Datenverknüpfung und -auswertung werden in den kommenden Jahren durch Fortschritte im Bereich der Künstlichen Intelligenz weiter rasant wachsen. Umso wichtiger ist es, dass der Gesetzgeber nicht nur auf den aktuellen Stand der Technik reagiert, sondern einen normativen Rahmen schafft, der auch künftige Entwicklungen antizipiert. Hierzu gehört die grundlegende Frage, in welchem Umfang der Staat Daten seiner Bürgerinnen und Bürger verknüpfen und analysieren darf, ohne den Wesensgehalt der Grundrechte auf informationelle Selbstbestimmung und Privatsphäre zu verletzen. Diese Frage ist nicht bloß eine juristische, sondern letztlich eine zutiefst politische und gesamtgesellschaftliche, die einer breiten öffentlichen Diskussion bedarf und nicht durch die bloße Einführung einer bestimmten Software präjudiziert werden darf.

VIII. Lösungsansätze: Der Weg zu einer souveränen polizeilichen Datenanalyse

Die Alternative zur Einführung von Palantir ist nicht der Verzicht auf moderne Datenanalyse, sondern die entschlossene Entwicklung eigener Lösungen. Es bedarf eines konsequenten Strategiewechsels, der kurzfristige operative Pragmatik mit langfristiger strategischer Souveränität in Einklang bringt.

Zunächst sollte Niedersachsen sich auf Bundes- und europäischer Ebene für ein koordiniertes Entwicklungsprogramm für eine souveräne polizeiliche Analyseplattform einsetzen. Die Entwicklung einer solchen Plattform übersteigt die Kapazitäten und finanziellen Möglichkeiten eines einzelnen Bundeslandes. Sie muss als gesamtstaatliche Aufgabe verstanden werden, idealerweise eingebettet in eine europäische Strategie. Die Europäische Union hat mit Initiativen wie GAIA-X im Cloud-Bereich bereits gezeigt, dass der politische Wille für digitale Souveränität grundsätzlich vorhanden ist. Was

fehlt, ist ein konkretes, zweckgebundenes Förderprogramm für sicherheitsbehördliche Analysewerkzeuge, das deutsche und europäische Unternehmen in die Lage versetzt, konkurrenzfähige Produkte zu entwickeln.

Darüber hinaus wäre ein offener, modularer Architekturansatz zielführend. Anstatt eine monolithische Komplettlösung eines einzelnen Anbieters zu beschaffen, könnte eine Plattformarchitektur entwickelt werden, die verschiedene spezialisierte Komponenten integriert. Ein solcher Ansatz ermöglicht es, einzelne Module bei Bedarf auszutauschen, ohne das Gesamtsystem zu gefährden. Er reduziert die Abhängigkeit von einem einzelnen Hersteller und schafft einen echten Wettbewerbsmarkt, an dem auch mittelständische europäische IT-Unternehmen teilnehmen können. Forschungseinrichtungen wie das Fraunhofer-Institut, das Deutsche Forschungszentrum für Künstliche Intelligenz und die Helmholtz-Gemeinschaft verfügen bereits über erhebliche Expertise im Bereich der Datenanalyse und Künstlichen Intelligenz, die für die Entwicklung einer solchen Plattform nutzbar gemacht werden kann.

Parallel dazu muss die Ausbildung und Gewinnung von IT-Fachkräften für den öffentlichen Dienst massiv verstärkt werden. Die beste Software nützt nichts, wenn es an qualifiziertem Personal fehlt, das sie entwickeln, betreiben und weiterentwickeln kann. Niedersachsen sollte gezielt Informatik-Absolventinnen und -Absolventen für den Polizeidienst anwerben und attraktive Karrierepfade im Bereich der IT-Sicherheit und Datenanalyse schaffen. Dies schließt eine wettbewerbsfähige Vergütung ebenso ein wie die Möglichkeit, an innovativen Projekten mitzuwirken, die gesellschaftlich relevant sind.

Für die Übergangszeit, bis eine souveräne Lösung einsatzbereit ist, sollte nicht auf eine ausländische Komplettlösung zurückgegriffen werden, sondern auf eine schrittweise Ertüchtigung der vorhandenen Systeme. Die bestehenden polizeilichen Datenbanken können durch gezielte Investitionen in Schnittstellen und Interoperabilität bereits deutlich besser vernetzt werden. Open-Source-Technologien im Bereich der Datenanalyse und des maschinellen Lernens bieten leistungsfähige Bausteine, die an die spezifischen Anforderungen der Polizeiarbeit angepasst werden können. Dieser Weg ist weniger spektakulär als die Beschaffung einer „schlüsselfertigen“ US-Lösung, dafür aber langfristig tragfähiger und souveränitätswahrend.

Nicht zuletzt sollte die bestehende Zusammenarbeit der Länder im Rahmen des Programms Polizei 2020 stärker für die Entwicklung gemeinsamer Analysefähigkeiten genutzt werden. Statt dass jedes Bundesland isoliert über die Beschaffung einer Analysesoftware entscheidet, wäre ein gemeinsames Vorgehen nicht nur ökonomisch effizienter, sondern würde auch die Verhandlungsposition gegenüber Anbietern stärken und die Entwicklung interoperabler Lösungen fördern. Ein solches koordiniertes Vorgehen könnte durch die Innenministerkonferenz initiiert und durch das Bundesministerium des Innern fachlich und finanziell unterstützt werden. Die technische

Umsetzung könnte auf der Expertise des Bundesamtes für Sicherheit in der Informationstechnik aufbauen, das über die notwendige Kompetenz verfügt, um Sicherheitsanforderungen für eine solche Plattform zu definieren und deren Einhaltung zu überwachen.

IX. Datenschutzkonforme Ausgestaltung als Daueraufgabe

Unabhängig davon, welche technische Lösung letztlich zum Einsatz kommt, muss der bürgerrechts- und datenschutzkonforme Umgang mit sicherheitsbehördlichen Datenbanken als Daueraufgabe begriffen werden, die über die einmalige Schaffung einer gesetzlichen Ermächtigungsgrundlage hinausgeht. Das Bundesverfassungsgericht hat klargestellt, dass die automatisierte Datenanalyse einer besonders strengen Verhältnismäßigkeitsprüfung unterliegt. Dies bedeutet, dass der Gesetzgeber nicht nur den Einsatz der Technologie als solchen regeln, sondern auch wirksame institutionelle und verfahrensrechtliche Sicherungen vorsehen muss.

Hierzu gehört ein effektives Kontrollregime, das sowohl eine unabhängige Vorabkontrolle als auch eine fortlaufende Evaluierung des Einsatzes umfasst. Der Landesbeauftragte für den Datenschutz muss personell und technisch so ausgestattet werden, dass er die eingesetzte Software und ihre Anwendung tatsächlich wirksam kontrollieren kann. Dies setzt voraus, dass die Kontrollinstanzen vollen Zugang zum Quellcode und zu den verwendeten Algorithmen haben – eine Anforderung, die bei proprietärer Software eines ausländischen Herstellers strukturell kaum erfüllbar ist, bei einer eigenen oder Open-Source-basierten Lösung aber grundsätzlich gewährleistet werden kann.

Ferner bedarf es klarer gesetzlicher Regelungen zur Zweckbindung und zu Löschfristen. Daten, die für einen bestimmten Ermittlungszweck erhoben oder aus verschiedenen Quellen zusammengeführt wurden, dürfen nicht unbegrenzt vorgehalten und für beliebige andere Zwecke genutzt werden. Die automatisierte Zusammenführung von Daten aus verschiedenen Verfahren erfordert zudem eine besonders sorgfältige Qualitätssicherung, um zu verhindern, dass fehlerhafte oder veraltete Daten zu falschen Schlussfolgerungen und ungerechtfertigten Eingriffen in die Rechte Betroffener führen.

Schließlich muss die Transparenz gegenüber der Öffentlichkeit und dem Parlament gewährleistet sein. Eine regelmäßige Berichterstattung über den Umfang und die Ergebnisse des Einsatzes von Datenanalysewerkzeugen sollte gesetzlich vorgeschrieben werden, um eine demokratische Kontrolle dieser eingriffsintensiven Technologie sicherzustellen. Gerade weil die automatisierte Datenanalyse im Bereich der Gefahrenabwehr und Straftatenverhütung per definitionem im Vorfeld konkreter Straftaten ansetzt, ist die parlamentarische Aufsicht von besonderer Bedeutung.

X. Zusammenfassende Bewertung und Handlungsempfehlungen

Der Entschließungsantrag der CDU-Fraktion identifiziert ein reales und dringendes Problem: Die niedersächsische Polizei benötigt moderne, leistungsfähige Werkzeuge zur Datenanalyse. Die vorgeschlagene Lösung – die Einführung der Palantir-Software – ist allerdings aus Gründen der digitalen Souveränität, des Datenschutzes und der langfristigen strategischen Ausrichtung der deutschen Sicherheitsarchitektur erheblich problematisch und kritisch zu sehen.

Die Nutzung von Palantir würde Deutschland in einem Kernbereich staatlicher Souveränität von einem US-amerikanischen Unternehmen abhängig machen. Die Risiken eines erzwungenen Technologieentzugs durch US-Exportkontrollmaßnahmen, der notwendige Einsatz US-amerikanischen Wartungspersonals in hochsensiblen Bereichen und die prinzipielle Möglichkeit nachrichtendienstlicher Zugriffe unter US-Recht stellen Risiken dar, die durch technische Maßnahmen allein nicht eliminiert werden können. Die begrenzt aussagekräftige Fraunhofer-Analyse vermag diese Bedenken nicht auszuräumen, zumal sie die existenzielle Frage der Datenverfügbarkeit im Falle eines Technologieentzugs gar nicht adressiert.

Zudem würde die Einführung von Palantir als vermeintliche Übergangslösung den ohnehin schwierigen Aufbau souveräner europäischer Alternativen faktisch unmöglich machen, indem sie den relevanten Markt verschließt und die für die Entwicklung eigener Produkte notwendige Nachfrage absorbiert.

Es ist eine Frage der politischen Prioritätensetzung, ob man den Weg des geringsten Widerstands wählt und eine verfügbare US-Softwarelösung einführt, oder ob man die deutlich anspruchsvollere, aber 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 zunehmend zum entscheidenden Faktor staatlicher Handlungsfähigkeit wird, spricht eindeutig für die zweite Option. Es wäre geradezu fahrlässig, die innere Sicherheit eines Landes auf eine Technologie zu gründen, deren Verfügbarkeit von den außenpolitischen Entscheidungen eines 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 Souveränlösung investiert werden. Die Kosten für den Betrieb von Palantir in den bereits nutzenden Bundesländern sind erheblich und stellen langfristig eine finanzielle Belastung dar, die in keinem angemessenen Verhältnis zu dem steht, was mit denselben Mitteln an eigener Entwicklungskapazität hätte aufgebaut werden können. Jeder Euro, der in eine ausländische Abhängigkeit fließt, fehlt für den Aufbau eigener Kompetenzen.

Der richtige Weg besteht darin, die Schaffung einer verfassungskonformen Rechtsgrundlage für die automatisierte Datenanalyse umgehend voranzutreiben und gleichzeitig die Entwicklung einer souveränen, modularen und offenen Analyseplattform als gesamtstaatliche Aufgabe in Angriff zu nehmen. Dies erfordert politischen Willen, erhebliche Investitionen und eine enge Zusammenarbeit zwischen Bund, Ländern, Forschungseinrichtungen und der europäischen IT-Wirtschaft. In der Übergangszeit sind die vorhandenen polizeilichen IT-Systeme gezielt zu ertüchtigen und durch Open-Source-Komponenten zu ergänzen.

Die Sicherheit der Bürgerinnen und Bürger und die Wahrung ihrer Grundrechte sind keine Gegensätze, sondern zwei Seiten derselben Medaille. Eine moderne polizeiliche Datenanalyse muss beiden Ansprüchen gerecht werden – und das kann sie nur auf der Grundlage technologischer Souveränität, algorithmischer Transparenz und wirksamer demokratischer Kontrolle. Niedersachsen hat die Gelegenheit, hier eine verantwortungsvolle Vorreiterrolle einzunehmen und einen Weg zu beschreiten, der nachhaltig und zukunftsfähig ist, anstatt einer kurzfristigen, aber strategisch fragwürdigen Lösung zu folgen. Die Debatte über den Entschließungsantrag der CDU-Fraktion sollte deshalb zum Ausgangspunkt einer breiten und grundlegenden Auseinandersetzung mit der Frage werden, wie Deutschland seine digitale Souveränität im Bereich der inneren Sicherheit dauerhaft sichern und stärken kann – nicht durch Abhängigkeit, sondern durch Eigenständigkeit.

Frankfurt am Main / Berlin, 09.03.2026

Prof. Dr. Dennis-Kenji Kipker
Research Director & CII-Founder