Humanistische Union

Digitale Souveränität in Zeiten plattformisierter Polizeiarbeit

Einleitung

Die digitale Transformation staatlicher Sicherheitsbehörden hat in den vergangenen Monaten eine neue politische Brisanz erlangt. Europäische Staaten sehen sich zunehmend mit der Frage konfrontiert, wie sie ihre technologische Handlungsfähigkeit sichern können, ohne in strukturelle Abhängigkeiten von globalen Technologieanbietern und den ihnen nahestehenden Regierungen zu geraten. Deutschland bildet in diesem Zusammenhang ein aufschlussreiches Beispiel: Die Einführung der Datenintegrations- und Analyseplattform *Gotham* des US-Unternehmens Palantir in mehreren Landespolizeien hat – im Lichte der politischen Entwicklungen in den USA in der zweiten Amtszeit von Präsident Trump – eine intensive Debatte über staatliche Kontrolle, technologische Souveränität und demokratische Verantwortlichkeit ausgelöst. Während Polizeipraktiker*innen die Plattform als unverzichtbares Instrument zeitgemäßer Ermittlungsarbeit darstellen, warnen Kritiker*innen vor einer schleichenden Privatisierung zentraler Wissens- und Entscheidungsinfrastrukturen des Staates und einer Verlagerung von Kontrolle in Richtung USA (Egbert 2024; Ulbricht/Egbert 2024).

Der Konflikt um Palantir zeigt, dass traditionelle Vorstellungen staatlicher Souveränität – verstanden als territoriale und rechtliche Herrschaft – im digitalen Zeitalter nicht mehr ausreichen. Die Frage, wer über welche Daten, Schnittstellen, Algorithmen und Plattformen verfügt, entscheidet heute maßgeblich darüber, wie Staatlichkeit praktiziert werden kann. Souveränität wird damit zu einer infrastrukturellen Frage: Wer kontrolliert die Systeme, durch die staatliches Wissen erzeugt, verarbeitet, operationalisiert und zunehmend überhaupt erst ermöglicht wird?

Der Beitrag rekonstruiert vor diesem Hintergrund die politischen, technischen und gesellschaftlichen Auseinandersetzungen um Palantir in Deutschland, ordnet sie in die breitere Debatte um digitale Souveränität ein und diskutiert die Frage, welche Alternativen zu Palantir-Plattformen derzeit entwickelt und verhandelt werden. Ziel ist es, die mit der Plattformisierung der Polizei verbundenen Souveränitätsfragen und die zentralen Konfliktlinien der aktuellen Diskussion herauszuarbeiten.

Die Argumentation des Beitrags ist wie folgt aufgebaut: Zunächst wird skizziert, wie der Begriff der *digitalen Souveränität* in der Forschung verstanden wird, wie er sich in den vergangenen Jahren in der EU-Politik verschoben hat und welche weltpolitischen Entwicklungen diese Debatte prägen. Anschließend werden Entstehung und Funktionsweise von *Palantir Gotham* erläutert, um technologische Versprechen und demokratiepolitische Risiken der Plattformarchitektur sichtbar zu machen. Darauf aufbauend wird die Einführung von *Gotham* in mehreren deutschen Landespolizeien nachgezeichnet. Es folgt eine Analyse der politischen Auseinandersetzungen auf Bundesebene, in denen unterschiedliche Verständnisse digitaler Souveränität artikuliert werden. Abschließend werden derzeit verhandelte Alternativen zu Palantir-Plattformen diskutiert und Bedingungen für eine souveränere, grundrechtsverträgliche Architektur

polizeilicher Analyseinfrastrukturen ausgelotet.

Digitale Souveränität im Lichte weltpolitischer Entwicklungen und digitalökonomischer Oligopolisierung

Digitale Souveränität bezeichnet die Fähigkeit von Individuen, Organisationen und Staaten, digitale Infrastrukturen, Datenflüsse und IT-Systeme selbstbestimmt zu gestalten, zu kontrollieren und normativ zu rahmen. In der Fachdebatte umfasst sie die Verfügungsmacht über Daten, Software, Hardware und Netze sowie die Fähigkeit, Abhängigkeiten von Anbietern oder außereuropäischen Rechtsordnungen strategisch zu begrenzen. Digitale Souveränität stellt keinen autarken Endzustand dar, sondern ein relationales Konzept gradueller Handlungsspielräume innerhalb global verflochtener Plattformökonomien und transnationaler Technologiekonzerne (Bannerman 2022; Baur 2025; Bellanova et al. 2022). Souveränität wird damit zu einer Frage der Gestaltung und Kontrolle epistemischer Grundlagen staatlichen Handelns – sprich, jener Wissensordnungen, auf denen politische Entscheidungen beruhen.

Der Begriff *digitale Souveränität* verbindet dabei die traditionelle Souveränitätsidee der Selbstbestimmung mit der digitalen Gesellschaft, das heißt der allumfassenden Durchdringung von Gesellschaft und Lebenswelten durch Datenflüsse, Plattformlogiken und Algorithmen. Betont wird in diesem Zusammenhang die doppelte Dimension digitaler Souveränität: nach außen die Unabhängigkeit von fremden Mächten, nach innen die Selbstbestimmungsfähigkeit der Bürger*innen. Europäische digitale Souveränität soll also Rechtsstaatlichkeit, Grundrechte und Freiheit sichern, ohne in Isolationismus abzurutschen (Calderaro/Blumfelde 2022; Pohle 2020; Pohle/Thiel 2021).

Kritisiert wird gleichzeitig die politische Instrumentalisierung des Begriffs. Denn *digitale Souveränität* ist längst zu einem Schlagwort verkommen, das von Wirtschaftsverbänden, Tech-Unternehmen und führenden Politiker*innen gleichermaßen beansprucht wird – oft als leere Worthülse, hinter der vage Protektionismus- oder Innovationsrhetorik verborgen wird (Pohle 2024). Die Gefahr liegt insbesondere darin, dass der Begriff zentralisierte Kontrollambitionen kaschiert und gleichzeitig unrealistische Erwartungen an technologische Unabhängigkeit weckt.

Parallel zu den geopolitischen Verwerfungen sowie der stetig steigenden Macht der großen, meist US-amerikanischen Internetkonzerne hat sich gerade in der EU-Politik ein mehrschichtiges Verständnis digitaler Souveränität etabliert (Calderaro/ Blumfelde 2022; Pohle 2024; Roberts et al. 2021). Es umfasst zum einen die Fähigkeit, regulatorische Standards zu setzen und durchzusetzen – etwa über Datenschutz-Grundverordnung, Digital Services Act, Digital Markets Act oder Data Act. Diese regulatorische Souveränität projiziert normative Kontrolle nach außen, stößt aber an Grenzen, wenn die zugrunde liegenden Infrastrukturen nicht in europäischer Hand sind, da die Regelsetzung nicht den Besitz und die Steuerung eigener Systeme ersetzt. Zum anderen rückt eine infrastrukturelle Dimension in den Blick: die Fähigkeit, kritische digitale Infrastrukturen – Netze, Cloud-Plattformen, Datenräume, KI-Systeme – unabhängig betreiben, auditieren und bei Bedarf ersetzen zu können. Projekte wie GAIA-X oder „European Cloud“-Initiativen zielen darauf, Alternativen zu US-amerikanischen Hyperscalern zu schaffen (Baur 2025). Doch der Aufbau solcher Alternativen ist komplex, langwierig und politisch umstritten, wie man an den aktuellen Entwicklungen rund um GAIA-X sieht (Kleinz 2025). Solange zentrale Infrastrukturen von US-

Unternehmen betrieben werden, bleibt europäische Autonomie fragil – zumal US-Gesetze wie der CLOUD Act einen extraterritorialen Zugriff auf bei US-Anbietern gespeicherte Daten ermöglichen, selbst wenn Server physisch in Europa stehen.

Die Risiken des CLOUD Act verdeutlichen aktuelle Vorfälle: 2025 sperrte Microsoft vermutlich auf US-Sanktionsbeschluss hin Office-Accounts des Internationalen Strafgerichtshofs (IStGH) in Den Haag, inklusive des Kontos des Chefanklägers Karim Khan. Die Daten lagen in einem Microsoft-Rechenzentrum in Irland, dennoch griff US-Recht. Der CLOUD Act verpflichtet US-Firmen zum Zugriff auf von ihnen kontrollierte Daten, unabhängig vom physischen Standort (Rojszczak 2020). Der Chefjustiziar von Microsoft Frankreich bestätigte in einer Anhörung im Französischen Senat im Juni 2025 zwar, dass europäisch gehostete Daten keinen Schutz vor US-Behörden bieten, bestritt aber, Khan ausgesperrt zu haben (Sawall 2025). Grund für den mutmaßlichen Eingriff von Microsoft – auf Geheiß der Trump-Administration – war ein politischer: Sanktioniert wurde Khan, weil er unter anderem gegen Israels Premierminister Benjamin Netanyahu Haftbefehl wegen möglicher Kriegsverbrechen erlassen hatte (Laaf 2025). Ähnlich betraf es den französischen IStGH-Richter Nicolas Guillou, ebenfalls beteiligt an dem Haftbefehl gegen Netanyahu. US-Sanktionen führten bei ihm zum umfassenden Ausschluss aus digitalen Infrastrukturen: Deaktivierung von Amazon-, Airbnb-, PayPal- und Expedia-Konten, Annullierung von Buchungen sowie Blockade von American Express, Visa und Mastercard. Selbst europäische Banken beendeten Geschäftsbeziehungen mit ihm, um sekundäre Sanktionsrisiken zu vermeiden (Zellinger 2025).

Diese Fälle zeigen die Abhängigkeit europäischer Institutionen von US-Plattformen. Für Polizeidaten bei Palantir gilt Analoges: US-Behörden könnten unter CLOUD Act etwa bei Terrorermittlungen oder Sanktionsprüfungen Zugriff fordern – mit gravierenden Folgen für Datenschutz und Souveränität. Vor diesem Hintergrund wird Palantirs Einführung in den deutschen Polizeien zu einem exemplarischen Konfliktfeld, das Spannungen zwischen Effizienzgewinnen, rechtlichen Anforderungen und geopolitischen Abhängigkeiten verdeutlicht.

Palantir Technologies und die Funktionsweise von *Gotham*

Palantir Technologies wurde 2003 im kalifornischen Palo Alto von Peter Thiel, Alex Karp und weiteren Gründern ins Leben gerufen – im Kontext der US-Sicherheitsarchitektur nach den Anschlägen vom 11. September 2001. Finanziert durch In-Q-Tel, den Investmentarm der CIA, zielte das Unternehmen von Beginn an darauf, große Mengen heterogener Daten – von strukturierten Datenbanken bis hin zu unstrukturierten Freitexten – so zu integrieren und auszuwerten, dass bislang verborgene Zusammenhänge für Analyst*innen sichtbar werden. Erste Kunden waren Geheimdienste und das Militär, es folgten Strafverfolgungsbehörden, zivile Behörden sowie Unternehmen aus circa 35 verschiedenen Branchen.

Palantir bietet vier Plattformen an: *Gotham* für Sicherheitskunden, *Foundry* für Unternehmen und *Apollo* für kontinuierliche Softwareverteilung, ergänzt durch die 2023 lancierte *AIP* zur eigenständigen KI?Entwicklung auf Basis großer Sprachmodelle (Egbert/Ulbricht 2024; Iliadis/Acker 2022; Ta?kale 2025).

Das zentrale Produkt für Sicherheitsbehörden ist *Gotham*, das als „Datenbetriebssystem“ konzipiert ist. Es führt bestehende Datenbestände nicht zentral zusammen, sondern macht sie über standardisierte Schnittstellen (APIs) föderiert zugänglich. In einem anpassbaren Datenmodell („Dynamic Ontology“) werden Entitäten wie Personen, Fahrzeuge, Adressen, Ereignisse oder Kommunikationsverbindungen erfasst und verknüpft (Palantir 2022). Nutzer*innen suchen quer über vormals getrennte Datenbanken und erhalten Ergebnisse als Netzwerkgrafiken, Karten, Zeitachsen oder Heatmaps. Die Oberfläche erinnert an Suchmaschinen mit zentraler Suchleiste und explorativer Logik (Iliadis/Acker 2022).

Palantir betont insbesondere die datenschutzfreundliche Architektur ihrer Produkte: Daten bleiben bei der Behörde, Zugriff ist granular geregelt und Abfragen werden protokolliert (Bowman et al. 2023; Cipierre/Hiesserich 2022). Dennoch liegt hier der Kern bürgerrechtlicher Kritik: Die proprietäre Logik der Verknüpfung – welche Entitäten relevant sind, wie Kanten gewichtet werden, welche Muster hervorgehoben werden – entzieht sich externer Kontrolle. Dadurch verschiebt sich die Definitionsmacht darüber, was in polizeilichen Daten „sichtbar“ wird, zu einem privaten Anbieter. Die „Ontologie“ fungiert als semantische Schicht, die Daten in lesbare Objekte transformiert und Assoziationen schafft – ein Prozess, der Erkenntnisse präformiert, ohne dies transparent zu machen (Galis/Karlsson 2024).

Die politische Geschichte Palantirs verstärkt diese Bedenken. Das Unternehmen war an umstrittenen Projekten beteiligt: US-Migrationskontrollen und Abschiebungen durch ICE, militärische Zielerfassung (etwa Drohnenangriffe), Massenüberwachungsprogramme (Iliadis/Acker 2022; Knight/Gekker 2020). Kritiker*innen sehen darin den Import sicherheitspolitischer Logiken – Problematisierung von Migration, Protest und Netzwerken –, die mit europäischen Rechtsstaaten kaum vereinbar sind. Palantirs Geschäftsmodell, das Software mit Beratung kombiniert und langfristig durch Lizenz- und Trainingsgebühren verdient, schafft zudem Vendor Lock-in sprich Bindung an einen IT-Anbieter: Kunden passen interne Prozesse an die Plattform an, weshalb ein Ausstieg teuer und komplex werden kann (Vlassis 2024).

Aus polizeilicher Sicht überwiegen praktische Vorteile: schnellere Recherche, bessere Übersicht in komplexen Fällen und effiziente Verknüpfung unverbundener Datenquellen. Diese Ambivalenz – operativer Mehrwert versus strukturelle Risiken für Transparenz und Souveränität – prägt, wie im Folgenden gezeigt wird, die derzeitige Debatte um Palantir in Deutschland.

Einführung von *Gotham* in deutschen Polizeien

Seit 2017 wurde *Gotham* schrittweise in mehreren Bundesländern implementiert: zunächst in Hessen als hessenDATA (2017), gefolgt von Nordrhein-Westfalen (Datenbankübergreifende Analyse und Recherche [DAR], 2021), Bayern (Verfahrensübergreifende Recherche und Analyse [VeRA], 2024) und Baden-Württemberg (VeRA, 2025). Die Einführungsprozesse erfolgten überwiegend unter Berufung auf sicherheitspolitische Dringlichkeit und das Fehlen funktional äquivalenter Alternativen, die unmittelbar implementierbar sind.

In Hessen begründete Innenminister Peter Beuth (CDU) das beschleunigte Vergabeverfahren ohne Ausschreibung mit dem Bedarf an raschen Analysekapazitäten nach dem Breitscheidplatz-Anschlag (Hessischer Landtag: Drucksache 19/6864). In Nordrhein-Westfalen betonte Innenminister Herbert Reul (CDU), dass fragmentierte Datenbanken die polizeilichen Ermittler*innen bremsen, eine einheitliche Plattform dem entgegenwirken würde und die Analyse vorhandener Daten dadurch beschleunigt würde (Reul 2020). Ähnlich äußerte sich Bayerns Innenminister Joachim Herrmann (CSU), der eine schnellere und effektivere Auswertung und Verknüpfung vorhandener Daten durch VeRA anpreist und damit unter anderem „kriminelle Netzwerke“ leichter entdecken sowie „Gefährder und Banden“ schneller ermitteln möchte (zit. n. Bayerische Staatsregierung 2024). Der baden-württembergische Innenminister Thomas Strobl (CDU) sagte anlässlich des Erwerbs von VeRA 2025: „Nur wenn die Polizei weiß, was sie weiß – und das am besten sekundenschnell –, kann sie die Menschen bestmöglich schützen“ (zit. n. Staatsministerium Baden-Württemberg 2025).

Diese Begründungen folgen einem konsistenten Argumentationsmuster: Problematisiert werden historisch gewachsene Fachverfahren, fragmentierte Datenbestände und organisatorische Silostrukturen, die als Hemmnisse effizienter Analyse erscheinen. In diesem Deutungsrahmen wird *Gotham* als technologisches Gegenmittel inszeniert, das Desilosierung, Standardisierung und netzwerkbasierte Erkenntnis verspricht – ein Leitmotiv, das sich von der 2016 von der Innenministerkonferenz verabschiedeten Saarbrücker Agenda bis zum Bundesprogramm Polizei 2020 (P20) verfolgen lässt. Unter dem Signum der Effizienzsteigerung fungiert die Plattform als Antwort auf zersplitterte IT-Landschaften: konkret auf eine Vielzahl spezialisierter Fachanwendungen und zeitintensive manuelle Rechercheprakticken. Die einheitliche Benutzeroberfläche soll heterogene Datenbestände semantisch integrieren, analytische Prozesse beschleunigen und damit operative Entscheidungsabläufe verdichten.

Besondere Kontroversen löste der bayerische Mantelrahmenvertrag zu VeRA aus. Dieser eröffnet anderen Landespolizeien die Möglichkeit, ohne eigene Ausschreibung unmittelbar mit Palantir Technologies in Vertragsverhandlungen zu treten. Damit fungiert der Vertrag faktisch als bundesweiter Eintrittskanal: Er wahrt formal die föderale Autonomie, begünstigt jedoch zugleich die Marktdominanz eines US-amerikanischen Produkts. Hinzu kamen zeitlich befristete, im Mantelrahmenvertrag festgelegte Preisnachlässe (um circa die Hälfte), die Entscheidungsdruck erzeugten und kurzfristige Beschaffungslogiken gegenüber langfristigen Souveränitätserwägungen privilegierten (Kukral 2025).

Parallel verfolgt das Bundesprogramm P20 das Ziel, eine herstellerunabhängige Datenplattform zu etablieren, die perspektivisch auch Analysefunktionen integrieren soll. Da die Umsetzung jedoch stockt, wird *Gotham* vielfach als „Brückenlösung“ betrachtet. Gerade diese Übergangssemantik birgt Risiken: Übergangsinstrumente können durch die Anpassung organisatorischer Routinen, Schulungsformate und technischer Architekturen dauerhafte Abhängigkeiten erzeugen (Vendor Lock-In).

Die Einführung von *Gotham* ist somit nicht lediglich als technologischer Modernisierungsschritt zu verstehen, sondern markiert einen strukturellen Paradigmenwechsel in der polizeilichen Informationsarchitektur – mit weitreichenden Implikationen für Fragen staatlicher Souveränität in sicherheitsrelevanten Infrastrukturen.

Rechtliche Bewertung von Datenanalyseplattformen der Polizei

Die Debatte um die Implementierung der Datenintegrations- und Datenanalyseplattformen bei der deutschen Polizei erhielt 2023 durch ein wegweisendes Urteil des Bundesverfassungsgerichts (BVerfG) zur automatisierten Datenanalyse neue Dynamik (vgl. Bäuerle et al. 2025). Anlass waren Verfassungsbeschwerden gegen Neuregelungen in den Polizeigesetzen von Hamburg und Hessen, die den Einsatz von automatisierter Datenanalyse – in Hessen (nachträglich) für die Einführung von hessenDATA 2018 formuliert – zur Kriminalitätsbekämpfung erlaubten. § 25a Hessisches Sicherheits- und Ordnungsgesetz (HSOG) gestattete etwa, „in einem begründeten Einzelfall […] gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse“ zu verarbeiten, um Straftaten gemäß § 100a StPO vorzubeugen oder Gefahren für Staat, Leben oder Freiheit abzuwehren.

Das BVerfG erklärte beide Regelungen für verfassungswidrig. Es beanstandete insbesondere das Fehlen hinreichend bestimmter Eingriffsschwellen, unklare tatbestandliche Voraussetzungen sowie Verstöße gegen das Recht auf informationelle Selbstbestimmung (BVerfG Leitsätze zum Urteil des Ersten Senats vom 16.02.2023 — 1 BvR 1547/19 — 1 BvR 2634/20 — Automatisierte Datenanalyse). Automatisierte Datenanalyse stelle einen gewichtigen Grundrechtseingriff dar und bedürfe daher einer präzisen gesetzlichen Grundlage mit klar definierten Schutzmechanismen. Diesen Anforderungen genügten die beanstandeten Normen aus Sicht des BVerfG nicht.

Ein generelles Verbot entsprechender Systeme wie *Gotham* sprach das Gericht jedoch nicht aus. Vielmehr forderte es verfassungskonforme Ausgestaltungen mit effektiven Schutzvorkehrungen. In Hamburg wurde die einschlägige Norm vollständig gestrichen, da dort keine entsprechende Software implementiert war (BVerfG Leitsätze zum Urteil des Ersten Senats vom 16.02.2023 — 1 BvR 1547/19 — 1 BvR 2634/20 — Automatisierte Datenanalyse). In Hessen blieb hessenDATA in Teilen weiter in Betrieb; bestimmte Funktionen wurden deaktiviert, und der Landesgesetzgeber erhielt eine Frist zur Neuregelung. Im Sommer 2023 verabschiedete der Hessische Landtag eine überarbeitete Fassung, die unter anderem Zeug*innen und Angehörige von Beschuldigten vom Anwendungsbereich ausnimmt (Voigts 2023).

Gegen diese Neuregelung wurden abermals verfassungsrechtliche Einwände erhoben, unter anderem von der Gesellschaft für Freiheitsrechte (GFF) und der Humanistischen Union Marburg, die bereits das erste Verfahren unterstützt hatten. Kritiker*innen bemängeln weiterhin zu weit gefasste Eingriffsbefugnisse und eine unzureichende Eingrenzung des betroffenen Personenkreises. Pointiert wurde formuliert: Wer im Baumarkt Leim erwerbe, könne als potenzielle*r Klimaaktivist*in kategorisiert und damit zum Gegenstand automatisierter Datenanalyse werden (GFF 2024).

Politische Auseinandersetzungen um digitale Souveränität und Palantir

Die Auseinandersetzung um Palantir in Deutschland spitzte sich 2023 und 2024 zu und fand ihren Ausdruck in mehreren parlamentarischen Debatten auf Bundesebene. Ausgangspunkt war eine Plenardebatte im

Deutschen Bundestag im Dezember 2023, angestoßen durch einen Antrag der Unions-Fraktion mit dem Titel *Handlungsfähigkeit der Strafverfolgungsbehörden sichern*, in dem die damalige Bundesregierung aufgefordert wurde, die Entscheidung des Bundesinnenministeriums rückgängig zu machen, die Bundesplattform VeRA nicht weiterzuverfolgen. In dieser Debatte traten unterschiedliche Auffassungen von digitaler Souveränität deutlich hervor: Die CDU/CSU stellte vor allem die operative Handlungsfähigkeit des Staates in den Mittelpunkt und argumentierte, Souveränität bedeute, effektiv gegen Kriminalität vorgehen zu können; Palantir erscheine aus dieser Perspektive als das derzeit verfügbare Instrument mit den nötigen Funktionen. Kritische Hinweise auf Abhängigkeiten oder mangelnde Transparenz wurden von Teilen der Fraktion als „antiamerikanische Ressentiments“ zurückgewiesen (Bundestags-Drucksache 20/9495).

Die damaligen Regierungsfraktionen von SPD, Grünen und FDP vertraten hingegen ein stärker rechtsstaatlich und geopolitisch fundiertes Verständnis: Zwar wurde der Bedarf an modernen Analysewerkzeugen anerkannt, doch warnte man vor einem unreflektierten Transfer zentraler Sicherheitsinfrastrukturen an einen US-Anbieter. Vertreter*innen der SPD betonten, Ermittler*innen müssten die Funktionsweise der Systeme nachvollziehen können; Black-Box-Lösungen seien schwer mit rechtsstaatlichen Prinzipien vereinbar. Die Grünen hoben das Souveränitätsrisiko hervor, das entstünde, wenn eine Polizei-Analyseplattform maßgeblich von einem Unternehmen betrieben wird, das einem anderen Rechts- und Wertesystem verpflichtet ist. Die FDP wiederum verband Effizienz- und Grundrechtsperspektiven: Digitale Souveränität müsse IT-Architekturen so gestalten, dass sie sowohl handlungsfähige Strafverfolgung als auch hohe Datenschutzstandards ermöglichen, was ein gewisses Maß an technologischer Eigenständigkeit voraussetze (Deutscher Bundestag Stenografischer Bericht 142. Sitzung. Plenarprotokoll 20/142).

Vertieft wurde die Debatte in einer Anhörung des Innenausschusses im April 2024, bei der Expert*innen aus Ministerien, Polizeibehörden, der deutschen IT-Industrie, Datenschutzaufsicht, Wissenschaft und Zivilgesellschaft zu Wort kamen. Dort ließen sich grob vier Positionen unterscheiden: ein strategisch industrielles Verständnis, das auf den Aufbau eigener Plattformkompetenzen und die Reduktion struktureller Abhängigkeiten zielt; ein operativ pragmatisches Verständnis, das Souveränität primär als Fähigkeit der Polizei begreift, angesichts wachsender Datenmengen handlungsfähig zu bleiben; hybride Positionen, die eine zeitlich befristete Nutzung von Palantir mit dem parallelen Aufbau eigener Infrastrukturen verbinden wollen; sowie rechts- und grundrechtszentrierte Stimmen, die Souveränität vor allem als die Fähigkeit sehen, digitale Systeme wirksam an die Verfassung zu binden und demokratisch zu kontrollieren (Deutscher Bundestag, Ausschuss für Inneres und Heimat 2024).

Bemerkenswert ist, dass diese Konfliktlinien nicht strikt entlang typischer Parteigrenzen verlaufen, sondern auch unterschiedliche institutionelle Interessen widerspiegeln: Polizeigewerkschaften und IT-Verbände argumentieren anders als Datenschutzbehörden oder bürgerrechtliche Organisationen. Die Palantir-Debatte hat sich damit als eine Arena erwiesen, in dem konkurrierende Vorstellungen von Souveränität – effektive Strafverfolgung, technologische Eigenständigkeit, industrieller Standort und Grundrechtsbindung – gegeneinander abgewogen werden.

Gibt es deutsche/europäische Alternativen zu Palantir?

Die Frage nach Alternativen zu Palantir ist zu einem Prüfstein der Debatte um digitale Souveränität geworden. Oft wird sie verkürzt mit Ja oder Nein beantwortet – entweder mit Verweis auf fehlende „vollwertige“ Konkurrenzprodukte oder mit dem Hinweis auf kleinere europäische Anbieter. Tatsächlich ist die Lage komplexer.

Auf nationaler Ebene existiert eine Reihe von Unternehmen, die Module für Fallbearbeitung, Datenintegration oder grafbasierte Analysen anbieten, etwa Rola Security, T-Systems oder weitere mittelständische Anbieter. Diese Systeme sind häufig tief in bestehende polizeiliche Fachverfahren integriert, verfügen aber in der Regel nicht über die „ontologische“ Flexibilität und User-Interface-Operationalität, die *Gotham* auszeichnen. Zudem fokussieren sie meist bestimmte Funktionsbereiche (etwa Fallmanagement) statt eine übergreifende Analyseplattform zu bieten.

In Reaktion auf die Palantir-Debatte haben sich beispielsweise sieben deutsche IT-Unternehmen – darunter Branchengrößen wie SAP und Rola – zum Konsortium NaSA (Nationale Souveräne Analyseplattform) zusammengeschlossen. NaSA strebt eine modulare, mehrherstellerfähige Plattform an, die eine funktionale Alternative zu Palantir bereitstellen soll. Der Ansatz betont ausdrücklich die Vermeidung von Vendor Lock-In durch standardisierte Schnittstellen und die Möglichkeit, einzelne Module auszutauschen. Gleichzeitig machen Vertreter*innen des Konsortiums deutlich, dass ein solches Vorhaben ohne langfristige Finanzierungs- und Abnahmezusagen kaum realisierbar ist: Palantir selbst habe viele Jahre defizitär gearbeitet und sei erst durch umfangreiche US-Regierungsaufträge wirtschaftlich tragfähig geworden (NaSA o.D.).

Daneben existieren konzeptionelle Vorschläge, Plattformkern und Anwendungen stärker zu trennen. Ein von Atos und der Beratung Cassini vorgelegtes Papier skizziert eine staatlich betriebene Basisplattform, auf der unterschiedliche – auch kommerzielle – Analyse-Apps laufen könnten (Atos 2022). Digitale Souveränität würde hier in der Kontrolle über die Daten- und Infrastruktur-Schicht verortet werden, während Wettbewerb auf der Anwendungsebene stattfinden soll. Voraussetzung wäre allerdings, dass der Staat bereit ist, den Aufbau und Betrieb einer solchen Basisplattform langfristig zu tragen und klare technische Standards zu setzen, wofür sich insbesondere das Programm P20 anbieten würde.

Insgesamt lässt sich festhalten: Es gibt deutsche und europäische Ansätze, die mittelfristig zu tragfähigen Alternativen ausgebaut werden könnten. Gegenwärtig erreichen sie allerdings weder funktional noch organisatorisch die Stellung, die Palantir durch seine frühe Marktpräsenz und massive staatliche Förderung einnehmen konnte. Die Frage ist daher weniger, *ob* Alternativen grundsätzlich möglich sind, sondern *unter welchen politischen, finanziellen und institutionellen Bedingungen* sie entstehen und sich gegen einen etablierten Anbieter behaupten können.

Zusammenfassung

Der deutsche Streit um Palantirs *Gotham* ist mehr als eine technische Beschaffungsfrage – er steht

exemplarisch für das grundlegende Dilemma moderner Demokratien: Wie können Sicherheitsbehörden so digitalisiert werden, dass sie handlungsfähig bleiben, ohne zentrale Wissens- und Entscheidungsinfrastrukturen an private, häufig nichteuropäische Plattformunternehmen auszulagern? Im Kern gehen drei Spannungsfelder ineinander: Erstens das Verhältnis von Effizienz und Grundrechtsschutz. Datenintegrations- und Analyseplattformen machen polizeiliche Arbeit zweifellos effektiver, erweitern aber die Möglichkeiten tiefer Eingriffe in die informationelle Selbstbestimmung und erhöhen das Risiko von Diskriminierung und Fehlverdacht. Zweitens das Verhältnis von kurzfristiger Problemlösung und langfristiger Pfadabhängigkeit. Was als pragmatische Übergangslösung eingeführt wird, kann durch Anpassung organisatorischer Routinen, Schulungsformate und technischer Architekturen dauerhafte Abhängigkeiten erzeugen. Drittens das Verhältnis von nationaler und transnationaler Regulierung. Europäische Regelwerke wie die DSGVO oder der Data Act setzen zwar Rahmenbedingungen, lösen aber nicht das Problem, dass zentrale Komponenten sicherheitsrelevanter Infrastrukturen selbst transnationalen Rechtsregimen unterliegen.

Vor dem Hintergrund geopolitischer Risiken wie des CLOUD Act und der US-Sanktionen gegen europäische Institutionen wird Palantirs Einführung in Landespolizeien zu einem Kristallisationspunkt digitaler Souveränität, die sich von territorialer zu einer infrastrukturellen Frage verschiebt: Wer kontrolliert die Systeme, durch die staatliches Wissen erzeugt und operationalisiert wird? Das BVerfG-Urteil von 2023 fordert verfassungskonforme Ausgestaltungen mit präzisen Schwellenwerten und Schutzmechanismen, während parlamentarische Debatten unterschiedliche Souveränitätsverständnisse (operative Handlungsfähigkeit versus rechtsstaatliche Kontrolle) aushandeln. Alternativen wie das NaSA-Konsortium sind mittelfristig machbar, erfordern jedoch staatliche Investitionen und offene Standards, um Vendor Lock-In zu vermeiden.

Dr. Simon Egbert *ist Wissenschaftlicher Mitarbeiter am AI Ethics Research Hub der Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg und Leiter eines Forschungsprojektes zu polizeilichen Bodycams an der Universität Bielefeld. Er hat Social Sciences und Internationale Kriminologie studiert und 2018 an der Universität Hamburg im Fach Soziologie promoviert. Er hat national und international insbesondere zu Themen der Digitalisierung der Polizei, Datenanalyseplattformen und Prognosealgorithmen publiziert.*

Literatur

Atos 2022: Aufbau einer souveränen Recherche- und Analyseplattform für die Polizeien, https://atos.net/wp-content/uploads/2022/09/WP-Aufbau-einer-souveraenen-Recherche-und-Analyseplattform-fuer-die-Polizeien.pdf (nicht mehr aufrufbar; letzter Zugriff: 12.10.2025).

Bannerman, S. 2022: Platform imperialism, communications law and relational sovereignty, in: *New Media & Society*, Jg. 26, H. 4, S. 1–18; *https://doi.org/10.1177/14614448221077284*.

Bäuerle, M./Denker, K./Geminn, C./Schöndorf-Haubold, B. (Hrsg.) 2025: Big Data und KI bei der Polizei: Das Palantir-Urteil in der interdisziplinären Diskussion, Frankfurt am Main/New York.

Baur, A. 2025: European ambitions captured by American clouds: Digital sovereignty through Gaia-X? In: *Information, Communication & Society*, Jg. 29, H. 2, S. 417-434; https://doi.org/10.1080/1369118X.2025.2516545.

Bayerische Staatsregierung 2024: Herrmann: Staatsregierung beschließt Verbandsanhörung für Änderungen im Polizeiaufgabengesetz, in: *Dies.* vom 27.02.2024, https://www.bayern.de/herrmann-staatsregierung-beschliesst-verbandsanhoerung-fuer-aenderungen-im-polizeiaufgabengesetz/.

Bellanova, R./Carrapico, H./Duez, D. 2022: Digital/sovereignty and European security integration: An introduction, in: *European Security*, Jg. 31, H. 3, S. 337–355; https://doi.org/10.1080/09662839.2022.2101887.

Bowman, C./Jagasia, A./Vrabec, H. 2023: Palantir's Response to NTIA on Privacy, Equity, and Civil Rights, in: *Palantir Blog* vom 20.03.2023, https://blog.palantir.com/palantirs-response-to-ntia-on-privacy-equity-and-civil-rights-ee6eb0fbecc7.

Calderaro, A./Blumfelde, S. 2022: Artificial intelligence and EU security: The false promise of digital sovereignty. in: *European Security*, Jg. 31, H. 3, S. 415–434. https://doi.org/10.1080/09662839.2022.2101885.

Cipierre, P./Hiesserich, J. 2022: Palantir und Digitale Souveränität, in: *Palantir Blog* vom 23.02.2022, https://blog.palantir.com/palantir-und-digitale-souver%C3%A4nit%C3%A4t-bewahrung-der-handlungsf%C3%A4higkeit-in-einer-welt-in-bewegung-dd110ca31edf.

Deutscher Bundestag, Ausschuss für Inneres und Heimat (Hrsg.) 2024: Anhörung zur Analysesoftware Bundes-VeRA, in: *Deutscher Bundestag* vom 22.04.2024, https://www.bundestag.de/webarchiv/Ausschuesse/ausschuesse20/a04_inneres/anhoerungen/998570-998570.

Egbert, S. 2024: Algorithmisches Polizieren in Deutschland: Von Predictive Policing zu plattformisierter Polizeiarbeit, in: *Zeitschrift für Jugendkriminalrecht und Jugendhilfe*, Jg. 35, H. 2, S. 122–130.

Egbert, S./Ulbricht, L. 2024: Data integration and analysis platforms as digital platforms: A conceptual proposal, in: *Information, Communication & Society*, Jg. 27, S. 1–22; https://doi.org/10.1080/1369118X.2024.2442394.

Galis, V./Karlsson, B. 2024: A world of Palantir – ontological politics in the Danish police's POL-INTEL, in: *Information, Communication & Society*, Jg. 27, H. 13, S. 2438-2456; https://doi.org/10.1080/1369118X.2024.2410255.

Gesellschaft für Freiheitsrechte (GFF) 2024: GFF erhebt Verfassungsbeschwerde gegen Gesetzesnovelle: Hessen setzt verfassungswidrige Big-Data-Analyse fort, in: *GFF* vom 25.06.2024, https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-vb-big-data-analyse.

Iliadis, A./Acker, A. 2022: The seer and the seen: Surveying Palantir's surveillance platform, in: *The Information Society*, Jg. 38, H. 5, S. 334–363. https://doi.org/10.1080/01972243.2022.2100851.

Kleinz, T. 2025: Warum Europa meistens an der digitalen Souveränität scheitert, in: *Der Spiegel* vom 09.04.2025, https://www.spiegel.de/netzwelt/netzpolitik/gaia-x-galileo-limux-warum-europa-meistens-an-der-digitalen-souveraenitaet-scheitert-a-f7114aa7-8445-461d-b0ee-1598c312e0cd.

Knight, E./Gekker, A. 2020: Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures, in: *Surveillance & Society*, Jg. 18, H. 2, S. 231–243; https://doi.org/10.24908/ss.v18i2.13268.

Kukral, T. 2025: Palantir-Nutzung ohne rechtliche Grundlage? In: *Tagesschau.de* vom 28.07.2025, https://www.tagesschau.de/inland/innenpolitik/palantir-baden-wuerttemberg-100.html.

Laaf, M. 2025: Diese E-Mail ist unzustellbar, in: *Die Zeit* vom 23.07.2025, https://www.zeit.de/digital/internet/2025-07/microsoft-email-sperre-karim-khan-donald-trump-istgh.

NaSA o.D.: Nationale souveräne Analyseplattform: Das Projekt NaSA, https://www.linkedin.com/posts/heinz-kreuter-6831936b_nationale-souveräne-analyse-plattform-activity-7140730946109992961-tHkA/?utm_source=share&utm_medium=member_desktop&rcm=ACoAADJSnrwBs8skObMJBi8HMDtJKhWl5lye
.

Palantir 2022: Ontology: Finding meaning in data (Palantir RFx Blog Series, #1), in: *Palantir Blog* vom

03.10.2022, https://blog.palantir.com/ontology-finding-meaning-in-data-palantir-rfx-blog-ser-ies-1-399bd1a5971b.

Pohle, J. 2020: Digitale Souveränität, in: Klenk, T./Nullmeier, F./Wewer, G. (Hrsg.): *Handbuch Digitalisierung in Staat und Verwaltung*, Wiesbaden, S. 1-13; https://doi.org/10.1007/978-3-658-23669-4_21-1.

Pohle, J. 2024: Unthinking digital sovereignty: A critical reflection on EU narratives, in: *Policy & Internet*, Jg. 16, H. 2, S. 247–265; https://doi.org/10.1002/poi3.437.

Pohle, J./Thiel, T. 2021: Digitale Souveränität, in: Piallat, C. (Hrsg.): *Der Wert der Digitalisierung. Gemeinwohl in der digitalen Welt*, Bielefeld, S. 319–340.

Reul, H. 2020: Schriftlicher Bericht des Ministers des Innern für die Sitzung des Innenausschusses am 19.11.2020 zu dem Tagesordnungspunkt „Umstrittene Polizei-Software der Firma Palantir für das LKA NRW Antrag der Fraktion Bündnis 90/Die Grünen vom 09.11.2020. Landtag Nordrhein-Westfalen, https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-4200.pdf.

Roberts, H./Cowls, J./Casolari, F./Morley, J./Taddeo, M./Floridi, L. 2021: Safeguarding European values with digital sovereignty: An analysis of statements and policies, in: *Internet Policy Review*, Jg. 10, H. 3; https://doi.org/10.14763/2021.3.1575.

Rojszczak, M. 2020: CLOUD act agreements from an EU perspective, in: *Computer Law & Security Review*, Jg. 38, 105442, S. 1-14; https://doi.org/10.1016/j.clsr.2020.105442.

Sawall, A. 2025: Microsoft kann US-Zugriff auf EU-Cloud nicht verhindern, in: *Golem* vom 20.07.2025, https://www.golem.de/news/anton-carniaux-microsoft-kann-us-zugriff-auf-eu-cloud-nicht-verhindern-2507-198283.html.

Staatsministerium Baden-Württemberg 2025: Ermittlungsbehörden erhalten neue Instrumente, in: *Baden-Württemberg Staatsministerium* vom 29.07.2025, https://stm.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/ermittlungsbehoerden-erhalten-neue-instrumente.

Ta?kale, A. R. 2025: Manufacturing the Leviathan: Palantir's 'Technological republic' and the nationalist faction of the tech oligarchy, in: *Science as Culture*, 1–11; https://doi.org/10.1080/09505431.2025.2607360.

Ulbricht, L./Egbert, S. 2024: In Palantir we trust? Regulation of data analysis platforms in public security, in: *Big Data & Society*, Jg. 11, H. 3, S. 1–15; https://doi.org/10.1177/20539517241255108.

Vlassis, V. 2024: More than software vendors. The peculiar case of Palantir's data integration platforms, in: *Information, Communication & Society*, Jg. 27, S. 1-20; https://doi.org/10.1080/1369118X.2024.2442399.

Voigts, H. 2023: Hessen: Viel Kritik am Sicherheitsgesetz, in: *Frankfurter Rundschau* vom 28.06.2023, https://www.fr.de/rhein-main/landespolitik/hessen-viel-kritik-am-sicherheitsgesetz-im-landtag-92370202.html.

Zellinger, P. 2025: „Digitale Auslöschung": Wie US-Sanktionen einen europäischen Richter lahmlegen, in: *Der Standard* vom 26.11.2025, https://www.derstandard.at/story/3000000298066/digitale-ausloeschung-wie-us-sanktionen-einen-europaeischen-richter-lahmlegen.

---

https://www.humanistische-union.de/publikationen/vorgaenge/vorg-254/publikation/digitale-souveraenitaet-in-zeiten-plattformisierter-polizeiarbeit/
Abgerufen am: 21.09.2026