Ein neues Betriebssystem des Staates

Warum Palantir rechtsstaatliche Strukturen verändert

Hannah Ruschemeier & Rainer Mühlhoff

03.09.2026 doi: 10.59704/540a9b8960e14eea

Palantir verfolgt das Ziel, das Betriebssystem des Staates[1] zu werden. Das Unternehmen verkauft mit seiner Software zur Verarbeitung staatlicher Daten eine proprietäre Infrastruktur, die festlegt, wie staatliche Stellen Daten verknüpfen, Informationen auswerten und Entscheidungen vorbereiten. Die Produkte sollen bestehende Arbeitsabläufe verändern und die Organisationen, die sie einsetzen, selbst umgestalten. Damit greift Palantir bereits jetzt in die staatliche Entscheidungsarchitektur ein – in den USA ebenso wie in anderen Ländern. Francesca Bria hat die engen Verbindungen des Unternehmens zu politischen Entscheidungsträger:innen in ihrem Projekt *„The authoritarian stack“*[2] dokumentiert. Palantir schafft durch seine Produkte eine proprietäre Infrastruktur, die mehr als eine Datenplattform sein soll – sie soll Organisationen verändern und zu diesen Organisationen gehört auch der Staat.

Die rechtsstaatliche Problematik des Einsatzes von Palantir-Produkten im staatlichen Bereich erschöpft sich nicht in den aufsehenerregenden Äußerungen Peter Thiels oder den nicht weniger exzentrischen Auftritten des Palantir-CEOs Alex Karp. Entscheidend ist vielmehr der Selbstanspruch des Unternehmens. Dieser tritt sowohl im aufschlussreichen Palantir-Manifest[3] hervor, das unmissverständlich Machtansprüche formuliert, das Geschäftsmodell als moralische Mission verklärt und vor Demokratieverachtung strotzt, als auch im infrastrukturellen Design der Palantir-Produkte selbst. Das Unternehmen beansprucht dabei nicht lediglich die Rolle eines staatlichen Auftragnehmers, sondern positioniert sich als funktional überlegene Alternative zum Staat selbst.

Palantir-Systeme als staatliche Infrastruktur

Palantir bietet Softwarelösungen in nahezu allen Bereichen staatlicher Aufgaben an – vom Militär und der inneren Sicherheit bis hin zur Daseinsfürsorge für Gesundheit, Verwaltung und Sozialwesen. Die Firma vermarktet ihre Software als Mittel zur Gewinnung verwertbarer Erkenntnisse, zur Erkennung von Mustern und zur Unterstützung komplexer operativer Entscheidungen. In den USA unterhält die Firma milliardenschwere Verträge mit dem Verteidigungsministerium[4] und zahlreichen weiteren staatlichen Bereichen, im Vereinigten Königreich mit dem nationalen Gesundheitssystem NHS.[5] Die in Deutschland im Einsatz befindlichen Produkte von Palantir ermöglichen sowohl eine Aufbereitung von Daten, die bereits staatlicherseits vorhanden sind, als auch eine Datenanalyse durch Mustererkennung, z.B. zur Gefährdungsidentifikation. Zurzeit nutzen Polizeibehörden in Bayern, Hessen und Nordrhein-Westfalen Palantir-Systeme; Baden-Württemberg kommt im Laufe des Jahres 2026 hinzu.[6] Bayern hat zudem einen Rahmenvertrag abgeschlossen, dem andere Bundesländer und

[1] United States Securities And Exchange Commission, Registration Statement, Under the Securities Act of 1933, Palantir Technologies Inc., https://www.sec.gov/Archives/edgar/data/1321655/000119312520230013/d904406ds1.htm, zuletzt abgerufen am 13.08.2026.

[2] The Authoritarian Stack, *How Tech Billionaires Are Building a Democratic America – And Why Europe Is Next*, https://www.authoritarian-stack.info/, zuletzt abgerufen am 13.08.2026.

[3] Paul Nemitz, *Die Waffen des Silicon Valley, Eine Kritik an Alex Karps Manifest der digitalen Gewalt*, Verfassungsblog, 15.06.2026, https://verfassungsblog.de/palantir-manifest/, zuletzt abgerufen am 13.08.2026.

[4] S. Fn. 2

[5] The Guardian, *The Guardian View on NHS Records: Patients Are not Raw Material for Big Tech, Ministers Should End Palantir's Contract Before Medical Confidentiality is Sacrificed to Silicon Valley's Appetite for Public Data*, 04.06.2026, https://www.theguardian.com/commentisfree/2026/jun/04/the-guardian-view-on-nhs-records-patients-are-not-raw-material-for-big-tech, zuletzt abgerufen am 13.08.2026.

der Bund ohne weitere Vergabeverfahren beitreten können. Durch kostenlose Testnutzungsräume versucht die Firma, staatliche Akteure an sich zu binden, idealerweise ohne öffentliche Ausschreibungsverfahren.[7]

Am Beispiel NHS[8], mit dem Palantir einen Siebenjahresvertrag abgeschlossen hat, zeigen sich Entwicklungen, vor denen Kritiker:innen bereits seit Langem warnen: Erstens überträgt der Staat Infrastrukturen, auf die er für die Erfüllung seiner Aufgaben zwingend angewiesen ist, an ein privates Unternehmen. Zweitens weitet der Einsatz von Palantir die Zugriffs- und Nutzungsbefugnisse auf staatliche Daten schrittweise aus und unterläuft damit deren Zweckbindung. Drittens bleibt vielfach undurchsichtig, wie die Palantir-Systeme funktionieren – und damit auch, wer für die Entscheidungen verantwortlich ist, die auf ihrer Grundlage getroffen werden.

Staatliche Kernaufgaben: Gesundheit und Sicherheit

Gesundheitsversorgung[9] und Sicherheit[10] sind nach dem deutschen Verfassungsverständnis Grundaufgaben des Staates. Die Übertragung wesentlicher Infrastrukturen in diesen Bereichen an Unternehmen wie Palantir ist weder eine klassische Auftragsvergabe durch die öffentliche Hand noch eine konventionelle Privatisierung, sondern geht mit einem Verlust an staatlicher Kontrolle und einer Veränderung von Entscheidungslogiken staatlichen Handelns einher.

Seinen genuinen Aufgaben kann sich der Staat nicht entziehen, ohne damit zugleich den demokratisch legitimierten Herrschaftsanspruch aufzugeben und die freiheitliche Verfassungsordnung zu gefährden. Daraus folgt, dass zwar eine private Auslagerung staatlicher *Aufgaben* möglich und ggf. sogar geboten sein kann, während eine Auslagerung staatlicher *Funktionen* ausgeschlossen sein muss. Die Grenze wird dort überschritten, wo der Staat die Kontrolle über die Erfüllung seiner Aufgaben verliert. Führt die Etablierung privater Infrastrukturen etwa dazu, dass Gesundheitssystem und Polizei nur arbeitsfähig sind, wenn Palantirs Systeme laufen, erzeugt dies ein solches Szenario des funktionalen Kontrollverlusts.

Mitarbeiter:innen von Palantir haben personalisierte Zugangskennungen für Landeskriminalämter; Updates werden vor Ort aufgespielt.[11] Im Bereich der Polizei, die das Gewaltmonopol des Staates ausübt, ist dies offensichtlich rechtsstaatlich defizitär. Neben Fragen der Gesetzesbindung und Transparenz entsteht ein Sicherheitsrisiko: Wissen über polizeiinterne Datenverarbeitungsprozesse und -strukturen sowie Organisationswissen der Polizei gelangt an ein privates Unternehmen. Zugleich bleibt unklar, wer für Entscheidungen verantwortlich ist, wenn der Staat zwar formal die Verantwortung trägt, die technischen Entscheidungsstrukturen aber nicht selbst kontrollieren kann.

Diese Abhängigkeiten beschränken sich nicht auf die technische Ebene: Je länger Behörden zentrale Verwaltungs- und Sicherheitsaufgaben über dieselbe proprietäre Plattform organisieren, desto stärker richten sich Arbeitsabläufe, Datenstrukturen, Aus- und Fortbildung sowie organisatorisches Wissen an den Vorgaben und Eigenschaften dieser Plattformen aus. Die Software formt damit schrittweise staatliche Abläufe und Entscheidungsarchitekturen. Der Staat nutzt sie dann nicht nur als Werkzeug für im Voraus definierte, von den Möglichkeiten der Software unabhängige Zwecke, sondern übernimmt ihre Kategorien, Arbeitslogiken und Formen der Informationsaufbereitung. Bei technischen Diensten, die in dieser Weise tief in den inhaltlichen und materiellen Gehalt staatlicher Prozesse vordringen, ist ein Wechsel zu einem anderen Anbieter dann nicht nur aus finanziellen Gründen erschwert: Die Behörde hat sich organisatorisch an die Software angepasst.

[6] SWR, *Landtag beschließt Nutzung umstrittener Polizei-Software von Palantir*, 12.11.2025, https://www.swr.de/swraktuell/baden-wuerttemberg/landtag-beschliesst-nutzung-von-palantir-100.html, zuletzt abgerufen am 13.08.2026.
[7] The Stack, *Government Warned on Free (and competition-free) Palantir Contracts Over Ukraine Scheme*, 17.10.2023, https://www.thestack.technology/government-warned-over-free-and-competition-free-palantir-contracts/, zuletzt abgerufen am 13.08.2026.
[8] Robert Booth, *Palantir's Access to Identifiable NHS England Patient Data Is 'Dangerous', MPs Say*, The Guardian, 11.05.2026, https://www.theguardian.com/society/2026/may/11/palantir-access-nhs-england-patient-data, zuletzt abgerufen am 13.08.2026.
[9] BVerfG, 1 BvR 347/98, 06.12.2005.
[10] BVerfG, 1 BvR 1547/19, 1 BvR 2634/20, 16.02.2023.

Epistemische Abhängigkeiten

Rechtsstaatlich entscheidend ist, dass der Staat die Infrastruktur seiner Wissensproduktion auf proprietäre Plattformen verlagert. Denn damit verändert sich grundlegend, welche Informationen sichtbar werden, welche Zusammenhänge Behörden erkennen und welche Schlussfolgerungen sie als naheliegend betrachten. Plattformen wie Gotham ordnen Informationen nicht lediglich neu, sondern prägen die Kategorien, nach denen Behörden ihre Daten interpretieren. Sie beeinflussen damit bereits die Phase, in der aus Daten überhaupt erst entscheidungsrelevantes Wissen entsteht. Der Staat gibt so nicht nur technische Funktionen aus der Hand, sondern einen Teil der operativen Bedingungen staatlicher Entscheidungsfindung. Die Macht solcher Plattformen ist epistemisch: Sie prägen und strukturieren den Wissens- und Erkenntnishorizont staatlicher Institutionen.

Das zeigt zugleich, warum sich digitale Souveränität hier nicht auf die geopolitische Abhängigkeit von amerikanischen Technologieunternehmen reduzieren lässt. Für den Aspekt der Souveränität ist vielmehr entscheidend, welche Rolle proprietäre Analyseplattformen innerhalb staatlicher Institutionen übernehmen – unabhängig davon, ob ein US-amerikanisches oder ein europäisches Unternehmen sie entwickelt. Die häufig erhobene Forderung nach einer „europäischen Alternative“ zu Palantir (wie z.B. der französischen Firma ChapsVision[12]) greift deshalb zu kurz. Auch ein europäischer Anbieter würde den rechtsstaatlichen Grundkonflikt nicht auflösen, der darin besteht, dass seine Plattformen die institutionellen Arbeitsweisen von Polizei, Sicherheitsbehörden oder Gesundheitsverwaltung strukturieren, ihre Prozesslogik materiell gestalten und darüber Abhängigkeit und materielle Eingriffe produzieren. Der rechtsstaatliche Einwand richtet sich daher nicht primär gegen bestimmte Unternehmen, sondern gegen eine Form staatlicher Digitalisierung, in der private Plattformen die epistemische Infrastruktur staatlichen Handelns bereitstellen.

Aus demselben Grund knüpft unsere Kritik nicht an den politischen Überzeugungen einzelner CEOs wie Alex Karp oder Peter Thiel oder an bestimmte Ideologien der Tech-Industrie an. Solche Faktoren mögen die Bewertung einzelner Unternehmen verschärfen, sie begründen aber nicht das rechtsstaatliche Problem selbst, das auch bei alternativen Unternehmen bestehen würde, deren Führungspersonal nicht durch antidemokratische öffentliche Stellungnahmen auffallen würde.

Zweckbindung als Voraussetzung von Kontrollierbarkeit

Palantirs Geschäftsmodell beruht auf der Verarbeitung von Daten, weshalb der Zugang zu staatlichen Daten eine zwingende Voraussetzung für den Betrieb dieser Systeme ist. In der deutschen Debatte wird immer wieder beschwichtigend betont, dass bei der Verwendung dieser Systeme keine staatlichen Daten in private Hände abfließen können, da die Software *„on-premises“* (also z.B. auf Servern bei der Polizei selbst)[13] gehostet würde.

Das gut dokumentierte Phänomen des *function creep*[14] zeigt aber, dass technische Zugriffsmöglichkeiten, wenn sie einmal bestehen, auch genutzt werden, und zwar weit über ihren ursprünglichen Zweck hinaus. Als jüngstes und extremes Beispiel ist die Nutzung von Werbedaten durch die amerikanische Immigrationsbehörde ICE zu nennen[15], deren Vorgehen erheblichen rechtsstaatlichen Bedenken ausgesetzt ist. Vor diesem Missbrauchspotenzial wird seit Langem gewarnt. Auch beim britischen NHS begann die Zusammenarbeit mit Palantir mit der Aufbereitung von Daten und Nutzeroberflächen. Später dann erhielt Palantir Zugang zu personenbezogenen Patient:innendaten[16], um KI-Anwendungen zu trainieren.

[11] Konrad Litschko und Gareth Joswig, *Palantir in Deutschland, Überwachung first, Bedenken second*, taz, 15.06.2026, https://taz.de/Einsatz-von-Palantir-in-Deutschland-Fast-alle-Bundeslaender-sind-dagegen-ein-Grund-zur-Entwarnung/!6186360/, zuletzt abgerufen am 13.08.2026.

[12] Jörg Diehl, Florian Flade und Lorenz Jeric, *Datenanalyse-Software, Verfassungsschutz setzt auf Palantir-Alternative*, tagesschau, 13.05.2026, https://www.tagesschau.de/investigativ/ndr-wdr/verfassungsschutz-palantir-100.html, zuletzt abgerufen am 13.08.2026.

[13] Marie-Claire Koch, *„Ein erheblicher Grundrechtseingriff“: Über Risiken beim Einsatz von Palantir*, heise online, 16.07.2025, https://www.heise.de/hintergrund/Polizeiliche-Datenanalyse-Kommt-Palantir-bald-fuer-uns-alle-10489336.html, zuletzt abgerufen am 13.08.2026.

Nach öffentlicher Kritik soll die Vertragsverlängerung nun geprüft werden.

Aus grundrechtlicher Perspektive ist nicht erkennbar, wie der Zweckbindungsgrundsatz und andere datenschutzrechtliche Anforderungen eingehalten oder überhaupt überprüft werden können. Die Palantir-Software Gotham kann Informationen in Polizeidatenbanken über Millionen von Menschen aufbereiten, zusammenführen und analysieren. Je mehr Datenbestände eine solche Plattform verknüpft und je vielfältiger sie kategorisiert und auswertet, desto schwieriger wird es, die ursprünglichen Zwecke der Datenerhebung und die daran geknüpften Schutzvorkehrungen – Grundlagen des Daten- und Persönlichkeitsschutzes – aufrechtzuerhalten. Insbesondere bei prädiktiven Analysen im Sicherheitsbereich droht damit die Zweckbindung ihre Funktion als Grenze staatlicher Datenverarbeitung zu verlieren – unabhängig von Palantir. Rechtsstaatlichkeit setzt voraus, dass staatliche Machtausübung kontrollierbar und begrenzt bleibt. Das gilt auch für die Verarbeitung von Daten.

Die rechtspolitische Diskussion über die Ausweitung des Einsatzes von Palantir-Software zeugt von verfassungsrechtlicher Ignoranz. Das Bundesverfassungsgericht hat in zahlreichen Verfahren, u. a. zum Palantir-Einsatz in Hessen[17], klare Anforderungen an den rechtsstaatlichen Einsatz automatisierter Datenanalyse formuliert; der LDI in Nordrhein-Westfalen hat den Einsatz der Software für rechtswidrig[18] befunden. Der hessische Innenminister sieht bereits jetzt ohne die Software von Palantir „eine erhebliche Sicherheitslücke“[19]. Damit hat Palantir sein Ziel bereits erreicht.

Staatliche Verfahren müssen Machtkonzentration verhindern

Das Versprechen, das hinter der Anschaffung von Systemen wie denen von Palantir steht, ist ein ökonomisches Verständnis von Effizienzsteigerung durch Integration von Systemen und Daten über Behördengrenzen hinweg, Echtzeitverfahren und prädiktive Analyse. Sie sollen damit die bürokratischen Reibungen beseitigen, die durch Zuständigkeiten, getrennte Datenbestände, festgelegte Verfahrensschritte und Dokumentationspflichten entstehen. Aus rechtsstaatlicher Perspektive ist jedoch nicht jede Form administrativer Reibung ein Defizit. Vielmehr erfüllen sie als organisatorische Begrenzungen eine wichtige Schutzfunktion. Sie beschränken den Zugriff staatlicher Stellen auf Informationen, verteilen Verantwortung auf unterschiedliche Institutionen und erschweren die Konzentration staatlicher Macht, wodurch das Risiko ihres Missbrauchs verringert wird. Die normative Organisation staatlicher Verfahren ist deshalb keine bloße Ineffizienz, sondern ein institutioneller Sicherungsmechanismus für Grundrechtsgeltung, Gewaltenteilung und Gesetzesbindung. Was ein Softwareunternehmen als Effizienzgewinn betrachtet, kann aus rechtsstaatlicher Perspektive den Abbau jener institutionellen Schranken bedeuten, die staatliche Machtausübung kontrollierbar halten.

Kontrollierbare Machtausübung setzt zudem voraus, dass staatliches Handeln transparent und nachvollziehbar bleibt: Gesetze werden öffentlich verkündet und sind damit verfassungsrechtlich überprüfbar, geheime Grundrechtseingriffe unterliegen höheren Anforderungen[20], handelnde staatliche Stellen sind identifizierbar. Wenn die Entscheidungslogik eines staatlichen Systems selbst für die Behörde nicht nachvollziehbar ist, kann auch ihr Handeln nicht wirksam kontrolliert werden. Eine nachgeschaltete staatliche Gefährdungshaftung reicht bei so weitreichenden Grundrechtseingriffen nicht aus, zumal Betroffene Schaden und Rechtsverletzung schwer nachweisen können.

Hier zeigt sich ein grundlegender Unterschied zwischen der Logik digitaler Plattformen und rechtsstaatlichen Prinzipien. Digitale Plattformen sollen

[14] Bert-Jaap Koops, *The Concept of Function Creep*, Taylor & Francis, 16.03.2021, https://www.tandfonline.com/doi/full/10.1080/17579961.2021.1898299, zuletzt abgerufen am 13.08.2026.
[15] Rainer Mülhoff und Hannah Ruschemeier, *Von personalisierter Werbung zur staatlichen Verfolgung, Zweckbindung als Grundrechtsschutz im Zeitalter von KI*, Verfassungsblog, 03.02.2026, https://verfassungsblog.de/von-personalisierter-werbung-zur-staatlichen-verfolgung/, zuletzt abgerufen am 13.08.2026.
[16] S. Fn. 8.

Informationsgrenzen überwinden, Datenbestände zusammenführen und Entscheidungsprozesse möglichst nahtlos organisieren. Private Systeme wie Palantir zielen außerdem auf Abschirmung gegenüber Wettbewerber:innen und Bindung der Nutzer:innen an das Ökosystem der Plattform, um Abhängigkeiten und Lock-in-Effekte zu schaffen. Der demokratische Rechtsstaat verfolgt dagegen kein lineares Projekt der ökonomischen Optimierung durch einen einzelnen Anbieter: Seine Institutionen sind deshalb nicht primär darauf ausgelegt, staatliches Handeln nach externen Maßstäben möglichst ökonomisch effizient zu gestalten, sondern staatliche Macht rechtlich zu binden und organisatorisch zu verteilen.

Somit liegt das rechtsstaatliche Problem proprietärer Analyseplattformen nicht allein auf technischer oder wirtschaftlicher Ebene. Mit ihrer Einführung übernimmt der Staat schrittweise eine außerstaatliche Vorstellung davon, was gute Organisation bedeutet: Integration eines zentralen privaten Systems statt funktionaler Trennung der verschiedenen Zweckkontexte, kontinuierliche Lagebilder statt anlass- und zweckgebundener Informationsaufbereitung, Verhaltensvorhersagen statt substanzieller Verdachtsmomente. Die eigentliche Herausforderung liegt deshalb nicht darin, dass staatliche Verfahren digitalisiert werden. Sie liegt darin, dass sich mit proprietären Plattformen ein Organisationsverständnis etabliert, das rechtsstaatliche Sicherungen systematisch als Reibungsverluste interpretiert. Ein demokratischer Rechtsstaat darf seine Verfahren aber nicht allein nach ihrer ökonomischen Effizienz bewerten.

Eine materielle Privatisierung staatlicher Kernaufgaben ist mit den rechtsstaatlichen Anforderungen an das staatliche Gewaltmonopol nicht vereinbar. Durch die Integration proprietärer, nicht kontrollierbarer digitaler Systeme auf infrastruktureller Ebene erfolgt kein singulärer „Ausverkauf von Hoheitsrechten“, sondern eine schleichende Aushöhlung demokratischer Legitimation, Gewaltenteilung und Gesetzesbindung sowie effektiver Rechtsschutzmöglichkeiten – zentrale Elemente unseres rechtsstaatlichen Verständnisses.

Beide Autor:innen haben im gleichen Umfang zu diesem Artikel beigetragen.

[17] S. Fn. 10; siehe hierzu auch André Bartsch, *Welche Daten? Zur geplanten Einführung automatisierter Datenanalysen bei BKA, Bundespolizei und Staatsanwaltschaften*, Verfassungsblog, 30.08.2024.

[18] Marcel Rosenback und Alexander Sarovic, *Umstrittenes US-Unternehmen, NRW-Datenschutzbeauftragte hält Einsatz von Palantir-Software für unzulässig*, Der Spiegel, 15.04.2021, https://www.spiegel.de/netzwelt/palantir-nrw-datenschuetzerin-haelt-einsatz-von-software-fuer-unzulaessig-a-af196b3f-b93c-475d-86d7-8e569d25490c, zuletzt abgerufen am 13.08.2026.

[19] Nils Metzger, *US-Analysesoftware für deutsche Polizei, Trotz wirrem Polit-Manifest: Länder halten an Palantir fest*, zdfheute, 22.04.2026, https://www.zdfheute.de/politik/deutschland/palantir-manifest-polizei-innenminister-bundeslaender-reaktion-kritik-100.html, zuletzt abgerufen am 13.08.2026.

[20] BVerfG, 1 BvR 370/07, 1 BvR 595/07, 27.02.2008.

AUTOR*INNEN

Hannah Ruschemeier
Hannah Ruschemeier ist Inhaberin des Lehrstuhls für Öffentliches Recht an der Universität Osnabrück.
Rainer Mühlhoff
Prof. Dr. Rainer Mühlhoff, Philosoph und Mathematiker, ist Professor für Ethik der Künstlichen Intelligenz an der Universität Osnabrück. Er forscht zu Ethik, Datenschutz und kritischer Sozialtheorie in der digitalen Gesellschaft. Foto (c) 2020 Felix Noak.

EMPFOHLENE ZITATION

Ruschemeier, Hannah; Mühlhoff, Rainer: Ein neues Betriebssystem des Staates: Warum Palantir rechtsstaatliche Strukturen verändert, Verfassungsblog, 03.09.2026, doi: 10.59704/540a9b8960e14eea.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260903-145039-0.