Der Staat als digitaler Vasall

Wie die §§ 98d, 98e StPO-E die digitale Souveränität aushöhlen

Janique Brüning

03.09.2026 doi: 10.59704/fab009eb174bdd19

Ende April 2026 beschloss die Bundesregierung den Entwurf des „Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“ und normierte mit den §§ 98d und 98e StPO-E zwei neue Ermittlungsbefugnisse. Gleichsam im Vorbeigehen entscheidet der Regierungsentwurf aber auch mit, welche technische Infrastruktur der Staat künftig nutzen will, um ermittlungsrelevantes Wissen zu erzeugen. Der Entwurf setzt dabei voraus, dass leistungsfähige Analyseplattformen verfügbar sind und kalkuliert in der Kostenbegründung damit, jene Systeme, die bereits in der Gefahrenabwehr eingesetzt werden, weiter zu nutzen. Somit setzt der Entwurf auch auf das Auswertungstool Gotham des US-amerikanischen Unternehmens Palantir. Das eigentliche Problem betrifft damit nicht nur zu niedrige materielle Eingriffsschwellen oder einen fehlenden Richtervorbehalt. Ein Staat, der die Technik seiner Grundrechtseingriffe nicht hinreichend prüfen und unabhängig vom Hersteller weiterbetreiben kann, beherrscht den Eingriff nicht und verstößt gegen den Grundsatz der digitalen Souveränität.

Zwei neue Instrumente staatlicher Wissenserzeugung

§ 98d Abs. 1 StPO-E erlaubt, biometrische Daten aus einem Strafverfahren mit öffentlich zugänglichen Daten aus dem Internet abzugleichen. Erfasst sind nicht nur frei auffindbare Bilder, Videos oder Stimmen, sondern auch Inhalte, die erst nach Registrierung, Genehmigung oder Entgeltzahlung zugänglich sind. Der Abgleich darf der Sachverhaltsaufklärung sowie der Identifizierung oder Lokalisierung eines Beschuldigten oder Zeugen dienen. Er setzt den Verdacht einer Straftat von auch im Einzelfall erheblicher Bedeutung voraus, muss subsidiär sein und darf keine Echtzeitdaten einbeziehen.

Noch weiterreichende Befugnisse gewährt § 98e StPO-E. Die Vorschrift erlaubt, rechtmäßig gespeicherte personenbezogene Daten aus unterschiedlichen präventiven und repressiven polizeilichen Datei- und Informationssystemen auf einer Analyseplattform verfahrensübergreifend weiterzuverarbeiten. Das System darf gem. § 98e Abs. 4 StPO-E u.a. Beziehungen zwischen Personen, Gruppen, Institutionen, Orten und Objekten herstellen, Informationen klassifizieren und visualisieren, Suchkriterien gewichten und Daten statistisch auswerten. Ausdrücklich können ausweislich der Entwurfsbegründung auch KI-Systeme und Sprachmodelle eingesetzt werden.[1] Voraussetzung ist der Verdacht einer auch im Einzelfall schwerwiegenden Straftat i.S.d. § 100a Abs. 2 StPO.

Mit dem Einsatz dieser Ermittlungsbefugnisse verschiebt sich der Schwerpunkt der Informationsgewinnung. Ausgangspunkt der StPO war bislang eine konkrete Ermittlungsmaßnahme, mit der anlässlich eines Tatverdachts Daten zu einem bestimmten Sachverhalt erhoben und anschließend ausgewertet wurden. Demgegenüber zielen die in den §§ 98d, 98e StPO geregelten Befugnisse nicht auf die Erhebung neuer Daten, sondern auf die weitergehende Auswertung bereits vorhandener Datenbestände. Durch deren nachträgliche Verknüpfung können bislang nicht erkennbare Zusammenhänge aufgedeckt und daraus neue Erkenntnisse gewonnen werden.

[1] Bundesregierung, *Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen*, 01.07.2026, BT-Drucks. 21/6806, S. 14.

Die rein strafprozessuale Kritik greift, aber zu kurz

Das BVerfG hat in seiner sog. Palantir-Entscheidung[2] zur automatisierten Datenanalyse in Hessen und Hamburg betont, dass diese Form der Datenverarbeitung ein eigenes Eingriffsgewicht[3] besitze, das nicht nur von der ursprünglichen Datenerhebung abhänge, sondern auch von Umfang und Sensibilität der Bestände, der Offenheit der Methode und der Aussagekraft der erzeugten neuen Ergebnisse.[4] Insbesondere müssten Datenbestände und Analysemethoden umso enger begrenzt werden, je leistungsfähiger das System und je sensibler die ausgewerteten Daten seien.

Der Regierungsentwurf versucht, diese Stufenlogik in § 98e StPO umzusetzen: Zunächst dürfen nur Vorgangs- und Falldaten einbezogen werden. Daten aus Telekommunikationsüberwachungen, Funkzellenabfragen, Quellen-Telekommunikationsüberwachungen oder Asservaten können dagegen nur ergänzend berücksichtigt werden, soweit dies erforderlich ist, während Daten aus Online-Durchsuchungen und akustischen Wohnraumüberwachungen in anderen Verfahren vollständig ausgeschlossen sind. Die Entwurfsbegründung nutzt diese Abstufung jedoch vor allem, um das Eingriffsgewicht zu reduzieren.[5] Denn statt zu fragen, welche „unterschiedliche[n] Vorkehrungen und Kombinationen von Schutzmechanismen“[6] die verbleibende Eingriffsintensität erfordert, wird dargelegt, aus welchem Grund der Eingriff nicht ganz so schwer wiege.

Vor allem die formellen Schutzmechanismen vermögen nicht zu überzeugen. § 98d Abs. 4 StPO-E überträgt die Anordnung grundsätzlich der Staatsanwaltschaft, bei Gefahr im Verzug dürfen ausnahmsweise ihre Ermittlungspersonen handeln. Ein Richtervorbehalt, der selbst für eine einfache Durchsuchung verfassungsrechtlich geboten ist,[7] fehlt gänzlich.

Die automatisierte verfahrensübergreifende Datenanalyse nach § 98e StPO-E enthält nicht einmal eine eigenständige Anordnungsregel. Dabei gelten für sie materiell-rechtlich strengere Voraussetzungen als nach § 98d StPO-E, da sich der Tatverdacht auf eine in § 100a Abs. 2 StPO bezeichnete Straftat beziehen muss. Die Nutzung eines derart eingriffsintensiven Analyse- und Verknüpfungssystems wird damit vollständig in die Sphäre der Polizei verlagert, auch wenn die Staatsanwaltschaft gem. §§ 161, 163 StPO die Sachleitungsbefugnis des Ermittlungsverfahrens innehat. Davon scheint auch der Regierungsentwurf auszugehen, andernfalls wäre der in § 98d Abs. 4 StPO-E normierte „Staatsanwaltsvorbehalt“ überflüssig. Abgesehen davon, dass völlig unklar ist, wer sicherstellen soll, dass die materiellen Anordnungsvoraussetzungen des § 98e StPO-E eingehalten werden, verstößt der fehlende Richtervorbehalt in beiden Vorschriften gegen die bisherige Regelungslogik der StPO, nach der die formellen Schutzstandards umso enger zu ziehen sind, je eingriffsintensiver die Maßnahmen und je enger die materiellen Eingriffsvoraussetzungen sind.

In formeller Hinsicht ist zu konstatieren, dass die in § 98d Abs. 2 und § 98e Abs. 5 S. 2 StPO-E jeweils vorgesehene Protokollierung zwar Anwendung, Zeitpunkt, einbezogene Daten und Organisationseinheit dokumentiert. Sie gewährleistet aber nicht, dass die am Strafverfahren Beteiligten, insbesondere auch die Verteidigung, nachvollziehen können, welche Suchbegriffe, Gewichtungen, Modellannahmen zu einem Ergebnis geführt haben.[8]

Insgesamt ist zu erwarten, dass die §§ 98d, 98e StPO-E in ihrer derzeitigen Ausgestaltung in Karlsruhe nicht bestehen werden, zumal hier nicht einmal alle Kritikpunkte aufgeführt werden können.

---

[2] BVerfG, 1 BvR 1547/19 und 1 BvR 2634/20, 16.02.2023.
[3] S. Fn. 2, Rn. 67 ff.
[4] S. Fn. 2, Rn. 76.
[5] S. Fn. 1, S. 22.
[6] S. Fn. 2, Rn. 75.
[7] Janique Brüning, *Der Richtervorbehalt im strafrechtlichen Ermittlungsverfahren* (2004), S. 123 ff.
[8] Strafverteidigervereinigungen, *Stellungnahme der Strafverteidigervereinigungen zum Referent:innenentwurf des BMJV zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen*, 06.04.2026, S. 8.

Digitale Souveränität wird ausgeblendet

Darüber hinaus steht zu befürchten, dass der Regierungsentwurf den Grundsatz der digitalen Souveränität bei der Normierung der neuen Befugnisse nicht im Blick hatte. Die der digitalen Analyse zugrunde liegende Infrastruktur bleibt im Regelungskonzept der §§ 98d Abs. 2 und 98e Abs. 4 StPO-E unerwähnt. Aber die Kostenbegründung lässt erkennen, welche infrastrukturellen Voraussetzungen der Entwurf implizit zugrunde legt.[9] Dort wird vorausgesetzt, dass Länder, die bereits eine Software zur automatisierten Datenanalyse in der Gefahrenabwehr einsetzen, keine neue Plattform beschaffen, sondern die vorhandenen Systeme für die Strafverfolgung lediglich anpassen müssten. In Hessen beruht HessenDATA auf Palantirs Gotham[10], Nordrhein-Westfalen[11] und Bayern setzen ebenfalls Palantir-Produkte ein, Baden-Württemberg hat deren Einführung vorbereitet[12], wenn auch eine Entwicklungskooperation mit Airbus Defence and Space und Schwarz Digits zur Schaffung einer souveränen europäischen Analyseplattform auf den Weg gebracht werden soll.[13] Die §§ 98d, 98e StPO-E schaffen damit nicht nur neue Eingriffsbefugnisse, sondern öffnen faktisch auch die strafprozessuale Tür für eine private US-amerikanische Infrastruktur.

Wer bestimmt, was der Staat erkennt?

Dies erscheint mit Blick auf den Umstand, dass die Strafverfolgung eine hoheitliche Aufgabe ist, nicht unproblematisch. Die Strafverfolgung ist die Kehrseite des staatlichen Gewaltmonopols: Weil der Staat den Bürgern die eigenmächtige Durchsetzung ihrer Interessen verwehrt, muss er die Aufklärung und Ahndung von Straftaten selbst übernehmen. Im Rahmen des Legalitätsprinzips bestimmt die Staatsanwaltschaft als Herrin des Ermittlungsverfahrens dessen Richtung, bewertet die Ergebnisse und trägt die Verantwortung.[14] Private dürfen keine eigenständigen Ermittlungen vornehmen.[15]

Nun tritt der private Anbieter einer Analyseplattform nicht als privater Ermittler auf. Vielmehr stellt er die Infrastruktur bereit, innerhalb derer der Staat ermittelt. Die private Plattform ist damit aber mehr als ein bloßes technisches Hilfsmittel. Die Plattform ist die Voraussetzung dafür, dass der Staat bestimmte Erkenntnisse überhaupt erst gewinnen kann. Ohne diese Technik sind bestimmte Formen der Auswertung und damit des Wissenszugriffs nicht mehr möglich. Eine umfassende Analyseplattform legt fest, welche Daten zusammengeführt werden können, welche Beziehungen sichtbar werden, welche Kategorien zur Verfügung stehen und welche Verdachtsmomente als relevant erscheinen. Die Forschung zur Palantir-Plattform der dänischen Polizei zeigt, dass deren „Ontologie“ nicht nur Daten ordnet.[16] Die Plattform stellt ein Vokabular bereit, in dem Personen, Handlungen und Beziehungen polizeilich lesbar werden. Solche Klassifikationen bilden die Wirklichkeit nicht neutral ab. Sie reduzieren Komplexität und strukturieren Wahrnehmung. Auch wenn diese Ontologie nicht herstellerseitig fixiert ist, sondern vom Staat konfiguriert werden kann, hat das Unternehmen einen erheblichen Einfluss auf die Auswertungsarchitektur und damit auf das generierte neue Wissen.

Wenn das System die Wirklichkeit vorsortiert

Das Problem besteht darin, dass ein Analysesystem Informationen erzeugt, Institutionen diese Informationen übernehmen und anschließend auf dieser Grundlage handeln. Der KI-Algorithmus hat damit nicht bloß Auswirkungen auf die gesellschaftliche Wirklichkeit, er formt sie gleichsam.

Das ist im Strafverfahren besonders folgenreich, weil das Analysetool Menschen und Beziehungen etwa als verdächtig oder unverdächtig oder relevant oder irrelevant klassifiziert. Aus einer modellabhängigen

[9] S. Fn. 1, S. 2 f.
[10] Katharina Iskandar, *Eine Software, die fast alles weiß*, FAZ, 30.04.2025, https://www.faz.net/aktuell/rhein-main/region-und-hessen/palantir-und-polizei-hessendata-als-vorbild-fuer-ganz-deutschland-110438575.html, zuletzt abgerufen am 29.07.2026.
[11] Landtag Nordrhein-Westfalen, Ausschussprotokoll 18/946, S. 43.
[12] Landtag von Baden-Württemberg, Drs. 17/9329, auch zur Nutzung in Bayern.
[13] Landtag von Baden-Württemberg, Drs. 18/160, S. 3.

Wahrscheinlichkeitsaussage kann ein Verdacht entstehen, der letztlich dazu führen kann, dass Strafverfahren angestoßen werden.

Das Problem wird auch nicht dadurch gelöst, dass § 98e Abs. 4 S. 2 StPO-E vorsieht, dass die Letztentscheidung bei einem Menschen liegen soll. § 98e Abs. 4 StPO-E verlangt zwar eine anlassbezogene, manuell ausgelöste Suche und verbietet unmittelbar nachteilige Entscheidungen, die ausschließlich auf der Analyse beruhen. Doch wer ausschließlich auf der Grundlage der vom System erzeugten Zusammenhänge entscheidet, entscheidet eben nicht unabhängig vom System. Die Strafverfolgungsbehörden sind damit infrastrukturell determiniert. Dass das gegen den verfassungsrechtlich verankerten Grundsatz digitaler Souveränität verstoßen könnte, wenn diese Infrastruktur nicht vom Staat beherrscht wird, wurde bereits eindrücklich dargelegt.[17]

Auch das in § 98e Abs. 4 S. 5 StPO-E abgegebene Versprechen, diskriminierende Algorithmen technisch und organisatorisch auszuschließen, hilft nur, wenn es technisch erfüllbar und staatlich überprüfbar ist.[18] Schon bei der Quellen-Telekommunikationsüberwachung zeigt sich das Grundproblem rechtlicher Beschränkungen von technischen Möglichkeiten:[19] Der Gesetzgeber kann zwar ein bestimmtes „Design“ vorschreiben. Diese rechtlichen Schutzmechanismen greifen allerdings nicht, wenn beschränkende technische Vorkehrungen oder Kontrollmöglichkeiten zur Einhaltung eben jener Schutzmechanismen fehlen.

Unternehmerische Grundannahmen als Rahmenbedingung staatlicher Erkenntnis

Das beschriebene Problem stellt sich zwar grundsätzlich beim Einsatz von KI-gestützten Tools.[20] Doch es verschärft sich, wenn die KI-Technologie von einem privaten Unternehmen betrieben wird. Dies gilt erst recht, wenn dessen Führungspersonen weltanschauliche Grundannahmen teilen, die nicht auf dem Boden eines demokratischen Rechtsstaats fußen. Denn dann besteht die Gefahr, dass diese unternehmerischen Grundannahmen zu Rahmenbedingungen der staatlichen Erkenntnisbildung werden.

Nach Ansicht des Palantir-Chefs Alexander Karp solle Technik einem politischen Selbstverständnis dienen.[21] Mitgründer Peter Thiel erklärte bereits 2009, er glaube nicht länger, dass Freiheit und Demokratie miteinander vereinbar seien.[22] Beide gehen davon aus, dass ethische Bedenken zur Gefahr für die Demokratie verklärt würden.[23]

Der Staat darf seine Eingriffsbefugnisse jedoch nicht allein nach Maßstäben technischer Machbarkeit oder operativer Effizienz ausgestalten.

Europa braucht digitale Souveränität

Aus all diesen Einwänden folgt nicht, dass ein moderner Rechtsstaat auf digitale oder gar KI-gestützte Ermittlungswerkzeuge verzichten sollte. Auch folgt daraus kein Totalboykott US-amerikanischer Digitalprodukte. Allerdings macht es einen Unterschied, ob das Tool Texte verarbeitet oder als Analyseplattform tief in den Erkenntnisprozess der Strafverfolgungs-, Gefahrenabwehr- und Sicherheitsbehörden eingreift.

Der Regierungsentwurf schafft nicht nur zwei der eingriffsintensivsten Ermittlungsbefugnisse mit äußerst geringen formellen Schutzstandards, sondern trifft zugleich beiläufig in der Kostenbegründung die infrastrukturelle Vorentscheidung darüber, auf welcher Plattform das für die Strafverfolgungsbehörden ermittlungsrelevante Wissen erzeugt wird. Weder wird der Anbieter beim Namen genannt noch werden die damit verbundenen Abhängigkeiten problematisiert. Digitale Eingriffsbefugnisse können aber nicht ohne die technischen Ermöglichungsbedingungen gedacht werden. Wird darauf verzichtet, droht die normative Kraft des Faktischen. Mit dem kostengünstigen Weiterbetrieb nicht eingehegter US-amerikanischer Analysetools besteht die Gefahr, dass technische Machbarkeit zum

[14] Ausführlich Janique Brüning, *Big Data und Künstliche Intelligenz im Strafverfahren*, in: Kusche/Stefanopoulou (Hrsg.), *Digitalisierung als total social fact der Kriminalwissenschaften* (2024), S. 133 (137 f.).

[15] Dazu Janique Brüning, *Privatisierungstendenzen im Strafprozess – Chancen und Risiken der Mitwirkung sachverständiger Privatpersonen im strafrechtlichen Ermittlungsverfahren*, StV (2008), S. 100.

[16] Vasilis Galis und Björn Karlsson, *A World of Palantir – Ontological Politics in the Danish Police's POL-INTEL*, Information, Communication & Society 27 (2024), DOI: 10.1080/1369118X.2024.2410255, S. 2438-2456.

Maßstab der staatlichen Sicherheitsarchitektur erhoben wird. Der Staat könnte sich dann zum abhängigen Vasalen US-amerikanischer Big-Tech-Fürsten machen, mit der Folge, dass das Gebot der digitalen Souveränität zur inhaltsleeren Absichtserklärung degradiert würde.

AUTOR*IN

Janique Brüning

Janique Brüning ist Professorin für Strafrecht, Strafprozessrecht, Wirtschaftsstrafrecht und Sanktionenrecht an der Christian-Albrechts-Universität zu Kiel und Direktorin des Instituts für Kriminalwissenschaften sowie des Zentrums für Digitalisierung und Recht. Sie ist zudem Richterin am Schleswig-Holsteinischen Oberlandesgericht.

EMPFOHLENE ZITATION

Brüning, Janique: Der Staat als digitaler Vasall: Wie die §§ 98d, 98e StPO-E die digitale Souveränität aushöhlen, Verfassungsblog, 03.09.2026, doi: 10.59704/fab009eb174bdd19.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260903-145242-0.

[17] Mario Martini und Jonas Botta, *Polizeiliche Datenanalyse mittels KI*, DÖV (2025), S. 1033-1042; Simon Diethelm Meyer, *Der Einsatz künstlicher Intelligenz durch Sicherheitsbehörden*, GSZ (2025), S. 156-161 (160 f.); Ulrich Kelber und Vyacheslav Bortnikov, *Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten*, NJW (2023), 2000-2006, s. auch Arno Rolf, *Digitalisierung ohne Demokratie*, Informatik Spektrum (2025) S. 79-88, DOI: 10.1007/s00287-025-01593-3.

[18] Kritisch auch Gesellschaft für Freiheitsrechte e.V., *Stellungnahme zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz „Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen“*, 02.04.2026, S. 9 f.

[19] Ausführlich dazu Mario Martini und Sarah Fröhlingsdorf, *Catch Me If You Can: Quellen-Telekommunikationsüberwachung zwischen Recht und Technik*, NVwZ – Extra 24 (2020), S. 1-15.

[20] Dazu exemplarisch Simon Diethelm Meyer, Fn. 17 (S. 157).

[21] Alex Karp und Nicholas W. Zamiska, *The Technological Republic: Hard Power, Soft Belief, and the Future of the West* (2025).

[22] Peter Thiel, *The Education of a Libertarian*, Cato Unbound, 13.04.2009, https://www.cato-unbound.org/2009/04/13/peter-thiel/education-libertarian/, zuletzt abgerufen am 29.07.2026.

[23] Dazu Paul Nemitz, *Die Waffen des Silicon Valley: Eine Kritik an Alex Karps Manifest der digitalen Gewalt*, Verfassungsblog, 15.06.2026, DOI: 10.59704/88f05b5989b2ded0; Andreas Brenneis, Kai Denker, Petra Gehring, *Data is Power – Code is Ideology: Selbstmarketing und politische Positionierungen an der Spitze von Palantir*, in: Bäuerle/Denker/Geminn/Schöndorf-Haubold, *Big Data und KI bei der Polizei* (2025), S. 225-250; im Ergebnis auch Alexander C. Karp, *Our Oppenheimer Moments, The Creation of A.I. Weapons*, New York Times, 25.07.2023, https://www.nytimes.com/2023/07/25/opinion/karp-palantir-artificial-intelligence.html, zuletzt abgerufen am 02.08.2026.