Palantir als Türöffner für die Dystopie

Tobias Singelnstein & Ida Dankenbring

31.08.2026 doi: 10.59704/447202106ca0e11e

Die Palantir-Software „Gotham“ ist weit mehr als ein Tool zur besseren Auswertung polizeilicher Daten. Mit ihrer Einführung bei der Polizei etabliert sich vielmehr eine neue, datengetriebene Sozialkontrolle. Sie ist Türöffner einer entsprechenden Dystopie. Dies gilt nicht allein, weil dieser Schritt die deutschen Polizeibehörden langfristig an die Plattform des US-Anbieters und dessen Anwendungen bindet. Vielmehr wird die Einführung auch die Entwicklung hin zu Massendatenauswertung, KI-Einsatz, Risikoprognosen und präemptiven Techniken im Feld sozialer Kontrolle massiv beschleunigen – und damit einen Paradigmenwechsel in der Sozialkontrolle vorantreiben, der sich bereits seit längerem abzeichnet, dem es aber bislang an Tempo fehlt.

Polizeiliche Datenverarbeitung in der Sicherheitsgesellschaft

Die Einführung von Palantir ist nicht allein Produkt des technologischen Fortschritts, sondern ordnet sich in einen gesellschaftlichen Kontext ein, in dem ein wachsendes Bedürfnis nach individueller, bürgerlicher Sicherheit besteht. Innere Sicherheit ist in Deutschland seit den 1990er Jahren zu einem bestimmenden Thema der gesellschaftlichen Debatte geworden: Sicherheitsbedürfnisse in der Bevölkerung gewinnen an Bedeutung. Sie werden von Medien und Politik aufgegriffen, transportiert und verstärkt. Politik und Behörden sehen sich der Herausforderung gegenüber, diesen Bedürfnissen gerecht zu werden – und können umgekehrt auch ihrerseits soziale Probleme als Sicherheitsprobleme definieren.[1]

Diese als Sicherheitsgesellschaft[2] beschriebene, kreislaufartige Entwicklung geht mit einem neuen Präventionsverständnis einher. Bis in die 1990er Jahre wurde unter Prävention die Reaktion auf Straftaten und die Abwehr konkreter Gefahren einerseits und sozialstaatliche Disziplinierung andererseits verstanden.[3] Diese Anknüpfungspunkte werden heute nicht mehr als ausreichend wahrgenommen. Es scheint unzumutbar geworden zu sein, auf das Eintreten einer konkreten Gefahr zu warten. Stattdessen soll soziale Kontrolle schon weit im Vorfeld konkreter Anlässe Risiken erkennen und deren Eintrittswahrscheinlichkeit minimieren.[4]

Für das Unterfangen, Risiken zu prognostizieren und abweichendes Verhalten vorherzusagen, bedarf es umfangreicher Daten und elaborierter Formen der Auswertung solcher Massendaten. An beidem fehlt es deutschen Sicherheitsbehörden bislang. Die nun schon seit Jahrzehnten avisierte Modernisierung der behördlichen IT-Infrastruktur – aktuell betrieben unter dem Titel „Bund-Länder-Programm P20“ – geht nur höchst schleppend voran. Von ambitionierteren Formen der Datenverarbeitung ganz zu schweigen.

Als Lichtblick in dieser Lage präsentierte sich vor gut 10 Jahren das sogenannte *Predictive Policing*, also die Ermittlung von risikobehafteten Personen oder Orten durch Massendatenauswertung auf Basis statistischer Annahmen.[5] Was in den USA gang und gäbe ist, könne auch in Deutschland die Polizeiarbeit revolutionieren, versprach allen voran ein kleines Unternehmen aus NRW und verkaufte ab 2014 auf diese Weise einer Reihe von Ländern sein Softwareprodukt mit dem Namen „Precobs“ zur ortsbezogenen Prädiktion von

[1] Tobias Singelnstein, *Neue Gesichter sozialer Kontrolle: Abstrakte Außenseiter*, MSchKrim (2025), S. 175-185 (175 f.); Aldo Legnaro/Daniela Klimke, *Einleitung: Die Sekuritisierung des Lebens*, in: Legnaro/Klimke (Hrsg.), *Kriminologische Diskussionstexte II* (2022), S. 89-102 (92).

[2] Aldo Legnaro, *Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze*, Leviathan (1997), S. 271-284; Tobias Singelnstein/Peer Stolle, *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert* (2012).

[3] Axel Groenemeyer, *Wege der Sicherheitsgesellschaft*, in: Groenemeyer (Hrsg.), *Wege der Sicherheitsgesellschaft: Transformationen der Konstruktion und Regulierung von Unsicherheiten* (2010), DOI: 10.1007/978-3-531-92604-9_1.

Wohnungseinbruchsdiebstählen. Der Lichtblick entpuppte sich indes schnell als Strohfeuer: Der Ansatz war technisch wenig ausgereift, konnte nur auf sehr beschränkte Daten zurückgreifen, deckte nur einzelne Delikte ab und blieb so letztlich auch in seinem polizeilichen Nutzen sehr beschränkt.[6] Viele Bundesländer stellten die Nutzung von „Precobs“ in der Folge wieder ein, andere setzten auf eigene Entwicklungen. Aber: Der Traum von der automatisierten Massendatenauswertung zur Risikoprognose in der Polizeiarbeit war auch in Deutschland geboren.

In dieser Lage sorgen Palantirs Produkte und die Möglichkeiten künstlicher Intelligenz für eine neue Dynamik. Mit ihnen kann die Polizei große Datenmengen schneller und effizienter als je zuvor durchsuchen, verknüpfen und gefundene Verbindungen nutzer:innenfreundlich darstellen. Diese neuen Möglichkeiten der Massendatenauswertung versprechen, dass der Traum von der vorhersagenden Polizeiarbeit Wirklichkeit werden könnte.

Was Palantir kann und will

Wie groß das Interesse an der neuen Technik ist, zeigt sich daran, dass mehrere Bundesländer die Palantir-Software eingekauft haben; auch auf Bundesebene wird dies erwogen. Die Nutzung des umstrittenen Produkts wird damit gerechtfertigt, dass nur polizeiliche Datenbanken verknüpft würden, auf die die Beamt:innen ohnehin Zugriff hätten. Durch die Software würde das Durchsuchen der Daten und das Erkennen von Verbindungen lediglich effizienter und besser, die Aufbereitung der Ergebnisse übersichtlicher. Durch menschliche Arbeit könnten vergleichbare Ergebnisse entweder nur unter erheblichem Zeitaufwand oder aufgrund der großen Datenmengen ggf. auch gar nicht geleistet werden.

Diese Erzählung bildet jedoch nur einen Ausschnitt der Entwicklung ab und negiert deren Tragweite. Zum einen greift bereits das Verbinden und Durchsuchen verschiedener polizeilicher Datenbanken mit anderer Intensität in das Recht auf informationelle Selbstbestimmung der Betroffenen ein als die bisherige Praxis der polizeilichen Datenverarbeitung. Insbesondere die Einhaltung des datenschutzrechtlichen Zweckbindungsgrundsatzes wird grundlegend in Frage gestellt.[7]

Zum anderen und vor allem aber geht das Potenzial der Software „Gotham“ weit über die damit skizzierte Nutzung – die Verknüpfung bereits bestehender Datenbanken – hinaus. Die Vision des Unternehmens Palantir mit Alex Karp an dessen Spitze ist es, die Funktionsweise sämtlicher Sicherheits- und Migrationsbehörden in den USA, aber auch in anderen Ländern auf Grundlage künstlicher Intelligenz umzugestalten und dadurch an einer Veränderung der westlichen Gesellschaft nach seinen Vorstellungen mitzuwirken.[8] Ziel ist also nicht bloß die Effizienzsteigerung polizeilicher Arbeit, sondern eine umfassende Einflussnahme auf das gesellschaftliche Zusammenleben und die Herstellung einer ganz bestimmten Vorstellung von sozialer Ordnung. Dementsprechend beschränken sich auch die technischen Entwicklungsperspektiven nicht nur auf das Durchsuchen polizeilicher Datenbanken, sondern bewegen sich in Richtung einer umfassenden sozialen Kontrolle mit dem Ziel der Prädiktion.

Was heißt das konkret? Erstens ist „Gotham“ nicht auf bereits gespeicherte polizeiliche Daten beschränkt. Schon jetzt ist die Software technisch in der Lage, beliebige weitere Datenquellen und Datenbestände zu integrieren und in Suchen bzw. Analysen einzubeziehen.[9] Dies können Daten anderer Behörden (z.B. Meldeämter, Sozialämter oder Ausländerbehörden)

[4] Tobias Singelnstein/Peer Stolle, *Die Sicherheitsgesellschaft. Soziale Kontrolle im 21. Jahrhundert* (2012), S. 34; Aldo Legnaro, *Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze*, Leviathan (1997), S. 271-284 (281).

[5] Zu einer techniksoziologischen Einordnung dieser Prognosen s. Simon Egbert, *(Technik-)Soziologische Charakteristika prädiktiver Algorithmen*, in: Kusche/Stefanopoulou (Hrsg.), *Digitalisierung als total social fact der Kriminalwissenschaften* (2024), S. 29-44.

[6] Simon Egbert, *Predictive Policing – Algorithmische Vorhersagen in der polizeilichen Kriminalprävention*, in: Wollinger (Hrsg.), *KI in der Prävention* (2026), S. 107-136 (112 ff.).

[7] Vgl. zur Problematik das Urteil des BVerfG zur Verwendung von HessenDATA, 1 BvR 1547/19, 1 BvR 2634/20 vom 16.02.2023, sowie die Stellungnahmen von Franziska Görlitz, Jonas Botta und dem Chaos Computer Club zu den Gesetzesentwürfen der Länder Hessen und Sachsen-Anhalt.

oder solche von privaten Unternehmen (wie zum Beispiel der Schufa, Telekommunikationsunternehmen oder Banken) ebenso sein wie Daten, die im Wege der OSINT-Recherche (Open Source Intelligence) ermittelt wurden, aus Leaks stammen und/oder im Darknet zum Verkauf angeboten werden. Schon heute kann die Polizei Daten anderer staatlicher Behörden sowie manuell gespeicherte Daten aus dem Internet, wie zum Beispiel Social-Media-Profile, durch die Software durchsuchen lassen.[10] Mittels „Gotham“ wäre es perspektivisch ohne Weiteres möglich, all diese Datenbestände automatisiert auszuwerten und so in vollem Umfang für die Polizei nutzbar zu machen. Ob und inwieweit diese Möglichkeiten genutzt werden, ist eine politische und gegebenenfalls rechtliche Entscheidung. Die technischen Voraussetzungen dafür sind schon jetzt gegeben.

Zweitens kann die Palantir-Software mit diesen Daten auch ganz andere Auswertungen, Analysen, Arbeiten umsetzen, als die Polizei sie bislang betreibt. Nach der gegenwärtigen Erzählung soll das Programm lediglich Suchanfragen effizienter und effektiver bearbeiten, die von Beamt:innen im Rahmen ihrer üblichen strafprozessualen und gefahrenabwehrrechtlichen Ermittlungen gestellt werden. Weitergehende Schlussfolgerungen ziehen die Beamt:innen dann selbst. Tatsächlich geht das Potenzial der Software aber weit über diese Funktion hinaus. Im Wege der Mustererkennung könnte „Gotham“ die ihm zur Verfügung stehenden Daten einerseits automatisiert nach Kriterien durchsuchen, die die Beamt:innen vorher als Risikofaktoren definiert haben. Bei dieser Technik, die auch „Precobs“ nutzt, kann der Fokus je nach verwendeten Daten und Variablen auf verschiedenen Straftaten, Situationen oder möglichen Täter:innen liegen und die Ergebnisse geographisch oder in Form von Netzwerken dargestellt werden.[11] Andererseits könnte die Software durch *machine learning* auf Grundlage der Daten auch eigenständig Faktoren ermitteln, die statistisch betrachtet mit einem erhöhten Risiko für abweichendes Verhalten korrelieren; ein erklärbarer Zusammenhang ist dabei nicht notwendig.[12] Im Anschluss könnten dann die über jeden Einzelnen vorliegenden Daten permanent auf die ermittelten Risikofaktoren hin untersucht und so auch ganz ohne konkreten Anlass Risikoprognosen für konkrete Räume und Personen erstellt werden. Die Software würde dann nicht mehr eine unterstützende Rolle bei Ermittlungen spielen, sondern richtungsweisenden Einfluss auf polizeiliches Handeln nehmen.

Eine andere Sozialkontrolle

Auf diese Weise könnte Palantir erreichen, was das gesellschaftliche Präventionsstreben sich erträumt und was „Precobs“ nicht vermochte: Eine Polizeiarbeit, die weit im Vorfeld konkretisierter Gefahren oder Verdachtssituationen risikohafte Personen und Orte präventiv bearbeitet, um Schäden möglichst frühzeitig zu verhindern. Durch eine solche Risikoermittlung mittels Massendatenauswertung würde die Vorverlagerung sozialer Kontrolle eine ganz neue Dimension erlangen. Als problematisch gelten dann bereits Personen und Orte, die statistisch betrachtet ein erhöhtes Risiko für abweichendes Verhalten aufweisen.

Diese Vorverlagerung betrifft zum einen die *Feststellung* von Risikofaktoren: Handlungen, Beziehungen, Eigenschaften, gesellschaftliche Positionierung und räumliche Faktoren, die in sich weder eine Straftat oder Gefahr darstellen noch einen Anfangsverdacht begründen, rücken so in den polizeilichen Fokus und werden als (potentielle) Abweichung definiert. Formelle Sozialkontrolle erfährt so bereits durch diese neuen Detektionsweisen eine erhebliche – sowohl zeitliche als auch gegenständliche – Ausweitung ihres Wirkungsbereiches. Zu erwarten ist, dass sich diese Entwicklung auch auf die gesellschaftliche Wahrneh-

[8] Wie diese Gesellschaft aussehen soll, hat das Unternehmen erst kürzlich in 22 Thesen dargestellt: https://x.com/PalantirTech/status/2045574398573453312, zuletzt abgerufen am 27.07.26.

[9] Palantir wirbt gerade damit, verschiedenste Formen von Daten verbinden und durchsuchen zu können: https://www.palantir.com/docs/foundry/data-integration/overview/, zuletzt abgerufen am 31.08.2026

[10] S. bspw. die gesetzlichen Grundlagen aus § 47a Abs. 3 Satz 2 PolG BW und § 25a Abs. 2 Satz 3 HSOG.

[11] Mareile Kaufmann/Simon Egbert/Matthias Leese, *Predictive Policing and the Politics of Patterns*, The British Journal of Criminology (2019), S. 674-692 (680).

mung von Sicherheit und ihrer Bedrohungen auswirkt und in der Bevölkerung dann schon Risikofaktoren statt tatsächlich abweichendes Verhalten als Gefahr interpretiert werden.

Entscheidend für die Veränderung der Sozialkontrolle ist allerdings nicht allein die Ermittlung der Risikofaktoren, sondern auch die anschließende Reaktion auf die erkannten Risiken in Form der *Intervention*. Je nach angestrebtem Ziel kann diese Intervention sehr unterschiedlich aussehen: Das Risiko kann durch die Polizei oder andere Behörden weiter erforscht werden, um es besser aufzuklären und im Blick zu behalten; ebenso kann die Konkretisierung des Risikos von vornherein verhindert werden, indem es unmittelbar bearbeitet wird, wie dies etwa bei Upload-Filtern der Fall ist; daneben kann auch eine abstrakte Vorsorge in Form von *Social Scoring* betrieben werden, indem Personen anhand der Risikofaktoren in Kategorien eingeteilt werden, mit denen verschiedene Vor- oder Nachteile wie etwa räumliche Zugänge verbunden sind.[13]

Diese Entwicklungen würden bedeuten, dass die polizeiliche Praxis erheblich schwieriger nachzuvollziehen und zu kontrollieren wäre. Denn je weiter im Vorfeld einer möglichen Gefahr wir uns bewegen, desto unschärfer wird, wieso welche Person oder welcher Ort von der Software und in der Folge von der Polizei als Risiko definiert wird und welche Norm als gefährdet wahrgenommen wird.[14] Zum anderen geht damit eine neue Stufe der Abstraktion und Vereinfachung einher. Statt durch konkrete Gefahren oder Straftaten wird die staatliche Reaktion durch abstrakte Kategorien der Gefährlichkeit ausgelöst. Die komplexen Zusammenhänge der Entstehung von Kriminalität werden durch Massendatenauswertung auf einfache Faktoren reduziert und die errechneten Wahrscheinlichkeiten auf den Einzelfall übertragen.[15] Strukturelle gesellschaftliche Verhältnisse, Zuschreibungsprozesse sowie Hintergründe des Einzelfalls werden dabei ausgeblendet. Dadurch setzt eine Kriminalisierung sozialer Probleme noch früher an als bisher.[16] Gleichzeitig verschafft die Quantifizierung, die in der scheinbar objektiven Berechnung der KI liegt, dieser Konstruktion von Abweichung zusätzliche Legitimität.[17]

Fazit

Die Einführung der Palantir-Software wäre bzw. ist ein Meilenstein in dem Bestreben, das Feld sozialer Kontrolle grundlegend und abstrakt-präventiv umzugestalten. Das technische Potenzial der Software – das weit über die bisherigen Begründungsnarrative hinausgeht – droht, neuen Formen sozialer Kontrolle, die auf statistischer Risikoberechnung und Interventionen im Vorfeld konkreter Anlässe basieren, einen kräftigen Entwicklungsschub zu verschaffen. In der Folge entstehen neben den klassischen Formen polizeirechtlicher und strafrechtlicher Sozialkontrolle andere Weisen, (potentielle) Abweichungen zu erkennen und zu behandeln. Diese sind abstrakter, fehleranfälliger, selektiver und schwerer zu kontrollieren.

[12] Simon Egbert, (*Technik-)Soziologische Charakteristika prädiktiver Algorithmen*, in: Kusche/Stefanopoulou (Hrsg.), *Digitalisierung als total social fact der Kriminalwissenschaften* (2024), S. 29-44 (32 ff.).
[13] Tobias Singelnstein, *Neue Gesichter sozialer Kontrolle: Abstrakte Außenseiter*, MSchKrim (2025), S. 175-185 (180 f.).
[14] Tobias Singelnstein, *Neue Gesichter sozialer Kontrolle: Abstrakte Außenseiter*, MSchKrim (2025), S. 175-185 (182).
[15] Zur kritischen, technischen Einordnung prädiktiver Verfahren s. Simon Egbert, (*Technik-)Soziologische Charakteristika prädiktiver Algorithmen*, in: Kusche/Stefanopoulou (Hrsg.), *Digitalisierung als total social fact der Kriminalwissenschaften* (2024), S. 29-44 (40).
[16] Vgl. Fn. 14

AUTOR*INNEN

Tobias Singelnstein
Prof. Dr. Tobias Singelnstein ist Professor für Strafrecht, Strafprozessrecht und Kriminologie am Fachbereich Rechtswissenschaft der Johann Wolfgang Goethe-Universität Frankfurt.
Ida Dankenbring
Ida Dankenbring ist wissenschaftliche Mitarbeiterin an der Professur für Kriminologie und Strafrecht (Prof. Dr. Singelnstein) an der Goethe-Universität in Frankfurt.

EMPFOHLENE ZITATION

Singelnstein, Tobias; Dankenbring, Ida: Palantir als Türöffner für die Dystopie, Verfassungsblog, 31.08.2026, doi: 10.59704/447202106ca0e11e.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260831-145404-0.

[17] Steffen Mau, *Das metrische Wir. Über die Quantifizierung des Sozialen* (2017). S. 27 ff.