



AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Einsatz von Palantir in Niedersachsen

für den Ausschuss für Inneres und Sport des Niedersächsischen Landtages zum Antrag der Fraktion der CDU: „Polizeiarbeit in das Zeitalter der Digitalisierung überführen - verfahrensübergreifende Datenanalysen in Echtzeit ermöglichen“

Manuel HonkHase Atug der AG KRITIS als geladener Sachverständiger in der mündlichen Anhörung
am 12. März 2026 im Landtag Niedersachsen

Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen.....	3
2 Erforderliches Vorwort.....	4
3 Stellungnahme.....	5
3.1 Konkret zum Antrag.....	5
3.2 Wie funktioniert Palantir?.....	9
3.3 KI in Palantir.....	11
4 Lösungsmöglichkeit.....	12
5 Fazit.....	13

1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) erstellt.

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus bis zu 42 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen. Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

2 Erforderliches Vorwort

Vorab ist festzustellen, dass das amerikanische Unternehmen Palantir von undemokratischen und durchaus auch extremistisch auftretenden Menschen gesteuert wird. Der CEO Alex Karp findet das Töten von Menschen auf Basis von Metadaten¹ legitim und möchte die USA tödlicher machen². Mitgründer und Investor Peter Thiel wird inzwischen als Autokratie- und Faschismus-Befähiger^{3 4 5 6} angesehen, der die Autokratie-Umsetzung der USA fördert⁷ und sich dazu gerne öffentlich bekennt. Darüber hinaus findet er, dass die Freiheit mit der Demokratie nicht vereinbar ist. Damit meint er unternehmerische Freiheit und fördert die De-Demokratisierung und die Deregulierung, um Demokratie auszuhöhlen und zu unterwandern.

CEO Karp erklärte öffentlich, dass Feinde der USA auch unter Einsatz ihrer Software (sogenanntes Targeting) getötet werden und ist stolz darauf, die US-amerikanische Behörde United States Immigration and Customs Enforcement (ICE) als größte Polizei- und Zollbehörde des Ministeriums für Innere Sicherheit (DHS) der USA mit Palantir Software auszustatten, die Menschen nach Parametern und Echtzeitanalysen von Daten aus Behörden und Ergebnissen der Strafverfolgung, öffentlichen Daten aus dem Internet – sogar durch Ankauf von Milliarden von Standort- und anderen Datensätzen der Werbeindustrie – und Einsatz von KI mit entsprechenden Fehlerquoten und Kollateralschäden als Ziele identifizieren und unrechtmäßig Deportieren oder sogar im Verlauf der Maßnahmen unnötig und unrechtmäßig töten⁸.

Mit der neuen amerikanischen nationalen Sicherheitsstrategie wurde Europa klar als Feind erklärt.

Diese Entwicklung macht eine Diskussion über den Einsatz einer solchen Software oder eines solchen Konzerns in Deutschland – und damit die Finanzierung dieser Ziele durch deutsche Steuergelder – absurd. Insbesondere vor dem historischen Hintergrund der Geschichte Deutschlands.

1 <https://netzpolitik.org/2024/palantir-und-alexander-karp-toeten-auf-basis-von-metadaten/>

2 <https://www.spiegel.de/wirtschaft/unternehmen/palantir-chef-alex-karp-der-philosoph-der-amerika-toedlicher-macht-a-f8491341-d16f-4576-af58-1bd7e5bd02aa>

3 <https://www.blaetter.de/ausgabe/2026/februar/toxische-tech-abhaengigkeit>

4 <https://www.zeit.de/news/2025-11/06/palantir-gegner-thiel-ist-ein-bekennender-faschist>

5 <https://www.golem.de/news/petition-palantir-des-faschisten-thiel-kein-partner-deutschlands-2511-201934.html>

6 <https://www.stuttgarter-zeitung.de/inhalt.umstrittene-polizeisoftware-palantir-gegner-thiel-ist-ein-bekennender-faschist.1c418b0a-24a8-46e0-9840-c7baf5ecf4ae.html>

7 <https://www.amnesty.de/pressemitteilung/usa-ueberwachungssoftware-palantir-babel-street-gegen-demonstrierende-migrant-innen>

8 <https://www.heise.de/hintergrund/USA-Die-Architektur-der-Abschiebung-und-Palantirs-Rolle-im-neuen-ICE-System-11152960.html>

3 Stellungnahme

Die AG KRITIS sieht hier eine erhebliche Verantwortung im KRITIS Sektor Staat und Verwaltung, um die kritische Dienstleistung „(polizeiliche und nicht-polizeiliche) Gefahrenabwehr“⁹ verfassungskonform und bei Beachtung der Grundrechte zu gewährleisten, um die Versorgungssicherheit der Bevölkerung sicherzustellen.

Viele weitere Referenzen, Informationen und Recherchemöglichkeiten zu Palantir und dem Umfeld wie z.B. die Verfassungsklagen der GFF, Zweckbindung, Rasterfahndung, Verhandelungen zwischen Polizeien, Gewerkschaften der Polizeien und Palantir, parlamentarische Drucksachen zu Palantir-Missbrauch, Infos zu Anhörungen in Innenausschüssen, Bundes-VerA (Palantir), Antworten auf kleine Anfragen, Polizeidatenbanken, Wissenschaftliche Dienste des Bundestags, IFG-Anfragen, hypothetische Datenneuerhebung und Zweckbindung, Polizeilicher Informations- und Analyseverbund (PIAV), P20¹⁰ (vormals P2020), das Informationsmodell der Polizei (IMP), Positionspapiere des BfDI und vieles mehr findet sich in der unregelmäßig aktualisierten:

Palantir Linkliste von HonkHase

<https://atug.de/Palantir/Palantir%20Linkliste.txt>

3.1 Konkret zum Antrag

Es wird ein Anwendungsfall dargestellt „für eine gezielte auf eine Einzelperson bezogene Auswertung vorhandener polizeilicher Erkenntnisse [...] um zu verhindern, dass diese schwere Straftaten begehen“. Des Weiteren wird auf „Extremismusbekämpfung“ verwiesen und dass es darauf ankommt „frühzeitig zu erkennen, ob bestimmte Personen oder Gruppierungen Straftaten vorbereiten oder Terroranschläge planen“.

Im Widerspruch dazu wird aber weiter unten aufgeführt, dass „die Plattform Hessendata jährlich rund 15 000 Mal zum Einsatz [kam] und ist somit fester Bestandteil des polizeilichen Alltags“ geworden ist. Offensichtlich gibt es keine 15.000 Fälle an Terroranschlägen, Extremismusbekämpfung und schweren Straftaten in Hessen pro Jahr. Hier stellt sich also die Frage, ob es um schwerste Straftaten und Gefahrenabwehr im Sinne der erwähnten Terroranschläge geht oder ob es um eine massenhafte Nutzung im Polizeialltag und damit einer Normalisierung von Palantir gehen soll, was insofern also das offensichtlich Ziel der Einführung von Palantir sein soll.

9 https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/Staat-Verwaltung/staat-verwaltung_node.html

10 P20 dient der Harmonisierung des Informationswesens und Datenbestandes der Polizeien des Bundes und der Länder in einem gemeinsamen Datenhaus. Das standardisierte polizeiliche Datenmodell (Informationsmodell der Polizei - IMP) existiert davon schon unabhängig.



Es stellt sich schon jetzt die **Frage der Verhältnismäßigkeit in Bezug auf die massenhaften Eingriffe in die Grundrechte** und wie der **verfassungskonforme Polizeialltag** gemäß Antrag der CDU aussehen soll.

Weiter heißt es ehrlicher Weise, eine belastbare Gefährdungseinschätzung „ist nur möglich, wenn sämtliche Informationen aus polizeilichen Datenbanken schnell und richtig verknüpft und systematisch ausgewertet und zusammengetragen werden“.

Es geht also um eine **Rasterfahndung** und die **vollständige Verarbeitung ALLER Informationen aus polizeilichen Datenbanken** für mehrere Tausend Analysen im Jahr alleine für ein Bundesland. Also aller ca. 200 Polizeidatenbanken und -dateien. Einschließlich der **Daten aller Menschen, die sich an die Polizei gewandt haben**, um Anzeige zu erstatten und auch Daten von Menschen, die **Opfer von Straftaten** wurden oder als **Zeugen dazu Angaben gemacht** haben. Dazu Daten von **gesetzlichen Vertretern, Haltern und anderen Auskunftspersonen**, die in den polizeilichen Vorgangsbearbeitungssystemen gespeichert sind. Also **Daten von Menschen, die weder Täter, Tatverdächtige oder Gefährder sind**.

Da dies gemäß Verfassung nicht zulässig ist, stellt sich uns die Frage, wieso vorher die ca. 200 Datenbanken und -dateien separiert wurden und ein Vollzugriff für die tägliche Polizeiarbeit nicht zulässig ist aber jetzt einfach aufgehoben werden soll. Das Stichwort hierzu heißt **Zweckbindung**. Die Strafverfolgungsbehörden haben die Daten zweckgebunden erhalten und dürfen diese nicht einfach für alle möglichen anderen Analysen **zweckentfremdet Missbrauchen**.

Tatsächlich ist daher zuvor eine vollständiger Kennzeichnung aller Daten in diesen ca. 200 Datenbanken und -dateien vorzunehmen und nur die dürfen verarbeitet werden, die bei z.B. den erwähnten Terroranschlägen zulässig analysiert werden dürfen. Für mehrere tausend Analysen im Jahr im Rahmen des allgemeinen Polizeialltags ist das **nicht zulässig**. Das ist offenbar laut Antrag nicht vorgesehen oder berücksichtigt worden.

Eine europäische oder deutsche Palantir-Alternative würde diese offensichtliche Verfassungswidrigkeit im Übrigen nicht beheben.

Auch bei „anwachsende Datenflut“ und den „neuen und vielfältigen Möglichkeiten der Künstlichen Intelligenz“ **dürfen und müssen Verfassung und Grundgesetz Berücksichtigung finden**. Und das ist dringend geboten.

Die AG KRITIS teilt die Meinung „Der Einsatz einer modernen und leistungsstarken Analysesoftware ist daher alternativlos“, allerdings im gesetzlichen Befugnisrahmen und vor allem nicht mit Palantir oder „vergleichbaren Alternativen“, die dann ebenfalls offensichtlich verfassungswidrig sind, da sie **technisch eine Rasterfahndung abbilden**. Näheres dazu und zu den echten Lösungsansätzen der AG KRITIS folgt in späteren Abschnitten.

Es ist richtig, dass „bereits zahlreiche Länder reagiert und ihre Polizeigesetze geändert haben“. Leider ist versäumt worden, zu erwähnen, dass beispielsweise die Gesellschaft für Freiheitsrechte e.V. (GFF) **bereits erfolgreiche und teilweise noch laufende Verfassungsklagen** vorgenommen hat. Es empfiehlt sich hier also eine vorab gesetzeskonforme Prüfung und Umsetzung, statt offensichtlich verfassungswidrig voranzuschreiten und dann zu scheitern. **Einer Demokratie ist das nicht förderlich**, da es das Vertrauen in die Strafverfolgungsbehörden und in die Politik kontinuierlich unterwandert und aushöhlt.

Zu Aussagen wie „Nach Angaben der Hessischen Landesregierung konnten mithilfe dieser Software bereits mehrere Ermittlungserfolge erzielt werden“ können wir nur **unaufgeregt feststellen, dass der Zweck nicht die Mittel heiligt**. Insbesondere bei den Strafverfolgungsbehörden, die eine besondere Verantwortung zur Einhaltung der Freiheitlich-demokratischen Grundordnung (FDGO) haben.

Aussagen wie „Palantir solle als Übergangslösung genutzt werden“ sind **Nebelkerzen**, da NRW beispielsweise in 2025 den Vertrag schnell verlängert hat, da sie bereits aufgrund der Ontologie in Palantir (näheres dazu in späteren Abschnitten) **vollständig abhängig von Palantir** sind und **nicht mehr wechseln können, selbst wenn sie wollten**. Vergleichbare Aussagen hat Bayern schon nach kurzer Zeit des Einsatzes verkündet. Hessen ist stolz darauf, abhängig zu sein und strebt keinen Wechsel an. Stattdessen schaut man sich bereits intensiv das Palantir AIP – das KI Modul – an, um es offenbar zukünftig in HessenData (beruht auf Palantir Gotham) einsetzen zu wollen.

Zu der Aussage „solange dazu keine vergleichbare deutsche oder europäische Alternativsoftware auf dem Markt verfügbar ist“ lässt sich nüchtern erneut feststellen, dass **alle ähnlichen Lösungen ebenfalls aufgrund des ontologischen Modells technisch einer Rasterfahndung entsprechen** werden und damit ebenfalls offensichtlich verfassungswidrig bleiben. Die Lösung lautet P20-Datenhaus^{11 12}, näheres dazu in späteren Abschnitten.

Die Aussage „Plattform HessenData jährlich rund 15 000 Mal zum Einsatz und ist somit fester Bestandteil des polizeilichen Alltags“ ist sehr bedenklich, weil dort massenhaft Daten aus den Polizeidatenbanken und -dateien enthalten sind. Der Einsatz von Palantir wurde immer dargelegt wurde nur zur Verhinderung von schwersten Straftaten diskutiert, eine pauschale Nutzung im Polizeialltag wurde ausgeschlossen.

Mit der Aussage „Gerade in dynamischen Einsatzlagen, wie bei akuten Bedrohungslagen, großangelegten überbehördlichen und überörtlichen Durchsuchungsmaßnahmen und Razzien oder bei der Bekämpfung der organisierten Kriminalität“ wird erneut dargestellt, dass Palantir nur bei schweren Gefährdungen zum Einsatz kommen soll. Dies kann offensichtlich nicht der

11 <https://www.heise.de/hintergrund/Missing-Link-Digitale-vernetzte-Polizei-Stand-der-Dinge-Kosten-Datenschutz-7134410.html?seite=all>

12 <https://www.bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html>

Fall sein, wenn parallel von 15.000 Nutzungen im Jahr in Hessen und zur Nutzung für den „polizeilichen Alltag“ gesprochen wird.

Wie man allerdings auf die Aussage „Soweit ersichtlich, ist das Softwareprodukt des Unternehmens Palantir aktuell die beste und effizienteste Lösung auf dem Weltmarkt.“ kommt, wird nicht näher dargelegt. **Palantir ist viel Mysterium um die Firma selber und Personenkult um Alex Karp als CEO.** Fakten und Informationen lassen sich kaum widerspruchsfrei öffentlich finden und jede Datenanalyse-Software, welche durch Datapipelines (näheres dazu in späteren Absätzen) alle polizeilichen Daten in ein ontologisches Modell überführt ist recht gleichwertig und nichts Besonderes.

Auch „Eine vergleichbare Alternativlösung gibt es derzeit nicht.“ wird **ohne Verweis auf eine Studie oder dergleichen behauptet**, was unseriös ist.

Als Hinweis sei hier erlaubt, dass, wenn in Ausschreibungen der LKAs eine Software erforderlich ist, die bereits auf dem Markt der Strafverfolgung etabliert ist und entsprechende Referenzen benenne kann, dies ein **Alleinstellungsmerkmal** darstellt, das ist richtig. Ob das aber den Anspruch erfüllt, Alternativlos zu sein, erschließt sich uns nicht. Eher deutet das auf ein **optimiertes Vergabeverfahren** hin, damit Palantir als einzige Lösung übrig bleibt. So wie hier ja im Antrag auch einzig Palantir als Lösung gesehen wird, ohne dies mit nachvollziehbaren Fakten sachlich zu belegen.

Immerhin werden CDU-Wünsche geäußert: „Es ist zwar wünschenswert, dass deutsche oder aber europäische IT-Unternehmen vergleichbare Software-Produkte entwickeln und anbieten“, die wir so im Raum stehen lassen.

Zu „Zumindest für eine Übergangszeit...“ kann nur nochmal wiederholt werden, dass **Palantir kommt, um zu bleiben** und eine **Übergangszeit eine Scheinbehauptung** ist, denn einen Migrationsplan von Palantir zu einer anderen – idealer einer eigenen P20-Datenhaus – Lösung liegt in keinem anderen Bundesland vor, welches Palantir einsetzt. Ein konkreter Migrationsplan wird gar nicht erst in Erwägung gezogen, da klar ist, dass die Polizei bei Anwendung von Palantir für die Gefahrenabwehr (gemäß Landesrecht) vollständig abhängig werden. Dann wäre Palantir in der Tat alternativlos.

Zu „Palantir [...] durch das Fraunhofer-Institut auf Herz und Nieren geprüft“ lässt sich nüchtern feststellen, dass es sich um eine **weitere Nebelkerze** handelt. Teile der Software wurden technisch geprüft und "In der Software wurde keine sogenannte Backdoor identifiziert" als Aussage festgestellt. Dies wurde also einmalig vorgenommen und **ist mit jedem Update als Aussage hinfällig**. Zum anderen benötigt Palantir keine technischen und somit nachweisbaren Hintertüren, da **Mitarbeitende von Palantir immer wieder Vollzugriff auf Daten und Software haben**, um die Datapipelines zu bauen, Updates einzuspielen und Administration bzw. Konfiguration der Software vorzunehmen. In **Hessen und NRW wurden 2 bis 4**

Mitarbeitende von Palantir öffentlich erwähnt, in **Bayern sieben Mitarbeitende von Palantir**, die sogar in einem separaten Raum alleine tätig sind und Montags mittags aus verschiedenen Ländern einfliegen, um Freitags wieder zurück zu fliegen.

Wie diese Mitarbeitenden sich bei Anordnung von Trump, Thiel, Karp, einem FISA Gericht oder anderen US-Autokratischen Vorgaben verhalten werden, darf gerne in Anbetracht der aktuellen geopolitischen Geschehnisse vermutet oder gewünscht werden. Bayern hat dazu klargestellt, dass es eine Klausel im Vertrag hat und daher der Abgriff der Daten verhindert wird. Wir bezweifeln die Wirksamkeit einer solchen Klausel vor dem Hintergrund der amerikanischen Durchgriffsmöglichkeiten (Section 702, FISA-Court).

Dazu sei noch erwähnt, dass selbst die Schweizer Armee in ihrem Armee-Stab Bericht zu „Palantir Technologies Inc.“¹³ festgestellt hat, dass eine **Abhängigkeit von Palantir zu hoch** wäre und das **Risiko nicht tragbar** ist¹⁴¹⁵.

Die **Schlussfolgerung** „Es ist möglich, die Software so einzusetzen, dass ein nicht autorisierter Datenabfluss an Dritte ausgeschlossen werden kann.“ ist daher **folgerichtig falsch**.

3.2 Wie funktioniert Palantir?

Die geplante Nutzung von Software wie Palantir oder vergleichbarer Alternativen, die **ontologische Datenmodelle** nutzt, ist **offensichtlich verfassungswidrig**.

Zur Nutzung müssen Mitarbeitende von Palantir sogenannte **Datapipelines** bauen. Diese Daten-Pipelines lesen aus den bestehenden Polizei-Datenbanken kontinuierliche alle Informationen aus und speisen diese strukturiert in Palantir als Datenbasis ein.

Daten aus diesen polizeilichen Datenbanken wurden allerdings mit **Zweckbindung** erhoben, beispielsweise Zeugendaten und -aussagen und dürfen nicht ohne weiteres anderweitig genutzt bzw. **zweckentfremdet missbraucht** werden.

Durch das kontinuierliche und strukturierte Einspeisen aller Daten in Palantir stellt diese Form der Verarbeitung eine **Rasterfahndung by Design und Default** dar.

Die Zweckbindung der Daten muss vor Einspeisung in die Daten-Pipelines von Palantir durch Kennzeichnung der Daten sichergestellt werden. Daher ist eine Klassifizierung der Daten in allen polizeilichen Datenbanken der Strafverfolgungsbehörden vor einem solchen Softwareeinsatz vorzunehmen und **nur verfassungsrechtlich legitimierte Daten dürfen in ein automatisches Datenanalyse und -recherchesystem überführt werden**. Dies muss sowohl

13 <https://cdn.repub.ch/s3/republik-assets/repos/republik/article-wie-palantir-hartnaeckig-den-schweizer-staat-umwarb/files/505a33d5-adbd-49f8-baca-5864df625564/armeestaab-evaluation.pdf>

14 <https://www.republik.ch/2025/12/08/wie-hartnaeckig-palantir-die-schweiz-umwarb>

15 <https://www.republik.ch/2025/12/09/warum-palantir-zum-risiko-fuer-die-schweiz-wird>

gesetzlich als auch technisch sichergestellt werden, anderenfalls bleibt der offensichtlich verfassungswidrige Zustand erhalten, selbst bei Einsatz von alternativen Lösungen.

Diese Daten-Pipelines werden des Weiteren nicht von den Strafverfolgungsbehörden selber, sondern von Mitarbeitenden von Palantir entwickelt und gepflegt. Dadurch haben diese **Palantir-Mitarbeitenden Zugriff auf die Verarbeitungslogik als auch auf die Daten** selber.

Palantir setzt wie erwähnt **Ontologie**¹⁶ ein, um die Daten der Strafverfolgungsbehörden mittels Daten-Pipelines kontinuierlich in die eigene Datenbasis zu integrieren. Ontologie steht dabei für ein formales Bedeutungsmodell, das definiert, wie Daten der jeweiligen Landespolizei verstanden, verknüpft und im operativen nutzbar gemacht werden. Palantir beschreibt also alle Eigenschaften, Merkmale und Beziehungen der Daten zueinander einheitlich und strukturiert als gemeinsame Bedeutungswelt in einem zentralen System.

Durch Palantir wird also ein **digitaler Zwilling einer Strafverfolgungsbehörde** geschaffen, die alle Daten, Prozesse, Regeln und Nutzerinteraktionen in einem einheitlichen Modell strukturiert zentral zusammengeführt und maschinell verarbeitet, durchsucht und logisch verknüpft.

Beispiel: Es wird ein **Mensch als semantisches Objekt** angelegt, dem Merkmale wie Name, Geburtsdatum, Handys, Adressen und andere Elemente als **Merkmale zugeordnet** werden. Aber eben auch eine Tätowierung, eine Narbe, Fotos und Videos oder Fallaktennummern. Darüber hinaus z.B. auch Fahrzeuge, dem wiederum als Merkmale Kennzeichen, die Marke und Farbe zugeordnet werden. Und bei Handys dann die Nummern und damit auch alle Kommunikationen und Kommunikationspartnerinnen dieser Nummer und alle Daten aus IMSI-Catcher Überwachungen, Standorte durch stille SMS oder Bewegungsdaten durch Zeitstempel bei Standorten. Darüber hinaus werden auch Fingerabdrücke und Lichtbilder, Fallakten der Ermittler mit ihren Berichten, die Sammlung einzelner polizeilicher Vorgänge wie die Aufnahme eines Verkehrsunfalls oder digitalisierte Asservate diesen Objekten zugeordnet. Die Ermittlerinnen können auch Daten aus dem Internet bzw. den Sozialen Medien einspeisen und analysieren. Und nicht nur Social Media oder Telekommunikationsdaten, sondern auch Daten der Einwohnermeldeämter oder Waffenregister, alles kann per Data-Pipeline eingebunden und zugeordnet werden. Manuell kann alles was man möchte, importiert werden, auch wenn keine Data-Pipeline existiert.

Das alles ist als **Beziehungsgeflecht der Objekte und Merkmale in Palantir** visualisiert und umgehend verfügbar. Mit **allen Daten aus allen Datenbanken, die in Palantir eingespeist wurden**. Auch, wenn diese verfassungsmäßig nicht von der Strafverfolgungsbehörde hätten verarbeitet werden dürfen. Faktisch wird damit nicht nur eine **Rasterfahndung standardmäßig implementiert und die Zweckbindung aufgehoben**, sondern auch das **verfassungsmäßige Trennungsgebot unterwandert** und aufgehoben.

16 <https://www.heise.de/hintergrund/Missing-Link-Machtzentrale-Palantir-eine-Software-lenkt-Organisationen-10463034.html?seite=all>

Aufgrund dieser Beziehungsgeflechte im ontologischen Datenmodell basierende und datengetriebene Entscheidungen und Prozesse der Strafverfolgungsbehörden **verändern sogar die Arbeitsweise der Polizei und machen sie und ihre hoheitlichen Aufgabe damit abhängig von einem externen System und Anbieter namens Palantir**. NRW und Bayern haben öffentlich bereits mehrfach Ihre **totale Abhängigkeit von Palantir** kommuniziert.

3.3 KI in Palantir

Für einen zukünftigen Einsatz von KI sind alle Palantir Plattformen darauf ausgelegt, KI-Modelle und Machine-Learning-Funktionen nahtlos einzubinden, um Analysen und automatische Entscheidungen zu ermöglichen. Die KI Modelle können dabei einfach mittels Palantirs Artificial Intelligence Platform (AIP) integriert werden. So wird **Palantir mit KI Integration** beispielsweise bei **ICE in den USA** oder beim **Targeting (Zielauswahl) für Israel in Gaza** genutzt.

Die **Ontologie spielt im Zusammenhang mit KI in Palantir eine Schlüsselrolle**, da qualitativ hochwertige Daten immer die Grundlage für maschinelles Lernen darstellen. Der sogenannte „AIP Pipeline Builder“ soll LLM-Funktionen in die Daten-Pipelines integrieren. Das Ontologie-System verbindet die Daten mit KI-Modellen und Prozessen und erlaubt dabei, **Aktionen direkt an Objekte zu knüpfen. KI basierte Automatisierung** (auch sogenanntes "Decision Automation") wird damit möglich und eine Vorstellung der Wirksamkeit bekommt man, wenn man zum Einsatz von Palantir bei ICE in den USA recherchiert.

Auch das stark umstrittene **Predictive Policing**¹⁷ wird damit ermöglicht.

¹⁷ <https://www.heise.de/meinung/Missing-Link-Predictive-Policing-die-Kunst-Verbrechen-vorherzusagen-4425204.html>

4 Lösungsmöglichkeit

Der Wunsch nach Datenverknüpfung, Such- und Analysemöglichkeiten, einfachem Datenaustausch- und Zugriff der Polizeien ist nachvollziehbar. Seit 2005 werden Bemühungen unternommen, diesen Wunsch im Rahmen des Programms „Polizei 2020“ (heute: „P20-Datenhaus“) umzusetzen.

Die Lösung ist daher, das P20-Datenhaus aufzubauen und mit einer funktionierenden Suchfunktion auszustatten. Dazu ist es notwendig, in allen Bundesländern für jeden einzelnen Datenpunkt die jeweilige Rechtsgrundlage, die eine Speicherung und Verarbeitung erlaubt, mit abzulegen.

In das P20-Datenhaus wird für bestimmte Aufgaben oder Szenarien dann auch eine Analyse-Komponente integriert werden müssen. Damit diese realitätsnah entwickelt werden kann, empfehlen wir die rechtzeitige und tiefgehende Einbindung der anwendenden BeamtInnen in den Entwicklungsprozess. In diesem Rahmen wäre unter Umständen ein rechtssicherer Einsatz von Palantir nicht pauschal ausgeschlossen, aus Gründen der digitalen Souveränität ist dieser jedoch auch in diesem Szenario weiterhin klar abzulehnen.

Die bisher sichtbaren Verzögerungen und Herausforderungen bei der Umsetzung von P20 sind keine ausreichende Begründung für den Einsatz von Palantir und damit für den Verzicht auf die Berücksichtigung der Rechtsgrundlagen für die Speicherung oder Verarbeitung der jeweiligen Datenpunkte.

Die Aufgabe der Koordination der Zusammenarbeit der Länderpolizeien bei der Kriminalitätsbekämpfung ist gesetzlich durch § 1 (1) BKAG geregelt. Das BKA ist dafür zuständig. Die Forderung nach dem Einsatz von Palantir-Software ist vor allem ein Zeichen fehlender Rechtsdurchsetzung des Innenministeriums. Die Forderung nach dem Einsatz von Palantir ist aus unserer Sicht die Kapitulationserklärung vor der Komplexität der polizeilichen Datenhaltung. Es ist unerträglich, dass diese zentrale, hoheitliche Aufgabe des BKA auf algorithmische Systeme aus dem amerikanischen Ausland ausgelagert werden soll.

Es ist für den Wiederaufbau des verlorenen Vertrauens in die Bürgerrechtstreue der dem Bundesministerium des Inneren nachgeordneten Behörden unumgänglich, die massiven Verzögerungen beim Projekt Polizei2020 nicht nur lückenlos aufzuklären, sondern dieses Projekt umgehend abzuschließen.

Auch dienstrechtliche Konsequenzen für die massiven Verzögerungen in den genannten Projekten sind notwendig, falls konkrete, personenbezogene Verfehlungen behördenintern bekannt geworden sind oder werden.

5 Fazit

Strafverfolgungsbehörden benötigen Digitalisierung und modernes Arbeiten.

Die Verfassung und das Grundgesetz müssen dabei aber berücksichtigt und eingehalten werden.

Beides ist miteinander vereinbar und wirksam nutzbar.

Am süßen Nektar der Palantir Software zu saugen, die offensichtlich verfassungswidrig ist, rechtfertigt nicht, Verfassung und Grundgesetz zu relativieren, Massenüberwachung vorzunehmen oder Rasterfahndung nutzen zu wollen. Das ist und bleibt nicht FDGO konform.

Statt viel Geld in **bürgerrechtsverachtende Spionagesoftware aus dem Hause Palantir** zu investieren wäre es daher zielführender, P20 endlich zu priorisieren und umzusetzen. Dabei ist die **Kennzeichnung aller polizeilichen Daten vorzunehmen und die Zweckbindung zu achten**.

Manuel HonkHase Atug, Gründer und Sprecher der unabhängigen AG KRITIS zum Wunsch des Einsatzes von Palantir:

„Wer Palantir in Deutschland etablieren möchte, schafft eine Infrastruktur, die missbraucht werden kann.

Palantir ist nicht nur Software, sondern **Machtinfrastruktur**. Sie mag Sicherheitsbehörden als effizientes Ermittlungswerkzeug dienen – in einem anderen politischen Kontext kann sie jedoch schnell zum **Instrument systematischer Überwachung und Verfolgung** werden.

Die deutsche Geschichte zeigt, dass modernere Verwaltungs- und Datentechnologien bereits einmal **Voraussetzung für Entrechtung und Vernichtung von Menschen** waren.

Auch aktuelle Beispiele aus den USA verdeutlichen, wie datengetriebene Analyseplattformen in migrations- und sicherheitspolitischen Kontexten eingesetzt werden, siehe ICE in den USA. Der **Zweck einer solchen Machtinfrastruktur ist nicht statisch**; er verschiebt sich mit politischen Rahmenbedingungen und einem Kontextwechsel.

Gerade deshalb muss der Staat besonders sorgfältig prüfen, ob er sich technologisch und politisch an einen Anbieter wie Palantir binden will, dessen Führung offen politische Positionen vertritt, die **grundlegende demokratische Prinzipien massiv infrage** stellen.

Wer diese Risiken relativiert, verkennt die **politische Dimension digitaler Sicherheitsarchitekturen**. Denn Infrastrukturen für Sicherheit sind immer auch Infrastrukturen für Macht — und **Macht verlangt demokratische Kontrolle, bevor sie installiert wird**.“