AG KRITIS

Rede von Manuel Atug von der AG KRITIS

für die Anhörung des Innenausschuss des Niedersächsischen Landtages

zum Einsatz von Palantir in Niedersachsen

zum Antrag der Fraktion der CDU: „Polizeiarbeit in das Zeitalter der Digitalisierung überführen - verfahrensübergreifende Datenanalysen in Echtzeit ermöglichen“

am 12.03.2026

Manuel ‚HonkHase‘ Atug

Gründer und Sprecher der unabhängigen AG KRITIS

Der Sachverständige dankt allen ehrenamtlich tätigen Expertinnen der AG KRITIS und den vielen Sicherheitsforscherinnen aus der Community für ihre Unterstützung.

Kontakt

Manuel ‚HonkHase‘ Atug

E-Mail: HonkHase@ag.kritis.info

Webseite: https://ag.kritis.info

Vorab finden wir es sehr verstörend, dass im hohen Haus der Anbieter der gewünschten Software als offensichtlicher Befürworter an der Anhörung teilnimmt, und nur dieser eine Anbieter alleine an der Diskussion beteiligt wird. Unabhängigkeit sieht anders aus.

Polizeien sollen selbstverständlich digitalisieren. Und ja, es gibt Lösungsmöglichkeiten. Aber nicht durch Palantir oder sogenannte „alternative Lösungen".

Zur Anmerkung von Palantir, dass es große Erfolge gäbe und nicht mal die Kritiker das bezweifeln möchte ich klar und unaufgeregt anmerken: Doch, gerne mal aus der eigenen Blase herausgucken, dann wird diese Fakenews in der realen Welt aufgeklärt. Die AG KRITIS kennt keine wissenschaftliche und unabhängige kriminologische Evaluierung dazu.

Wie funktioniert Palantir und warum sind europäische Alternativen ebenfalls offensichtlich verfassungswidrig?

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. Hypothetische Datenneuerhebung wäre dann auch noch in dem Kontext relevant, wird in der Debatte aber komplett ignoriert.

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 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 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.

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.

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 wird damit ermöglicht.

Lösungsmöglichkeit

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.

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.

Mehr Details dazu in unserer Stellungnahme der AG KRITIS.

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.

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.

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.“