Wenn wir nicht eingreifen, könnte durch Werkzeuge wie die Software Palantir in nicht allzu ferner Zukunft eine automatisierte Sicherheitsarchitektur jeden Menschen unbemerkt erfassen – lückenlos, dauerhaft, ohne Widerspruchsmöglichkeit. Wer zur falschen Zeit am falschen Ort ist oder statistisch „abweicht“, wird zum Verdachtsfall. Jeder Verdacht wird zur Vorverurteilung und Unauffälligkeit wird zur Überlebensstrategie. Der Einsatz von Palantir muss darum strikt begrenzt, gesetzlich reguliert und unter echte, unabhängige Kontrolle gestellt werden. Von **Detlef Koch**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/250804_Die_Software_Palantir_Der_sehende_Stein_des_Ueberwachungszeitalters_NDS.mp3

Podcast: Play in new window | Download

Blicken wir zunächst in Tolkiens *Herr der Ringe*: Dort sind die **Palantíri** (Singular: Palantír) magische Seh-Steine, mit denen man über große Entfernungen kommunizieren und ferne Ereignisse beobachten kann. Diese allsehenden Kugeln verleihen Wissen und Macht, bergen aber auch Gefahren: Sie zeigen nur selektive Wahrheiten und können vom Bösen missbraucht werden. Sauron etwa nutzt einen Palantír, um andere in die Irre zu führen und geistig zu unterwerfen. Tolkiens Lehre: Technik, die unkontrollierte Sicht gewährt, wird gefährlich, wenn Machthunger ins Spiel kommt.

Dass sich ein modernes Überwachungsunternehmen aus dem Silicon Valley ausgerechnet *Palantir* nennt, ist also eine bewusste Provokation. Es suggeriert eine Vision grenzenloser Einsicht und Kontrolle über Informationen – mitsamt den ethischen Fragen, die Tolkien mit den Palantíri verknüpft hat.

Neoliberal und autoritär: Die Ideologie hinter Palantir

Peter Thiel, Mitgründer und Spiritus Rector von Palantir, liefert die ideologische Blaupause: Er vereint radikalen Neoliberalismus mit antidemokratischem Elitendenken. 2009 erklärte Thiel unverhohlen: *„I no longer believe that freedom and democracy are compatible.“* – Freiheit und Demokratie seien nicht mehr vereinbar. Er beklagte, Wohlfahrtsstaat und Frauenwahlrecht hätten den „kapitalistischen“ Liberalismus sabotiert. Thiel misstraut dem Mehrheitsprinzip – die „unbedachte Masse“ verhindere wahre Freiheit. Stattdessen schwärmt er von einer technokratischen Eliteherrschaft: Er schätzt Denker wie Carl Schmitt

(*Der Führer schützt das Recht*), sympathisiert mit monarchistischen Ideen und knüpft Kontakte in neoreaktionäre Kreise. Politisch finanzierte er Donald Trump und andere antiliberale Bewegungen großzügig.

Gleichzeitig predigt Thiel libertären Markt-Fundamentalismus. Er propagiert, Steuern und Regulierung seien von Übel, und sagt provokativ: „Competition is for losers“ – Wettbewerb sei etwas für Verlierer. Unternehmer sollten Monopole anstreben, ungestört vom Staat. Diese Weltanschauung – libertär in der Ökonomie, autoritär in der Politik – prägt Palantirs Selbstverständnis.

Passend dazu wählte man bewusst den Namen *Palantir*. Die Tolkien’schen Seh-Steine symbolisieren allsehende, zentrale Macht über Information. Palantir präsentiert sich folgerichtig als allwissendes Instrument für Sicherheitsbehörden – *das* Werkzeug, um Datenströme zu durchleuchten. CEO Alex Karp behauptet, Palantir stärke liberale Gesellschaften, ohne selbst illiberal zu sein. Doch Kritiker verweisen auf die Realität: Eine Firma mit Thiels antidemokratischer DNA und engen Verbindungen zu US-Geheimdiensten soll den „sehenden Stein“ des digitalen Zeitalters liefern. Dieser symbolische Allmachtsanspruch – totale Einsicht in alle Daten – weckt entsprechendes Unbehagen.

Palantir Gotham – Architektur einer allsehenden Analyseplattform

Palantir Gotham ist die Software-Plattform, die diese Vision technisch umsetzt. Ursprünglich für Geheimdienste entwickelt, dient Gotham heute als universelles Big-Data-Analysewerkzeug für Sicherheitsbehörden. Die Plattform verschmilzt heterogene Datenquellen zu einem einheitlichen sogenannten Ontologie-Modell: Das heißt, Personen, Orte, Ereignisse und ihre Beziehungen werden als verknüpfte Objekte abgebildet. Das ermöglicht eine bundesweite Suche über alle Datenbestände – ein Ermittler kann mit einer Abfrage sämtliche Polizeidatenbanken, Telefonüberwachungslogs, Internetdaten etc. gleichzeitig durchforsten.

Gotham präsentiert die Treffer, führt Daten zusammen und macht Zusammenhänge in Graphen sichtbar. So entstehen digitale Netzwerke wie an einer „Pinnwand“: Mit wenigen Klicks lassen sich alle direkten und indirekten Kontakte einer Person aufspüren; zuvor verborgene Verbindungen treten zutage. Auch geografische Analysen sind integriert – etwa kann die Software alle relevanten Personen anzeigen, die sich in einem bestimmten Zeitraum im Umkreis eines Tatorts aufhielten.

Diese Fähigkeiten haben Gotham den Ruf eines *„digitalen Kraken“* eingebracht, der seine Daten-Tentakel überall ausstreckt. Gotham selbst bietet jedoch Mechanismen für

Datenschutz-Compliance: differenziert abgestufte Zugriffsrechte, umfassende Protokollierung jeder Abfrage und optionales Maskieren sensibler Daten. Palantir betont, dass Audit-Trails und Berechtigungskonzepte fest eingebaut sind, um Missbrauch vorzubeugen.

Inzwischen hat Palantir auch KI-Funktionalitäten eingebettet. Module wie *Ava* durchforsten automatisch die Daten nach Mustern und Anomalien. Machine-Learning-Algorithmen können etwa bei der Gefahrenprognose helfen (z.B. in Predictive-Policing-Modellen). Palantir versichert jedoch, Gotham bleibe ein *„Mensch-in-der-Schleife“*-System – die KI liefert nur Vorschläge, die menschliche Analytiker prüfen und freigeben. Sämtliche KI-Ergebnisse sind mit den zugrundeliegenden Rohdaten verknüpft und im Audit-Log protokolliert. So sollen Transparenz und Kontrolle gewahrt bleiben. Gleichwohl bleibt die genaue Algorithmik firmengeheim und für Außenstehende eine Blackbox.

Unstrittig ist Palantirs Leistungsfähigkeit: Milliarden Datensätze lassen sich in Minuten durchsuchen, was zuvor Tage gedauert hätte. Doch auch hier gilt: *Garbage in, garbage out* – will sagen: Fehlerhafte oder voreingenommene Eingabedaten führen zu fehlerhaften Ausgaben. Die Software liefert Hypothesen, keine Wahrheiten. Palantir selbst sagt, man baue „Entscheidungshilfen, keine Entscheidungsautomaten“ – die Verantwortung bleibt beim Menschen.

Palantir in Deutschland: Ausbreitung und verfassungsrechtliche Hürden

In Deutschland ist Palantir (Stand Juli 2025) vor allem in vier Bundesländern im Polizeieinsatz. **Hessen** führte Ende 2017 als erstes *HessenData* ein – im Eilverfahren ohne Ausschreibung. Das System läuft seit 2018 und wurde als Anti-Terror-Tool beworben (ein angeblich vereitelter Anschlag 2018 wurde später angezweifelt). **Nordrhein-Westfalen** folgte 2020 mit *DAR*, das nach regulärer Ausschreibung Palantir nutzt und alle Polizeidatenbanken des Landes verknüpft. **Bayern** entschied sich 2022 für Palantir (*VeRA*) und startete 2023 einen Pilotbetrieb – zunächst ohne gesetzliche Grundlage, was der Datenschutzbeauftragte scharf kritisierte. Inzwischen arbeitet Bayern an der Gesetzesanpassung, VeRA läuft testweise mit echten Daten. **Baden-Württemberg** beschaffte 2023 Palantir, musste aber erst das Polizeigesetz ändern (Juli 2025), um den Einsatz zu erlauben – geplant ist ein Probelauf unter parlamentarischer Aufsicht. Damit werden ab 2025 vier Länder Palantir verwenden.

Hamburg hatte zwar eine Ermächtigung für Palantir geschaffen, doch nach dem BVerfG-Urteil 2023 – das diese Norm verwarf – wurde dort kein System eingeführt. **Berlin** erwägt, Palantir über den bayerischen Rahmenvertrag zu beziehen, zögert aber mangels

Gesetzesgrundlage noch. Auf **Bundesebene** hatte das BKA Palantir fest eingeplant, doch im Juli 2023 stoppte Innenministerin Nancy Faeser (SPD) das Vorhaben nach dem Karlsruher Urteil. Der Bund will nun eine eigene Software entwickeln. Einige konservativ regierte Länder (Bayern, BaWü, perspektivisch Berlin) treiben Palantir zwar voran, doch die meisten Länder halten sich vorerst zurück.

Rechtliche Auseinandersetzungen: Der entscheidende Präzedenzfall war das Urteil des Bundesverfassungsgerichts vom 16. Februar 2023. Karlsruhe erklärte die Palantir-Ermächtigungen in Hessen und Hamburg für verfassungswidrig. Grund: Die Gesetze erlaubten eine *zu* breite Datenanalyse ohne hinreichende Schwellen. Insbesondere fehlte die Trennung zwischen Daten tatsächlicher Verdächtiger und solcher Unbeteiligter – Letztere wurden als „Beifang“ bislang mitdurchleuchtet, was das Recht auf informationelle Selbstbestimmung verletzte.

Das Bundesverfassungsgericht (BVerfG) forderte klare Grenzen: Nur bei konkreter Gefahr oder einem definierten Verdachtsgrad dürfen derart invasive Big-Data-Tools eingesetzt werden. Zudem müssten Daten unbescholtener Bürger technisch gekennzeichnet und besonders geschützt werden. Als Folge des Urteils musste Hessen sein Polizeigesetz nachbessern (was wiederum als unzureichend kritisiert wird). Hamburgs Norm wurde sofort aufgehoben. Die Gesellschaft für Freiheitsrechte e. V. (GFF) hat inzwischen auch gegen Hessens neues Gesetz Verfassungsbeschwerde angekündigt, ebenso gegen NRW und Bayern.

Die meisten Länder warten diese Verfahren ab und nehmen vorerst Abstand von Palantir. Palantir ist hierzulande zwar auf dem Vormarsch, bewegt sich aber in einem rechtlichen Graubereich, den erst Gesetzesreformen und weitere Urteile auflösen werden.

Risiken: Grundrechtsbedenken, Bias und fehlende Kontrolle

Grundrechte in Gefahr: Aus Sicht von Bürgerrechtlern gefährdet Palantir zentrale Grundrechte. Die Software schafft eine beispiellose Durchleuchtung persönlicher Daten – das Recht auf **informationelle Selbstbestimmung** (Art. 2 in Verbindung mit Art. 1 Grundgesetz (GG)) und das **Fernmeldegeheimnis** (Art. 10 GG) sehen Kritiker massiv verletzt. Eine Plattform, die zig Datenbanken fusioniert und automatisiert auswertet, greift tief in die Privatsphäre auch Unbeteiligter ein. Das BVerfG hat betont, dass schon das maschinelle Verknüpfen von Daten einen eigenständigen schweren Grundrechtseingriff darstellt. Palantir erzeugt neue Verdachtsmomente, wo vorher keine waren – Menschen geraten allein aufgrund von Datenmustern ins Visier. So kann es Unschuldige treffen (Opfer, Zeugen, Zufallsbekanntschaften), was rechtsstaatliche Prinzipien unterläuft. Zudem

befürchten viele ein Klima der **Massenüberwachung**: Wenn Bürger annehmen müssen, dass all ihre Kontakte, Bewegungen und Kommunikationen langfristig registriert und analysiert werden, wirkt das einschüchternd. Die Ausübung von Meinungs- und Versammlungsfreiheit könnte leiden – ein weiterer Schritt hin zum Überwachungsstaat.

Auch **Diskriminierung** durch algorithmische Verzerrungen (Bias) ist ein Risiko. Palantir wertet historische Daten aus – und diese sind oft von bestehenden Vorurteilen geprägt. Wurden etwa bestimmte Viertel jahrelang „überpoliziert“, erscheint dort statistisch mehr Kriminalität, was Palantirs Analysen dann als „Gefahren-Hotspot“ bestätigen würde. Rassistische Voreingenommenheit (**Racial Bias)** und andere Vorurteile könnten so fortgeschrieben werden. Ohne Transparenz über die Algorithmen bleibt unklar, welche Fehlerquellen im System wirken.

Ferner kritisieren Datenschützer die **Zweckentfremdung** von Polizeidaten: Palantir hebt die Trennwände zwischen verschiedenen Zwecken auf. Daten, die für einen konkreten Anlass erhoben wurden, werden nun für ganz andere Zwecke genutzt – bis hin zur präventiven „Gefährder“-Suche ohne konkreten Anlass. Das verletzt das Prinzip der Zweckbindung. Schließlich ist Palantir eine Blackbox in privater Hand. Weder Öffentlichkeit noch unabhängige Stellen können nachvollziehen, wie genau das System zu seinen Schlussfolgerungen kommt. Diese Intransparenz erschwert die demokratische Kontrolle. Gleichzeitig wirft die Abhängigkeit von einem privaten US-Anbieter Fragen der **digitalen Souveränität** auf. Experten warnen vor möglichem US-Zugriff und einem Verlust staatlicher Hoheit über sensible Daten.

Schlussbetrachtung und Ausblick

Wohin führt der Weg, wenn wir nicht eingreifen? Eine dystopische Perspektive: In nicht allzu ferner Zukunft könnte eine automatisierte Sicherheitsarchitektur jeden Menschen unbemerkt erfassen, verknüpfen und bewerten – lückenlos, dauerhaft, ohne Widerspruchsmöglichkeit. Algorithmen taxieren unsere Leben in Echtzeit, erstellen Risikoprofile, identifizieren vermeintlich „auffällige“ Kontakte oder Bewegungsmuster – gespeist aus digitalen Schatten, nicht aus konkreten Taten. Die Schwelle zur Intervention sinkt: Polizeiliche Maßnahmen erfolgen dann nicht mehr auf Grundlage eines konkreten Verdachts, sondern auf Basis undurchsichtiger Rechenmodelle, die ihre Kriterien nicht offenlegen.

Wer zur falschen Zeit am falschen Ort ist oder statistisch „abweicht“, wird zum Verdachtsfall. Und wer davon betroffen ist, erfährt es womöglich nie. Die demokratische Kontrolle – parlamentarische Aufsicht, gerichtlicher Rechtsschutz, öffentliche Rechenschaft

– Fehlanzeige. Entscheidungen werden von einem privat programmierten Code vorbereitet, der sich jeder politischen Verantwortung entzieht. Die offene Gesellschaft – die auf Vertrauen, Öffentlichkeit und rechtsstaatlicher Prozedur beruht – wird in eine Gesellschaft vorauseilenden Gehorsams verwandelt. Jeder Verdacht wird zur Vorverurteilung und Unauffälligkeit wird zur Überlebensstrategie.

Diese Zukunft ist kein Science-Fiction-Szenario. Sie wird gebaut – mit Mitteln wie Palantir.

Wenn wir nicht handeln, wird nicht nur der Datenschutz erodiert, sondern der Grundpfeiler demokratischer Gesellschaft: die Achtung vor dem Einzelnen als frei entscheidendes Subjekt. Stattdessen droht eine Welt, in der Maschinen Verdachtsmomente erzeugen und Menschen in Datenströmen verschwinden. Eine Welt, in der das Recht auf Abweichung, auf Opposition oder auch nur auf Zweifeln durch automatisierte Konformitätsmodelle ersetzt wird, verwandelt das Lebenselixier jeder Demokratie in einen giftigen Cocktail des Totalitarismus.

Wer das verhindern will, muss jetzt Grenzen ziehen

Eine sogenannte Sicherheitssoftware wie Palantir darf nicht als Trojaner in den Rechtsstaat einziehen. Ihr Einsatz muss strikt begrenzt, gesetzlich reguliert und unter echte, unabhängige Kontrolle gestellt werden. Keine Funktion ohne demokratische Legitimation. Keine Analyse ohne Nachvollziehbarkeit. Keine Blackbox in den Händen eines ideologisch aufgeladenen US-Konzerns mit autoritärer Schlagseite.

Wir brauchen eine breite, öffentliche Debatte über **digitale Souveränität** und die Frage, wem wir die Macht über unsere Daten, unsere Profile und damit unser gesellschaftliches Dasein überlassen wollen. Es reicht nicht, auf technische „Lösungen“ zu vertrauen. Wir müssen politische Verantwortung übernehmen – und klarstellen:

Technik hat dem Menschen zu dienen, nicht umgekehrt.

Wer Sicherheit über Freiheit stellt, bekommt am Ende weder das eine noch das andere – sondern Überwachung, Willkür und eine entkernte Demokratie.

Titelbild: tadamichi / Shutterstock