Die neue Macht des Datenapparats: In Zeiten von Unsicherheit, gesellschaftlicher Zerrissenheit und geopolitischen Umbrüchen hoffen viele auf ein Werkzeug, das Klarheit schafft: auf Daten, Fakten und schnelle Antworten. Die Software Palantir verspricht genau das und ist gleichzeitig eine der größten demokratischen Herausforderungen unserer Zeit. Denn die Software rechnet nicht nur, sie entscheidet maßgeblich mit: ob im Krankenhaus, im Gerichtssaal oder an der Grenze. Deshalb bedarf es Wachsamkeit bezüglich dieses Unternehmens – und eine grundsätzliche Debatte über Kontrolle, Transparenz und Verantwortung. Von **Günther Burbach**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/250815_Der_digitale_Doktor_Wenn_die_Software_Palantir_ueber_Klinik_Gerichtssaal_und_Grenzzaun_mit_entscheidet_NDS.mp3

Podcast: Play in new window | Download

I. Justiz und Rückfälligkeit – Wenn Algorithmen über Schicksale wachen

Stellen Sie sich eine Welt vor, in der ein Richter nicht allein nach Gesetz und Gewissen urteilt, sondern sich auch auf ein Dashboard stützt: Rot = hoher Risikoscore, Grün = niedriges Rückfalltempo. Diese Ebene ist näher, als Sie denken. In Großbritannien zeigte eine Anfrage nach dem Freedom-of-Information-Act, dass Palantir dem Justizministerium und der Gefängnisverwaltung selbstredend „sichere Datenverknüpfung“ zur Ermittlung von Rückfallrisiken angeboten hat. Statt Einzelfallprüfung dominierte am Ende ein Algorithmus, der Statistiken auswertet, ohne Empathie, Lebensgeschichte oder Kontext.

Solche Prognosen klingen nach Effizienz, aber sie stecken voller Risiken. Fehlerhafte oder voreingenommene Daten führen zur Fehleinschätzung ganzer Gruppen. Wenn zum Beispiel Menschen aus bestimmten Vierteln überproportional in Polizeikontakten erscheinen, wird der Score automatisch in Richtung Überwachung ausspringen, eine klassische Self-Fulfilling Prophecy. Noch bedenklicher: Wer sich auf Prognosesoftware verlässt, redet im Zweifel von „Datenbasis“ statt von „judizieller Abwägung“. Und das schwächt die Tragfähigkeit gerichtlicher Entscheidungen.

Besonders brisant: Das Bundesverfassungsgericht hat im Februar 2023 Teile der rechtlichen Grundlagen für automatisierte Polizeianalyse in Hessen und Hamburg als verfassungswidrig eingestuft. Die Begründung: Datenschutz und rechtsstaatliche Prinzipien wurden nicht ausreichend berücksichtigt, eine Warnung, die symbolisch für ganz Europa

gelten kann.

II. Gesundheit als Datenplattform – NHS unter Palantirs Federführung

Die britische National Health Service (NHS) hatte 2023 einen Mega-Vertrag mit Palantir abgeschlossen: 330 Millionen britische Pfund für eine zentrale Datenplattform, die alle Gesundheitsdaten in Echtzeit bündeln soll. Von der Bettenverwaltung über Wartezeiten bis hin zur Intensivstation-Zuteilung. Pläne sahen vor, dass Patientenströme und Ressourcen digital optimiert werden.

Doch in der Ärzteschaft regte sich Widerstand. Die British Medical Association (BMA) warnte, dass die technologische Direktive Palantirs „am Interesse der Patienten“ vorbei agiere. Es gehe nicht um Effizienz, sondern um Kontrolle. Journalistische Recherchen deckten auf: Mehr als 400 von 586 Seiten des Vertrags waren geschwärzt, Transparenz gleich null. Die Folge: Weniger als die Hälfte der Kliniken waren angeschlossen, viele warten auf Klärung ihrer Datenschutzbedenken. Dabei dürfte es weniger um Technik als um Vertrauen gehen: Wer entscheidet, was digital zugänglich ist, und wer bewahrt die Kontrolle?

Wenn ein Unternehmen wie Palantir die Infrastruktur für Gesundheit aufbauen soll, geht es nicht nur um Bits und Bytes, sondern um Vertrauen und Autonomie. Das Schweigen über die Vertragspassagen wirkt wie eine Kampfansage an eine demokratische Gesellschaft: Vertrauen opfert man, wenn Effizienz alles wird.

III. Migration & Grenzsicherung – Daten als Spürhunde des Staates

Wer migriert? Woher kommen Menschen, wer sind ihre Verbindungen? In den USA beantwortet Palantir solche Fragen direkt. Die Plattform ICM (Investigative Case Management), die von Palantir geliefert wird, ist zentraler Bestandteil der Ermittlungen der Einwanderungsbehörde ICE. Sie arbeitet mit Profilanalysen, Netzwerkverfolgen und Risikoeinschätzungen, um Abschiebungen zu steuern oder zu verhindern.

Daten, die in diesem Kontext gesammelt werden, schleifen durch mehrere Behörden spurlos. Das hat Auswirkungen, auch wenn Palantir im öffentlichen Bewusstsein nicht sichtbar ist. Denn wer die Datenlandschaft gestaltet, beeinflusst Entscheidungsebenen, die bis heute individuell und durch Prozesse geprägt sein sollten, nicht durch Eine-Hinweis-Lösung. Es ist kurzsichtig zu glauben, Palantir-Techniken seien nur Tools, in Wahrheit formen sie politische Handlungsmöglichkeiten. Effektivität darf nicht zum Ersatz für demokratischen Diskurs werden.

IV. Souveränität unter Druck – Europas Abhängigkeit von US-Software

Nicht nur als Bürger, auch als Gesellschaft stehen wir, meist unbemerkt, unter der Regie der einflussreichsten Datenanalysten: US-Firmen, die weltweit Informationen auswerten. Der CLOUD Act gibt US-Behörden Zugriff auf Daten von US-Anbietern, auch wenn diese Daten in Europa gespeichert sind. Damit wird unsere digitale Souveränität untergraben: Was wir nicht kontrollieren können, ist gesellschaftsrelevant.

Europa reagiert – etwa mit dem Data Act -, doch das ist ein Flickenteppich. Wer entscheidet IT-Standards? Wer bestimmt, wann und wie Daten fließen? Es fehlt nicht an Regeln, sondern an echten Kontrollmöglichkeiten dessen, was unter unserer Verfasstheit stattfindet.

V. Palantir als Alarmsystem – Nutzen versus Einfluss

Es wäre naiv zu behaupten, Palantir hätte nur Risiken, in vielen Fällen rettet Software Leben: Militärische Abstimmungen, Rettungseinsätze, epidemiologische Analysen. Wissenschaftliche Arbeit ist heute unvorstellbar ohne Algorithmen. Aber wir müssen uns im Klaren sein: Wer die Kontrolle hat, bestimmt auch den Takt. Wo Systeme keine Transparenz haben, kann sich Macht verselbstständigen.

Der kritische Punkt lautet: Haben demokratische Gesellschaften das Gestaltungsrecht über Palantir oder übernimmt die Technik dieses Recht? Wenn Entscheidungen zunehmend auf Daten und nicht auf Diskurs basieren, verschiebt sich unser Selbstverständnis: Wir werden zu Objekten, nicht mehr zu Subjekten demokratischer Prozesse.

VI. Forderungen – Mehr als nur Technik bleiben

Aus all dem ergeben sich klare Grundanforderungen:

- **Volle Transparenz**: Verträge müssen öffentlich einsehbar sein. Vertragsteile, die Geheimhaltung verlangen, müssen begründet und begrenzt sein.
- **Menschlicher Entscheidungszwang**: KI darf beraten, nicht entscheiden. Jeder Einsatz muss mit menschlicher Autorität rückgekoppelt sein.
- **Offene Audits**: Algorithmen müssen auditierbar sein – auch mit Zugriff durch unabhängige Instanzen.
- **Rechtssichere Widerspruchsmöglichkeiten**: Bürger*innen müssen digitale

Entscheidungen anfechten können – nicht als Ausnahme, sondern als Standard.

- **Strategische Anstrengungen für europäische Alternativen**: IT-Systeme sollten europäischen Rechtstraditionen entsprechen, nicht US-Standards folgen.

VII. Szenarien der Zukunft – zwei Pfade, eine Entscheidung

Best-Case-Szenario:
Europa schafft eigene Plattformen, die offen, transparent und überprüfbar sind. Systeme funktionieren als unterstützende Tools: im Gesundheitssystem, in der Justiz, in der Verwaltung. Menschen behalten die Kontrolle, statt Daten die Entscheidung.

Worst-Case-Szenario:
Es entsteht ein quasi undurchsichtiger Layer, der Regierungssysteme flankiert und künftig Entscheidungen mitbestimmt. Funktionserweiterungen geschehen schleichend. Vertrauen bröckelt, Rechte werden technologisch ausgehebelt, ein Paradies für technokratische Kontrolle.

Epilog: Wachsamkeit ist Bürgerpflicht

Dieser Text ist keine Botschaft eines Technophoben. Es ist eine Warnung davor, wie schnell Instrumente der Effizienz zu Mitteln der Kontrolle werden können und wie dringend es ist, Verantwortung zu übernehmen. Wer Kontrolle abgibt, dem entwischen die Grundfeste der Demokratie. Palantir ist ein Prüfstein – zeigen wir, dass alles sehende Steine nur so mächtig sind, wie wir es zulassen.

Titelbild: Alan Mazzocco / Shutterstock

Quellen:

1. **Justiz & Rückfälligkeit**
   - „Tech firm Palantir spoke with MoJ about calculating prisoners’ reoffending risks“, *The Guardian*, 16.11.2024.
2. **Karlsruher Urteil**
   - „German police use software to fight crime – court says unlawful“, *Reuters*, 16.2.2023.

3. **NHS-Vertrag**
   - „Patient privacy: fears US ‘spy-tech’ firm Palantir wins NHS contract“, *The Guardian*, 21.11.2023;
   - *FT.com*: Daten-Einbindung, Vertragsstruktur, Beteiligungsquote.
4. **Migration & ICE**
   - DHS-Datenschutz-Impact-Assessment zu ICM, Juni 2016;
   - „Palantir IPO: Big-Brother tool in ICE’s toolbox”, *The Guardian*, September 2020.
5. **Ukraine & Kriegsverhalten**
   - „Ukraine is using Palantir’s software for targeting, CEO says“, *Reuters*, 2.2.2023.
6. **CLOUD Act & Datenschutz**
   - EDPB/EDPS Joint Response to US CLOUD Act, EDPB/EDPS, offizielle EU-Dokumentation.