A4 - Palantir & Co. – Das ist keine Sicherheit!

In vier Bundesländern wird Palantir-Software bereits eingesetzt: Hessen, Bayern, Baden-Württemberg & Nordrhein-Westfalen[1,2]. Jetzt öffnet die Bundesregierung unter dem Vorwand der Strafverfolgung und Terrorismusbekämpfung mit drei Gesetzesvorschlägen zur Erweiterung der digitalen Ermittlungsbefugnissen der Polizei und dem Einsatz von biometrischer Analyse von Fotos im Internet[3] Tür und Tor für den bundesweiten Einsatz automatisierter Datenanalyse. Und auch die neue Brandenburger Landesregierung hat sich im Koalitionsvertrag vorgenommen, das Polizeigesetz zu reformieren, um den Einsatz von neuen Recherchemöglichkeiten zu ermöglichen[4], und somit ihre Offenheit für die Einführung automatisierter Datenanalyse-Tools signalisiert.
Das gilt es zu verhindern!

Nicht immer Palantir, aber immer problematisch: automatisierte Datenanalyse

Bei der automatisierten Datenanalyse werden Daten aus bisher voneinander getrennten Datenbanken zusammengefasst und aufbereitet[5], häufig mit Hilfe von künstlicher Intelligenz (KI)[1]. Einbezogen werden dafür nicht nur polizeieigene Datenbanken, sondern je nach Bundesland auch das Melderegister und andere Datenbanken, auf die die Polizei in der Regel keinen Zugriff hat[6]. Dabei spielt es keine Rolle, ob man in der Vergangenheit bereits strafrechtlich auffällig geworden ist oder nicht, auch Zeug*innen, Opfer von Straftaten oder Auskunftspersonen, die mit der Polizei in Kontakt getreten sind können durchleuchtet werden[7].

Verletzungen unserer Rechte sind eingebaut / Privatsphäre? Jetzt nicht mehr.

In Deutschland gibt es ein Recht auf Anonymität: Das Recht auf informationelle Selbstbestimmung garantiert, dass niemand für uns entscheiden darf, wo und durch wen unsere persönlichen Daten verarbeitet werden[8]. Die Grundrechte-Charta der EU garantiert uns außerdem den Schutz unserer persönlichen Daten,

das heißt sie dürfen nur mit unserer Zustimmung und nur für bestimmte Zwecke genutzt werden[9].

Die Erstellung von übergreifenden Datenbanken, wie sie für die automatisierte Datenanalyse nötig sind, steht im direkten Konflikt mit diesen Datenschutzrechten. Denn es werden dabei tiefgreifende und detaillierte Persönlichkeitsprofile aller Personen erstellt, die in Deutschland schon einmal Kontakt zur Polizei hatten[10]. Wer Opfer einer Straftat wurde oder zur Polizei geht, um Anzeige zu erstatten oder eine Zeugenaussage zu machen, sollte sich nicht Sorgen machen müssen, später bei einer automatisierten Datenanalyse als potentielle Verdachtsperson durchleuchtet zu werden. Selbst durch das Absetzen eines Notrufs kann man potentiell in dieser Datenbank landen. Das Ausmaß der darin aufgenommenen Daten ist gigantisch, allein in Bayern sind es ungefähr 39 Millionen Personendatensätze[11]. Sollten die Vorhaben der Bundesregierung sich durchsetzen und auch die Untersuchung des Internets ermöglicht werden, werden noch größere Datenmengen einbezogen werden.

Bei Abfragen der Polizei werden all diese persönlichen Daten analysiert, egal ob es Verdachtsanlässe gibt oder nicht[11]. Die daraus resultierenden Ergebnisse können weit über die ursprüngliche Suchanfrage hinausgehen und strukturell fehlerhaft sein. [10] Dabei fehlt es im bisherigen Einsatz auch an Möglichkeiten, um vor Fehlern bei der automatisierten Datenanalyse zu schützen[7] und an Transparenz für betroffene Personen[10].

Indirekte Einschränkung unserer Freiheit

Freiheit braucht ein gewisses Maß von Anonymität. Wer nicht darauf vertrauen kann, dass das Ausleben unserer im Grundgesetzt festgeschriebenen Freiheiten ohne staatliche Konsequenzen bleibt, wird diese nicht mehr nutzen. Die Enormität potentiell abgreifbarer persönlicher Daten kann zur Einschüchterung bei der Auslebung von unseren Grundrechten wie der Meinungs- und Versammlungsfreiheit führen. Denn durch den Einsatz von Tools zur automatisierten Datenanalyse ist nicht mehr vorhersehbar, wodurch man Datenspuren hinterlässt und bei Abfragen durch die Polizei durch einen „verdachtserzeugenden Treffer“ auftauchen kann[10].

Keine Daten für Neonazis

Hinzu kommt: Unbefugte Datenabfragen durch die Polizei haben in Deutschland System. Dabei sind die Fälle des „NSU 2.0“ und „Nordkreuz“, bei denen rechtsextreme Polizisten unerlaubter Weise personenbezogene Daten abgefragt haben, um politische Gegner auszuspionieren oder Drohschreiben zu versenden[12], nur die Spitze des Eisbergs.

Das unbefugte Abfragen von Daten selber führt dabei selten zu ernsthaften rechtlichen oder beruflichen Konsequenzen[13]. Erst wenn die unbefugte Datenabfrage mit einer anderen Straftat kombiniert wird, gibt es nennenswerte

rechtliche Folgen. Die Einführung von Software zur automatisierten Datenanalyse würde Stalking durch Beamte oder Fälle wie den „NSU 2.0“ noch weiter verschärfen.

Was da ist, wird auch genutzt

Systeme zur automatisierten Datenanalyse sollen eingeführt werden, um bei der Bekämpfung von Terrorismus und anderer schwerwiegender Kriminalität zu helfen[3,7]. Expert*innen bezweifeln, dass es nach ihrer Einführung dabei bleibt[14]. Eine Sorge, die sich in den Bundesländern, in denen diese Systeme bereits genutzt werden bewahrheitet. Es zeigt sich zunehmends, dass der Großteil der Suchanfragen sich um deutlich weniger schwerwiegende Straftaten dreht, deren Gefahrenlage die Grundrechtseinschnitte nicht rechtfertigt[6].

Dass zur „Terrorbekämpfung“ eingeführte Sonderrechte der Polizei missbraucht werden, auch zur Einschüchterung von unangenehmem politischem Protest, zeigt sich außerdem auch am Beispiel des Bayerischen Polizeiaufgabengesetzes und der Letzten Generation. Im Namen der „Terrorismusbekämpfung“ wurde der Polizei in Bayern die Berechtigung eingeräumt, Personen unter der Begründung der „drohenden Gefahr“ für 30 Tage (mit Verlängerung bis zu 60 Tage) ohne Gerichtsverfahren ins Gefängnis zu sperren[15]. Dieser Paragraph wurde später angewendet, um der Polizei zu erlauben, Klimaaktivist*innen der Letzten Generation für ihren friedlichen Protest einzusperren und sie einzuschüchtern[16]. Das zeigt: Wenn die Polizei erstmal ein Werkzeug hat, wird sie es auch nutzen, unabhängig von seinem ursprünglich vorgesehenen Zweck.

CIA-gefördert und neo-faschistisch: Palantir bringt keine Sicherheit

Im Kontext der automatisierten Datenanalyse steht ganz besonders ein Konzern im Fokus: Palantir. Der US-amerikanische Konzern wurde mit Startkapital der CIA gegründet und verkauft seither Softwarelösungen im Bereich Sicherheit und Militär an Sicherheitsbehörden und Militärs weltweit[17]. Auch die US-Abschiebebehörde ICE nutzt deren Software, um Migrant*innen ausfindig zu machen[18].

Während Palantir sich gerne als „Verteidiger des Westens“ präsentiert[19], ist es alles andere als ein Freund demokratischer Institutionen, stattdessen ist es zentral im Netzwerk der Tech-Oligarchen rund um Trump. Der Palantir-Gründer Peter Thiel vertritt extrem rechte Ideologien und ist für Aussagen wie „Ich glaube nicht länger, dass Freiheit und Demokratie miteinander vereinbar sind“ bekannt[20]. Er hat US-Vizepräsident J.D. Vance schon früh gefördert und war instrumentell in seinem Aufstieg zur Vizepräsidentschaft, auch sonst war Thiel zentral im Rechtsruck der USA[19]. Auch der Palantir-CEO Alexander Karp ist in der Vergangenheit immer wieder durch menschenrechts- und demokratiekritische Aussagen aufgefallen[5].

Dabei sind nicht nur die neo-faschistischen Tendenzen des Unternehmens problematisch. Der Einsatz von Palantir-Software untergräbt auch die staatliche Souveränität Deutschlands. So ist das Risiko einer langfristigen Abhängigkeit von dem Unternehmen mehr als real. Hinzu kommt, dass bei einer Prüfung der Software durch das Schweizer Militär herauskam, dass durchaus „die Möglichkeit besteht, dass sensible Daten durch die amerikanische Regierung und Geheimdienste eingesehen werden können"[17]. Weder der deutsche Staat noch die deutsche Polizei sollten jemals das Risiko eingehen, dass potentiell persönliche Daten der Bevölkerung an Unternehmen, sowie andere Staaten und deren Geheimdienste abfließen.

Für die GRÜNE JUGEND Brandenburg folgt daraus:

- Wir fordern die Rücknahme der Gesetzesentwürfe der Bundesregierung zur Stärkung digitaler Ermittlungsbefugnisse der Polizei
- Wir lehnen alle Formen von automatisierter Datenanalyse entschieden ab
- Wir lehnen den Einsatz von sämtlichen Softwarelösungen des Konzerns Palantir ab
- Wir werden uns gemeinsam mit anderen zivilgesellschaftlichen Bündnispartner*innen gegen die Einführung von Softwares zur automatisierten Datenanalyse in Brandenburg einsetzen
- Wir werden uns in Zusammenarbeit mit anderen Landesverbänden, dem Bundesvorstand und der breiten Zivilgesellschaft der Einführung von Softwares zur automatisierten Datenanalyse im Bund entgegenstellen

Quellen

1. Kühne, M. & Kanakakis, A. Patchwork Policing. Verfassungsblog https://doi.org/10.59704/c877215905499466 (2025) doi:10.59704/c877215905499466.

2. Verfassungsbeschwerde gegen Regeln für Polizei-Software. BR24 https://www.br.de/nachrichten/bayern/verfassungsbeschwerde-gegen-regeln-fuer-polizei-software,UrlUmVi (2025).

3. Leisegang, D. & Köver, C. Rechtlich fragwürdig: Bundesregierung will biometrische Fotofahndung im Netz. netzpolitik.orghttps://netzpolitik.org/2026/rechtlich-fragwuerdig-bundesregierung-will-biometrische-fotofahndung-im-netz/ (2026).

4. SPD Brandenburg & CDU Brandenburg. Koalitionsvertrag 2026 – 2029 Zwischen SPD Und CDU in Brandenburg: Verantwortung Für Brandenburg. (2026).

5. Constanze. Verfassungsbeschwerde: Das Problem heißt nicht nur Palantir. netzpolitik.orghttps://netzpolitik.org/2025/verfassungsbeschwerde-das-problem-heisst-nicht-nur-palantir/ (2025).

6. Edelhoff, L. J., Blum, P. & Flade, F. Wird die umstrittene Palantir-Software in Deutschland unangemessen genutzt? tagesschau.de https://www.tagesschau.de/investigativ/ndr-wdr/palantir-einsatz-deutschland-100.html (2025).

7. dpa. Palantir hat Zugriff auf Millionen Daten: Verfassungsbeschwerde gegen Regeln für Polizei-Software eingereicht. Der Tagesspiegel Online https://www.tagesspiegel.de/politik/digitalisierung-ki/palantir-hat-zugriff-auf-millionen-daten-verfassungsbeschwerde-gegen-regeln-fur-polizei-software-eingereicht-14071667.html (2025).

8. bpb. Das Recht auf informationelle Selbstbestimmung | Persönlichkeitsrechte. bpb.de https://www.bpb.de/themen/rechtjustiz/persoenlichkeitsrechte/244837/das-recht-auf-informationelle-selbstbestimmung/ (2017).

9. GRCh. Charta der Grundrechte der Europäischen Union.

10. Digitale Gesellschaft et al.Gemeinsame Stellungnahme Im Rahmen Der Verbändebeteiligung Zu Den Gesetzentwürfen Zur Stärkung Digitaler Ermittlungsbefugnisse in Der Polizeiarbeit Sowie Zum Gesetzentwurf Zur Stärkung Digitaler Ermittlungsbefugnisse Zur Abwehr von Gefahren Des Internationalen Terrorismus. (Digitale Gesellschaft, 2026).

11. DSK. Entschließung Der Konferenz Der Unabhängigen Datenschutzaufsichtsbehörden Des Bundes Und Der Länder Vom 17. September 2025: Automatisierte Datenanalyse Durch Polizeibehörden Verfassungskonform Gestalten! (Datenschutzkonferenz, 2025).

12. Frankfurter Rundschau. Nicht nur in Hessen: Polizei in ganz Deutschland fragt unbefugt Daten ab. Frankfurter Rundschauhttps://www.fr.de/politik/hessen-deutschland-polizei-fragt-unbefugt-daten-ab-nsu-20-drohschreiben-frankfurt-13844413.html (2020).

13. dpa/mv. Datenabfrage - Strafen, aber keine Entlassung für Polizisten. Süddeutsche.dehttps://www.sueddeutsche.de/panorama/disziplinarstrafen-datenabfrage-strafen-aber-keine-entlassung-fuer-polizisten-dpa.urn-newsml-dpa-com-20090101-250627-930-725764 (2025).

14. Neuerer, D. Polizei-Software: Experten sehen in Palantir eine Gefahr für die Demokratie. https://www.handelsblatt.com/politik/deutschland/polizei-software-experten-sehen-in-palantir-eine-gefahr-fuer-die-demokratie/100207797.html (2026).

15. Baur, D. Bayerisches Polizeiaufgabengesetz: Urteil mit Zwischentönen. Die Tageszeitung: taz (2023).

16. Balbierer, T. ‘Letzte Generation’: Kritik an wiederholter Präventivhaft für Klima-Aktivist in Bayern. SZ.dehttps://www.sueddeutsche.de/bayern/bayern-letzte-generation-protest-klimakleber-praeventivhaft-1.5751359 (2023).

17. Fichter, A. et al. Wie hartnäckig Palantir die Schweiz umwarb. Republik https://www.republik.ch/2025/12/08/wie-hartnaeckig-palantir-die-schweiz-umwarb (2025).
18. Bhuiyan, J. Documents offer rare insight on Ice’s close relationship with Palantir. The Guardian (2025).

19. deutschlandfunk.de. Palantir in Deutschland - Datenschützer warnen vor Polizei-Software aus den USA. Deutschlandfunk https://www.deutschlandfunk.de/palantir-deutschland-polizei-software-datenschutz-100.html (2025).

20. Charim, I. Tech-Investor Peter Thiel: Der Auszug der Milliardäre aus der Verantwortung. Die Tageszeitung: taz (2024). Powered by TCPDF (www.tcpdf.org)