Dieser Text wurde zuerst am 07.04.2025 auf www.netzpolitik.org unter der URL ‹https://netzpolitik.org/2025/automatisierte-rasterfahndung-tuer-zu-fuer-palantir-und-co/› veröffentlicht. Lizenz: Constanze Kurz, Stefan Ullrich, Netzpolitik, CC BY-NC-SA 4.0

Palantir-Pavillon, Weltwirtschaftsforum, Davos, Schweiz, 17.1.2017. (Foto: Cory Doctorow, Flickr, CC BY-SA 2.0)

Automatisierte **Rasterfahndung:** Tür zu für Palantir und Co.

Die angehende Regierung befürwortet Polizeiarbeit mit automatisierten Black-Box-Systemen, um die riesigen Datenbestände der Polizeien zu rastern. Die Idee der Merzschen Union, die auch von den Sozialdemokraten unterstützt wird, mit Konzernen wie Palantir zusammenzuarbeiten, ist ethisch und rechtlich hochproblematisch.

Autoren: Constanze Kurz

Constanze Kurz ist promovierte Informatikerin, Autorin und Herausgeberin von Büchern, zuletzt Cyberwar. Ihre Kolumne „Aus dem Maschinenraum“ erschien von 2010 bis 2019 im Feuilleton der FAZ. Sie lebt in Berlin und ist ehrenamtlich Sprecherin des Chaos Computer Clubs. Sie war Sachverständige der Enquête-Kommission „Internet und digitale Gesellschaft“ des Bundestags. Sie erhielt den Toleranz-Preis für Zivilcourage und die Theodor-Heuss-Medaille.

Stefan Ullrich

Dr. Stefan Ullrich ist promovierter Informatiker und Philosoph, der sich kritisch mit den Auswirkungen der allgegenwärtigen informationstechnischen Systeme auf die Gesellschaft beschäftigt. Er ist Referent für Digitale Bildung in der KI-Ideenwerkstatt für Umweltschutz.

Als vor ein paar Tagen erste Papiere den Verhandlungsstand der Arbeitsgruppen [1] der angehenden Regierungskoalitionäre in der Innenpolitik aufzeigten, gab es wenige Überraschungen. Vieles erinnerte deutlich an die Lektüre der Wahlprogramme. Derzeit brütet eine 19-köpfige Verhandlungsgruppe aus CDU, CSU und SPD über den Ergebnissen der Arbeitsgruppen.

Ein Ergebnis war das Ziel, in Zukunft massenhaft vorhandene Polizeidaten zusammenzuführen und automatisiert auszuwerten: „Für bestimmte Zwecke sollen unsere Sicherheitsbehörden, unter Berücksichtigung verfassungsrechtlicher Vorgaben und digitaler Souveränität, die automatisierte Datenrecherche und -analyse […] vornehmen können.“ Bisher ist das nur in drei Bundesländern gängige Praxis und wird derzeit mit mehreren Verfassungsbeschwerden bekämpft [2].

Die Merzsche Union setzt sich schon länger offensiv für ein Produkt des Konzerns Palantir ein [3]. Das börsennotierte militärnahe US-Tech-Unternehmen bietet eine proprietäre Software namens „Gotham“ an, die auf Beamtendeutsch „Bundes-VeRA“ heißt. Schon im Wahlprogramm hatte die Union versprochen, dass die Bundespolizei und das Bundeskriminalamt alsbald mit diesem Produkt ertüchtigt werden sollen.

Das Verhandlungspapier spricht nun von „Sicherheitsbehörden“, was eine Erweiterung zum bisher Geforderten darstellt. Denn neben Polizeien könnte das auch Geheimdienste umfassen [4], die im quasi rechtsfreien Raum schon mindes-

tens seit 2014 mit solchen Werkzeugen arbeiten.

Die Sozialdemokraten schrieben in ihr Wahlprogramm den Wunsch, der Bundespolizei „automatisierte (KI-basierte) Datenanalysen“ zu erlauben [5]. Innenministerin und Sozialdemokratin Nancy Faeser hatte sich allerdings in ihrer Ampel-Amtszeit gegen die Nutzung von Palantir in Bundesbehörden ausgesprochen.

Etwas wahrhaft Magisches

Offenbar nehmen die Demnächst-Koalitionäre an, dass solche Software-Produkte für die Polizei einen hohen Nutzen haben. Das ist zwar bisher nicht wissenschaftlich belegt, aber das Marketing von Anbietern wie Palantir bei den Verantwortlichen in Politik und Polizei blieb wohl nicht ohne Wirkung. Früher beschrieb man es mit dem jetzt als unmodern geltenden Begriff „Data Mining“. Heute soll eine nicht näher spezifizierte „KI“ die Informationen aus lauter heterogenen polizeilichen Datenbanken zusammenbringen und dann diejenigen Menschen auf Knopfdruck herausfischen, die potentiell eine Gefahr darstellen.

Der Moment, einen solchen Produkteinsatz kräftig auszubauen, ist günstig: Alles, was auch nur im Entferntesten nach Künstlicher Intelligenz aussieht, wird gerade mit Innovation und Effizienzsteigerung gleichgesetzt. Es ist eine Variante des alten Versprechens von Big Tech, ungeachtet von Datenschutz- und Antidiskriminierungsgesetzen wahrhaft Magisches mit Hilfe von Daten zu vollbringen.

Verbunddateien, Datenbanken, Auskunftssysteme

Die teilweise schon Jahrzehnte bestehenden Datenbanken der Polizeien haben im Laufe ihrer Dienstjahre eine Vielzahl an unterschiedlichsten Daten angehäuft. Es gibt Verbunddateien, die der Personen- und Sachfahndung dienen, mit Kriminalakten und Haftinformationen, dazu Biometriedaten wie Fingerabdrücke, Gesichtsbilder oder gar DNA-Profile. Es gibt aber auch Fallbearbeitungssysteme oder auch erkennungsdienstliche Datenbanken, ebenfalls mit biometrischen Informationen. Nicht zu vergessen die großen Antiterror- und Rechtsextremismusdateien, die seit vielen Jahren geführt werden. Dazu kommen noch Auskunfts- und Informationssysteme, die Fahndungen und Ermittlungen unterstützen sollen, außerdem riesige Vorgangsbearbeitungssysteme, die mit Daten aus dem polizeilichen Alltag wie Anzeigen oder Verkehrsunfällen befüllt sind.

Ein einziger Datenschatz, der gehoben werden muss, wenn es nach den Anbietern entsprechender Software wie Palantir und nach den Konservativen mit ihrem latenten Law-and-Order-Fetisch geht. Mit „KI“-Hilfe sollen neue Muster in großen Datensätzen gesucht werden: Informationsnuggets werden regelrecht „geschürft“. Dazu müssen vorliegende Daten automatisiert klassifiziert werden, auch hinsichtlich ihrer Verbindungen untereinander.

Ein unmittelbarer Nutzen für die Polizei scheint klar: Auch unbekannte Muster werden in bekannte Klassen überführt. Ein zweiter praktischer Nebeneffekt der Nutzung des nun in KI umgetauften Data Minings ist die Erkennung von „Ausreißern“. Das ist der Fachbegriff für Datenpunkte, die stark vom restlichen Vergleichsdatensatz abweichen. Je nach Einsatzzweck des IT-Systems können diese Ausreißer automatisch ignoriert werden, um beispielsweise schönere Info-Graphiken zu bekommen, oder aber – ganz im Gegenteil – genauer unter die Lupe genommen werden.

Ein in der Informatik lange bekanntes Problem von Data Mining ist die Sicherstellung des rechtskonformen Betriebs einer solchen Raster-Suchmaschine [6]. Denn auch wenn personenbezogene Daten in einem System nicht direkt vorhanden sind oder aufwendig anonymisiert wurden, kann ein entsprechendes Data-Mining-System solche privaten Daten ableiten – gewollt oder ungewollt.

Informatikfachleute, die solche Systeme entwerfen, herstellen, betreiben oder verwenden, müssen daher große Sorgfalt an den Tag legen, um Datenschutzrechte einhalten zu können. Diese Sorgfalt ist teuer und führt im Extremfall sogar dazu, dass ein solches System rechtlich oder ethisch abzulehnen ist [7]. Doch im Falle von Palantir steht alles auf dem Kopf: Aus den Polizeisystemen sollen ja gerade nicht direkt vorhandene Daten abgeleitet werden, um einen Personenbezug herzustellen. Entsprechend umfassend sind die ethischen Fragen, die im Raum stehen.

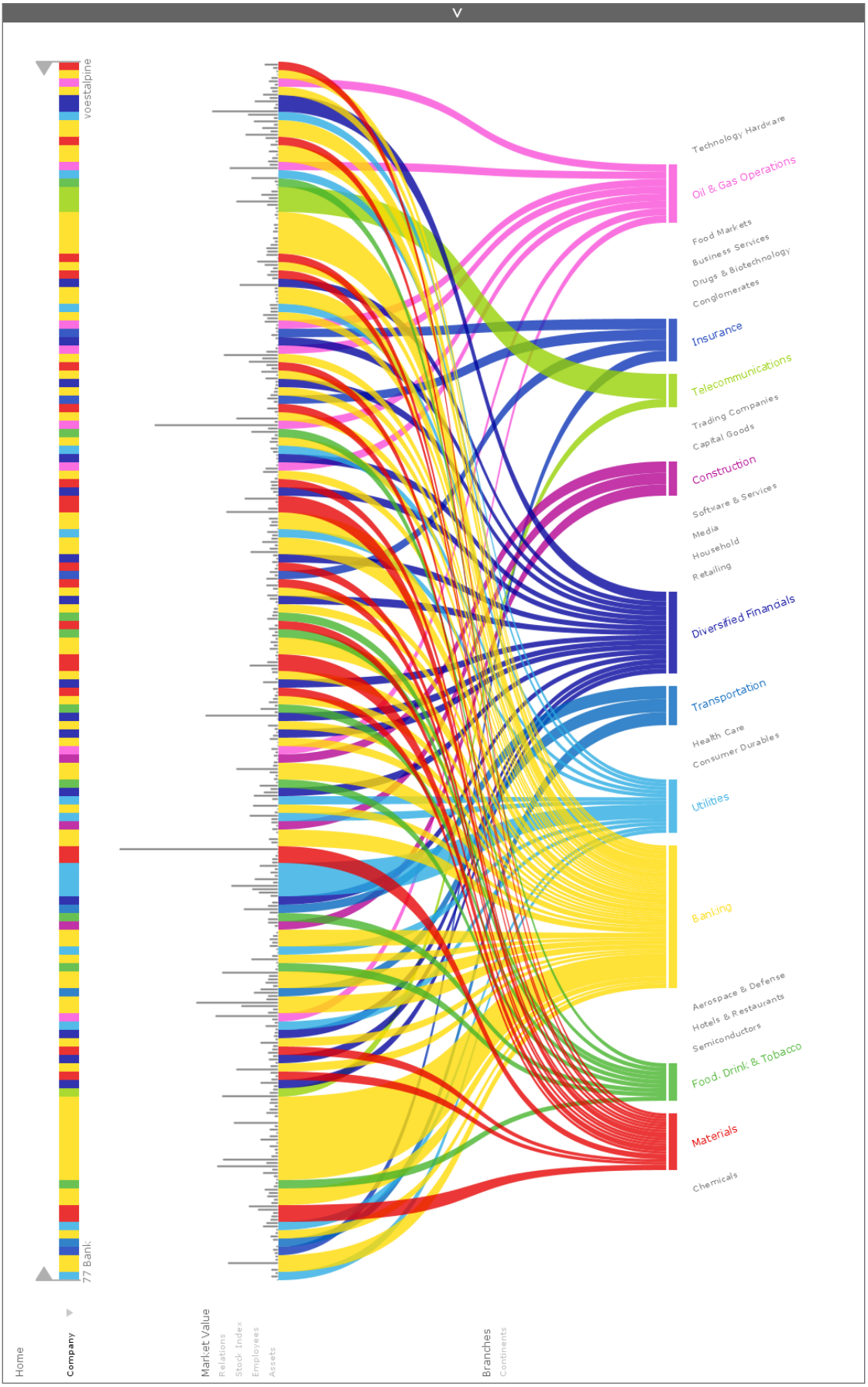
Der feisten Datenrallye stehen nicht nur ethische Bedenken, sondern auch ein Urteil des höchsten deutschen Gerichts im Weg [8]. Das Bundesverfassungsgericht beschäftigte sich mit zwei Landesgesetzen, die den Polizeien das Palantir-Produkt genehmigt hatten. Die betroffenen Paragraphen des hessischen Sicherheits- und Ordnungsgesetzes und des hamburgischen Gesetzes über die Datenverarbeitung der Polizei wurden 2023 als verfassungswidrig befunden. Das Gericht kritisierte die enorm hohe Streubreite und Intensität der Grundrechtseingriffe.

Profiling- und Diskriminierungsvorsorge

Seit den Zeiten von „Big Data“ suggeriert die These „Daten sind das neue Öl“, dass wir es mit einer ungenutzten sprudelnden Quelle zu tun hätten. Warum beschränken höchstrichterliche Urteile – vom Volkszählungsurteil bis zum jüngsten Palantir-Urteil [9] – die Polizei darin, diesen Datenschatz zu heben? Der Grund erschließt sich leicht an typischen Beispielen: In Polizeidatenbanken dürfen zum Beispiel auch Merkmale über Menschen gespeichert werden, die eine „Volkszugehörigkeit“ oder einen „Phänotyp“, die „äußere Erscheinung“ oder Religionszugehörigkeit, verwendete Sprachen, Dialekte oder Mundarten festhalten. Das sind ohne Zweifel höchst sensible Daten, auch mit hohem Diskriminierungspotential.

Denn Datenschutz bedeutet auch Diskriminierungsvorsorge und beschränkt die Profilbildung über Menschen. Die Europäische Datenschutzgrundverordnung und die begleitende Richtlinie zum Datenschutz für Justiz und Inneres [10] sind in dieser Hinsicht eigentlich klar formuliert:

Publiziert auf Free21 am 03.06.2025, 6:00 Uhr



KP "Visual Data Mining" 1
Prototyp in Java/ Processing für Universitätsprojekt Visual Data Mining. 2.000 Unternehmen aus Forbes 200029.118 Unternehmensbeziehungen. (Graphik: Stefan Wagner, TU Dresden, Flickr, CC BY-NC-SA 2.0)

> Profiling, das zur Folge hat, dass natürliche Personen auf Grundlage von besonderen Datenkategorien nach Artikel 10 [der Richtlinie] diskriminiert werden, ist nach dem Unionsrecht verboten."

Und das Profiling würde im konkreten Falle einer Palantir-Rasterfahndung nicht nur Beschuldigte betreffen, sondern auch eine Vielzahl anderer Personen. Das sind etwa Geschädigte oder Zeugen, sofern ihre Daten in den behördlichen Datenbanken gespeichert und verarbeitet werden.

Auch deswegen gilt der Grundsatz der Zweckbindung. Das bedeutet in einfachen Worten, dass Daten für einen bestimmten Zweck erhoben wurden und nicht einfach ins Blaue hinein umfunktioniert werden können. Also dürfen Personendaten aus Polizeidatenbanken nur dann für einen anderen Zweck verwendet werden, wenn dieser neue Zweck dem Schutz eines mindestens ebenso bedeutenden Rechtsguts dient wie der ursprüngliche Erhebungszweck.

Es bleibt aber eine Tür offen für Palantir und Co.: Denn für präventive Polizeiarbeit, die schwere Straftaten verhindern soll, ist diese Zweckbindung gelockert. Es ist allerdings verfassungsrechtlich umstritten, ob auch automatisierte Datenanalysen die Zweckbindung entkernen können. Immerhin gelten seit dem Palantir-Urteil vom Februar 2023 neue verfassungsrechtliche Anforderungen, die sowohl quantitative als auch qualitative Grenzen setzen, was die Art der Daten betrifft, die von der Software automatisiert ausgewertet werden dürfen. Es ist demnach nicht verfassungsgemäß, wenn die Polizei „mit einem Klick umfassende Profile von Personen, Gruppen und Milieus" erstellt.

Bestehende Datenschutzrechte werden ad absurdum geführt

Palantir arbeitet schon heute mit den Polizeien in Hessen, Hamburg und Nordrhein-Westfalen eng zusammen. In welchem Ausmaß und mit welchen Palantir-Softwarefunktionen und wie genau dabei auch höchst sensible Informationen über Menschen verarbeitet werden, ist öffentlich nicht einsehbar und strukturell geheim. Wie die namensgebenden Palantíri in Tokiens „Der Herr der Ringe" bleiben die Softwaresysteme des Konzerns in geheimen Räumen, nur konzerneigene Hüter haben echten Zugang. Der Konzern Palantir entzieht sich der öffentlichen Diskussion weitgehend und damit der Rechenschaft.

Diese Intransparenz der Polizeiarbeit mit Black-Box-Systemen macht Datenschutzverletzungen quasi über Bande unkenntlich und unkontrollierbar [11]. Es führt zugleich bestehende Datenschutzrechte ad absurdum, die jeder Mensch eigentlich hat: beispielsweise das Recht zu erfahren, welche Daten über einen selbst vorliegen oder deren Löschung oder Berichtigung zu verlangen. Diese Rechte angemessen zu wahren, wird kaum machbar sein. Informationen über Menschen liegen ja dann nicht mehr nur in herkömmlicher Form vor, etwa in einer Datenbank, sondern werden auch innerhalb des „KI"-Systems gespeichert und verarbeitet. Ob und wie Konzerne wie Palantir personenbezogene Informationen in ihren „KI"-Systemen korrigieren oder löschen können, ist eine offene Frage.

Im konkreten Fall von Palantir verbinden sich mit dem Konzern auch noch problematische Motive und nationalistische Ideologien, die von den beiden prominenten Männern der Chefetage des Konzerns offen vertreten werden: Peter Thiel und Alexander Karp. Ausgerechnet diesem Konzern mit seiner undurchsichtigen Überwachungssoftware massenhaft Polizeidaten anzuvertrauen, scheint eine wirklich schlechte Idee [12].

Es ist daher nicht länger die Frage, ob die Systeme von Palantir und Co. ethisch und rechtlich problematisch sind und gesellschaftsfeindlich und demokratiezerstörend eingesetzt werden könnten, sondern wie dies verhindert werden kann.

Quellen:

[1] Netzpolitik.org, Ingo Dachwitz „Koalitionsverhandlungen: Gruselprogramm für Grund- und Freiheitsrechte", am 25.3.2025: *<https://netzpolitik.org/2025/koalitionsverhandlungen-gruselprogramm-fuer-grund-und-freiheitsrechte/>*

[2] Netzpolitik.org, Tomas Rudl „Hessendata: Erneute Verfassungsbeschwerde gegen polizeiliche Big-Data-Analysen", am 25.6.2024: *<https://netzpolitik.org/2024/hessendata-erneute-verfassungsbeschwerde-gegen-polizeiliche-big-data-analysen/>*

[3] Netzpolitik.org, Constanze Kurz „Polizeiliche Datenanalyse: Innenausschuss diskutiert Palantir-Alternativen", am 22.4.2024: *<https://netzpolitik.org/2024/polizeiliche-datenanalyse-innenausschuss-diskutiert-palantir-alternativen/>*

[4] Netzpolitik.org, Gastbeitrag (Unbekannt) „Big Data bei den Geheimdiensten: Die Ampel muss automatisierte Analysen begrenzen", am 22.9.2024: *<https://netzpolitik.org/2024/big-data-bei-den-geheimdiensten-die-ampel-muss-automatisierte-analysen-begrenzen/>*

[5] Netzpolitik.org, Tomas Rudl „Bundestagswahl: Das steht über Daten und Digitales in den Wahlprogrammen", am 07.2.2025: *<https://netzpolitik.org/2025/bundestagswahl-das-steht-ueber-daten-und-digitales-in-den-wahlprogrammen/>*

[6] Gesellschaft für Informatik e.V., Henrik Grosskreutz, Benedikt Lemmen, Stefan Rüping „Data-Mining, Privacy-Preserving", am 8.7.2010: *<https://gi.de/informatiklexikon/data-mining-privacy-preserving>*

[7] Gesellschaft für Informatik e.V., „Ethischer Kompass für Informatik-Fachleute", Datum unbekannt: *<https://gi.de/fileadmin/GI/Allgemein/PDF/GI_Ethischer_Kompass.pdf>*

[8] Netzpolitik.org, Daniel Leisegang „Urteil des Bundesverfassungsgerichts: Automatisierte Datenanalyse für die vorbeugende Bekämpfung von Straftaten ist verfassungswidrig", am 16.2.2023: *<https://netzpolitik.org/2023/urteil-des-bundesverfassungsgerichts-automatisierte-datenanalyse-fuer-die-vorbeugende-bekaempfung-von-straftaten-ist-verfassungswidrig/>*

[9] ebd.

[10] Europäische Union „RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates", vom 27. April 2016: *<https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680>*

[11] Netzpolitik.org, Constanze Kurz „BKA-Gesetz: „Schon jetzt verfassungswidrig"", am 27.8.2024: *<https://netzpolitik.org/2024/bka-gesetz-schon-jetzt-verfassungswidrig/>*

[12] Netzpolitik.org, Markus Reuter „Palantir: Wer jetzt bei Peter Thiel Software kauft, hat wirklich nichts verstanden", am 24.3.2025: *<https://netzpolitik.org/2025/palantir-wer-jetzt-bei-peter-thiel-software-kauft-hat-wirklich-nichts-verstanden/>*