Wegducken vor den Fragen des digitalen Zeitalters

Die automatisierte Datenanalyse braucht menschenrechtliche Grenzen, weil menschliche Grenzen obsolet werden

Lena Rohrbach

31.08.2026 doi: 10.59704/bbb8810cdeeefb3d

Algorithmische Datenanalysen sollen beim Bundeskriminalamt (BKA) und bei der Bundespolizei Einzug halten. Mit Gesetzentwürfen zu neuen digitalen Ermittlungsbefugnissen will die Bundesregierung künftig auch den Polizeibehörden des Bundes ermöglichen, was mehrere Bundesländer bereits mit Software des Unternehmens Palantir umsetzen: die sogenannte automatisierte Datenanalyse. Doch die Gesetzentwürfe zeugen von Fahrlässigkeit im Umgang mit den Risiken algorithmischer Massendatenverarbeitung. Sie ducken sich vor den Herausforderungen unserer Zeit weg, indem sie zentrale Fragen des digitalen Zeitalters unbeantwortet lassen. Das hat gravierende Folgen für den Schutz unserer Grundrechte.

Automatisierte Datenanalyse

Als automatisierte Datenanalyse lassen sich Verfahren beschreiben, die sich in ihren grundrechtlichen Auswirkungen erheblich unterscheiden. Am grundrechtsfreundlichen Ende des Spektrums könnte eine technische Suche stehen, die eine verdachtsgeleitete menschliche Ermittlung unterstützt und dafür eine begrenzte Menge sinnvoll ausgewählter Daten innerhalb eines nachvollziehbaren Systems auswertet. Am anderen Ende des Spektrums finden wir, was die vorliegenden Gesetzentwürfe ermöglichen: „*Data Mining*“ in einer gigantischen Menge von Daten der Bevölkerung (auch völlig unbeteiligter Personen) mit komplexen, möglicherweise nicht mehr nachvollziehbaren KI-Systemen – auch solchen von privaten Unternehmen aus dem EU-Ausland, wie Palantir.

Seit über einem Jahrzehnt recherchiert Amnesty International zum Einsatz algorithmischer Systeme durch Behörden. Wir unterhalten uns dafür mit Menschen wie Batya Brown, einer jungen Mutter aus den Niederlanden. Sie berichtete von ihren Erfahrungen mit einer automatisierten Datenanalyse, die Hinweise auf Kindergeldbetrug entdecken sollte: „Es war so seltsam. Ich bekam einen Brief, in dem stand, dass ich zu Unrecht Kindergeld erhalten hatte.” Die Forderung der Behörde, das Geld zurückzuzahlen, war ein Schock. „Ich war Anfang 20. Ich habe zusätzlich zu meinem Job angefangen, als Putzfrau zu arbeiten. Ich sah einfach, wie mir alles entglitt.“[1]

Batya Brown war kein Einzelfall. Die niederländische Steuerbehörde verlangte von mehr als 20.000 Familien zu Unrecht hohe Summen an Kindergeld zurück, nachdem sie einen fehlerbehafteten und diskriminierenden Algorithmus eingesetzt hatte. Die niederländische Regierung trat Anfang 2021 in Reaktion auf den Skandal zurück. Auch in Frankreich[2], Serbien[3], UK[4] und zahlreichen weiteren Ländern diskriminierten automatisierte Systeme in Behörden systematisch marginalisierte Gruppen.

Das Urteil des Bundesverfassungsgerichts vom 16.02.2023[5] zur automatisierten Datenanalyse zeigt Möglichkeiten auf, Menschenrechtsverletzungen vorzubeugen und die Schwere von Grundrechtseingrif-

[1] Amnesty International, *EU: AI Act must ban dangerous, AI-powered technologies in historic law*, 28.09.2023, https://www.amnesty.org/en/latest/news/2023/09/eu-ai-act-must-ban-dangerous-ai-powered-technologies-in-historic-law/, zuletzt abgerufen am 14.07.2026.

[2] Amnesty International, *France: Discriminatory algorithm used by the social security agency must be stopped*, 16.10.2024, https://www.amnesty.org/en/latest/news/2024/10/france-discriminatory-algorithm-used-by-the-social-security-agency-must-be-stopped/, zuletzt abgerufen am 14.07.2026.

[3] Amnesty International, *Serbia: Trapped by Automation: Poverty and Discrimination in Serbia's Welfare State*, Index Number EUR 70/7443/2023, 04.12.2023, S. 8f., https://www.amnesty.org/en/documents/eur70/7443/2023/en/, zuletzt abgerufen am 14.07.2026.

fen zu mildern: durch Begrenzung von Art und Umfang der analysierten Daten, der Analysemethoden und -systeme und durch Schutzmaßnahmen gegen Diskriminierung. Diese Maßnahmen finden sich im Gesetzespaket nicht oder nur unzureichend wieder.

Unzureichender Schutz vor Diskriminierung

Automatisierte Datenanalysen greifen nicht nur in die informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein. Sie berühren auch die Gleichheitsgarantien des Grundgesetzes, insbesondere Art. 3 Abs. 3 GG. Die oftmals diskriminierenden Effekte von KI sind zahlreich empirisch belegt. Auch im Falle Batya Browns waren insbesondere Familien mit Migrationshintergrund betroffen.

Das BVerfG stellt fest, dass „mit einer weitergehenden Automatisierung von Polizeiarbeit (…) spezifische Diskriminierungsrisiken einhergehen, die verfassungsrechtlich umso weniger hinzunehmen sind, je mehr sich die Wirkungen der automatisierten Datenanalyse oder -auswertung einer nach Art. 3 Abs. 3 GG unzulässigen Benachteiligung annähern könnten“.[6]

Konkrete Vorgaben zum Schutz vor Diskriminierung bieten die Gesetzentwürfe allerdings nicht. Sie beschränken sich auf die Formulierung, „dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden dürfen“, die so auch in Landespolizeigesetzen zu finden ist (§§ 9b Abs. 5 S. 1, 22 Abs. 3 S. 4, 39 Abs. 5 S. 1, 63c Abs. 5 S. 1 BKAG-E[7], §§ 46 Abs. 3 S.4, 58b Abs. 5 S.1 BPolG-E, § 98e Abs. 4 S. 4 StPO-E[8]). Als Anleitung an die Praxis ist diese abstrakte Vorgabe ungenügend. Wie Diskriminierung durch KI verhindert werden kann, ist eine der entscheidenden Fragen des digitalen Zeitalters, der sich die Gesetzgebung stellen muss.

In den Begründungen stützt sich das Gesetzespaket stark auf die Schultern der europäischen KI-Verordnung,[9] die einige Maßnahmen zur Minderung von diskriminierenden Effekten in Hochrisiko-KI-Systemen vorschreibt. Doch diese Vorgaben stehen mit dem EU-Verfahren zum „Digitalen Omnibus“[10] wieder auf dem Prüfstand, mindestens ist ihr Inkrafttreten bereits auf Dezember 2027 verschoben worden. Die Befugnisse zur automatisierten Datenanalyse würden daher in Kraft treten, ohne dass der eingepreiste unionsrechtliche Schutzrahmen greift. Ohne effektiven Diskriminierungsschutz in den Gesetzen selbst entsteht so ein unvertretbares Risiko für diskriminierungsbetroffene Menschen.

Allheilmittel menschliche Kontrolle?

Ein gängiger Einwand gegen Bedenken, KI-Massendatenanalyse könne zu Diskriminierung oder Falschverdächtigungen führen, lautet: Die Ergebnisse des Systems würden von Menschen überprüft. Eine rein automatisierte Entscheidungsfindung sei ausgeschlossen – so steht es auch in den Gesetzesbegründungen.[11] Doch hier ist Vorsicht geboten.

Erstens ist dies nicht ganz richtig: Im Regelungstext sind rein automatisierte Entscheidungen nur dann ausgeschlossen, wenn sie „unmittelbar eine nachteilige Rechtsfolge für die betroffene Person“ haben oder diese „erheblich beeinträchtigt“ wird (§§ 9b Abs. 5 S. 3, 39b Abs. 5 S. 3, 63c Abs. 5 S. 3 BKAG-E, 58b Abs. 5 S.3 BPolG-E, 98e Abs. 4 S. 4 StPO-E). Automatisierte Entscheidungen mit nur mittelbar oder noch nicht erheblich negativen Folgen werden also nicht ausgeschlossen. Unklar bleibt, welche Möglichkeiten sich die Bundesregierung hier offenhalten möchte.

Zweitens wird die kritische Kraft einer menschlichen Überprüfung als Allheilmittel in Automatisierungsprozessen regelmäßig überschätzt. Auch im Falle Batya Browns hatte das System die Bescheide nicht automatisiert verschickt; Menschen haben dem Algorithmus vertraut. Zahlreiche Studien belegen den *„Automation Bias“*, die Neigung, automatisierten Systemen eine besondere Vertrauenswürdigkeit zuzuschreiben. Wie Mary Cummings nachweist, nimmt der *Automation Bias* unter Zeitdruck zu, da dieser die kritische Überprüfung automatisierter Empfehlungen erschwert

[4] Amnesty International UK, *Automated Racism: How Police Data and Algorithms Code Discrimination into Policing*, AI Index Number EUR 45/8992/2025, Februar 2025, S. 7- 11, https://media.amnesty.org.uk/documents/Automated20Racism20Report20-20Amnesty20International20UK20-202025.pdf, zuletzt abgerufen am 14.07.2026.
[5] BVerfG, 1 BvR 1547/19, 1 BvR 2634/20, 16.02.2023.
[6] S. BVerfG Fn. 5, Rn. 77.

und Nutzer*innen dazu verleitet, Vorschläge ungeprüft als korrekt anzunehmen.[12] Die Fähigkeit der Nutzer*innen, widersprüchliche Informationen als solche wahrzunehmen, nimmt ab, Fehlentscheidungen nehmen zu. Dabei wird die Notwendigkeit der automatisierten Datenanalyse häufig gerade mit zeitkritischen Ermittlungssituationen begründet.

Auch vermehrtes Wissen über KI, etwa aus Schulungen, führt jedenfalls nicht linear zu weniger Gutgläubigkeit. Im Gegenteil: Auch im Umgang mit KI ist der *„Dunning-Kruger-Effekt“* belegt, so dass Menschen mit wachsenden KI-Kenntnissen dieser sogar stärker vertrauen als Laien und Fehler noch seltener bemerken.[13] Erst tatsächliche Fachexpertise reduziert *Automation Bias* wieder, lässt ihn aber nicht verschwinden. Die in den Gesetzesentwürfen vorgesehene Schulung der Beamt*innen (§§ 9b Abs. 6 S. 1, § 39b Abs. 6 S. 1, 63c Abs. 6 S. 1 BKAG-E, 58b Abs. 6 S.1 BPolG-E) genügt daher noch nicht. Drei Voraussetzungen könnten einen gewissen Schutz bieten: detaillierte Anleitungen für Überprüfungen, ein auf menschliche Nachvollziehbarkeit ausgelegtes System und ein begrenzter Datensatz, dessen Analyse der Mensch noch überblicken kann. Derartige Vorgaben lassen die Gesetzentwürfe vermissen.

Hauptsache automatisiert?

Einen schlanken Fuß macht sich die Bundesregierung auch bei einer weiteren zentralen Frage: Wie müssen algorithmische Systeme beschaffen sein, um den Anforderungen an grundrechtskonforme Verfahrensgestaltung (Art. 1 Abs. 3 GG) und effektiven Rechtsschutz (Art. 19 Abs. 4 GG) zu genügen? Wann ist eine KI etwa zu komplex, um den Anforderungen zu genügen, die sich hieraus an ihre Nachvollziehbarkeit ergeben? Auch darauf gibt das Gesetzespaket keine Antworten. Ob einfache Entscheidungsbäume oder komplexe neuronale Netze, ob nachvollziehbare Systeme oder „Blackboxes“ genutzt werden – diese Entscheidung überlässt die Bundesregierung den Behörden. Sie schließt nicht einmal aus, dass Sicherheitsbehörden selbstlernende KI-Systeme, die sich im laufenden Einsatz selbständig verändern, nutzen. Damit gehen unvertretbare Risiken für Menschen und ihre Rechte auf Nicht-Diskriminierung und effektiven Rechtsschutz einher. Auch Audits und Datenschutzprüfungen der eingesetzten Systeme würden obsolet, wenn das Untersuchungsobjekt ein „moving target“ darstellt und schon morgen ganz anders arbeiten kann.

Mit dem Algorithmus auf den Heuboden

Für die Analyse dürfen sämtliche Daten, auf die Bundespolizei und BKA zur Erfüllung ihrer Aufgaben zugreifen können, in einer „Superdatenbank“[14] zusammengeführt und durch KI analysiert werden. Dazu gehören etwa sämtliche im polizeilichen Informationsverbund vorliegenden Fall- und Vorgangsdaten, Daten aus Asservaten (etwa beschlagnahmte Smartphones und Computer), Telekommunikationsdaten oder Informationen von anderen Behörden (etwa Geheimdiensten oder anderen Staaten). Zusätzlich können automatisiert abgerufene Informationen aus staatlichen Registern und Daten aus dem Internet eingespeist werden. Letztere können die Sicherheitsbehörden zwar nur für den Einzelfall hinzufügen, sie sind im Umfang jedoch nicht beschränkt, so dass etwa Aktivitäten in sozialen Medien auch zeitlich weit zurückreichend und in großen Mengen durch KI analysiert werden dürfen.

Die automatisierte Datenanalyse ermöglicht der Polizei, Datenmengen auszuwerten, die mit konventioneller Ermittlungsarbeit faktisch nicht beherrschbar

[7] Regierungserklärung zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, Kabinettsfassung vom 20.04.2026, S. 30ff., https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/OESI3/regE-ermittlungsbefugnisse-polizeiarbeit.pdf?__blob=publicationFile&v=5, zuletzt abgerufen am 31.08.2026.

[8] Regierungserklärung zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, Kabinettsfassung vom 20.04.2026, S. 11 f. 22, https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RegE/RegE_Digitale_Ermittlungsbefugnisse.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 31.08.2026.

[9] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.

[10] Rat der Europäischen Union, *Artificial Intelligence: Council gives final green light to simplify and streamline rules*, 29.06.2026, https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/, zuletzt abgerufen am 14.07.2026.

wären. Die Frage nach dem richtigen Umgang mit der Versuchung, deshalb einfach stets überall „reinzuschauen“, ist eine weitere der zentralen Fragen des digitalen Zeitalters. Im Gegensatz zu menschlicher Aufmerksamkeit und Arbeitszeit sind Rechenkapazitäten praktisch unbegrenzt, weshalb Beamt*innen auf der Suche nach der sprichwörtlichen Nadel im Heuhaufen ohne Probleme den gesamten Heuboden einbeziehen können. Dies gilt umso mehr, als die Gesetzentwürfe keinen Gerichtsvorbehalt vorsehen (was zu korrigieren wäre). Dabei können von der Analyse zahlreich auch Menschen betroffen sein, die dazu keinen Anlass gegeben haben: Zeug*innen, Betroffene, die eine Anzeige erstattet haben oder zufälliger „Beifang“, etwa aus Überwachungsmaßnahmen, Asservaten oder dem Internet. Das läutet einen Paradigmenwechsel im polizeilichen Handeln ein: vom verdachtsgeleiteten Vorgehen zum *„Data Mining“*. Dabei sucht der Algorithmus in gigantischen zusammengeführten Datenmassen nach Auffälligkeiten, auch wenn es keinen Anlass gibt, diese in einem bestimmten Datenbestand zu vermuten. So lassen sich tiefgreifende Persönlichkeitsprofile und Einsichten gewinnen, die weit über die ursprünglichen Erhebungszwecke der analysierten Daten und auch über das Ziel der eigentlichen Anfrage an das Analysesystem hinausgehen. Aus den mangelnden Einschränkungen in Art und Umfang der Daten sowie der Analysesysteme und -methoden ergibt sich ein unverhältnismäßiger Eingriff in die Rechte auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und den Schutz personenbezogener Daten (Art. 8 GRCh).

Das KI-betriebene *„Data Mining“* verletzt nicht nur das Übermaßverbot. Es kann auch zu *„Chilling Effects“* führen, abschreckenden Auswirkungen auf die Grundrechtsausübung. Menschen können nicht mehr überblicken, welche Verhaltensweisen im Alltag eine Datenspur hinterlassen könnten, die einen verdachtserzeugenden Treffer im System auslöst – etwa auf ein Social-Media-Posting zu antworten, eine Anzeige zu erstatten, Kontakt zu bestimmten Personen aufzunehmen oder eine Versammlung zu besuchen. Denn ein Treffer kann auch aufgrund unvorhersehbarer Korrelationen mit anderen Daten ausgelöst werden. Und gerade in Zeiten, in denen autoritäre Kräfte nach Regierungsmacht streben und Menschen in den USA auf Basis von Palantir-Analysen deportiert werden[15], weckt eine KI-Massenüberwachung gerechtfertigte Sorgen.

Die Gesetzgebung muss sich auch im digitalen Zeitalter am verdachtsorientierten und dadurch grundrechtsschonenderen Vorgehen menschlicher Polizeiarbeit orientieren. Zunächst müsste der zu durchsuchende Datenbestand eingegrenzt werden. Dabei könnten etwa Daten aus besonders eingriffsintensiven Maßnahmen oder von besonders geschützter Natur (wie biometrische Daten) ausgeklammert werden. Dies schlägt auch das BVerfG vor.[16]

Außerdem sollte eine im Entwurf zur Änderung der Strafprozessordnung angelegte Vorgabe geschärft, zum Regelfall erhoben und auch im BKA- und Bundespolizeigesetz verankert werden: Nach § 98e Abs. 2 StPO-E müssen wenigstens Daten aus besonders eingriffsintensiven Maßnahmen explizit ausgewählt werden, um in die Analyse einzufließen. Das soll

[11] S. Fn. 7, S. 30, 34 f.; Regierungserklärung zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus, Kabinettsfassung vom 20.04.2026, S. 18, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/OESI3/regE-ermittlungsbefugnisse-abwehr-terrorismus.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 31.08.2026; s. Fn. 8, S. 21 f.

[12] Mary Cummings, *Automation Bias in Intelligent Time Critical Decision Support Systems*, AIAA 1st Intelligent Systems Technical Conference, 2004, DOI: 10.2514/6.2004-6313, zuletzt abgerufen 14.07.2026.

[13] Michael C Horowitz, Lauren Kahn, *Bending the Automation Bias Curve: A Study of Human and AI-Based Decision Making in National Security Contexts*, International Studies Quarterly, Volume 68, Issue 2, 2024, DOI: 10.1093/isq/sqae020, zuletzt abgerufen 14.07.2026.

[14] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, 11.09.2024, S. 7, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Terrorismusbek%C3%A4mpfung-Gesetz.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 09.07.2026.

[15] Amnesty International Deutschland, *USA: Behörden setzen Software von Palantir und Babel Street gegen Demonstrierende und Migrant*innen* ein, 21.08.2025, https://www.amnesty.de/pressemitteilung/usa-ueberwachungssoftware-palantir-babel-street-gegen-demonstrierende-migrant-innen, zuletzt abgerufen am 14.07.2026.

[16] S. BVerfG Fn. 5, Rn. 87.

zudem nur „soweit dies erforderlich ist" zulässig sein. (Was impliziert, dass die sonstigen umfangreichen Datenbestände offenbar auch dann in die Analyse einbezogen werden, wenn dies nicht erforderlich ist und keine Anhaltspunkte dafür vorliegen, dass die einzubeziehenden Daten in Verbindung zum konkreten Suchanlass stehen könnten.) Um das *Massen-Data-Mining* auf dem Heuboden zu vermeiden, sollten Datenbestände grundsätzlich nur dann einbezogen werden dürfen, wenn es den – auch schriftlich begründeten – Verdacht gibt, dass dort etwas zu finden ist.

Leerstelle mit Programm?

Das digitale Zeitalter erfordert menschenrechtliche Grenzen, weil menschliche Grenzen an Bedeutung verlieren. Wie kann algorithmische Diskriminierung wie bei Batya Brown verhindert werden? Welche neuen Grenzen braucht es, wenn menschliche Aufmerksamkeit und Arbeitszeit als „natürliche Begrenzung" wegfallen und unbegrenzte Datenmengen analysierbar werden? Welche Systeme genügen rechtsstaatlichen Anforderungen und welche nicht? Die Bundesregierung steht in der dringenden Verantwortung, Antworten auf diese zentralen Fragen zu geben. Doch diese sucht man im Gesetzespaket vergeblich. Angesichts der erdrückenden Evidenz, die den Handlungsbedarf zum Schutz der Grundrechte aufzeigt, scheint diese Leerstelle Programm zu sein.

AUTOR*IN

Lena Rohrbach
Lena Rohrbach ist Referentin für Menschenrechte im digitalen Zeitalter und Rüstungsexportkontrolle bei Amnesty International.

EMPFOHLENE ZITATION

Rohrbach, Lena: Wegducken vor den Fragen des digitalen Zeitalters: Die automatisierte Datenanalyse braucht menschenrechtliche Grenzen, weil menschliche Grenzen obsolet werden, Verfassungsblog, 31.08.2026, doi: 10.59704/bbb8810cdeeefb3d.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260831-145424-0.