POLICY-BRIEF

Algorithmische Aufklärung: Warum Nachrichtendienste rechtliche Leitplanken für automatisierte Datenanalysen brauchen

Corbinian Ruckerbauer, Lilly Goll

September 04, 2024

Stiftung Neue Verantwortung is now interface

Since 2014, our team has worked on building an independent think tank and publishing well-researched analysis for everyone who wants to understand or shape technology policy in Germany. If we have learned something over the last ten years, it is that the challenges posed by technology cannot be tackled by any country alone, especially when it comes to Europe. This is why our experts have not only focused on Germany during the past years, but also started working across Europe to provide expertise and policy ideas on AI, platform regulation, cyber security, government surveillance or semiconductor strategies.

For 2024 and beyond, we have set ourselves ambitious goals. We will further expand our research beyond Germany and develop SNV into a fully-fledged European Think Tank. We will also be tapping into new research areas and offering policy insights to a wider audience in Europe, recruiting new talent as well as building expert communities and networks in the process. Still, one of the most visible steps for this year is our new name that can be more easily pronounced by our growing international community.

Rest assured, our experts will still continue to engage with Germany's policy debates in a profound manner. Most importantly, we will remain independent, critical and focused on producing cutting-edge policy research and proposals in the public interest. With this new strategy, we just want to build a bigger house for a wider community.

Please reach out to us with questions and ideas at this stage.

Table of Contents

Zusammenfassung

Nachrichtendienste stehen weltweit vor dem Problem, dass sie immer größere Datenmengen bewältigen müssen, die sie mit unterschiedlichen Methoden erheben. Deshalb greifen die Dienste – auch in Deutschland – auf Systeme zur automatisierten Datenanalyse zurück. Das Versprechen, das damit verbunden ist: Ihre Arbeit wird effektiver, zuvor verborgene Informationen werden sichtbar. Bisher waren es vor allem endliche Personalressourcen, die der Auswertung großer Datenmengen Grenzen gesetzt haben. Heute sollen automatisierte Datenanalysetools helfen, genau diese Grenzen zu überwinden. Doch der Einsatz solcher Werkzeuge hat seinen Preis. Grundrechte wie das Recht auf informationelle Selbstbestimmung oder das Fernmeldegeheimnis geraten unter Druck. Denn wo große Mengen Daten softwaregestützt analysiert werden, können sensible Informationen über die betroffenen Personen zu Tage gefördert werden. Auch aus solchen Daten, die zunächst harmlos wirken. Die Verwendung von Werkzeugen zur Auswertung solch großer Datenmengen verändert die Arbeit der Nachrichtendienste grundlegend; sie ermöglicht es ihnen, bisherige Erkenntnisgrenzen – etwa begrenzte Ressourcen oder eingeschränkte Informationszugänge – zu überwinden.

Schon seit mindestens zehn Jahren bauen deutsche Nachrichtendienste ihre Fähigkeiten zur automatisierten Datenanalyse aus.[1] Deutsche Datenschutzbehörden sehen das kritisch und mahnen, der rechtliche Rahmen werde der Einsatzpraxis nicht mehr gerecht.[2] Mithilfe komplexer Algorithmen sollen automatisiert Daten strukturiert und verknüpft, Verhaltensmuster analysiert, Beziehungs- und Kommunikationsnetzwerke erstellt und Auffälligkeiten identifiziert werden. Von einer solchen Verarbeitung betroffen sein können auch Menschen, deren Verhalten dafür keinen Anlass gegeben hat. Verschiedene Faktoren verschärfen die Eingriffe: die möglichen Einblicke in persönlichkeitsrelevante Bereiche sind besonders tief, die Eingriffe haben eine große Streubreite – betreffen also potenziell sehr viele Menschen auf einmal –, wodurch wiederum Einschüchterungseffekte entstehen können, wenn sich Menschen zunehmend überwacht fühlen. Dazu kommt, dass automatisierte Methoden anfällig für diskriminierende Verzerrungen, Manipulationen und andere Fehler sind. Betroffene können sich kaum dagegen zur Wehr setzen – nicht zuletzt deshalb, weil sie häufig gar nicht wissen, in welcher Weise Nachrichtendienste ihre persönlichen Daten auswerten.

1 Bundesamt für Verfassungsschutz (2015). Konzept zur Einrichtung einer Referatsgruppe 3C „Erweiterte Fachunterstützung Internet" im BfV (veröffentlicht von netzpolitik.org).

2 Datenschutzkonferenz (2023). Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten!

Die Arbeit der Nachrichtendienste und die Auswirkungen auf Grundrechte verändern sich. Doch der rechtliche Rahmen hinkt hinterher. Diese Diskrepanz ist ein ernstzunehmendes Problem für Demokratie und Rechtsstaat. Der Gesetzgeber sollte deshalb nun handeln und dieses Problem im Zuge der anstehenden Reform des Nachrichtendienstrechts angehen.[3] Für den Einsatz im polizeilichen Bereich hat das Bundesverfassungsgericht besprochen, wie solche Beschränkungen aussehen könnten.[4] Auf die Nachrichtendienste kann das Urteil zwar nicht unmittelbar übertragen werden, es bietet aber einen relevanten Orientierungsrahmen für grundrechtliche Abwägungen zur Nutzung ähnlicher Software durch die Nachrichtendienste. Es scheint immer klarer, dass die Einsatzpraxis auch im Bereich der Nachrichtendienste angesichts des fehlenden Rechtsrahmens nicht mit dem Grundgesetz vereinbar ist. Denn durch den Einsatz dieser Methoden wird der Überwachungsdruck drastisch erhöht – und zwar ohne, dass entsprechende Sicherungsmechanismen geschaffen werden, die missbräuchlichen Eingriffen in Grundrechte entgegenwirken.

Deshalb empfehlen wir dem Gesetzgeber im Zuge der von der Ampelkoalition angestrebten Neufassung des Nachrichtendienstrechts folgende Maßnahmen: Der Gesetzgeber sollte

- eine klare und verfassungskonforme Rechtsgrundlage für die bereits angewandten Methoden automatisierter Datenverarbeitung schaffen,
- eine Regelungssystematik für Grundrechtseingriffe durch automatisierte Datenverarbeitungsmethoden ausarbeiten, um in der Praxis zwischen unterschiedlich schwerwiegenden Einsätzen dieser Methoden unterscheiden zu können,
- und ausgehend von dieser Regelungssystematik wesentliche Beschränkungen für die unterschiedlichen Szenarien einführen, um die Verhältnismäßigkeit der Grundrechtseingriffe sicherzustellen,
- und die unabhängige Kontrolle der verwendeten Methoden stärken, beispielsweise indem er der BfDI bindende Anordnungsbefugnisse im Bereich der Nachrichtendienste zugesteht.

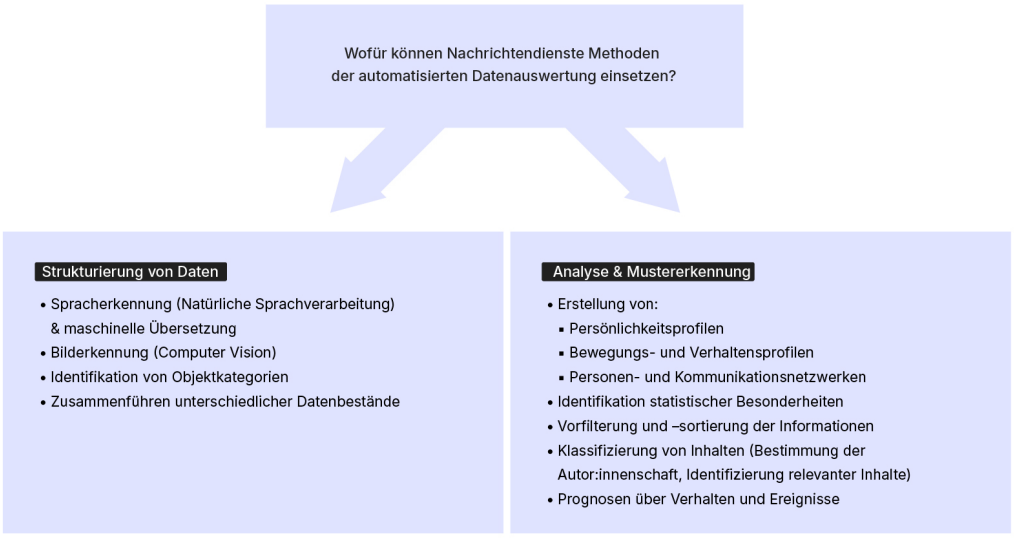
---

3 Die Ampelkoalition hat sich umfassende Anpassungen des Nachrichtendienstrechts vorgenommen. In einer Impulsreihe haben wir zahlreiche Vorschläge dazu erarbeitet: Impulse für die Reform des Nachrichtendienstrechts 2024

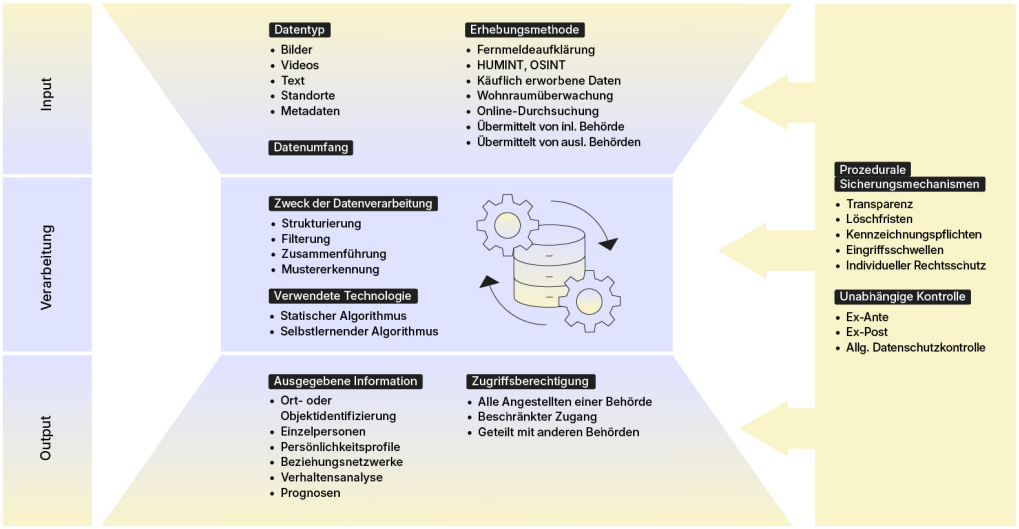
4 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178.

Grafiken aus der Publikation:

Einsatzszenarien für automatisierte Datenanalysemethoden bei den Nachrichtendiensten



Faktoren, die das Eingriffsgewicht automatisierter Datenanalysemethoden beeinflussen



Einleitung

Schon vor dem terroristischen Anschlag in Solingen waren Details zu den Plänen von SPD-Bundesinnenministerin Nancy Faeser an die Öffentlichkeit gedrungen, die

Befugnisse der Polizeibehörden zu erweitern. Unter anderem soll Polizeibehörden ermöglicht werden, „verschiedene Datenbestände technisch zusammenzuführen“ und durch automatisierte Analyseverfahren „neues Wissen zu erzeugen“.[5] Diesen Plänen scheinen – Stand Anfang September 2024 – nun auch FDP und Grüne zuzustimmen. Damit käme eine jahrelange Diskussion um den Einsatz automatisierter Datenauswertungstools im polizeilichen Bereich zu ihrem vorläufigen Ende.[6] Dass die Änderungen unter engen Voraussetzungen grundsätzlich zulässig sind, urteilte 2023 auch das Bundesverfassungsgericht – doch zugleich mahnte es die Notwendigkeit ausreichender Sicherungsmechanismen für die Grundrechte an.[7]

Die hier beschriebene politische Debatte bezog und bezieht sich dabei ausschließlich auf den polizeilichen Bereich. Blickt man hingegen auf die deutschen Nachrichtendienste, muss man konstatieren: Eine öffentliche Diskussion über automatisierte Datenauswertungsmethoden findet derzeit nicht statt – und das, obwohl die Dienste seit mehr als zehn Jahren ihre Fähigkeiten in diesem Bereich immer weiter ausbauen. Obwohl der Einsatz algorithmischer Datenauswertungsmethoden massive Auswirkungen auf die Grundrechte der Betroffenen hat, hat der Gesetzgeber hierfür noch keine spezifischen Regeln festgelegt. Den verfassungsrechtlichen Mindestanforderungen für solche Eingriffe werden die Dienste so nicht gerecht.[8] Dabei hatte das Bundesverfassungsgericht in dem oben bereits zitierten Urteil klargestellt, dass ein präzises Regelwerk nötig ist, wenn Sicherheitsbehörden solche Methoden einsetzen, um die Verhältnismäßigkeit solcher grundrechtsintensiven Maßnahmen sicherzustellen.[9] Die Suche nach Wegen, große Datenmengen automatisiert auszuwerten, ist vor dem Hintergrund neuer Formen der Informationsbeschaffung zu sehen. Medienberichte haben erst kürzlich wieder gezeigt, wie umfassende Standortdaten von Millionen von Bürger:innen in Deutschland einfach eingekauft werden können.[10] Weltweit nutzen Nachrichtendienste – offenbar auch die deutschen – solche Daten.[11] Außerdem

5 Meister (2024). Wir veröffentlichen den Entwurf zum neuem BKA-Gesetz.

6 Leisegang & Rudl (2024). Überwachung, wie sie Bürger erwarten; Deutscher Bundestag (2024). Anhörung zur Analysesoftware Bundes-VeRA.

7 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178.

8 Deutscher Bundestag (2024). Verarbeitung von Daten aus dem Internet und sozialen Netzwerken durch Sicherheitsbehörden, S.11.

9 Obwohl in diesem Urteil Regelungen aus Polizeigesetzen Gegenstand der Betrachtung waren, sind viele der grundsätzlichen Abwägungen auch für den nachrichtendienstlichen Bereich zutreffend. Wesentlicher Unterschied ist dabei, dass Nachrichtendiensten, im Gegensatz zu Polizeibehörden, keine Zwangsbefugnisse zur Verfügung stehen. Für die nachrichtendienstliche Datenerhebung verringern sich wegen des niedrigeren Eingriffsgewichts im Vergleich zum polizeilichen Bereich auch die Eingriffsschwellen. Gleichzeitig ist aber auch klar: Für die Vereitelung identifizierter Gefahren werden die gesammelten Informationen in der Regel meist an Behörden der Gefahrenabwehr mit entsprechenden Zwangsbefugnissen übermittelt. Und das allgemein verdeckte Vorgehen der Nachrichtendienste spricht wiederum für eine Intensivierung des Grundrechtseingriffs – denn das Risiko für Einschüchterungseffekte in der Bevölkerung durch ein Gefühl des allgemeinen Beobachtetseins wie in Kapitel 4.2 beschrieben wird dadurch gesteigert.

10 Meineck & Dachwitz (2024). Wie Datenhändler Deutschlands Sicherheit gefährden.

11 Ruckerbauer & Wetzling (2024). Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen.

werden frei im Internet abrufbare Informationen von Sicherheitsbehörden automatisiert erfasst. Die Menge der Daten und die Vielfalt der Quellen, aus denen sie stammen, nimmt zu. Die Behörden stehen deshalb vor einem Berg unstrukturierter Daten und suchen die sprichwörtliche Nadel im Heuhaufen. Die Kombination aus wachsenden Datenmengen und steigender Leistungsfähigkeit der Auswertungswerkzeuge führt zu immer umfassenderen und granularen Erkenntnissen. In Verbindung mit bestehenden Regelungs- und Kontrolllücken, die wir in einer Impulsreihe zur anstehenden Nachrichtendienstreform beleuchtet haben, ist damit auch dem Missbrauch Tür und Tor geöffnet. Es droht ein unverhältnismäßiger Ausbau der Überwachung.

In diesem Impulspapier zeigen wir, warum die bestehenden Regelungen nicht geeignet sind, um die automatisierte Datenanalyse effektiv auf ein verfassungskonformes Maß zu beschränken. So wird die Ampel derzeit weder ihrem eigenen Anspruch gerecht, das Nachrichtendienstrecht zukunftsfest auszugestalten,[12] noch erfüllt der Status quo verfassungsrechtliche Mindeststandards. Doch auch wenn sich die Diskussionen innerhalb der Ampelkoalition derzeit schwierig gestalten:[13] Die Reform des Nachrichtendienstrechts ist ein zentrales innenpolitisches Vorhaben und soll noch in diesem Jahr im Kabinett beschlossen werden. Der Gesetzgeber sollte also die sich nun bietende Gelegenheit nutzen und im Zuge der Reform Regeln für den Einsatz solcher Technologien formulieren sowie deren Einhaltung sicherstellen.

Wie Nachrichtendienste Werkzeuge zur automatisierten Datenauswertung nutzen

Warum die Datenflut die Nachrichtendienste vor Herausforderungen stellt

Die massive Verbreitung digitaler Technologien und deren Nutzung in allen Lebensbereichen führt zu einer regelrechten Explosion der verfügbaren Daten. Spätestens seit den Snowden-Enthüllungen wissen wir, in welchem Umfang Nachrichtendienste diese Datenmengen nutzen. Und schon lange vor dem aktuellen KI-Hype haben sich Dienste mit der Frage beschäftigt, wie sie diese

12 Bundesregierung (2023). Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts.
13 Ogorek (2024). Nachrichtendienste: Ein neues Recht für die Zeitenwende!

unüberschaubaren Datenmengen effizient auswerten können. Schon 1993 sagte das US Scientific and Technical Intelligence Committee für die US-Dienste voraus, dass ein Paradigmenwechsel nötig sein werde, um dem „information-overload“ und dem wachsenden Informationshunger gleichermaßen gerecht zu werden. Gemeint waren damit Werkzeuge zur automatisierten Datenverarbeitung.[14]

Und diese Prognose hat sich bewahrheitet: Der britische technische Aufklärungsdienst GCHQ beklagte 2011, dass die Datenbeschaffung zwar gut funktioniere, die Auswertung dieser Datenmengen aber mangelhaft sei.[15] Die gleiche Erfahrung machte der Bundesnachrichtendienst (BND) Anfang des vergangenen Jahrzehnts. Die Datenmengen, die in der Fernmeldeaufklärung erfasst wurden, waren so groß, dass es zu einer „hohen Belastung der Systeme“ kam und man deshalb entschied, bestimmte Inhalte nicht mehr zu erfassen.[16] Das Ergebnis: Weil die Möglichkeiten zur Auswertung begrenzt waren, musste der BND die Kapazitäten fokussieren und Überwachungstätigkeiten priorisieren.

Erschwerend kam nach Einschätzung des Verfassungsschutzes noch die Fragmentierung der Daten hinzu: „Die ‚Nomadisierung‘ des Nutzerverhaltens, die Internationalisierung der angebotenen Dienste, die Verschlüsselung der Kommunikation sowie die mangelnde Verpflichtbarkeit ausländischer Provider wird […] zunehmend zur Lückenhaftigkeit der Auswertung des Kommunikationsverhaltens der beobachteten Personen führen.“[17]

Der Mensch wird bei der Datenauswertung zum Nadelöhr. Nachrichtendienste sahen sich kaum mehr in der Lage die Masse der von ihnen erfassten Informationen auszuwerten. Das Problem hat sich in den letzten Jahren nur verschärft, denn die Datenmengen aus der Fernmeldeaufklärung steigen und Nachrichtendienste nutzen zunehmend auch die Möglichkeit, massenhaft Daten von Datenhändlern einzukaufen (ADINT)[18] und öffentlich zugängliche Daten systematisch auszuwerten (OSINT).[19] Die Folge: stetig wachsende Datenberge, die ausgewertet werden müssen.

14 STIC. Preparing US Intelligence for the Information Age: Coping With the Information Overload.
15 Biddle (2017). How Peter Thiel's Palantir helped the NSA spy on the whole world; Babuta, Oswald und Janjeva (2020) Artificial Intelligence and UK National Security, S. 12 und Hornung (2022) Künstliche Intelligenz zur Auswertung von Social Media Massendaten, S. 13ff.
16 Biermann (2014). Die geheime Überwachungswunschliste des BND.
17 Bundesamt für Verfassungsschutz (2015). Konzept zur Einrichtung einer Referatsgruppe 3C „Erweiterte Fachunterstützung Internet“ im BfV.
18 Tau (2024). Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State.
19 CTIVD (2022). Publication review report on automated OSINT.

Wie Nachrichtendienste technologisch aufrüsten

Um die wachsenden Datenmengen auch auswerten zu können, suchen die Nachrichtendienste deshalb nach technischen Lösungen. Hier kommen die Werkzeuge zur automatisierten Auswertung großer Datenmengen ins Spiel. Deren Einsatz kann allerdings tief in Grundrechte eingreifen. Um besser zu verstehen, inwiefern Grundrechte wie das Recht auf informationelle Selbstbestimmung verletzt werden können, richten wir im Folgenden zunächst einen Blick darauf, welche Art von Werkzeugen Nachrichtendienste weltweit verwenden. Die unterschiedlichen Einsatzzwecke werden weiter unten auch in Abbildung 1 dargestellt.

Durch die Snowden-Enthüllungen wurde beispielsweise das Abhörprogramm *XKeyscore* der US-Nachrichtendienste bekannt. Mit diesem Programm wurden riesige Datenmengen aus der Internetkommunikation ausgeleitet. Um diese riesigen Datenmengen auswerten zu können, identifizierten die US-Nachrichtendienste diese Lösung: Werkzeuge, mit denen sich die unüberschaubaren Datenmengen strukturieren und durchsuchen ließen. Dafür finanzierten sie unter anderem das Unternehmen *Palantir*, und kooperierten eng mit diesem, um geeignete Software zu entwickeln.[20] Ein Beispiel für die Strukturierung von Daten sind Technologien, die Sprache und Bilder interpretieren und so beispielsweise in Videoaufnahmen enthaltene Gespräche automatisiert transkribieren oder Gegenstände identifizieren.[21] Zudem können Softwarelösungen dafür verwendet werden, verschiedenste Formate von Textinhalten zu erfassen. Mit solcher Software lassen sich beispielsweise bestimmte Informationen wie Telefonnummern, Kontoverbindungen, Personen, Organisationen oder Standorte extrahieren.

Doch Analysewerkzeuge können noch weitergehende Informationen liefern. Sie können eingesetzt werden, um Daten zu analysieren, Zusammenhänge herzustellen und statistische Besonderheiten zu erfassen. So werden regelrecht neue Informationen generiert; das Bundesverfassungsgerecht spricht hier von „Data-Mining“.[22] Beispielsweise können so aus Metadaten der Fernmeldeüberwachung Kommunikationsnetzwerke oder aus einer großen Menge Standortdaten, wie sie Datenhändler anbieten,[23] Bewegungsprofile erstellt werden.

20 Biddle (2017). How Peter Thiel's Palantir helped the NSA spy on the whole world.

21 Katz (2021). Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation, S. 10f.

22 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 31.

23 Meineck & Dachwitz (2024). Wie Datenhändler Deutschlands Sicherheit gefährden.

Möglich sind auch Verhaltensanalysen, die durch Anwendung komplexer Algorithmen auf personenbezogene Daten Erkenntnisse und Prognosen über individuelles Verhalten und Aussagen über Empfindungen oder Meinungen erstellen.[24] Die Übergänge zwischen unterschiedlichen Arten von Werkzeugen sind dabei oft fließend und viele Softwarelösungen beinhalten mehrere Funktionen.

Heute gibt es eine kaum zu überblickende Anzahl an Anbietern von Softwarelösung zur Erfassung, Strukturierung, Verarbeitung und Analyse großer Datenmengen. Schon seit geraumer Zeit setzen US-Nachrichtendienste KI-Technologien zur Auswertung der Daten aus der Fernmeldeaufklärung und anderen Quellen ein.[25] Die Anwendungsfelder sollen zukünftig massiv ausgebaut werden. Die *National Intelligence Strategy 2023* betont beispielsweise, dass eine Stärkung der Fähigkeiten in den Bereichen *Big Data* und Künstliche Intelligenz notwendig sei.[26] Microsoft hat für die US-Nachrichtendienste einen digitalen Assistenten auf Basis des Sprachmodells GPT4 entwickelt, mit dem künftig auch Informationen der höchsten Geheimhaltungsstufe verarbeitet werden können, ohne dass diese über das verarbeiten der *Prompts*, also der Eingaben der Nachrichtendienstmitarbeitenden in die Bedienoberfläche, abfließen.[27] Und in einem 2022 öffentlich vorgestellten Forschungsprojekt der US-Nachrichtendienste wurde ein Werkzeug namens *HAYSTAC* entwickelt, das auf Grundlage von massenhaft gesammelten Standortdaten von Menschen mithilfe selbstlernender Systeme „anormale" Bewegungsmuster ausfindig machen soll.[28] Auch im Vereinigten Königreich werden KI-Technologien zur Analyse der „stetig wachsenden, fragmentierten und komplexen Daten"[29] genutzt.[30]

Welche rechtlichen und ethischen Fragen automatisierte Datenauswertungsmethoden aufwerfen

Nachrichtendienste nutzen also zunehmend Systeme zur automatisierten Datenverarbeitung – darunter auch selbstlernende Systeme. Sicherheitsbehörden halten diese Werkzeuge für geeignet, um aus den großen Datensammlungen, die ihnen zur Verfügung stehen, Erkenntnisse zur Ausübung ihres Auftrags zu gewinnen. Mit dem Erkenntnisgewinn gehen aber massive Auswirkungen auf das

24 Harris, S, Bradford, Janjeva (2023) Behavioural Analytics and UK National Security.
25 NSA/CSS (2023). GEN Nakasone Offers Insight into Future of Cybersecurity and SIGINT.
26 ODNI (2023). National Intelligence Strategy, S. 5.
27 Manson (2024). Microsoft Creates Top Secret Generative AI Service for US Spies.
28 Gross (2022). IARPA Explores AI to Reimagine Physical Safety and Combat Disinformation.
29 The Alan Turing Institute (2022). Partnership between MI5 and The Alan Turing Institute.
30 MI5 (2024). Analysing intelligence.

fragile Gleichgewicht zwischen dem Schutz der Freiheitsrechte auf der einen und den Sicherheitsinteressen auf der anderen Seite einher. Und hieraus ergibt sich ein Handlungsbedarf für den Gesetzgeber. Denn bisher beruht die Abwägung zur Verhältnismäßigkeit von Datenerhebungen auf der Annahme, dass Menschen diese Daten auswerten.[31] Doch die Realität der Auswertung großer Datenmengen entfernt sich immer weiter von dieser Vorstellung. Entsprechend müssen neue Regeln erdacht werden, die die Balance zwischen den geschützten Rechtsgütern und den betroffenen Grundrechten schützen können. Denn selbst wenn es einen gesellschaftlichen Konsens darüber gibt, dass man den Schutz von Grundrechten zugunsten des flächendeckenden Einsatzes von automatisierten Datenanalysenmethoden schwächt, so erfordern die Prinzipien von Demokratie und Rechtsstaatlichkeit eine einfachgesetzliche Grundlage. Denn die Tragweite dieser Entscheidung für den Einzelnen und die Gesellschaft als ganzes ist viel zu groß, als dass sie von der Exekutive allein getroffen werden sollte.

In Deutschland beispielsweise wird die Neujustierung dieses Gleichgewichts zu einer „der fundamentalen Herausforderungen eines künftigen Nachrichtendienstrechts, die spezifischere Datenverarbeitungsbefugnisse unumgänglich macht“.[32] Wie wichtig angesichts der potenziell verheerenden Grundrechtsauswirkungen von automatisierten Datenanalysemethoden ein präzises Regelwerk ist, hat das Bundesverfassungsgericht (BVerfG) in einem Urteil zum Einsatz durch Polizeibehörden klargestellt.[33] Auch wenn das Urteil nicht ohne Weiteres auf die Nachrichtendienste übertragbar ist, werden darin dennoch allgemeine verfassungsrechtliche Abwägungen zur Grundrechtswirkung solcher Methoden formuliert, die der Gesetzgeber bei der anstehenden Reform berücksichtigen sollte. Denn wie wir in Kapitel 5 zeigen, wird der aktuelle Rechtsrahmen der Einsatzpraxis nicht gerecht. Zunächst wollen wir im Folgenden Kapitel aber die öffentlich bekannten Erkenntnisse zum Einsatz automatisierter Datenanalyseverfahren bei deutschen Nachrichtendiensten beleuchten.

Was wir über den Einsatz automatisierter Analyseverfahren durch deutsche Nachrichtendienste wissen

Welche Technologien zur Auswertung großer Datenmengen deutsche Nachrichtendienste genau nutzen, darüber ist kaum etwas bekannt. Erst jüngst

31 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 70.
32 Löffelmann & Zöller (2022). Nachrichtendienstrecht.
33 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178.

betonte die Bundesregierung in einer Antwort auf eine Kleine Anfrage der Bundestagsfraktion Die Linke, dass eine öffentliche Auskunft über den KI-Einsatz der Nachrichtendienste nicht möglich sei, da dies Rückschlüsse auf spezifische Vorgehensweisen und Fähigkeiten ermögliche und so die Arbeit der Dienste gefährde.[34] Andere Nachrichtendienste geben weitaus detaillierter über verwendete Technologien und etwaige Herausforderungen bei ihrem Einsatz Auskunft.[35] Einige Informationen darüber, wie deutsche Nachrichtendienste automatisierter Datenverarbeitungstechnologien nutzen, sind aber dennoch öffentlich zugänglich. Im Folgenden diskutieren wir die Fähigkeiten von BND, BfV und dem Militärischen Nachrichtenwesen der Bundeswehr. Das Bundesamt für den Militärischen Abschirmdienst klammern wir hier aus, es ist aber davon auszugehen, dass hier ähnliche Technologien verwendet werden.

Spätestens seit 2014 bauen deutsche Dienste ihre Fähigkeiten zur Analyse großer Datenmengen aus

BfV

2015 veröffentlichte netzpolitik.org ein internes Dokument des BfV, in dem die Behörde die Anstrengungen auf diesem Feld beschreibt. So wurde schon 2014 damit begonnen, zwei Referate zur „zentralen Analysestelle in Bezug auf komplexe Datenmengen“ aufzubauen.[36] Mithilfe dieser Referate sollten Fähigkeiten entwickelt werden, große Daten aus unterschiedlichsten Quellen auszuwerten. Denn die große Menge und die Heterogenität der vom BfV gesammelten Daten führte dazu, dass sie nicht mehr vollständig ausgewertet werden konnten.[37] Dabei erkannte das BfV bereits, dass die Entwicklung und Anwendung solcher Datenauswertungsmethoden eine technische wie rechtliche Herausforderung darstellt. Nach Einschätzung des Nachrichtendiensts werden bei der „Entwicklung, Anwendung und Umsetzung Fragestellungen in den Vordergrund treten, die eine herausgehobene technische Expertise sowie die Einordnung in einen komplexen Rechtsrahmen erfordern, ohne dass das G-10 [=Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses] einschlägig ist.“[38] Unter anderem sollte die

34 Deutscher Bundestag (2024). Drucksache 20/12191.

35 Konkel (2024). The US intelligence community is embracing generative AI.

36 Bundesamt für Verfassungsschutz (2015). Konzept zur Einrichtung einer Referatsgruppe 3C „Erweiterte Fachunterstützung Internet“ im BfV.

37 Bundesamt für Verfassungsschutz (2015). Konzept zur Einrichtung einer Referatsgruppe 3C „Erweiterte Fachunterstützung Internet“ im BfV.

38 Bundesamt für Verfassungsschutz (2015). Konzept zur Einrichtung einer Referatsgruppe 3C „Erweiterte Fachunterstützung Internet“ im BfV. Dieser Aussage scheint die in späteren Gerichtsurteilen (wie beispielsweise EGMR Big Brother Watch, Rn. 363)

Fähigkeit aufgebaut werden, auf Grundlage von angefallenen Metadaten der Fernmeldeaufklärung „Übersichten der Kommunikationspartner und -häufigkeiten, zeitliche und räumliche Verteilung der Kommunikationen“ und Beziehungsnetzwerke zu erstellen.

BND

Auch beim BND war man spätestens 2014 um die Entwicklung von Fähigkeiten zur automatisierten Datenanalyse bemüht. Im Rahmen eines Projekts namens *AIDA* sollten Analyseverfahren entwickelt werden, um Daten besser zusammenführen und mit leistungsfähigeren Algorithmen durchsuchen zu können.[39] Passend dazu berichteten Medien 2015 über ein als Verschlusssache deklariertes Papier, demzufolge BND und Bundeswehr mit *Palantir* bei der Datenanalyse kooperieren.[40] 2018 hingegen verneinte die Bundesregierung in Reaktion auf eine Kleine Anfrage, dass im Geschäftsbereich des BMVg Produkte der Firme *Palantir* eingesetzt werden.[41] Ebenfalls 2015 wurde berichtet, dass das BND beabsichtige, die Software *Hana* der Firma SAP zu lizensieren. Diese Software sollte ebenfalls dazu eingesetzt werden, „viele verschiedene Daten miteinander [zu] verknüpfen, um Muster herauszulesen“[42] – sie sollte insbesondere eingesetzt werden, um Metadaten aus der Telekommunikationsüberwachung zu analysieren.

Auch Angestelltenportraits auf der Website des BND lassen die technischen Anstrengungen des Auslandsnachrichtendiensts erkennen. Beispielsweise entwickelt der BND nach eigenen Angaben selbst „Machine-Learning- und Deep-Learning-Verfahren zur Lösung unterschiedlichster spannender Probleme“.[43] Der portraitierte KI-Experte des BND sieht insbesondere im „Zusammenführen verschiedener Datenquellen und Daten“ eine interessante Aufgabe.[44] Auch im Zusammenhang mit der Auswertung der Informationen aus der Fernmeldeaufklärung beschreibt der BND, dass durch Verschmelzung unterschiedlicher Daten „Verhaltensmuster von Schleusernetzwerken“ erkannt und Personen ausfindig gemacht werden können, die sich ähnlich verhalten.[45] Zukünftig sollen „verstärkt Algorithmen gebaut werden, die Abweichungen leichter finden“.[46]

verworfene Annahme zugrunde zu liegen, dass die Analyse von Metadaten von Kommunikationsvorgängen keinen Eingriff in das Fernmeldegeheimnis darstelle.

39 Meister (2014). Live-Blog aus dem Geheimdienst-Untersuchungsausschuss.

40 Fuchs (2015). BND beauftragt CIA-Firmen.

41 Deutscher Bundestag (2018). Drucksache 19/2552, S.18.

42 Biermann (2015). BND speichert 220 Millionen Telefondaten – jeden Tag.

43 Bundesnachrichtendienst (2024). Ich entwickle KI-basierte Prototypen für den BND.

44 Bundesnachrichtendienst (2024). Ich entwickle KI-basierte Prototypen für den BND.

45 Bundesnachrichtendienst (2024). Ich suche die Fehler in der Matrix.

46 Bundesnachrichtendienst (2024). Ich suche die Fehler in der Matrix.

Ein Bundestagsabgeordneter aus den Reihen der Ampelkoalition zeigt sich in diesem Jahr in der Anhörung im Innenausschuss zum Einsatz von *Palantir*-Software auf Bundesebene verwundert darüber, dass in der Diskussion der Eindruck entstehen könne, nur Software von *Palantir* sei in der Lage, große Datenmengen zu analysieren. Ihm seien zwei Systeme für solche Datenanalysen bekannt, die bei den deutschen Nachrichtendiensten bereits im Einsatz sind.[47]

Militärisches Nachrichtenwesen

Letztlich finden sich auch öffentliche Hinweise auf die Verwendung von grundrechtsrelevanten Datenanalysewerkzeuge im Militärischen Nachrichtenwesen. Zwar handelt es sich nach Auffassung der Bundesregierung nicht um einen Nachrichtendienst. Gleichwohl greifen die Überwachungsaktivitäten der entsprechenden Stellen der Bundeswehr tief in Grundrechte ein. Auch sie müssen deshalb ähnlichen verfassungsrechtlichen Mindeststandards gerecht werden. [48] Schon 2019 forderte das Amt für Heeresentwicklung ein System zur Auswertung großer Datenmengen mit den folgenden Fähigkeiten:

„Das System sammelt konsequent alle verfügbaren Daten über den Einsatzraum. Dies sind sowohl Inhalte aus Internet und anderen öffentlichen Medien als auch Ergebnisse nachrichtendienstlicher Informationsgewinnung im Einsatzraum. Diese Daten werden mit Hilfe von KI-Verfahren mit beobachteten Ereignissen korreliert.“[49]

Und im Juli 2024 verkündete die Bundeswehr, ein „generatives KI-Tool, das die digitale Verarbeitung und Textgenerierung revolutionieren kann“, entwickelt zu haben.[50] Ein Angehöriger des Zentrums Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum erklärte außerdem im August 2024, dass die Bundeswehr gestützt auf KI-Technologie „automatisierte Datenauswertung im Internet“ betreibe und menschliche Stimmen aus der Fernmeldeaufklärung analysiert.[51]

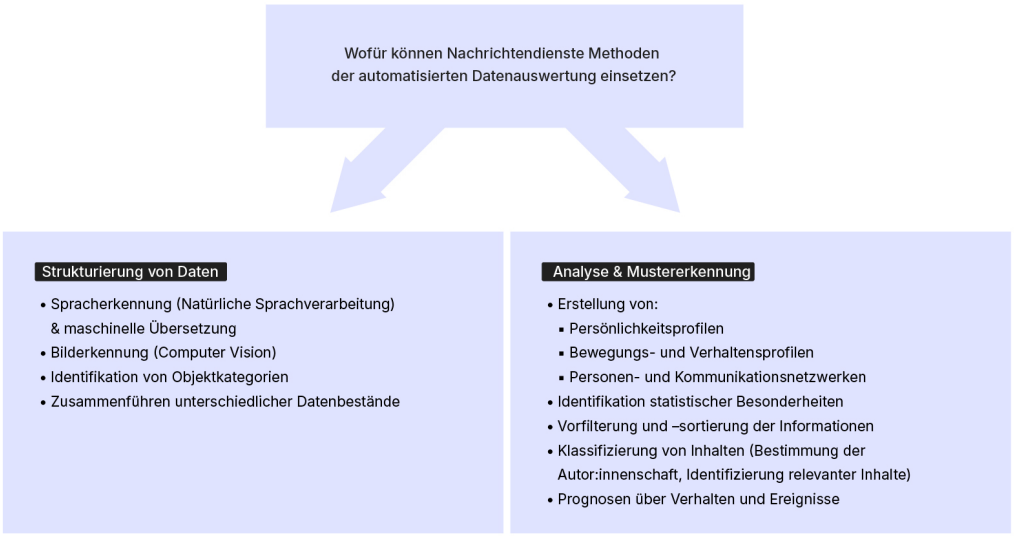
Grenzenlose Datenanalysen – ein wachsendes Problem für den Grundrechteschutz

Spätestens seit 2014 arbeiten also die deutschen Nachrichtendienste daran, ihre

47 Deutscher Bundestag (2024). Wortprotokoll der 74. Sitzung des Ausschusses für Inneres und Heimat, S. 18.
48 Ruckerbauer & Wetzling (2023). Zügellose Überwachung? Defizite der Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr. Kelber (2023). Das Militärische Nachrichtenwesen – ein Nachrichtendienst ohne Regeln?
49 Amt für Heeresentwicklung (2019). Künstliche Intelligenz in den Landstreitkräften.
50 Kommando CIR (2024). Post auf X.
51 Venekamp (2024). Militärische Künstliche Intelligenz in Waffensystemen.

Fähigkeiten zur Analyse großer Datenmengen auszubauen. Ziel ist es dabei unter anderem mehr über das Verhalten von Personen herauszufinden. Mit wem kommuniziert die beobachtete Person, wie verhält sie sich, wo hält sie sich auf und welche Erkenntnisse kann man aus diesen Informationen ableiten? So sollen diese Werkzeuge sensible Einblicke in das Leben der beobachteten Personen ermöglichen und den Diensten die Arbeit erleichtern. Eingesetzt werden diese Fähigkeiten zu unterschiedlichen Zwecken. In Abbildung 1 wird dieses breite Anwendungsspektrum dargestellt. Sie erhebt keinen Anspruch auf Vollständigkeit, sondern soll die Bandbreite der Einsatzzwecke verdeutlichen. Denn unterschiedliche Zwecke ziehen auch unterschiedliche Grundrechtswirkungen nach sich.

Einsatzszenarien für automatisierte Datenanalysemethoden bei den Nachrichtendiensten



Die Verwendung dieser Technologien durch deutsche Nachrichtendienste greift dabei ganz erheblich in Grundrechte ein und verschiebt die Balance zwischen Sicherheitsinteressen und dem Grundrechteschutz. Der gesetzliche Rahmen wird, wie wir im Kapitel 4 zeigen, den damit verbundenen Herausforderungen nicht im Ansatz gerecht. Denn er schafft weder eine einfachgesetzliche Ermächtigung für den Einsatz, noch definiert er dringend benötigte Regeln für den Einsatz.

An Dringlichkeit gewinnt das Problem vor allem wegen drei paralleler und fortlaufender Entwicklungen:

- Die Leistungsfähigkeit der verwendeten Systeme und die zur Verfügung stehenden Rechenkapazitäten zur Auswertung großer Datenmengen steigt nicht erst seit dem derzeitigen KI-Hype immer weiter.
- Die Menge der Daten steigt mit der zunehmenden Digitalisierung aller Lebensbereiche.
- Nachrichtendienste nutzen neue Formen der Informationserhebung, um auf einen größeren Teil dieser Daten zuzugreifen.

Und das Problem wird dadurch verschärft, dass auch bei der Datenerhebung zahlreiche gesetzliche Regelungslücken bestehen. So gibt es beispielsweise weder für den Einkauf von Datensammlungen bei privaten Händlern[52], noch für die systematische Sammlung öffentlich einsehbarer Informationen[53], gesetzliche Regelungen. Auch im Bereich der Fernmeldeaufklärung gibt es problematische Lücken, insbesondere was die Metadaten von Kommunikationsvorgängen angeht. So kritisiert ein ehemaliges Mitglied des Unabhängigen Kontrollrats, dass die nach §26 BNDG eröffnete Möglichkeit, Metadaten aus der Fernmeldeaufklärung bis zu sechs Monate auf Vorrat zu speichern. Diese Sammlung von Metadaten kann dann mit allen Mitteln ausgewertet werden, ohne dass dies an bestimmte inhaltliche Aufklärungsinteressen gebunden wäre. Nach Auffassung der Richterin ist das auch nicht mit der Rechtsprechung des Europäischen Gerichtshof für Menschenrechte vereinbar.[54]

Diese zunehmend intensiven Grundrechtseingriffe weiterhin ausschließlich mit den sehr allgemeinen Bestimmungen zur Datenverarbeitung der Nachrichtendienste zu rechtfertigen, ist ein unhaltbarer Zustand. Wie diese Datenanalysen und ihr rechtlicher Rahmen gegen verfassungsrechtliche Grundsätze verstoßen, diskutieren wir in Kapitel 5. Zunächst aber wollen wir im folgenden Kapitel darstellen, warum diese Methoden der automatisierten Datenanalyse so tief in Grundrechte eingreifen können.

Wie automatisierte Datenverarbeitungsmethoden in Grundrechte eingreifen

Die automatisierte Verarbeitung personenbezogener Daten durch die Nachrichtendienste kann eine ganze Reihe von Grundrechten betreffen: angefangen vom Recht auf informationelle Selbstbestimmung[55] über das Fernmeldegeheimnis bis hin zur Versammlungs- und Pressefreiheit. In welche Rechte die automatisierte Datenanalyse eingreift, hängt davon ab, welche Daten verarbeitet und wie diese verwendet werden.[56]

52 Ruckerbauer & Wetzling (2024). Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen.

53 Sosna (2024). „Fundgrube Internet" – vom tatsächlich möglichen und rechtlich zulässigen Sammeln der Nachrichtendienste im Netz.

54 Steiner (2024). Big Brother Watch/Centrum för Rättvisa.

55 Dass das Recht auf informationelle Selbstbestimmung auch vor der Verknüpfung der eigenen personenbezogenen Daten schützt, stellte das BVerfG in mehreren Urteilen klar, zum Beispiel in BVerfG, Beschluss des Ersten Senats vom 10. November 2020 - 1 BvR 3214/15 -, Rn. 1-138, Rn. 55.

56 Vergleiche beispielsweise die Erläuterungen dazu, wie nachrichtendienstliche Datenkäufe in unterschiedliche Grundrechte eingreifen können: Ruckerbauer & Wetzling (2024). Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche

Arbeiten Sicherheitsbehörden mit personenbezogenen Daten, ist nicht nur die Datenerhebung selbst ein Grundrechtseingriff. Auch der weitere Datenverarbeitungsprozess kann den Grundrechtseingriff vertiefen oder einen eigenständigen Grundrechtseingriff begründen.[57] Und softwaregestützte Methoden können derart weitgehende Informationen erschließen, dass die bewährten datenschutzrechtlichen Grundprinzipien der Datenverarbeitung, etwa das Gebot der Zweckbindung, nicht mehr als Beschränkung ausreichen – stattdessen brauchen sie eine eigene rechtliche Grundlage.

Eingriffe in Grundrechte erfordern grundsätzlich eine rechtliche Grundlage. Wie spezifisch diese ausgestaltet sein muss, hängt vom Eingriffsgewicht ab. Prinzipiell gilt: Je tiefer der Grundrechtseingriff, desto spezifischer muss die Rechtsgrundlage sein. Im folgenden Teil wollen wir deshalb einen Blick darauf werfen, warum die mit der automatisierten Datenauswertung verbundenen Grundrechtseingriffe besonders schwerwiegend sein können.

Tiefe persönlichkeitsrelevante Einblicke

Die automatisierte Auswertung von Daten und insbesondere die Verknüpfung von Daten aus unterschiedlichen Quellen, wie beispielsweise aus Datenkäufen und der strategischen Fernmeldeaufklärung, ermöglichen die Erstellung von umfassenden Bewegungs-, Verhaltens- und Persönlichkeitsprofilen – vergleichbar mit dem Einsatz von *Profiling*.[58] Schon durch die Auswertung großer Mengen von bei Datenhändlern erworbenen Informationen können umfangreiche Erkenntnisse über persönliche Interessen und Vorlieben, politische Überzeugungen und Gesundheitszustand gewonnen werden.[59] Additive Grundrechtseingriffe sind hier zu berücksichtigen. Denn durch die Verknüpfung und Analyse von Daten aus unterschiedlichen Erhebungsmethoden, können die bereits erfolgten Eingriffe weiter verstärkt werden. Insgesamt muss das Maß der Überwachung begrenzt bleiben.[60]

Kommen automatisierte Methoden zum Einsatz, ist das Eingriffsgewicht nicht mit der manuellen Recherche in Datenbanken durch Mitarbeitende vergleichbar. Denn wo Analyst:innen lediglich begrenzte Datenmengen und -quellen bewerten können, um daraus nachrichtendienstliche Schlüsse zu ziehen, können mit automatisierten

Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen, S. 16.

57 BVerfG, Urteil des Ersten Senats vom 14. Juli 1999 - 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95 – Rn. 1-310, Rn. 163.

58 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 69f.

59 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 69f; Ruckerbauer & Wetzling (2024). Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen, S. 10.

60 BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 1-407, Rn. 287.

Datenauswertungsmethoden immense Mengen an Daten in kurzer Zeit durchforstet werden, um persönlichkeitsrelevante Korrelationen und Muster zu erkennen. Die effizientere Auswertung vorhandener Daten ist dabei eine für sich genommen positive Entwicklung; sie verändert aber eben auch die Abwägung der Verhältnismäßigkeit von Grundrechtseingriffen.

Unterlaufen des Zweckbindungsprinzips

Automatisierte Datenverarbeitungsmethoden drohen außerdem das Gebot der Zweckbindung auszuhöhlen. Das ist insbesondere dann der Fall, wenn ganze oder mehrere Datenbanken für die Ermittlung statistischer Auffälligkeiten benutzt werden. Denn grundsätzlich dürfen Daten nur zur Verfolgung des ursprünglichen Zwecks, für den sie erhoben wurden, verwendet werden. Werden aber große Mengen von Daten ausgewertet, die für unterschiedlichste Zwecke erhoben wurden, findet oft eine Zweckänderung statt. Die zweckverändernde Nutzung von Daten ist bei der Arbeit der Sicherheitsbehörden sinnvollerweise nicht ausgeschlossen. Denn traditionell beruht die Arbeit von Sicherheitsbehörden zu großen Teilen darauf, dass Informationen aus unterschiedlichen Quellen zusammengestellt werden.[61] Sehr wohl gilt hier aber, dass es eine gesetzliche Ermächtigung braucht, die die Voraussetzungen definiert. Ist das nicht gewährleistet, gefährdet dies den Grundrechteschutz, da so wesentliche Schutzprinzipien umgangen werden können.[62] Insbesondere stellt eine unbegrenzte Weiterverwendung von Daten einen Anreiz dar, möglichst große Datenmengen auf Verdacht vorzuhalten, um diese dann möglicherweise zu einem späteren Zeitpunkt auswerten zu können. Eine solche Rückhaltung von Daten auf Vorrat, ohne bestimmten Zweck, ist aber verfassungsrechtlich unzulässig. Grundsätzlich erhöht die Möglichkeit der zweckverändernden Nutzung das Eingriffsgewicht.

Große Streubreite des Eingriffs & Entstehen eines diffusen Überwachungsgefühls

Neben der Tiefe der persönlichkeitsrelevanten Einblicke verstärkt auch die große Streubreite der Maßnahmen das Eingriffsgewicht der automatisierten Datenanalyse. Denn mit der Streubreite steigt auch die Anzahl der potenziell Betroffenen. Deshalb gilt nach verfassungsrechtlichen Maßstäben: Je größer die einbezogenen Datenbestände und je mehr Arten von Datenquellen zur Auswertung verwendet werden, desto intensiver ist der Grundrechtseingriff.[63]

61 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 68.
62 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 70.

Im Zuge der automatisierten Datenauswertung können die verarbeiteten Daten auch eine Vielzahl von Personen betreffen, ohne dass diese jemals einer Straftat verdächtig gewesen wären. Bei der Prüfung der Gesetzesgrundlage für den Einsatz von *Palantir* durch die hessischen Polizeibehörden erkannte das BVerfG beispielsweise auch die Möglichkeit, dass personenbezogene Daten von Opfern und Zeug:innen verarbeitet werden, um andere Verbrechen aufzuklären. Auch in nachrichtendienstlichen Datenbeständen können Informationen erfasst sein, die nicht zu verdächtigten Personen gehören, wie Informant:innen, andere Hinweisgebende sowie Kontaktpersonen von Verdächtigen. Stammen die verarbeiteten Daten beispielsweise aus sehr ungezielten Maßnahmen zur Datenerhebung wie der strategischen Fernmeldeaufklärung, OSINT oder ADINT, werden sehr viele Menschen von dieser Datenverarbeitung erfasst, und zwar ohne, dass das ihr Verhalten Ausschlag darüber gegeben hätte. Die Eingriffsintensität erhöht sich dadurch signifikant.

Und noch ein weiteres, nicht leicht greifbares, aber doch schwerwiegendes Problem kommt in diesem Zusammenhang hinzu: Die große Streubreite kann zu einem diffusen Überwachungsgefühl in der Bevölkerung führen. Nach Auffassung des BVerfG ist die Gefahr hierfür hoch, wenn weder für Betroffene noch für die Öffentlichkeit nachvollziehbar ist, ob und in welchem Ausmaß die eigenen Daten automatisiert ausgewertet werden. Diese Unschärfe kann erhebliche Einschüchterungseffekte auf die Bevölkerung erzeugen und Menschen bei der Ausübung ihrer Grund- und Freiheitsrechte beeinträchtigen.[64]

Fehleranfälligkeit & Diskriminierungsgefahr

Die Intensität von Grundrechteingriffen nimmt zu, je höher die Fehleranfälligkeit der Methode zur automatisierten Datenauswertung ist.[65] Besonders groß ist das Potenzial für diskriminierende oder fehlerhafte Ergebnisse der Datenauswertung, wenn selbstlernende Algorithmen eingesetzt werden. Trainings-Datensätze können gesellschaftlich verankerte diskriminierende und verzerrende Annahmen enthalten. Wird die Software auf Grundlage solcher Daten trainiert, besteht ein hohes Risiko, dass Systeme diese Annahmen reproduzieren.[66] Zahlreiche Fälle diskriminierender Verzerrungen automatisierter Datenverarbeitungssysteme im sicherheitsbehördlichen Einsatz belegen das.[67]

63 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 76.
64 BVerfG, Beschluss des Ersten Senats vom 10. November 2020 - 1 BvR 3214/15 -, Rn. 1-138, Rn 112.
65 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 90.
66 Fraunhofer-Institut für Kognitive Systeme (2024). Künstliche Intelligenz (KI) und maschinelles Lernen.
67 Završnik (2019). Algorithmic justice: Algorithms and big data in criminal justice settings; Montasari (2023). Countering Cyberterrorism, S. 127; Cho (2023). Woman sues Detroit after facial recognition mistakes her for crime suspect; Gentzel (2021). Biased Face Recognition Technology Used by Government: A Problem for Liberal Democracy; Amnesty International (2018).

Ebenso können Datensätze, die analysiert werden, zuvor manipuliert worden sein, um Sicherheitsbehörden zu täuschen. Dieses Problem ist auch der Bundesregierung bekannt. Sie verweigerte die Beantwortung mehrerer Teilfragen einer Kleinen Anfrage der Bundestagsfraktion Die Linke zum KI-Einsatz von Bundesbehörden mit dem Verweis auf die Manipulationsanfälligkeit der Technologie: Es „könnten beispielsweise käuflich erworbene Daten ggf. vor dem Kauf und Einsatz durch die Nachrichtendienste bewusst verfälscht werden, um die Wirksamkeit der verwendeten KI zu beeinflussen oder bestimmte Ergebnisse tendenziös zu verfälschen."[68] Um eine solche mögliche Manipulation zu erschweren, möchte die Bundesregierung keine Auskunft zu den verwendeten Technologien geben. Das Risiko ist dabei sicherlich größer, je mehr öffentlich über die genaue Verwendung von KI-Technologien bekannt ist. Aber anfällig für Manipulationen sind sie auch so. Das Diskriminierungspotenzial und die eingeschränkte Zuverlässigkeit der automatisierten Verfahren haben zur Folge, dass die Intensität der damit verbundenen Grundrechtseingriffe steigt.

Fehlende Nachvollziehbarkeit & Kontrollierbarkeit der Ergebnisse

Die Entscheidungsmuster und -strukturen von selbstlernenden Algorithmen entwickeln sich durch jede Anwendung und Zufuhr von neuen Daten selbstständig weiter. Selbst für Expert:innen ist es häufig nur schwer nachvollziehbar, wie und warum ein selbstlernender Algorithmus zu einem bestimmten Ergebnis kommt.[69] Diese Besonderheit erkannte auch das BVerfG an. Demnach erhöhe sich das Eingriffsgewicht durch die erschwerte Nachvollziehbarkeit und Kontrollierbarkeit von selbstlernenden Technologien.[70] Bei der Überprüfung der polizeilichen Nutzung der *Palantir*-Software *Gotham* merkte das BVerfG an, dass die Verwendung selbstlernender Systeme nur mit besonderen Vorkehrungen gestattet ist.[71] Denn sonst lassen sich Informationen über eine Person generieren, ohne dass deren Richtigkeit verlässlich überprüft werden kann. Das gilt jedoch nicht ausschließlich für selbstlernende Systeme. Auch deterministische Algorithmen können so komplex sein, dass die Nachvollziehbarkeit der zugrundeliegenden Entscheidungsstrukturen nicht garantiert werden kann.[72] Wird von privaten Unternehmen entwickelte proprietäre Software eingesetzt, kann der Zugriff für Kontrollbehörden auf den

Trapped in the Matrix.

68 Deutscher Bundestag (2024). Drucksache 20/12191, S. 3.

69 Couchman (2019). Policing by Machine, S. 40f; Babuta, Oswald und Janjeva (2020). Artificial Intelligence and UK National Security, S. 30-31.

70 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 100.

71 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 100.

72 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 101.

zugrundeliegenden Code mitunter mit Verweis auf das Geschäftsgeheimnis beschränkt werden.[73]

Die Fehleranfälligkeit solcher automatisierter Datenverarbeitungsvorgänge in Kombination mit der eingeschränkten Nachvollziehbarkeit erhöhen den Grundrechtseingriff weiter.[74]

Erschwerter Zugang zu effektivem Rechtsschutz

Werden personenbezogene Daten automatisiert ausgewertet, erfahren die Betroffenen davon in der Regel nichts. Lässt sich nachweisen, dass sie mit hinreichender Wahrscheinlichkeit betroffen sind, haben sie zwar die Möglichkeit, die Zulässigkeit der Eingriffsbefugnis gerichtlich prüfen zu lassen. Doch da kaum Erkenntnisse darüber öffentlich verfügbar sind, welche automatisierten Datenauswertungsverfahren von den Nachrichtendiensten zu welchen Zwecken und auf welcher Datengrundlage erfolgen, ist ein solcher Nachweis der Betroffenheit nur schwer möglich.

Und selbst wenn genauere Informationen darüber vorlägen, welche Technologien die Nachrichtendienste für solche Analysen nutzen, bestünde die Schwierigkeit fort, detailliert nachzuweisen, wie die verwendeten Algorithmen in die eigenen Grundrechte eingreifen. Zudem begrenzt die oben bereits beschriebene eingeschränkte Nachvollziehbarkeit insbesondere bei selbstlernenden Systemen die Möglichkeit, beispielsweise diskriminierende Verzerrungen des Algorithmus zu erkennen.[75] Diese Einschränkung des effektiven Rechtsschutzes verstärkt das Gewicht des Grundrechtseingriffs.

Die Anwendung automatisierter Datenanalysemethoden kann also schwerwiegende Grundrechtseingriffe beispielsweise in das Recht auf informationelle Selbstbestimmung, das Fernmeldegeheimnis, die Versammlungs- oder Pressefreiheit begründen. Besonders schwer wiegen die Eingriffe wegen der Tiefe der persönlichkeitsrelevanten Einblicke, der großen Streubreite der Maßnahmen, der potenziellen Fehleranfälligkeit und der Diskriminierungsgefahr. Außerdem verstärkt die mangelnde Transparenz und der erschwerte Zugang zu effektivem Rechtsschutz das Eingriffsgewicht.

---

73 In den USA wurde eine Person auf Grundlage von Beweisen, die von einer Software generiert wurden, zur Todesstrafe verurteilt. Seiner Verteidigung wurde der Zugriff auf den Sourcecode der Software mit Verweis auf das Geschäftsgeheimnis verwehrt. Foss-Solbrekk (2021). Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly, S. 248.

74 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 102.

75 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 90.

Verfassungsrechtliche Mindeststandards werden bislang nicht erfüllt

Wie in Kapitel 3 beschrieben, arbeiten deutsche Nachrichtendienste seit mindestens zehn Jahren daran, ihre Fähigkeiten zur automatisierten Datenanalyse auszubauen. Bisher sind diese Anstrengungen weitgehend unbegleitet von einer politischen Debatte. Dabei kann die automatisierte Verarbeitung personenbezogener Daten, wie in Kapitel 4 gezeigt, schwer in Grundrechte eingreifen. Spezielle rechtliche Grundlagen mit ausreichenden Sicherungsmaßnahmen, wie sie das BVerfG für den Einsatz solch grundrechtsintensiver Analysemethoden vorschreiben, fehlen. Die bestehende Rechtsgrundlage wird der Einsatzpraxis der Nachrichtendienste nicht gerecht.[76] Der Gesetzgeber muss hier also dringend nachbessern.

Denn, dass Sicherheitsbehörden ihre Datenauswertung optimieren, um so ihren Aufgaben effektiver nachzukommen, ist legitim. Auch das Bundesverfassungsgericht merkt dies in einem Urteil an und bescheinigt selbst für den polizeilichen Bereich, dass der Einsatz automatisierter Datenanalysemethoden unter bestimmten Voraussetzungen verfassungskonform sein kann.[77] Voraussetzung ist aber, dass Sicherungsmaßnahmen ergriffen werden, um die Verhältnismäßigkeit zu gewährleisten.

Welche Vorgaben das Bundesverfassungsgericht dazu macht

Die Aufgabe für den Gesetzgeber, einen geeigneten Rechtsrahmen zu schaffen ist dabei komplex. Denn wie wir in den Kapiteln 2 und 3 gezeigt haben, sind die eingesetzten Technologie und deren Einsatzzwecke sehr vielseitig. Je nach Anwendungsfall unterscheiden sich auch die betroffenen Grundrechte und die Qualität des Eingriffs. Das Bundesverfassungsgericht hat in seinem Urteil zur gesetzlichen Grundlage für den Einsatz von *Palantir*-Software durch Polizeien in Nordrhein-Westfalen und Hamburg Anhaltspunkte für eine solche Regelungssystematik umrissen. Obwohl sich das Urteil nicht unmittelbar auf den Gegenstand des vorliegenden Impulspapiers bezieht, bietet es dennoch einen relevanten Orientierungsrahmen für grundrechtliche Abwägungen zur Nutzung ähnlicher Software durch die Nachrichtendienste.

76 Datenschutzkonferenz (2023). Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten!
77 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178.

In diesem Urteil unterschied das BVerfG beispielsweise zwischen einer einfachen Stichwortsuche, die auf unterschiedliche Datenbestände zugreift und komplexeren Anwendungen bis hin zu Verfahren, die neue Informationen und Zusammenhänge aus den verarbeiteten Daten gewinnen. Je offener die Suchverfahren gestaltet sind und je weniger diese von bestehenden Erkenntnissen abhängen, desto stärker greifen sie dem Gericht zufolge in Grundrechte ein. Der Gesetzgeber muss hier also zunächst eine Regelungssystematik entwickeln, die diesen Unterschieden gerecht wird.[78] Anknüpfen könnte Sie dabei an die von der Bundesregierung in Auftrag gegebene und derzeit in Ausarbeitung befindliche Überwachungsgesamtrechnung.[79]

Ausgehend von der Regelungssystematik sollte der Gesetzgeber dann geeignete Maßnahmen ergreifen, um die Verhältnismäßigkeit der Eingriffe weiter zu gewährleisten. Dafür schlägt das Gericht beispielsweise eine „anspruchsvoll ausgestaltete Eingriffsschwelle“ oder die „Einschränkung der Datenverarbeitungsmethode“ vor.[80] Jedenfalls gilt für das BVerfG: „Je geringere Anforderungen der Gesetzgeber an den Anlass einer Datenanalyse oder -auswertung stellt, umso genauer und enger muss er die Methode der Suche regeln“.[81] Insgesamt muss hier beachtet werden, dass algorithmische Auswertungsmethoden perspektivisch dazu geeignet sein können, durch Zusammenführung und Auswertung unterschiedlicher Datenquellen eine verfassungswidrige *Rundumüberwachung* zu bewirken. Eine solche intensive Überwachung verletzt laut BVerfG die Menschwürde, wenn sie „sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können“.[82]

Es gilt hier also effektive Begrenzungen zu finden, um diese Form der Datenauswertung in Einklang mit dem Grundgesetz zu bringen. Beschränken kann der Gesetzgeber diese Maßnahmen dabei an unterschiedlichen Stellen. In der Grafik sind zur Übersicht eine Reihe von Faktoren dargestellt, die das Eingriffsgewicht beeinflussen. Hier sollte der Gesetzgeber ansetzen und Beschränkungen festlegen, die die Verhältnismäßigkeit der Maßnahmen sicherstellen.

78 Einen Vorschlag für eine abgestufte Regelungssystematik hat beispielsweise Löffelmann im Zusammenhang mit dem polizeilichen Einsatz vorgelegt: Löffelmann (2024). Schriftliche Stellungnahme zur öffentlichen Sachverständigenanhörung am 22. April 2024 zu BT-Drs. 20/9495.

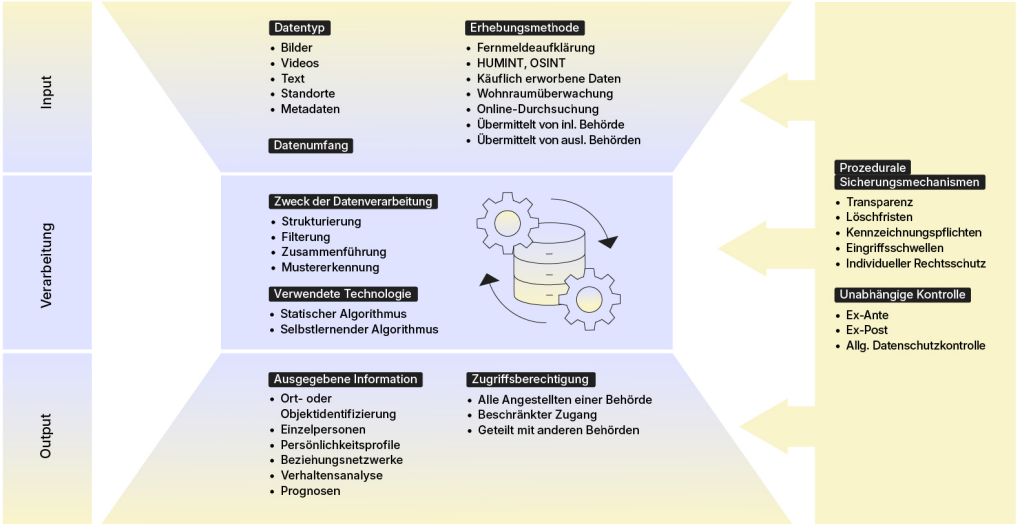
79 Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht (2024). Sicherheitsgesetze auf dem Prüfstand.

80 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 95.

81 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 95.

82 BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 1-407, Rn. 287.

Faktoren, die das Eingriffsgewicht automatisierter Datenanalysemethoden beeinflussen



Der rechtliche Rahmen hält nicht mit der Weiterentwicklung der Einsatzpraxis schritt

Denn bisher genügt der Rechtsrahmen verfassungsrechtlichen Mindestanforderungen nicht im Ansatz. Denn während die Verwendung neuer Technologien die Arbeit der Nachrichtendienste grundlegend verändert und es ihnen ermöglicht, bisherige Erkenntnisgrenzen – etwa begrenzte Ressourcen oder eingeschränkte Informationszugänge – zu überwinden, hinkt der rechtliche Rahmen hinterher.

Wie in Kapitel 4 beschrieben, kann bereits die Weiterverarbeitung von Daten und erst recht das Generieren neuer Erkenntnisse aus bereits erhobenen Daten, ein eigenständiger Eingriff in das Recht auf informationelle Selbstbestimmung sein. Und wo der Staat in ein Grundrecht eingreift und der Eingriff ein geringfügiges Maß überschreitet, muss er dafür eine gesetzliche Norm schaffen. Diese muss wiederum die Verhältnismäßigkeit des Eingriffs sicherstellen. Ein Beispiel: §19 BNDG ermächtigt den BND im Rahmen der Fernmeldeaufklärung Gesprächsinhalte im Ausland abzuhören. Die Anordnungsvoraussetzungen und Sicherungsmechanismen, die die Verhältnismäßigkeit sicherstellen werden in Abschnitt 4 des BNDG definiert.[83]

Wie in Kapitel 4 dargestellt, kann die automatisierte Datenanalyse aber in bestimmten Fällen ähnlich schwer in Grundrechte eingreifen, wie das bei der

83 Für eine Übersicht der Sicherungsmaßnahmen, siehe Ruckerbauer & Wetzling (2024). Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen.

Fernmeldeaufklärung der Fall ist. Beispielsweise, wenn umfassende Bewegungs- oder Persönlichkeitsprofile generiert werden. Eine Ermächtigungsnorm, die über die Generalklauseln hinausgeht, steht den Nachrichtendiensten dabei nicht zur Verfügung. Diese Generalklauseln sind allgemein gehaltene Normen, die den Nachrichtendiensten grundsätzlich die Verarbeitung von Daten ermöglichen. Schon die zulässigen Zwecke sind beispielsweise extrem weit gefasst: So dürfen personenbezogene Daten vom BNDG grundsätzlich verarbeitet werden, sofern sie zum Beispiel „Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung“ für Deutschland betreffen.[84] Die unbestimmte Formulierung der Generalklauseln ermöglicht eine gewisse Flexibilität nachrichtendienstlichen Handelns. Nach der einschlägigen Rechtsprechung des BVerfG können diese unbestimmten Normen aber nur Grundrechtseingriffe von geringer Intensität rechtfertigen.[85] Dem Gebot der Normenklarheit und Bestimmtheit, können die Generalklauseln angesichts der tiefen Grundrechtseingriffe durch automatisierte Datenanalysen nicht gerecht werden.[86] Auch in den gesetzlichen Bestimmungen für BfV und BAMAD stellen diese Generalklauseln keine substanzielle Begrenzung dar. Für das Militärische Nachrichtenwesen hingegen fehlt eine solche Generalklausel ebenfalls.[87]

Das Bundesverfassungsgericht hat zudem zu bedenken gegeben, dass geringere Anforderungen an den Anlass einer Datenanalyse dazu führen, dass die Methode der Suche genauer geregelt werden muss.[88] In den bestehenden gesetzlichen Normen hat der Gesetzgeber für die Nachrichtendienste bisher weder das eine, noch das andere getan. Eine spezifische Ermächtigungsnorm, die den Einsatz legitimiert und die Methode beschreibt gibt es für komplexe Analysen nicht. Ebenso fehlen spezifische Anforderungen an den Verarbeitungsanlass.

Für bestimmte Formen der Datenverarbeitung hat der Gesetzgeber zumindest Ansätze einer Regelung geschaffen. Für die Einrichtung sogenannter automatisierter Dateien wird in den Gesetzesgrundlagen ein Anordnungsverfahren definiert.[89] Automatisierte Dateien, als Begriff abgegrenzt zu nicht-automatisierten Dateien, umfassen in der Praxis solche Sammlungen, die nach bestimmten Merkmalen

84 §2 BNDG, siehe weitere Ausführung zur Generalklausel und der Kritik an deren Ausgestaltung in Löffelmann & Zöller (2022). Nachrichtendienstrecht, S. 97ff.

85 Ruckerbauer & Wetzling (2024). Informationsbeschaffung mit der Kreditkarte: Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen, S. 16.

86 Die unbestimmte Formulierung der Generalklauseln ermöglicht eine gewisse Flexibilität nachrichtendienstlichen Handelns. Nach der einschlägigen Rechtsprechung des BVerfG können diese unbestimmten Normen aber nur Grundrechtseingriffe von geringer Intensität rechtfertigen. Angesichts der in Kapitel 4 festgestellten erheblichen Intensität der Grundrechtseingriffe wird aber deutlich, dass die Generalklauseln nicht ausreichen, um die schweren Eingriffe zu legitimieren.

87 Genauer beleuchtet haben wir das rechtliche Vakuum, in dem sich das Militärischen Nachrichtenwesen mit seinen Überwachungstätigkeiten bewegt hier: Ruckerbauer & Wetzling (2023). Zügellose Überwachung? Defizite der Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr.

88 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 95.

89 §8 BNDG und § 14 BVerfSchG.

durchsucht werden können.[90] Weder gibt es aber eine Befugnisnorm, noch sind hier substanzielle Einschränkung vorgesehen. Für komplexere Formen der Datenanalyse kann dies also keineswegs die vom Bundesverfassungsgericht angemahnte rechtliche Grundlage mit hinreichender Eingrenzung der möglichen Verarbeitungen auf ein verhältnismäßiges Niveau sein. Der Vollständigkeit halber wollen wir aber dennoch einen Blick auf die Regelung richten.

Diese Normen, die ein verpflichtendes schriftliches Anordnungsverfahren für die Einrichtung automatisierter Dateien definieren, beschreiben diese Dateien nicht weiter. In der Anordnung müssen beispielsweise der Zweck, die Voraussetzung zur Speicherung und Nutzung der enthaltenen Daten, die Speicherungsdauer und die Zugangsberechtigungen definiert werden. Was in der Anordnung jedoch festgelegt wird, bleibt der Behörde überlassen. Im Folgenden braucht sie die Zustimmung der zuständigen Fachaufsicht.[91] Zudem muss die BfDI angehört werden. Ist die BfDI der Auffassung, dass die Datei und die ermöglichten Analyseverfahren nicht verfassungskonform sind, kann sie dies zwar anmerken. Der jeweilige Dienst ist aber nicht an die Einschätzung gebunden und kann das System trotzdem einsetzen.[92]

Für komplexere Analysen basierend auf Dateien, die von mehreren Behörden gemeinsam geführt werden, hat sich der Gesetzgeber nach Anweisung des BVerfG bereits an einer gesetzlichen Grundlage versucht. 2012 hatte die Bundesregierung im Rechtsextremismus-Datei-Gesetz (REDG) und später auch im Anti-Terror-Datei-Gesetz (ATDG)[93] eine Norm geschaffen, die die beteiligten Nachrichtendienste und Polizeibehörde dazu ermächtigt, die darin gespeicherten Daten *erweitert zu nutzen*. Das sollte dem Zweck dienen, Zusammenhänge herzustellen, zusammengeführte Daten statistisch auszuwerten und so unter anderem Beziehungsnetzwerke und Bewegungsprofile von Verdächtigen zu erstellen.[94] In einem Urteil von 2020 verwarf das BVerfG diese Norm wegen der zu unbestimmten Einschränkungen dieser Ermächtigung als verfassungswidrig. Seitdem wurde kein weiterer Versuch einer verfassungskonformen Neufassung der Norm unternommen – denn die Dateien werden kaum mehr verwendet.[95]

Unverändert genutzt werden komplexe Datenanalysen aber behördenintern.

---

90 Das Begriffspaar ist dabei der Fassung des BDSG entnommen und die Abgrenzung zwischen den beiden unscharf. Eine Datenbank, die unter diesen Begriff fällt, ist beispielsweise VERAS, die Datenbank Verkehrsanalysesystem, in der der BND personenbezogene Telekommunikationsmerkmale führt. Löffelmann & Zöller (2022). Nachrichtendienstrecht, S. 218f.

91 Also je nach Dienst Bundeskanzleramt, BMI oder BMVg.

92 Ruckerbauer (2024). Die Stärkung des Datenschutzbeauftragten als Schlüssel zu einer effektiveren Nachrichtendienstkontrolle.

93 §6a Antiterrordateigesetz. Deutscher Bundestag (2014). Drucksache 18/1565, S. 15.

94 Deutscher Bundestag (2012). Drucksache 17/8672, S. 19.

95 Angesichts des geringen Nutzens und der gleichzeitig schweren Grundrechtseingriffe empfahl der BfDI seit mehreren Jahren die Abschaffung sowohl der ATD als auch der RED. Die Bundesregierung erklärte hierzu 2022, dass sie sich im Koalitionsvertrag eine Revision der Datenbank vorgenommen und zu dieser Frage noch kein Ergebnis habe. Siehe BfDI 2019. Tätigkeitsbericht 2017 und 2018, S.84; BfDI (2020). Tätigkeitsbericht 2019, S.52; BfDI (2023). Tätigkeitsbericht 2022, S. 93 und Flade (2022). Die Anti-Terror-Datei, die niemand braucht.

Datenberge, die von Asservaten, wie zum Beispiel beschlagnahmte Computer oder Festplatten, oder aus der Fernmeldeaufklärung stammen oder aber systematisch auf öffentlich zugänglichen Webseiten zusammengetragen werden, werden offenbar mit Analysetools ausgewertet. Deshalb bemängelt auch die deutschen Datenschutzbehörden aus ihrer Kontrollpraxis: Im Bereich der Nachrichtendienste werden komplexe Formen der Datenanalyse eingesetzt, die mitunter auf maschinellem Lernen basieren und tief in Grundrechte eingreifen – ohne dass der Rechtsrahmen hierfür geeignete Grenzen setzt.[96]

Das BVerfG hat klargestellt, dass es eine tief in die Privatsphäre eingreifende Überwachungsmaßnahme darstellt, wenn Sicherheitsbehörden mit „einem Klick umfassende Profile von Personen, Gruppen und Milieus [...] erstellen". Deutsche Nachrichtendienste scheinen genau mit solchen Methoden zu arbeiten und bauen diese weiter aus. Zwar müssen aus grundrechtlicher Perspektive die Eingriffsschwellen im Vergleich zu Polizeibehörden nicht so hoch angesetzt werden. Sehr wohl benötigen aber auch Nachrichtendienste eine ausreichend normenklare Gesetzesgrundlage mit hinreichenden Beschränkungen, um so schwere Grundrechtseingriffe zu rechtfertigen.

Die festgestellte Regelungslücke wirft hier also Fragen hinsichtlich der Vereinbarkeit der Praxis mit dem Grundgesetz auf. Der Gesetzgeber sollte hier also dringend handeln und einen rechtssicheren Rahmen erstellen, um die Handlungsfähigkeit der Nachrichtendienste sicherzustellen und Grundrechte zu schützen. Im folgenden Kapitel erläutern wir einige Vorschläge dafür, wie der Gesetzgeber hier vorgehen könnte.

Welche Maßnahmen der Gesetzgeber ergreifen sollte

Der Gesetzgeber steht vor der Herausforderung, einen Rechtsrahmen zu schaffen, der einerseits den Nachrichtendiensten technologische Innovationen ermöglicht und andererseits einer unverhältnismäßigen Ausweitung der Überwachung einen Riegel vorschiebt. Weil der aktuelle Zustand kaum mit dem Grundgesetz vereinbar ist, müssen Bundesregierung und Parlament handeln. Angesichts der in Kapitel 3 skizzierten Trends werden die staatlichen Überwachungsfähigkeiten faktisch ausgeweitet, ohne dass dies demokratisch legitimiert ist und ohne dass Mechanismen zum Schutz von Grundrechten eingeführt werden. Um den

96 Datenschutzkonferenz (2023). Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten!

Nachrichtendiensten also Rechtssicherheit zu verschaffen und um, wie von der Ampelkoalition angestrebt,[97] eine wertungskonsistente Systematisierung der Grundrechtseingriffe vorzunehmen, sollte der Gesetzgeber die notwendigen Schritte in der anstehenden Reform ergreifen. Im Folgenden diskutieren wir Maßnahmen, die zu einer verfassungskonformen Praxis beitragen können.

Schaffen einer einfachgesetzlichen Grundlage für automatisierte Datenanalysen. Der Gesetzgeber sollte für die offenbar schon länger praktizierte Verwendung automatisierter Datenanalysemethoden eine einfachgesetzliche Grundlage schaffen. Die allgemeinen Generalklauseln genügen den verfassungsrechtlichen Anforderungen nicht.

Ausarbeiten einer Regelungssystematik. Wie in Abbildung 2 verdeutlicht, entscheidet eine große Zahl unterschiedlicher Faktoren darüber, wie intensiv Methoden der automatisierten Datenanalyse in Grundrechte eingreifen. Die Art der genutzten Daten, die Erhebungsmethode, mit der diese gewonnen wurden, und die weitere Verwendung der Ergebnisse der Analyse – all das hat Einfluss auf die Eingriffstiefe. Diese Varianz muss beim Schaffen einer Gesetzesgrundlage berücksichtigt werden.[98] Die aktuell von der Bundesregierung in Auftrag gegebene Überwachungsgesamtrechnung könnte sinnvolle Anhaltspunkte für eine Systematisierung geben.[99]

Begrenzung der auszuwertenden Daten. Der Gesetzgeber sollte ausschließen, dass Daten aus besonders grundrechtsintensiven Erhebungsmethoden, wie beispielsweise der Wohnraumüberwachung oder der Quellen-Telekommunikationsüberwachung, in automatisierte Analysemethoden einbezogen werden. Zudem sollte sichergestellt werden, dass eine Analysesoftware nicht direkt auf Daten aus dem Internet zugreift. Denn dadurch würde die Verarbeitung besonders großer Datenmengen befördert und das Eingriffsgewicht ganz erheblich gesteigert.[100] Zudem kann der Ausschluss bestimmter Datenarten wie beispielsweise biometrischer Daten das Eingriffsgewicht verringern.[101] Ebenso sollten besonders sensible Daten, die etwa den Kernbereich privater Lebensgestaltung betreffen, ausgeschlossen werden.

Voraussetzungen für den Einsatz. Um die Verhältnismäßigkeit der Eingriffe zu gewährleisten, sollten vom Gesetzgeber Eingriffsschwellen vorgegeben werden.[102] Zudem sollte bei besonders eingriffsintensiven Verfahren und insbesondere dort, wo

97 Bundesregierung (2023). Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts.
98 Einen Vorschlag für eine abgestufte Regelungssystematik hat beispielsweise Löffelmann im Zusammenhang mit dem polizeilichen Einsatz vorgelegt: Löffelmann (2024). Schriftliche Stellungnahme zur öffentlichen Sachverständigenanhörung am 22. April 2024 zu BT-Drs. 20/9495.
99 Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht (2024). Sicherheitsgesetze auf dem Prüfstand.
100 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 88.
101 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 87.
102 Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 118.

aus Datenmengen mit Hilfe statistischer Analysen neue Erkenntnisse generiert werden, der Einsatz schriftlich begründet werden müssen. Das würde dabei helfen, den Einsatz der Methoden zu fokussieren. Ein ungezieltes Einsetzen zum Aufspüren eventueller Gefahren, ohne dass zuvor ein Anlass vorgelegen hätte, wäre ein unverhältnismäßiger und verfassungswidriger Eingriff.[103]

Definieren von Zugangsbeschränkungen. Die Zugangsberechtigungen zu besonders eingriffsintensiven Systemen sollten sehr restriktiv vergeben werden. Zudem sollte darauf geachtet werden, dass Behördenmitarbeitende mit einem solchen Zugang besonders geschult sein müssen.[104]

Schaffen von Transparenz. Die öffentliche Debatte über den Einsatz automatisierter Analysewerkzeuge sollte gestärkt werden. Dafür sollte die Bundesregierung anders als bisher immerhin abstrakt über die eingesetzten Methoden berichten.

Stärkung der unabhängigen Kontrolle. Die kontinuierliche Prüfung der verwendeten Datenauswertungsmethoden sollte gestärkt werden. Der BfDI sollten bindende Anordnungsbefugnisse zugestanden werden, damit sie den Einsatz rechtswidriger Datenverarbeitungsmethoden wirksam beenden kann.[105] Ebenso sollte das Parlamentarische Kontrollgremium des Deutschen Bundestages die eingesetzten Datenverarbeitungsmethoden prüfen und proaktiv von den Diensten über neue Systeme informiert werden. Datenanalysen mit besonderem Eingriffsgewicht sollten der Vorabkontrolle eines unabhängigen Organs der Rechtskontrolle unterliegen. Weil die Analysewerkzeuge derart komplexe und umfassende Auswirkungen haben und dabei auf Daten aus unterschiedlichsten Erhebungsmethoden zurückgreifen, sollten sich die unterschiedlichen Aufsichtsorgane hierzu strukturiert austauschen. Geboten ist das vor allem, um additive Grundrechtseingriffe erfassen zu können. Aufsichtsbehörden sollten auch mit Möglichkeiten zur datengestützten Kontrolle ausgestattet werden.

Fazit

Seit einem Jahrzehnt bauen deutsche Nachrichtendienste ihre Fähigkeiten zur automatisierten Datenanalyse aus. Aus großen Datenmengen sollen so mit einem Klick Bewegungsprofile, Beziehungsnetzwerke und andere sensible Informationen über beobachtete Personen generiert werden. Händisch würde das Ermitteln solcher Informationen beispielsweise aus Metadaten der Telekommunikation sehr lange dauern – sofern es überhaupt möglich wäre.

103 BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 108.
104 Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20, Rn. 1-178, Rn. 89.
105 Ruckerbauer (2024). Die Stärkung des Datenschutzbeauftragten als Schlüssel zu einer effektiveren Nachrichtendienstkontrolle.

Durch die Verwendung automatisierter Datenanalysen erhöht sich der Überwachungsdruck, wie wir in Kapitel 4 dargelegt haben. Das Bundesverfassungsgericht urteilte deshalb, dass für den Einsatz solcher Methoden durch Sicherheitsbehörden grundsätzlich Vorkehrungen zur Wahrung der Grundrechte getroffen werden müssen. Diese Vorkehrungen, das hat die Analyse des bestehenden Rechtsrahmens in Kapitel 5 gezeigt, sind gegenwärtig nicht ausreichend getroffen. Bisher basierten die Verhältnismäßigkeitsabwägungen zu den Befugnissen von Sicherheitsdiensten in der Regel auf der Annahme, dass die Auswertung manuell erfolgt. Durch die automatisierte Analyse großer Datenmengen werden bisherige Erkenntnisgrenzen überwunden, die beispielsweise eine allzu große Streubreite der Eingriffe verhindert hatten. So verschiebt sich hier ein fragiles Gleichgewicht – ohne dass der Rechtsrahmen mit dieser Entwicklung Schritt gehalten hätte.

Dadurch droht das Verhältnis zwischen Sicherheitsinteressen und Grundrechteschutz in eine gefährliche Schieflage zu geraten. Die Ampelkoalition sollte dringend handeln und angesichts dieser Entwicklungen Leitplanken ziehen, an denen sich die Nachrichtendienste in ihrer Arbeit orientieren können. Tut sie das nicht, kann das nicht nur Auswirkungen auf individuelle Grundrechte, sondern auch schwerwiegende Konsequenzen für demokratische Grundprinzipen und den Rechtsstaat haben.

Die politische Debatte nach dem terroristischen Messerangriff in Solingen Ende August war von Forderungen nach einer Ausweitung sicherheitsbehördlicher Befugnisse von nahezu allen Parteien geprägt. Und klar ist, es sollten intensive Anstrengungen unternommen werden, um solche Taten in Zukunft zu verhindern – ob neue Befugnisse für Sicherheitsbehörden dazu beitragen, sei dahingestellt. Eines sollte aber allen politischen Entscheidungen, die folgen, vorausgesetzt sein: Feind:innen der Demokratie von innen und außen sollte man nicht den Gefallen tun, eine der Säulen liberaler Demokratien anzusägen, nämlich die Rechtsstaatlichkeit. Wenn wir also darüber diskutieren, ob die Befugnisse von Polizeien und Nachrichtendiensten Anpassungen brauchen, sollte die Grundvoraussetzung immer sein, dass das Handeln der Sicherheitsbehörden auch künftig mit dem Grundgesetz vereinbar ist. Denn wie resilient Demokratien sind, zeigt sich daran, ob sie in der Lage sind, ihre Werte auch unter Druck zu schützen. In Zeiten einer angespannten Sicherheitslage sollte die Ampelkoalition also unter Beweis stellen, dass die wehrhafte Demokratie handlungsfähig ist und rechtsstaatliche Grundsätze verteidigen kann. Dazu hat sie jetzt die Gelegenheit.

Die Autor:innen danken Hannah-Aeterna Borne, Luisa Seeling, Alina Siebert und Thorsten Wetzling für konstruktives Feedback, wertvolle Recherchearbeiten und grafische Gestaltung. Die Autor:innen sind allein verantwortlich für den Inhalt.

Authors

Corbinian Ruckerbauer
Policy Researcher Digital Rights, Surveillance and Democracy
cruckerbauer@interface-eu.org
+49 30 81 45 03 78 80

Lilly Goll
Student Assistant | Digital Rights, Surveillance and Democracy
lgoll@interface-eu.org
+49 30 81 45 03 78 80

Imprint

interface – Tech analysis and policy ideas for Europe
(formerly Stiftung Neue Verantwortung)

W www.interface-eu.org
E info@interface-eu.org
T +49 (0) 30 81 45 03 78 80
F +49 (0) 30 81 45 03 78 97

interface – Tech analysis and policy ideas for Europe e.V.
Ebertstraße 2
D-10117 Berlin

Design by Make Studio
www.make.studio
Code by Convoy
www.convoyinteractive.com