Die im Rahmen der „Reformen“ der Bundesregierung geplanten Änderungen beim Datenschutz sind gravierend. Unter vielem anderen soll erlaubt sein: Gesichter und Stimmen im Internet abgleichen, polizeiliche Datenbestände automatisiert verknüpfen, personenbezogene Informationen zum Training Künstlicher Intelligenz verwenden. Vorgesehen ist auch die dauerhafte Zusammenführung von Polizeidaten unabhängig von einem konkreten Vorgang – einschließlich der Daten von Opfern, Zeugen und Unbeteiligten. Außerdem ist ein massiver Ausbau geheimdienstlicher Überwachung und verdeckter Eingriffe geplant – und noch Vieles mehr. Von **Detlef Koch**.

Dieser Beitrag ist auch als Audio-Podcast verfügbar.

https://www.nachdenkseiten.de/upload/podcast/290924_Massive_Angriffe_auf_den_Datenschutz_geplant_Serie_zu_den_Sozial_Reformen_Folge_VII_NDS.mp3

Podcast: Play in new window | Download

Links zu den anderen Folgen der Serie finden sich unter dem Artikel.

Die Bundesregierung plant weitreichende Datenzugriffe und Erleichterungen für Unternehmen. An den intellektuellen Grenzen der Planer und den Machtphantasien der Politiker unserer Bundesregierung entscheidet sich, wie wirksam Bürgerinnen und Bürger ihre Freiheit noch verteidigen können.

Gesichter und Stimmen im Internet abgleichen, polizeiliche Datenbestände automatisiert verknüpfen, personenbezogene Informationen zum Training Künstlicher Intelligenz verwenden, sind nur die Spitze des Eisbergs einer Orwell’schen Dystopie. [1] Die Vorhaben, zu denen der Bundestag am 21. September 2026 eine Anhörung abhielt, würden die Möglichkeiten staatlicher Ermittlungen erheblich erweitern. [2]

Die Regierung verbindet damit nämlich die Aussicht, gesuchte Personen schneller zu finden und kriminelle Netzwerke besser zu erkennen. Doch um die gesuchten Personen zu finden, können auch Daten von Menschen verarbeitet werden, die weder einer Straftat verdächtig sind noch selbst einen Anlass für polizeiliche Maßnahmen gegeben haben. Die Bundesdatenschutzbeauftragte kritisiert zudem die vorgesehene dauerhafte Zusammenführung vorhandener Polizeidaten unabhängig von einem konkreten Vorgang – einschließlich der Daten von Opfern, Zeugen und Unbeteiligten. [3] Ob die Daten, die in eine Analyse eingehen, und die Schlüsse, die daraus gezogen werden dürfen, mit einem verfassungskonformen Grundrechtsschutz vereinbar sind, werden Gerichte klären müssen.

[4]

Modernisierung des Bundespolizeigesetzes

Schon allein die geplante Modernisierung des Bundespolizeigesetzes zeigt, wie weit der Ausbau staatlicher Zugriffsmöglichkeiten reicht. Der Regierungsentwurf 21/3051 erlaubt der Bundespolizei, verschlüsselte Kommunikation durch heimlichen Zugriff auf das Endgerät zu überwachen, Verkehrs- und Nutzungsdaten zu erheben sowie Mobilfunkkarten und Geräte zu identifizieren und zu lokalisieren. Drohnen sollen als Träger von Bild- und Tonaufnahmen eingesetzt werden können und hinzu kommen Befugnisse zur Drohnenabwehr.

Meldeauflagen und Aufenthaltsverbote erweitern die Möglichkeiten, Menschen bereits aufgrund einer Gefahrenprognose in ihrer Bewegungsfreiheit zu beschränken. Die Bundesregierung begründet diese Befugnisse unter anderem mit wirksamerer Gefahrenabwehr und der Bekämpfung von Schleuserkriminalität. [5]

In Waffen- und Messerverbotsbereichen der Bahn sollen Menschen ohne persönlichen Verdacht kontrolliert und durchsucht werden können. Die Regierungsbegründung formuliert ausdrücklich: „Die Kontrollen sind grundsätzlich anlasslos und stichprobenartig möglich.“ Wer dort unterwegs ist, muss also keine verdächtige Handlung begangen haben, um Gegenstand einer solchen Kontrolle zu werden.

Automatisierte Gefahrenerkennung und biometrische Echtzeitdetektion

Der Innenausschuss ergänzte das Vorhaben um automatisierte Gefahrenerkennung und biometrische Echtzeitdetektion. Kamerabilder sollen nach Bewegungen, Gegenständen und Aufenthaltsorten ausgewertet werden können; ein weiteres Verfahren soll Gesichter unmittelbar mit biometrischen Daten bestimmter Zielpersonen abgleichen. Die praktische Konsequenz: Auch unverdächtige Menschen im erfassten Kamerabereich können den biometrischen Abgleich durchlaufen.

Richterliche Anordnung, räumliche und zeitliche Begrenzung sowie das Verbot, Nichttreffer zu speichern, begrenzen das Verfahren. Sie verhindern jedoch nicht den vorausgehenden Abgleich unverdächtiger Personen. Außerdem soll die Bundespolizei unter festgelegten Voraussetzungen selbst den ersten gerichtlichen Antrag auf Abschiebungshaft oder Ausreisegewahrsam stellen können. [6]

Biometrischer Abgleich von Gesichtern und Stimmen

Daneben steht das Gesetz zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit. Hier geht es um den biometrischen Abgleich von Gesichtern und Stimmen mit Internetmaterial, die automatisierte Verknüpfung polizeilicher Datenbestände und die Verwendung personenbezogener Daten zum Entwickeln und Trainieren Künstlicher Intelligenz. Gesuchte Personen sollen schneller identifiziert und Zusammenhänge zwischen Personen, Orten und Straftaten leichter erkannt werden.

Damit wächst zugleich die Bedeutung jeder gespeicherten Information: Sie kann mit anderen Angaben zusammengeführt und zum Ausgangspunkt neuer Ermittlungsansätze werden. [7]

Die neuen Befugnisse der Geheimdienste

Die Reform des Nachrichtendienstrechts, Drucksache 21/7868, erweitert wiederum die Möglichkeiten von Bundesnachrichtendienst und Bundesamt für Verfassungsschutz. Vorgesehen sind technische Zugriffe bis hin zu privat genutzten Mobiltelefonen, biometrische Bildabgleiche, KI-Auswertungen und erleichterte Datenübermittlungen.

Der BND soll erhobene Kommunikationsinhalte ohne vorherige Sichtung sechs Monate, Metadaten bis zu zwölf Monate speichern dürfen. Die Regierung begründet dies mit der Abwehr von Spionage, Sabotage und Cyberangriffen sowie der rückwirkenden Auswertung von Informationen in Krisen. Zugleich soll die Datenschutzkontrolle von der Bundesdatenschutzbeauftragten zum Unabhängigen Kontrollrat wechseln. Ob dessen erweiterte Zuständigkeit wirksamen Schutz gewährleistet, muss sich an seinen tatsächlichen Kontrollmöglichkeiten messen lassen. [8]

Ausnahmen beim Datenschutz

Mit dem Ziel, wirtschaftliche Entlastung zu schaffen, fordert die Koalition, kleine und mittlere Unternehmen vom Anwendungsbereich der Datenschutz-Grundverordnung auszunehmen. Konkret kann also ein selbstständiger Psychotherapeut Traumata, Suchterkrankungen und intime Beziehungskonflikte dokumentieren oder ein Anwalt Angaben zu Strafvorwürfen, Schulden oder familiären Auseinandersetzungen verarbeiten, ohne als kleine Unternehmen die DSGVO beachten zu müssen, obwohl der Missbrauch ihrer Daten erhebliche persönliche und wirtschaftliche Schäden verursachen kann. Bei einer vollständigen Umsetzung der Reform ohne gleichwertigen Ersatz wären die Auskunfts-, Berichtigungs- und Löschungsrechte nach DSGVO nicht mehr gewährleistet. Auch die fortbestehende berufliche Schweigepflicht ersetzt dieses Schutzsystem nicht, denn Hacker finden ihre Information, auch wenn der Arzt oder der Anwalt schweigt.

Aber damit nicht genug: Die föderale Modernisierungsagenda konkretisiert einen weiteren Schritt: Die zusätzliche deutsche Pflicht zur Benennung betrieblicher Datenschutzbeauftragter nach § 38 Absatz 1 Bundesdatenschutzgesetz soll nämlich auch entfallen. Die europäischen Benennungspflichten bleiben bestehen. Für Unternehmen, die allein unter die deutsche Vorschrift fallen, würde damit eine gesetzlich vorgeschriebene interne Kontrollfunktion wegfallen. Was kann da schon schiefgehen?

Welche Daten werden von wem zusammengeführt?

Bei Sozialleistungen soll das Juli-Programm zur Missbrauchsbekämpfung den Datenaustausch zwischen Sozial-, Ausländer-, Melde-, Finanz-, Sicherheits- und Baubehörden sowie Kranken- und Pflegekassen ausweiten. Vorgesehen sind automatische Meldungen aus dem Ausländerzentralregister über leistungseinschränkende Sachverhalte, Auskunftspflichten von Energieversorgern über weitere Wohnsitze und Kundenbeziehungen sowie die uneingeschränkte Nutzung der Steuer-ID durch Sozialversicherungsträger. Die Sozialstaatskommission empfiehlt zusätzlich, den Vorrang der Datenerhebung bei den Betroffenen zurückzunehmen und erforderliche Angaben unmittelbar zwischen Behörden auszutauschen. Für automatisierte Nachweisabrufe soll eine Zustimmungsvermutung geprüft werden. Einfachere Anträge und weniger Nachweise sind der erklärte Nutzen. Gleichzeitig stellt sich die Frage, wie Betroffene noch nachvollziehen und beeinflussen können, welche Behörde welche Angaben über sie erhält.

Diese Vorhaben betreffen die Vertraulichkeit der Kommunikation, die Kontrolle über persönliche Informationen und die Freiheit, sich ohne individuellen Verdacht im öffentlichen Raum zu bewegen. Deshalb muss die Prüfung vor der Verabschiedung beginnen: Welche Menschen geraten in die Erfassung? Welche Daten werden zusammengeführt? Wer erfährt von einer falschen Zuordnung, und wie lässt sie sich berichtigen, bevor daraus eine weitere Maßnahme entsteht? Grundrechtsschutz muss bereits die Erhebung und Verwendung begrenzen. Er darf nicht erst beim Versuch beginnen, einen eingetretenen Schaden nachträglich zu korrigieren.

Wer Informationen über das *Leben der Anderen* [9] sammelt, verbindet und auswertet, gewinnt Einfluss auf das Verhalten und die psychische Stabilität seiner Bürger, wie uns ein Film gleichen Namens eindrucksvoll vor Augen führt. Datenschutz soll diese Macht begrenzen, aber was geschieht, wenn Opfer der lückenlosen Überwachung weder die Verarbeitung erkennen noch gegen ihre Folgen vorgehen können?

Wie aus Daten ein Verdacht wird

Die geplante dreimonatige Speicherung von IP-Adressen und erforderlichen Portnummern ist ein weiterer Baustein für ein mentales Gefängnis, das ganz ohne Stacheldraht und Schießbefehl auskommt. Solche Zuordnungsdaten helfen dabei, den Anschluss hinter fast jeder bekannten Internetadresse zu identifizieren. Die Bundesregierung begründet diesen massiven Grundrechtseingriff mit Aufklärung von Onlinebetrug und Verbreitung strafbarer Hassbotschaften. Gespeichert werden aber eben auch Daten von Menschen, gegen die überhaupt kein konkreter Verdacht besteht. Die Digitale Gesellschaft kritisiert den Aufbau dieses nachträglich auswertbaren Bestandes als unverhältnismäßig. [10]

Die geplante Speicherung schafft zusätzliche Möglichkeiten, eine bekannte Onlineaktivität einem Anschluss zuzuordnen und so Nutzerprofile anzulegen. Anschlussinhaber und tatsächliche Nutzer können allerdings verschieden sein. Eine technische Zuordnung darf deshalb nicht die Prüfung ersetzen, wer tatsächlich gehandelt hat.

Bei der biometrischen Internetsuche verschiebt sich eine weitere Grenze. Öffentlich zugängliche Bilder oder Tonaufnahmen sollen automatisiert nach Gesichtern beziehungsweise Stimmen durchsucht werden können. Das Polizeipaket sieht dabei keinen biometrischen Echtzeitabgleich vor. Auch eine nachträgliche Suche kann allerdings die praktische Anonymität im öffentlichen Raum verändern: Eine Aufnahme, die für sich genommen wenig aussagt, lässt sich möglicherweise einer Person und weiteren Aufnahmen zuordnen. Falsche Treffer können Ermittlungen gegen Unbeteiligte auslösen.

Besonders folgenreich wird die Verbindung unterschiedlicher Datenbestände. Aus Kontakten, Orten und Ereignissen entstehen zuvor schwer erkennbare Zusammenhänge. Darauf zielt der erhoffte Ermittlungsgewinn. Zugleich können zufällige Kontakte oder fehlerhafte Einträge zu einem verdächtig wirkenden Muster werden. Die Gesellschaft für Freiheitsrechte (GFF) beanstandete am 2. April 2026 unter anderem die Einbeziehung Unbeteiligter und zu niedrige Anforderungen an solche Eingriffe. Ihre Stellungnahme bezog sich auf die Entwurfsphase vor dem Kabinettsbeschluss vom 29. April.

Das Gesetz muss deshalb eng begrenzen, welche Daten zu welchem Anlass verknüpft werden dürfen. Auch die Ergebnisse müssen überprüfbar sein. Sonst könnten Betroffene zusätzlichen Kontrollen ausgesetzt werden, ohne den Ausgangspunkt des Verdachts zu kennen.

Eine weitere Zweckverschiebung betrifft das Training von Systemen Künstlicher Intelligenz (KI). Personenbezogene Polizeidaten sollen dafür unter erweiterten Voraussetzungen nutzbar werden. Angaben aus Ermittlungen würden damit auch der technischen Entwicklung dienen. Vorgesehene Schutzvorkehrungen und Datenausschlüsse begrenzen

das Vorhaben; eine pauschale Freigabe sämtlicher Polizeidaten ist nicht vorgesehen. Entscheidend bleibt der Schutz von Zeugen und anderen Unbeteiligten, auch gegenüber externen Entwicklern. [11]

Kontrolle muss den Befugnissen folgen

Die Bundesregierung plant einen massiven Ausbau geheimdienstlicher Überwachung und verdeckter Eingriffe. Nach dem am 12. August 2026 vom Kabinett beschlossenen Gesetzentwurf soll der BND im Rahmen seiner strategischen Fernmeldeaufklärung noch ungesichtete Kommunikationsinhalte bis zu sechs Monate und Verkehrsdaten bis zu zwölf Monate speichern dürfen. Damit wächst ein Datenbestand, der sich nachträglich durchleuchten lässt. IP-Adressen, Verbindungszeiten und Kommunikationskontakte können dabei auch ohne Kenntnis der Inhalte sensible Beziehungen und Verhaltensmuster offenlegen und so die privatesten Dinge von jedem von uns offenlegen. [12]

Hinzu kommen erweiterte Möglichkeiten für KI-gestützte Analysen, biometrische Bildabgleiche und die entschädigungslose Weiterverarbeitung unserer persönlichen Daten für Forschung und Entwicklung. [13] Daten sollen zudem leichter an andere Behörden, die Bundeswehr und sogar an private Stellen fließen können. Die Verbindung von längerer Speicherung, leistungsfähigerer Auswertung und erleichterter Weitergabe vergrößert das Risiko, dass Fehlzuordnungen entstehen, sich verbreiten und für Betroffene folgenreich werden.

Besonders bedrohlich sind die geplanten Befugnisse zum aktiven Eingreifen. Der BND soll unter bestimmten Gefahrenvoraussetzungen Warenlieferungen durch fehlerhafte Bauteile manipulieren und bei einer eigens festgestellten Gefährdungslage in ausländische IT-Systeme eindringen dürfen, um Produktionsabläufe zu sabotieren oder Server unbrauchbar zu machen. Damit würde der Dienst ausdrücklich auch zum Akteur verdeckter Sabotage. Solche Operationen werfen zusätzliche Fragen nach Fehlentscheidungen, Schäden für Unbeteiligte und internationaler Eskalation auf. [14]

Regierung stellt Handlungsfähigkeit über den Schutz der individuellen Freiheit

Die vorgesehene Vorabkontrolle besonders eingriffsintensiver Maßnahmen durch den Unabhängigen Kontrollrat und der Schutz des höchstpersönlichen Lebensbereichs sind notwendige Sicherungen. Sie beantworten jedoch nicht die politische Frage, wie weit staatliche Überwachungs- und Eingriffsmacht reichen soll. Heimliche Zugriffe auf private Geräte können tief in vertrauliche Kommunikation hineinreichen und auch Daten unbeteiligter Dritter erfassen. Werden dafür Sicherheitslücken offengehalten, bleiben diese

zugleich für kriminelle Angreifer nutzbar – ein Risiko, vor dem die GFF seit Langem warnt. Die Reform verlangt deshalb eine öffentliche Auseinandersetzung über wirksame Grenzen, individuelle Abwehrrechte und die Folgen staatlicher Cyberoperationen. Der Kabinettsbeschluss hat das parlamentarische Verfahren eröffnet.

Mehr Datenzugriffe verändern die Bedingungen, unter denen Menschen ihre Rechte verteidigen und psychisch unbelastet leben können. Die Regierung hat unmissverständlich deutlich gemacht, dass sie an wirksamen Kontrollen staatlicher Datenmacht nicht interessiert ist und staatliche Handlungsfähigkeit über den Schutz der individuellen Freiheit stellt.

Titelbild: Stokkete / Shutterstock

Mehr zum Thema:

Serie zu den Sozial-„Reformen“ – Folge I: Die Zerstörung des sozialen Friedens (Einführung)

Serie zu den Sozial-„Reformen“ – Folge II: Rente nach Kassenlage, Würde nach Vermögen

Serie zu den Sozial-„Reformen“ – Folge III: Armut unter Generalverdacht – wie aus sozialer Sicherung strafende Kontrolle wird

Serie zu den Sozial-„Reformen“ – Folge IV: Wie die Änderungen des Arbeitsrechts Grundrechte aushöhlen

Wohnen, Wärme und Infrastruktur: Wie die Bundesregierung am Volk vorbeiregiert (Serie zu den Sozial-„Reformen“ – Folge V)

Steuersenkungen, Deutschlandfonds, Industriestrom: Milliarden für das Kapital, aber nur „Hoffnung” für die Bürger (Serie zu den Sozial-„Reformen“ – Folge VI)

[«1] Bundesregierung (2026): *Entwurf eines Gesetzes zur Stärkung digitaler*

Ermittlungsbefugnisse in der Polizeiarbeit. Deutscher Bundestag, Drucksache 21/6132, 26. Mai.

[«2] Deutscher Bundestag (2026): *Geteiltes Echo zur Stärkung digitaler Ermittlungsbefugnisse*. Parlamentsnachrichten, hib 725/2026, 21. September.

[«3] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) (2026): *Digitale Ermittlungsbefugnisse*. Schriftliche Stellungnahme vom 2. Juni 2026. Deutscher Bundestag, Innenausschuss, Ausschussdrucksache 21(4)179.

[«4] Bundesverfassungsgericht (2023): *Urteil des Ersten Senats vom 16. Februar 2023 – 1 BvR 1547/19 und 1 BvR 2634/20: Automatisierte Datenanalyse*.

[«5] Bundesregierung (2025): *Entwurf eines Gesetzes zur Modernisierung des Bundespolizeigesetzes*. Deutscher Bundestag, Drucksache 21/3051, 3. Dezember.

[«6] Deutscher Bundestag, Innenausschuss (2026): *Beschlussempfehlung und Bericht zum Entwurf eines Gesetzes zur Modernisierung des Bundespolizeigesetzes*. Bundestagsdrucksache 21/6990, 8. Juli. Verfügbar unter: Originaldokument des Deutschen Bundestages (Zugriff: 22. September 2026).

[«7] Bundesregierung (2026a): *Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit*. Deutscher Bundestag, Drucksache 21/6132, 26. Mai.

[«8] Presse- und Informationsamt der Bundesregierung (2026): *Bundeskabinett beschließt Reform des Rechts der Nachrichtendienste*. Pressemitteilung 147, 12. August.

[«9] Falck, Marianne (2006): *Das Leben der Anderen*. Filmheft. Bonn: Bundeszentrale für politische Bildung.

[«10] Digitale Gesellschaft e. V. (2026): *Stellungnahme des Vereins Digitale Gesellschaft e. V. zur Vorratsdatenspeicherung*. Stellungnahme zum Referentenentwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren.

[«11] Sombetzki, P. und Vieth-Ditlmann, K. (2026): *Stellungnahme zu den Gesetzentwürfen zur Stärkung digitaler Ermittlungsbefugnisse und zu digitalen Ermittlungsmaßnahmen (BT-Drs. 21/6132, 21/6131 und 21/6806)*. 17. September 2026. Berlin: AW AlgorithmWatch gGmbH. Ausschussdrucksache 21(4)214 D, S. 7–8.

[«12] Bundesregierung (2026a): *Bundeskabinett beschließt Reform des Rechts der Nachrichtendienste*. Pressemitteilung Nr. 147 vom 12. August 2026. Berlin: Presse- und Informationsamt der Bundesregierung, Abschnitt 1 zur strategischen Aufklärung.

[«13] Bundesregierung (2026b): *Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts*. Bundesratsdrucksache 453/26 vom 14. August 2026. Berlin: Bundesrat, Artikel 2, § 60 BNDG-E, S. 132.

[«14] Informationsstelle Militarisierung (IMI) (2026): *BND: Sabotage*. IMI-Aktuell 2026/276, 30. April. Verfügbar unter: Originalbeitrag (Zugriff: 23. September 2026).