Stiftung
Neue
Verantwortung

Mai 2024 · Corbinian Ruckerbauer und Thorsten Wetzling

Informations-beschaffung mit der Kreditkarte

Wie nachrichtendienstliche Datenkäufe verfassungsrechtliche Mindeststandards unterlaufen

IN EIGENER SACHE

Wir ändern unseren Namen – aus Stiftung Neue Verantwortung (SNV) wird *interface*. Unsere Organisation wird zu einem europäischen Thinktank für Politik und Digitale Technologien.

Mehr dazu hier

interface

Inhalt

1. Einleitung 6

2. ADINT: Nachrichtendienste als Kunden auf dem boomenden Datenmarkt 8

2.1. Welche Akteure sind auf dem Datenmarkt aktiv? 8

2.2. Welche personenbezogenen Informationen sind auf dem Datenmarkt erhältlich? 10

2.3. Wie können Nachrichtendienste diese Informationen kaufen? 10

2.4. Wissensstand zur ADINT Praxis 13

2.5. Relevanz des Datenkaufs für die Nachrichtendienste 14

3. Zur Grundrechtsrelevanz des Kaufs von Daten 16

3.1. Die angebotenen Daten ermöglichen Einblicke in hochsensible Lebensbereiche 17

3.2. Der massenhafte Ankauf von Daten führt zu einer großen Streubreite des Eingriffs 18

3.3. Der Ankauf der Daten durch Nachrichtendienste erfolgt heimlich 20

3.4. Der Zugang für die Betroffenen zu effektivem Rechtsschutz ist beschränkt 21

3.5. Diskriminierungs- und Manipulationsrisiken durch den Datenkauf 22

3.6. Der Datenkauf begünstigt ein diffuses Überwachungsgefühl 23

3.7. Zusammenfassung 25

4. Ist die gesetzliche Grundlage für nachrichtendienstliche Datenkäufe mit verfassungsgerichtlichen Mindestanforderungen vereinbar? 26

4.1. Anforderungen an eine gesetzliche Grundlage für nachrichtendienstliche Datenkäufe 26

4.1.1. Bedarf es einer einfachgesetzlichen Grundlage? 26
4.1.2. Welche Elemente muss eine gesetzliche Grundlage enthalten? 28
4.1.3. Zwischenfazit 31

4.2. Genügt der aktuelle Rechtsrahmen für nachrichtendienstliche Datenkäufe den Mindestanforderungen? 32

4.2.1. Die Generalklausel als einzige Grundlage für Kauf, Speicherung und Verarbeitung von Daten 32

4.2.2. Spezifische, aber ungenügende Grundlage für die Übermittlung von gekauften Daten 35
4.2.3. Zusammenfassung 37

5. Anforderungen an die Kontrolle 38

5.1. Die Intensität der Grundrechtseingriffe bestimmt auch die erforderliche Kontrolltiefe 38

5.2. Ist eine gerichtsähnliche Vorabkontrolle für nachrichtendienstliche Datenkäufe nötig? 39

5.3. Qualitätskriterien der Kontrolle 40

5.3.1. Unabhängigkeit 40
5.3.2. Effektivität 41
5.3.3. Eigener Rechtsrahmen für die Kontrolle 42

5.4. Analyse und Bewertung des aktuellen Rechtsrahmens und der Praxis der Kontrolle 42

5.4.1. Ausreichende Kontrollbefugnisse der Kontrollgremien? 42
5.4.2. Ausreichende Kontrollpraxis? 46

5.5. Zwischenfazit: Unzureichende Kontrolle 48

6. Handlungsempfehlungen 49

6.1. Warum die Praxis nachrichtendienstlicher Datenkäufe grundlegende Veränderungen im Nachrichtendienstrecht und der Nachrichtendienstkontrolle erfordert 49

6.2. Konkrete Handlungsempfehlungen 51

6.2.1. Nehmt eine Systematisierung der Grundrechtseingriffe beim Datenkauf vor 51
6.2.2. Schafft Sicherungsmechanismen für Datenkäufe mit besonders schweren Auswirkungen auf Grundrechte 53
6.2.3. Schafft eine angemessene Kontrolle für nachrichtendienstliche Datenkäufe 55
6.2.4. Definiert Mindestanforderungen auch für den Kauf von Daten mit geringerer Grundrechtsrelevanz 56
6.2.5. Tauscht Euch mit Euren Kolleg:innen in anderen Ländern aus 57

7. Fazit 59

Die Autoren danken Hannah-Aeterna Borne, Lilly Goll, Luisa Seeling und Alina Siebert für konstruktives Feedback, wertvolle Recherchearbeiten und grafische Gestaltung. Die Autoren sind allein verantwortlich für den Inhalt.

Executive Summary

Auf dem Datenmarkt gekaufte Informationen werden für die Nachrichtendienste immer wichtiger. Datenhändler bieten dort mitunter Informationen an, die sie exklusiv an Nachrichtendienste als Kunden vertreiben (Tau, 2024a). Andere Datenhändler verkaufen Produkte, die zwar nicht allein auf Nachrichtendienste zugeschnitten sind, diese aber auch interessieren. Dazu zählen zum Beispiel Dateien mit hochsensiblen Informationen wie Wohnadressen, Gesundheitsinformationen, politische Überzeugungen, Interessenprofile oder Religionszugehörigkeit (Dachwitz, 2023b). Viele auf dem Datenmarkt erhältliche Produkte bieten den Diensten einen umfangreichen Zugang zu statischen und dynamischen, also kontinuierlich aktualisierten, Dateien. Sie lassen sich für ganz unterschiedliche Zwecke nutzen: Wer Informationen über Teilnehmende einer Demonstration benötigt, kann beispielsweise internetfähige Geräte, die sich zum Zeitpunkt der Versammlung in der Gegend befunden haben, über gekaufte Standortdaten identifizieren. Wer Mobilgeräte in Grenzgebieten aufspüren will, kann dies auf der Grundlage von auf dem Datenmarkt erworbenen Bewegungsdaten tun (vgl. Ng, 2022). Mit von Unternehmen angebotenen Anwendungen, die integrierte Datensätze aus dem Datenmarkt auswerten, lassen sich Nutzer:innen dauerhaft überwachen und deren Verhalten auf Auffälligkeiten analysieren.

Anders als in anderen westlichen Demokratien (Tau, 2023, 2024a) gibt es zwar noch keine konkreten, öffentlich bekannten Fälle, die belegen, wie deutsche Nachrichtendienste bei den versteckt oder offen agierenden Akteuren des Datenmarktes Datensätze gekauft oder abonniert haben. Doch es gibt gute Gründe, davon auszugehen, dass dies längst geschieht. Warum sonst sollte die Bundesregierung in ihrer Begründung zu den novellierten Vorschriften des BNDG[1] auf den „Ankauf [...] von umfänglichen Werbedatenbanken und anderen Datenbanken“ (Bundesregierung, 2023a, S. 43) abstellen?

In diesem Papier haben wir diese unterbelichtete Praxis (Kapitel 2) und deren Relevanz für den Grundrechtsschutz (Kapitel 3) genauer in den Blick genommen. Einige Formen des Datenkaufs stellen unserer Meinung nach einen erheblichen Eingriff in Grundrechte dar. Gemessen an den gebotenen Anforderungen an den Rechtsrahmen (Kapitel 4) und an die Kontrolle (Kapitel 5) ist der Status Quo unzureichend.

Im Unterschied zu anderen Methoden der nachrichtendienstlichen Informationsbeschaffung ist die hier beschriebene Praxis weder an ein Genehmigungsverfahren gebunden, noch wird die Verarbeitung von gekauften Daten im Nachhinein ausreichend kontrolliert. Datenkäufe bieten Nachrichtendiensten die Möglichkeit, an

1 Gesetz über den Bundesnachrichtendienst

Informationen zu gelangen, deren Erhebung mit anderen nachrichtendienstlichen Mitteln niemals gestattet gewesen wäre oder zumindest umfangreiche Genehmigungsverfahren vorausgesetzt hätte (ODNI, 2022, S. 13).

Der Ankauf von Werbedatenbanken sollte daher dringend einer besseren Regulierung und umfassenderen Kontrolle zugeführt werden. Der Gesetzgeber hat für den Sommer 2024 eine „wertungskonsistente Systematisierung der Regelungen zur Informationsbeschaffung“ (Bundesregierung, 2023b, S. 1) angekündigt. Schwere Grundrechtseingriffe sollten bei allen Methoden der Informationsbeschaffung einer ähnlichen Regelungs- und Kontrolldichte unterliegen. Bei der Praxis der nachrichtendienstlichen Datenkäufe, das zeigt dieser Impuls, ist dies noch nicht der Fall. Um den Weg zu einer verfassungskonformen Ausführung dieser nachrichtendienstlichen Beschaffungsmethode zu ebnen, schlagen wir vor:

- → eine Systematisierung der Grundrechtseingriffe beim Datenkauf vorzunehmen
- → Sicherungsmechanismen für Datenkäufe mit besonders schweren Auswirkungen auf Grundrechte zu schaffen
- → Mindestanforderungen auch für den Kauf von Daten mit geringerer Grundrechtsrelevanz zu definieren
- → den Austausch der deutschen Kontrollinstanzen mit ihren Kolleg:innen aus anderen Ländern zu intensivieren.

1. Einleitung

Die Bundesregierung plant in diesem Jahr eine große Reform des Nachrichtendienstrechts. Damit will sie im Koalitionsvertrag vereinbarte Vorhaben umsetzen. Das für die Reform federführende Bundesministerium für Inneres und Heimat hat schon einen Entwurf erarbeitet (Süddeutsche Zeitung, 2024).

Noch ist wenig über den genauen Inhalt der Reform bekannt. Die Bundesregierung hat aber im vergangenen Sommer angekündigt, sie wolle mit dieser Reform auch eine „wertungskonsistente Systematisierung der Regelungen zur Informationsbeschaffung" (Bundesregierung, 2023b, S. 1) vornehmen. Ein wesentliches Ziel dieser Systematisierung sollte sein, dass schwere Grundrechtseingriffe vergleichbaren Regelungs- und Kontrollvorgaben unterliegen, unabhängig davon, aus welcher Methode der nachrichtendienstlichen Informationsbeschaffung sie hervorgehen.

Wie wir in diesem Impuls über nachrichtendienstliche Datenkäufe zeigen, ist das derzeit mitnichten der Fall. Diese zunehmend bedeutsame Praxis sollte daher im Zuge der Reform dringend in den Blick genommen werden. Hier bietet sich dem Gesetzgeber eine wichtige Gelegenheit, den Grund- und Menschenrechtsschutz entscheidend zu verbessern. Noch bevor die Bundesregierung die große Reform des Nachrichtendienstrechts in den Bundestag einbringt, möchten wir dem Gesetzgeber in Erinnerung rufen, dass eine solche wertungskonsistente Systematisierung unbedingt voraussetzt, wesentliche Rechtslücken im Nachrichtendienstrecht und Defizite bei der Kontrolle nachrichtendienstlicher Tätigkeiten des Bundes zu identifizieren.[2]

In diesem Impuls richten wir den Blick auf die vielen Möglichkeiten der Nachrichtendienste, auf dem stetig wachsenden Datenmarkt umfassende Informationen kommerziell zu erwerben. Dass es dabei nicht ausschließlich um frei verfügbare Informationen geht und dass das Nachrichtendienstrecht und die Kontrollpraxis hier einiges aufzuholen haben, zeigen unter anderem die regulatorischen Bemühungen anderer Staaten (ODNI, 2024) und jüngere Berichte der Kontrollgremien aus den Niederlanden (CTIVD, 2021) und Norwegen (EOS-Committee, 2023, S. 15).

Grund genug für uns, den gegenwärtigen Wissensstand zu dieser Praxis, zu den wesentlichen Akteuren und einige Anwendungsbeispiele näher zu beleuchten (Kapitel 2). Danach steht die Frage im Raum, wie grundrechtsrelevant diese Praxis überhaupt sein kann und warum auch starke Eingriffe in Grundrechte aus dem Datenkauf

2 Mit Blick auf die anstehende Reform des Nachrichtendienstrechts haben wir auf der Internetseite www.nachrichtendienstreform-2024.de bereits Impulspapiere veröffentlicht, in denen die Kontrollbefugnisse und Kontrollpraxis von Aufsichtsgremien und der Rechtsrahmen des Militärischen Nachrichtenwesens der Bundeswehr thematisiert werden.

und der anschließenden Verarbeitung der Daten hervorgehen können (Kapitel 3). Im Anschluss klären wir, welche Regelungen der gegenwärtige Rechtsrahmen für diese Praxis vorsieht und warum er wesentlichen verfassungsrechtlichen Anforderungen nicht ausreichend gerecht wird (Kapitel 4). Die Defizite betreffen auch die Kontrolle. Auch hier klären wir zunächst, welche Anforderungen für die Kontrolle der nachrichtendienstlichen Informationsbeschaffung gelten. Es zeigt sich, dass die Befugnisse der verschiedenen Instanzen der Nachrichtendienstkontrolle in Deutschland und auch die uns bekannte Kontrollpraxis diesen Ansprüchen noch nicht genügen (Kapitel 5). Wir schließen unseren Impuls mit vier Kernforderungen an den Gesetzgeber, deren Umsetzung unserer Meinung nach den Weg zu einer verfassungskonformen Praxis dieser nachrichtendienstlichen Beschaffungsmethode ebnen kann (Kapitel 6).

2. ADINT: Nachrichtendienste als Kunden auf dem boomenden Datenmarkt

In diesem Kapitel richten wir den Fokus auf die Möglichkeiten der Informationsbeschaffung, die sich auf dem wachsenden Datenmarkt auch den deutschen Nachrichtendiensten bieten. Diese können dort auf direktem oder indirektem Wege personenbezogene Daten in unbekannter Größenordnung von Datenhändlern beziehen und tun dies wohl auch (Bundesregierung, 2023a, S. 42 f).[3] Um die Datentransaktionen zwischen Nachrichtendiensten und Datenhändlern besser zu verstehen, beleuchten wir zunächst die Akteure und die Funktionsweise des Datenmarktes. Dieses Papier beschäftigt sich nicht mit der wichtigen Frage, ob diese Daten überhaupt käuflich erwerbbar sein sollten, und welche legislativen Maßnahmen ergriffen werden sollten, um die fragwürdigen Datenerhebungspraktiken der Datenhändler zu unterbinden. Damit beschäftigt sich eine Vielzahl von Papieren, auf die wir an dieser Stelle verweisen (Nießen, 2024; Ryan & Christl, 2023; Ruschemeier, 2023).

2.1. Welche Akteure sind auf dem Datenmarkt aktiv?

Der Datenmarkt ist ein über Jahre gewachsenes Netz unterschiedlicher Akteure, die offen oder verschleiert datenbezogene Produkte oder Dienstleistungen anbieten. Eine zentrale Rolle spielen dabei die Datenhändler.

Sie interessieren sich für personenbezogene Daten von Verbraucher:innen, die bei der Nutzung von Apps, Webseiten, sozialen Medien und internetfähigen Geräten anfallen. Diese Daten erwerben die Datenhändler von Handels- und Dienstleistungsunternehmen, Kreditkartenfirmen und Zahlungsdienstleistern – oder von anderen Datenhändlern (Dachwitz, 2023a; Forbrukerrådet, 2020, S. 19). Zudem erfassen Datenhändler systematisch öffentlich zugängliche Quellen, wie beispielsweise Beiträge in sozialen Medien oder journalistischen Inhalten, und extrahieren personenbezogene Daten.

Eine wichtige Rolle kommt dabei den Daten zu, die aus dem Markt für gezielte Werbeanzeigen stammen. In sogenannten Real-Time-Bidding-Auktionen (RTB) können Werbetreibende zielgruppengenau ihre Anzeigen steuern. Hierbei können die Bietenden Informationen über die Nutzer:innen von Webseiten und Apps erhalten. Dazu gehören unter anderem der Standort der Personen, die besuchte Website oder die genutzte App, sowie weitere Informationen über die Nutzung – beispielsweise wie

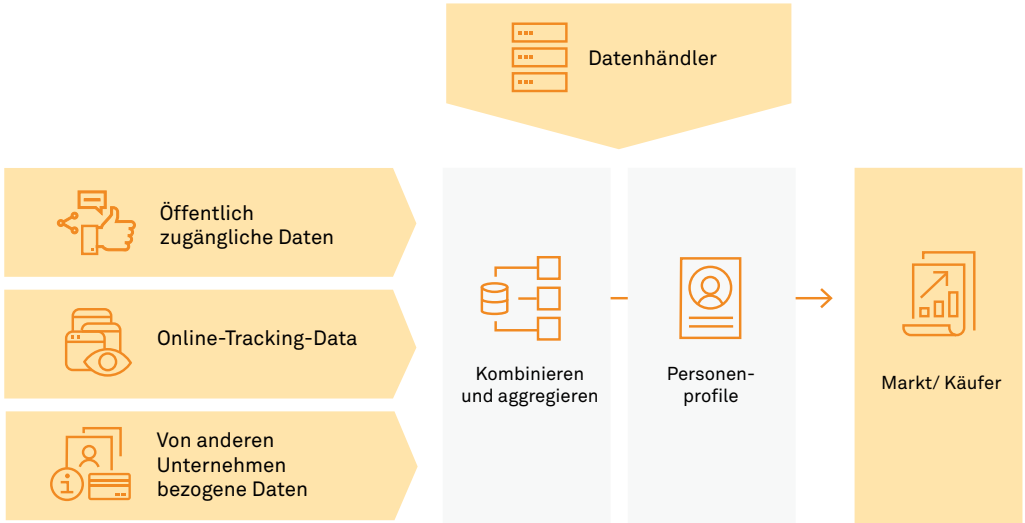
3 Für den BND wird diese Praxis in der Begründung zum Gesetzesentwurf explizit erwähnt, für BAMAD und BfV ist dies ebenfalls anzunehmen.

lange die Person auf der Website verweilt. Zudem werden einzigartige Nutzerkennungen wie smartphonespezifische Werbe-IDs übermittelt.[4] Das ermöglicht das Zusammenführen von Erkenntnissen aus unterschiedlichen RTB-Auktionen.

Die Teilnahme an RTB-Verfahren ist dabei weitgehend unbeschränkt. Deshalb können nicht nur Unternehmen, die ein Produkt bewerben wollen, auf digitale Anzeigeflächen in den Apps der Nutzer:innen bieten, sondern auch Unternehmen, deren Hauptgeschäftsmodell der Handel mit Daten ist. Und so stammt ein gewichtiger Anteil der auf dem Datenmarkt erhältlichen Informationen aus diesem RTB-Verfahren. Daher rührt auch der Name ADINT (Advertising Intelligence) für die Praxis des Datenkaufs der Nachrichtendienste.[5]

Diese aus sehr unterschiedlichen Quellen stammenden Daten werden von den Datenhändlern auch untereinander gehandelt, kombiniert, aggregiert und analysiert (Forbrukerrådet, 2020, S. 19). Dieses Zusammentragen und Analysieren der unterschiedlichen kleinteiligen Informationen ist die entscheidende Dienstleistung der Datenhändler. Auf dem Datenmarkt verkaufen die Datenhändler diese verarbeiteten Daten dann an Dritte (Forbrukerrådet, 2020, S. 18).

Rolle der Datenhändler im Datenmarkt



4 Smartphone-Betriebssysteme wie Android und iOS generieren diese Kennungen. Nutzer:innen ist es möglich, diese Werbe-ID zurückzusetzen, oder zu löschen.

5 Zur genaueren Funktionsweise dieses Real Time Bidding-Verfahrens siehe: Ryan & Christl (2023)

2.2. Welche personenbezogenen Informationen sind auf dem Datenmarkt erhältlich?

Zahlreiche Recherchen von Journalist:innen und Forscher:innen haben in den vergangenen Jahren gezeigt, wie breit das Spektrum an verfügbaren Informationen auf dem Datenmarkt ist und wie unterschiedlich die Quellen sind, aus denen diese stammen (Forbrukerrådet, 2020; Ryan & Christl, 2023; Sherman et al., 2023). Für sich genommen mag in den einzelnen erfassten Datenpunkten nicht immer eine besonders schützenswerte Information über eine betroffene Person enthalten sein. Das Zusammentragen der vielen, aus unterschiedlichen Quellen stammenden Informationen, beispielsweise Bewegungsdaten und Wohnadressen, erlaubt aber das Erstellen detaillierter Profile von Personen und Bevölkerungsgruppen (Reviglio, 2022, S. 11; Twetman & Bergmanis-Korats, 2021, S. 10). Die erhältlichen Daten umfassen auch sehr sensible und besonders schützenswerte Informationen wie persönliche Interessen und Vorlieben, sexuelle Orientierung, Gesundheitsdaten, die Zugehörigkeit zu marginalisierten Gruppen, politische Überzeugungen und religiöse Weltanschauung oder die Vermögensverhältnisse der Betroffenen (Christl & Toner, 2024; Dachwitz, 2023a; Ryan & Christl, 2023, S. 15 ff). Das betrifft nicht nur einzelne Personen, die von den Datenhändlern besonders ins Visier genommen werden. Über nahezu jede:n sind solche Informationen erhältlich (ODNI, 2022, S. 12). Recherchen zum Unternehmen XANDR beispielsweise haben gezeigt, welche großen Datenmengen schon einzelne Unternehmen zum Kauf anbieten: 650 000 Eigenschaftsprofile, denen jeweils Tausende bis Millionen von Personen zugeordnet sind, konnten von *XANDR* bezogen werden (Dachwitz, 2023b). In einem anderen gut dokumentierten Fall eines Datenhändlers, *Live Ramp*, werden die Daten von 700 Millionen Konsument:innen geführt (Christl & Toner, 2024, S. 5). Und diese Beispiele beschreiben nur zwei von unzähligen Unternehmen auf einem kaum zu überblickenden, milliardenschweren Markt.[6]

2.3. Wie können Nachrichtendienste diese Informationen kaufen?

Zunächst haben Nachrichtendienste die Möglichkeit, durch die Teilnahme am RTB-Verfahren und durch das Schalten von Werbeanzeigen selbst Informationen zu sammeln. Technisch ist das keine große Herausforderung. Schon 2017 haben Forscher:innen der Washington University gezeigt, wie wenige Ressourcen benötigt werden, um auf diesem Weg Informationen über Personen zu beschaffen (Vines et al., 2017).

6 Neben diesen spezialisierten Datenhändlern bieten auch andere Unternehmen, deren Kerngeschäft eigentlich ein anderes ist, Daten zum Kauf an. Und abseits von Unternehmen können auch Einzelpersonen legal oder illegal beschaffte Informationen zum Kauf anbieten.

Anwendungsbeispiel 1 – individuelles Tracking über das Schalten von Werbeanzeigen: Über das gezielte Schalten von Werbeanzeigen können Standortinformationen und Erkenntnisse über die verwendeten Apps und deren Nutzung ermittelt werden. Werden mehrere Nutzer:innen auf diese Weise überwacht, können durch die Nutzungsmuster von Messenger-Apps auch Erkenntnisse über Kommunikationsvorgänge extrapoliert werden. Wie niedrigschwellig – und folgenreich – diese Form der Überwachung sein kann, zeigt der Fall eines homosexuellen Priesters in den USA, der auf diese Weise öffentlich geoutet wurde: Eine Gruppe von erzkonservativen Angehörigen der katholischen Kirche gab Berichten zufolge vier Millionen Dollar aus, um über solche aus dem RTB-Verfahren gewonnenen Daten kompromittierende Erkenntnisse über Kirchenangestellte zu sammeln. Dafür kaufte die Gruppe unter anderem Informationen über Nutzer:innen der vornehmlich von queeren Personen genutzten Dating-App Grindr und wertete sie aus (Boorstein & Kelly, 2023).

Für die Nachrichtendienste bietet dieses Vorgehen die Möglichkeit, ein umfassendes Bewegungsprofil einer beobachteten Person zu erstellen

Statt diese Daten durch Teilnahme am RTB-Verfahren selbst zu erheben, können Nachrichtendienste diese Informationen aber auch über spezialisierte Datenhändler beziehen. Das können Datenhändler sein, die ihre Angebote vorrangig auf werbetreibende Unternehmen ausrichten. Einige schneiden ihre Angebote aber auch speziell auf die Bedürfnisse von Sicherheitsbehörden zu (Brayne, 2020, S. 25). Und diese machen zunehmend Gebrauch von den kommerziellen Angeboten (Tau, 2024a).

Eine Möglichkeit ist es, statische Daten zu kaufen. Am Beispiel von Angehörigen der US-Streitkräfte verdeutlichten Forscher:innen der Duke University, wie einfach Daten über Individuen erworben werden können (Sherman et al., 2023).

Anwendungsbeispiel 2 – Einkauf fertiger Datensätze: Datenhändler bieten Datensätze mit personenbezogenen Daten an. In der genannten Studie konnten die Forscher:innen Listen von Personenprofilen mit E-Mail-Adressen und Handynummern, Wohnadressen, Gesundheitsinformationen, politischen Überzeugungen, Interessensprofilen, Religionszugehörigkeit und anderen Informationen erwerben. Auch Standortdaten können auf diesem Weg erworben werden. Die Kosten pro Person lagen beim Kauf dieser Daten bei allen in der Studie besprochenen Datenhändlern im Cent-Bereich. Auch in Europa gibt es Beispiele für Datenhändler, die solche personenbezogenen Daten anbieten. In den Niederlanden erhielt ein Rechercheteam einen Datensatz mit Bewegungsdaten von vier

Millionen niederländischen Telefonen – verbunden mit der jeweils einzigartigen Werbe-ID (Dachwitz & Meineck, 2024).

Interessieren sich Nachrichtendienste dafür, welche Personen an einer Demonstration teilgenommen haben, können sie so eine Zusammenstellung aller Werbe-IDs der internetfähigen Geräte, die sich zum Zeitpunkt der Versammlung in der Gegend befunden haben, kaufen.

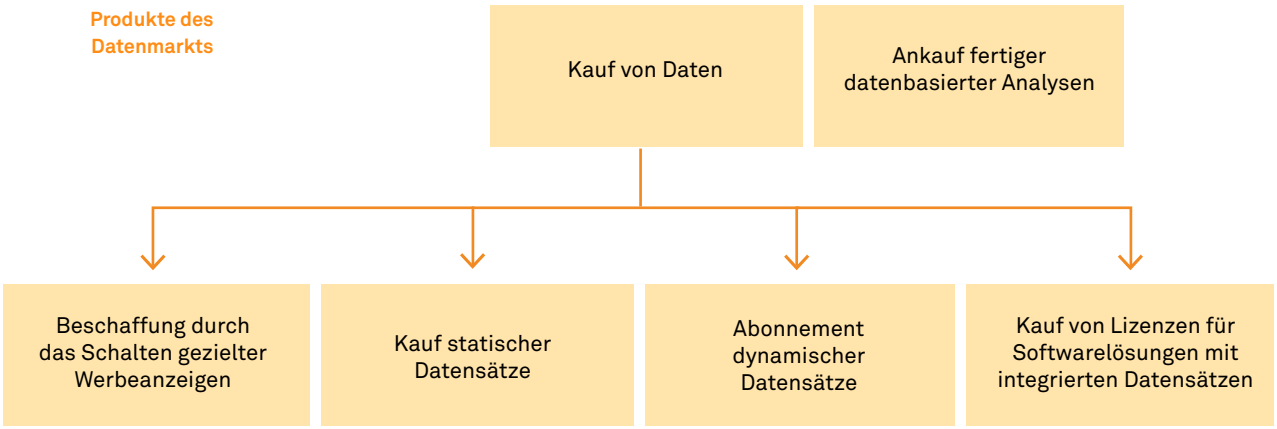
Alternativ kann der Zugang zu dynamischen Datensätzen abonniert werden, die stetig aktualisiert werden. Ein konkretes Beispiel der US Homeland Security veranschaulicht eine Weise der Nutzung solcher Live-Daten. Um illegale Grenzübertritte festzustellen, wurden täglich Bewegungsdaten von Mobilgeräten in Grenzgebieten abgerufen, um gewählte Routen abseits von Straßen zu erkennen (vgl. Ng, 2022). Angeboten werden auch Softwareprodukte, die solche Live-Daten über unterschiedliche Datenquellen beschaffen und aufbereiten. Den Sicherheitsbehörden wird dann ein Produkt angeboten, in dem die jeweils erwünschten Erkenntnisse ohne weiteren Analyseaufwand abgerufen werden können.

Anwendungsbeispiel 3 – Einkauf von Softwarelösungen mit integrierten Datensätzen: *Patternz*, von einer israelischen Firma beworbenes Produkt, wirbt damit, Daten aus dem RTB-Markt sowohl für die Analyse in Echtzeit als auch im Nachhinein zu nutzen (Sovereign Systems, ohne Jahr). So können nach Angaben der Firma umfassende Informationen über einzelne Nutzer:innen abgefragt werden. Dazu gehören beispielsweise Standortdaten, benutzte Apps oder Informationen über Personen, die sich häufig in der Nähe des Individuums aufhalten. Auf Grundlage der Standortdaten können laut der Werbeunterlagen der Firma mit der Software auch Gruppen von Menschen identifiziert werden, die sich häufig am selben Ort aufhalten. Nutzer:innen können dauerhaft getrackt werden und es kann eine Benachrichtigung eingestellt werden, sobald bestimmte Person(en) sich an einem bestimmten Standort aufhalten. Zudem wirbt die Firma mit der Möglichkeit, in den Daten auffälliges Verhalten zu identifizieren und die Sicherheitsbehörden auf die entsprechenden Individuen oder Gruppen aufmerksam zu machen.

Es braucht nicht viel Fantasie, um sich weitere Szenarien vorzustellen, in denen diese Software für die Nachrichtendienste von Interesse wäre.

In dem genannten Beispiel sind Zweifel an der Zuverlässigkeit der Aussagen des Unternehmens angebracht, da es sich um an Sicherheitsbehörden gerichtete Werbeunterlagen handelt. Recherchen, die sich mit der Software beschäftigten, konnten diese Angaben nicht überprüfen (Ryan & Christl, 2023, S. 13). Angesichts der auf dem Datenmarkt angebotenen Informationen erscheinen die Angaben zu den Grundfunktionen dieser Software aber durchaus plausibel.

Neben den genannten Konstellationen für Datentransaktionen wäre auch denkbar, dass fertige Analyseergebnisse eingekauft werden, die auf der Auswertung käuflich erwerbbarer Daten basieren.[7]



2.4. Wissensstand zur ADINT Praxis

Jüngste Recherchen zeigen, wie systematisch auch Sicherheitsbehörden und Nachrichtendienste Daten der Werbeindustrie kaufen. Besonders gut belegt ist die Praxis des Ankaufs von Daten von kommerziellen Anbietern in den USA (Tau, 2024b). Nachrichtendienste kaufen diese Daten und betrachten sie als schnell wachsenden und zunehmend bedeutenden Teil ihres Informationsumfelds (ODNI, 2022). Die Defense Intelligence Agency (DIA) hat in der Vergangenheit ohne richterliche Anordnung massenhaft Standortdaten von Nutzer:innen inner- und außerhalb der USA gekauft und diese analysiert. Dasselbe gilt für die National Security Agency (NSA) (Wyden, 2024).

7 Verschiedene denkbare Szenarien an der Schnittstelle zwischen Datenhändlern und Nachrichtendiensten beschreibt auch Sosna (2024, S. 54). Zudem könnten Daten auch freiwillig und ohne monetäre Gegenleistung von Unternehmen an die Sicherheitsbehörden herausgegeben werden. Die Grundrechtsrelevanz ändert sich dadurch kaum und auch hier wäre eine gesetzliche Regelung geboten. Siehe auch Wetzling und Dietrich (2022).

Auch in europäischen Staaten sind Beispiele für nachrichtendienstliche Datenkäufe zu finden. So hat die norwegische Aufsichtsbehörde EOS festgestellt, dass der militärische Nachrichtendienst massenhaft personenbezogene Daten gekauft hat, und bemängelt, dass hierfür keine ausreichende Gesetzesgrundlage vorliege (EOS-Committee, 2023, S. 15). Auch niederländische Nachrichtendienste nutzen Informationen, die sie käuflich erworben haben (CTIVD, 2021). Unter anderem analysieren sie Standortdaten, die bei der Versteigerung von digitalen Werbeanzeigen anfallen. Die niederländische Aufsichtsbehörde CTIVD mahnte hier ebenfalls dringenden Handlungsbedarf hinsichtlich der gesetzlichen Bestimmungen an, da die existierenden Regelungen angesichts der mit der Praxis verbundenen schwerwiegenden Grundrechtseingriffe keine ausreichenden Sicherungsmechanismen vorsehen.

Auch in Deutschland nutzen Nachrichtendienste offenbar die Möglichkeit, Daten käuflich zu erwerben. Über den konkreten Einsatz ist wenig bekannt und auch den öffentlichen Berichten der zuständigen Kontrollstellen ist, wie in Kapitel 5.4. besprochen wird, kaum etwas zu diesem Thema zu entnehmen. Aus den Erläuterungen zur BNDG-Novelle von 2023 geht aber hervor, dass zumindest der Bundesnachrichtendienst (BND) sich auf dem Datenmarkt Informationen beschafft. So beschreibt die Bundesregierung hier im Zusammenhang mit §10a Abs. 1, dass „spezielle Datenbanken“ genutzt werden, die auch „zahlungspflichtige Angebote“ umfassen können (Bundesregierung, 2023a, S. 42). Zu §10a Abs. 2 wird dann erläutert, dass dieser Absatz sich auch auf die „Übermittlung von Daten aus dem Ankauf z.B. von umfänglichen Werbedatenbanken und anderen Datenbanken mit vergleichbarer Eingriffsintensität“ beziehen (Bundesregierung, 2023a, S. 43). In den gleichzeitig neugefassten BVerfSchG[8] und MADG[9] finden sich auch jeweils Paragraphen zu „personenbezogenen Daten aus allgemein zugänglichen Quellen“. Hier wird die Praxis des Datenkaufs in der Begründung der Gesetzesänderung zwar nicht explizit benannt (Bundesregierung, 2023b). Es ist nach Auffassung der Autoren aber davon auszugehen, dass das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für den Militärischen Abschirmdienst (BAMAD) sich ebenfalls dieses Instruments bedienen.

2.5. Relevanz des Datenkaufs für die Nachrichtendienste

Warum kaufen Nachrichtendienste überhaupt Daten von kommerziellen Anbietern? Welche Vorteile bieten sich ihnen dabei? Die Arbeit der Nachrichtendienste verändert sich seit Anfang des letzten Jahrzehnts durch den zunehmenden Anteil an

8 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
9 Gesetz über den militärischen Abschirmdienst

verschlüsselter Kommunikation. Zugang zu Inhaltsdaten aus vielen Kommunikationsvorgängen sind so schwieriger zu ermitteln.[10]

Der Kauf von Daten bietet eine neue Möglichkeit der Datenbeschaffung für die Nachrichtendienste. Die Menge und Granularität der auf diesem Weg verfügbaren Informationen nimmt dabei stetig zu. Das liegt an der Verbreitung internetbasierter Dienstleistungen, mobiler Endgeräte wie Smartphones und der wachsenden Zahl von mit dem Internet verbundenen Gegenständen des alltäglichen Gebrauchs sowie der zunehmenden Dichte von Sensoren im öffentlichen Raum. Unternehmen verfügen so über Datenbanken, in denen millionenfach Profile von einzelnen Personen geführt werden (Christl & Toner, 2024, S. 4). Für die Nachrichtendienste sind diese Daten attraktiv.

Hinsichtlich ihrer Aussagekraft stehen die kommerziell erhältlichen Daten beispielsweise den im Rahmen der Vorratsdatenspeicherung von Telekommunikationsdaten zur Speicherung vorgesehenen Daten in nichts nach (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345): Diese Art der Datenspeicherung ist umstritten und wird in Deutschland derzeit nicht mehr praktiziert. Bei den käuflich erwerbbaren Daten kommen zudem, wie in Kapitel 2.2 beschrieben, noch Informationen wie die Zugehörigkeit der betroffenen Person zu marginalisierten Gruppen, ihre Charaktereigenschaften, Vermögensverhältnisse und ihr Konsumverhalten aus einer Vielzahl von Quellen in nahezu unbegrenzter Menge dazu. Das erhöht die Aussagekraft der auf dem Datenmarkt erworbenen Daten erheblich. Aufgrund der immer leistungsfähigeren Datenauswertungsmethoden und der wachsenden Rechenleistung werden die Erkenntnisse, die aus solchen Daten extrahiert werden können, noch weiter wachsen (C & Carter, 2023).

Und derzeit bietet sich ein gewichtiger Vorteil für die Nachrichtendienste, wenn sie Daten kaufen. Während andere Beschaffungsmethoden wie die strategische Fernmeldeaufklärung seit den Snowden-Enthüllungen mit gesetzlichen Einschränkungen versehen werden und versucht wird, die Einhaltung der gesetzlichen Vorgaben durch unabhängige Kontrollgremien sicherzustellen, sind die Sicherungsmechanismen beim Kauf von Daten rudimentär. So können elementare rechtsstaatliche Anforderungen an Grundrechtseingriffe umgangen werden (Cameron, 2023; Tau, 2024b). Auch kürzlich veröffentlichte interne Dokumente der US-Regierung zeigen, dass durch den massenhaften Datenkauf Informationen erworben werden können, deren direkte Erhebung den Sicherheitsbehörden niemals gestattet wäre oder zumindest umfangreiche Genehmigungsverfahren zur Voraussetzung hätte (ODNI, 2022, S. 13).

10 Zugleich wächst das absolute Ausmaß der über das Internet abgewickelten Kommunikationsvorgänge rasant. Über die weiter zugänglichen Metadaten lassen sich auch aus verschlüsselten Kommunikationsvorgängen wertvolle Erkenntnisse gewinnen, vor allem wenn die massenhafte Erfassung dieser Daten und zunehmend leistungsfähige Datenanalysewerkzeuge kombiniert werden. Die rechtlichen Anforderungen und die angelegte Kontrolle sind hier zudem derzeit deutlich schwächer als bei den im Rahmen der Fernmeldeaufklärung erfassten Inhaltsdaten (Wetzling, 2024, S. 8).

3. Zur Grundrechtsrelevanz des Kaufs von Daten

Wenn deutsche Nachrichtendienste personenbezogene Daten bei Datenhändlern kaufen, greifen sie in unterschiedliche Grundrechte ein. Welche Grundrechte jeweils betroffen sind, hängt davon ab, welche Daten beschafft werden und wie sie verwendet werden.

Werden Standortdaten erworben, kann eine Vielzahl von Grundrechten betroffen sein. Da Bewegungsprofile, auch wenn sie als anonymisierte Daten angeboten werden, sehr einfach der zugehörigen Person zugeordnet werden können, ist der Eingriff in das Recht auf informationelle Selbstbestimmung offensichtlich. Aus diesen Bewegungsprofilen lassen sich umfassende weitere Erkenntnisse ableiten.

Im Anwendungsbeispiel 1 in Kapitel 2.4. wurde zudem gezeigt, dass über gezielte Werbeanzeigen beispielsweise auch Rückschlüsse auf Kommunikationsvorgänge zwischen unterschiedlichen Personen gezogen werden können. Wie bei der Erhebung von Verbindungsdaten von Telefonaten (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345) kann also auch hier ein Eingriff in das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes vorliegen.

Je nach Art der erfassten Daten und deren Verwendung können sich auch Auswirkungen auf andere Grundrechte ergeben. Wie Anwendungsbeispiel 2 verdeutlicht, können durch den Kauf von Standortdaten beispielsweise systematisch die Teilnehmenden einer Demonstration erfasst werden. Hieraus können Einschüchterungseffekte für potenzielle Demonstrationsteilnehmende entstehen, die unter Umständen einen Eingriff in das Recht auf Versammlungsfreiheit darstellen können.

Auch das Recht auf Pressefreiheit kann betroffen sein: Werden Bewegungsprofile beispielsweise von Journalist:innen aus käuflich erworbenen Daten extrahiert, können Rechercheaktivitäten detailliert nachvollzogen und Quellen offengelegt werden.

Die Liste der hier genannten Grundrechte, die potenziell von der Praxis des nachrichtendienstlichen Datenkaufs betroffen sind, ist dabei nicht abschließend. Im Folgenden erörtern wir unterschiedliche Aspekte, die begründen, warum mit dem Datenkauf mitunter besonders schwere Grundrechtseingriffe verbunden sind.[11]

11 Wie später in den Kapiteln 4 und 5 erläutert wird, wirkt sich das Eingriffsgewicht auf die Anforderungen an die Ausgestaltung des gesetzlichen Rahmens und die Kontrolle aus.

3.1. Die angebotenen Daten ermöglichen Einblicke in hochsensible Lebensbereiche

Wie in Kapitel 2.2. illustriert, sind auf dem Datenmarkt hochsensible personenbezogene Daten erhältlich. Gestützt auf diese Daten können problemlos umfassende und granulare Persönlichkeitsprofile erstellt werden. In anderen Kontexten, nämlich in Urteilen zur Vorratsdatenspeicherung und zur Bestandsdatenauskunft, hat das Bundesverfassungsgericht (BVerfG) festgehalten: Bereits wenn Daten die Erstellung von genaueren Bewegungs- und Verhaltensprofilen ermöglichen, stellt deren Erhebung und Verarbeitung einen schweren Grundrechtseingriff dar (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 212; BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 - 1 BvR 2634/20, Rn. 1-178, Abs. 73).

Ebenfalls im Zusammenhang mit der Vorratsdatenspeicherung argumentierte der Europäische Gerichtshof (EuGH), dass die Verkehrs- und Standortdaten Aufschluss „über eine Vielzahl von Aspekten des Privatlebens der Betroffenen, einschließlich sensibler Informationen wie sexuelle Orientierung, politische Meinungen, religiöse, philosophische, gesellschaftliche oder andere Überzeugungen sowie den Gesundheitszustand“ (EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – Space-Net u.a., Rn. 61) geben können. Das Gericht betonte außerdem, dass man durch die Analyse dieser Daten präzise Rückschlüsse auf das Privatleben der Betroffenen ziehen kann, wie die „Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen dieser Personen und das soziale Umfeld, in dem sie verkehren“ (EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – Space-Net u.a., Rn. 61). Diese Aussagen sind zumindest für bestimmte angebotene Informationen auf dem Datenmarkt ebenso zutreffend. Häufig gehen sie in ihrer Aussagekraft noch darüber hinaus.

Auch Daten, die den Kernbereich privater Lebensgestaltung betreffen, werden auf dem Datenmarkt zum Kauf angeboten. Dieser verfassungsrechtlich besonders geschützte Bereich umfasst „innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art“ und auch „Gefühlsäußerungen und Ausdrucksformen der Sexualität“ (*Urteil des Ersten Senats vom 03. März 2004, 1 BvR 2378/98 -, Rn. 1-373*, Abschn. 120). Zur Entfaltung der Persönlichkeit in diesem Bereich gehört nach Auffassung des BVerfG die Möglichkeit, diese Dinge zum Ausdruck zu bringen, „und zwar ohne Angst, dass staatliche Stellen dies überwachen“ (*Urteil des Ersten Senats vom 03. März 2004, 1 BvR 2378/98 -, Rn. 1-373*, Rn. 120).

Erkenntnisse, die für sich genommen nicht diesem besonders geschützten Bereich zugerechnet werden können, können nach Kombination mit anderen Daten, beispielsweise aus anderen Methoden der Informationsbeschaffung, eine Relevanz für den Kernbereich ergeben.

Wenn Sicherheitsbehörden beispielsweise Bewegungsprofile der Nutzer:innen von Dating-Apps kaufen können, besteht berechtigter Grund zur Annahme, dass sie hieraus Erkenntnisse generieren können, die diesen von der Verfassung besonders geschützten Bereich betreffen. Auch das erhöht das Eingriffsgewicht. Hinzu kommt noch der Aspekt der großen Missbrauchsgefahr solcher sensibler Informationen (ODNI, 2022, S. 12).

Häufig wird eingewendet, die auf dem Datenmarkt angebotenen Informationen seien anonymisiert und deren Erwerb und Verwendung daher unproblematisch. Eine Deanonymisierung ist aber nahezu immer technisch möglich und häufig auch nur mit einem sehr geringen Aufwand verbunden (ODNI, 2022, S. 5; Sherman et al., 2023, S. 13; Tau, 2024b, S. 8; Vines et al., 2017). Besonders deutlich lässt sich das an den Bewegungsprofilen von Nutzer:innen erkennen, die sich leicht aus den angebotenen Daten erstellen lassen. Aus solchen Profilen lassen sich in der Regel sehr einfach der Wohn- und Arbeitsort einer Person herauslesen. Und ausgehend von diesen Informationen ist eine genaue Identifizierung der zum Bewegungsprofil gehörenden Person ein Leichtes.

3.2. Der massenhafte Ankauf von Daten führt zu einer großen Streubreite des Eingriffs

Die angebotenen Daten lassen aber nicht nur Rückschlüsse auf sensible und schützenswerte Informationen zu, sie liegen auch über nahezu jeden Menschen vor (ODNI, 2022, S. 14). Es ist davon auszugehen, dass umfassende Informationen über fast jede Person auf diesem Weg erworben werden können. Nachrichtendiensten mit Zugriff auf diese Daten bietet sich ein mit der anlasslosen Vorratsdatenspeicherung vergleichbares, schier unbegrenztes Reservoir an Informationen über jede:n Bürger:in.

Eine große Streubreite erhöht gemäß der einschlägigen Rechtsprechung des BVerfG die Schwere des Grundrechtseingriffs in empfindlichem Maße.[12] Denn auch hier wird, ohne dass eine Ausweichmöglichkeit für die Bürger:innen besteht, eine große Menge an Daten „ohne Anknüpfung an ein zurechenbares vorwerfbares Verhalten“ (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345,

12 Im Urteil *Bestandsdatenauskunft II* hat das BVerfG festgestellt, dass die Regelung schon deshalb ein nicht unerhebliches Eingriffsgewicht hat, da auf „annähernd flächendeckend vorrätig gehaltenen Daten zugegriffen“ werden kann (BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020, 1 BvR 1873/13 -, Rn. 39).

Rn. 219) erfasst. In Zusammenhang mit der strategischen Telekommunikationsüberwachung betonte das BVerfG in gleicher Weise, das Eingriffsgewicht werde dadurch gesteigert, dass die Streubreite hoch sei und so jede Person anlasslos betroffen sein könne (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 150).

Die Sammlung der Daten durch Datenhändler ist völlig losgelöst vom Verhalten der Bürger:innen und nicht auf einen bestimmten Personenkreis begrenzt. Dieser Datenerfassung zu entgehen ist nur sehr schwer möglich, denn die Nutzung digitaler Technologien ist mittlerweile Grundvoraussetzung für gesellschaftliche Teilhabe. Und gleichzeitig führt sie zwangsläufig dazu, dass die anfallenden Daten erfasst und kommerzialisiert werden.

Hinzu kommt: Beim Erwerb von Datensammlungen durch die Nachrichtendienste werden in der Regel nicht Informationen über einzelne Personen gekauft. Stattdessen wird, wie in Anwendungsbeispiel 2 beschrieben, eine große Menge personenbezogener Daten erworben. Die benötigten Daten werden dann herausgefiltert bzw. mit weiteren Daten aus anderen Formen der nachrichtendienstlichen Informationsbeschaffung trianguliert.[13]

Die Streubreite ist insbesondere vor dem Hintergrund der neuen Möglichkeiten zur Auswertung großer Datenmengen bedenklich. Zunehmend leistungsfähige Werkzeuge, beispielsweise zur Analyse unstrukturierter Daten, ermöglichen es, sensible Erkenntnisse aus Informationen zu generieren, die bisher verborgen blieben (C & Carter, 2023).

Durch die Erfassung von personenbezogenen Daten in behördlichen Systemen besteht immer auch die Gefahr, dass die betroffenen Personen Ziel weiterführender Ermittlungsmaßnahmen werden. Das kann auch dann schon der Fall sein, wenn das Verhalten einer Person keinerlei Anlass dazu gegeben hat und sich der oder die Betroffene nur zufällig an einem bestimmten Ort aufgehalten hat (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 219). Gibt es zum Beispiel einen konkreten Verdacht gegen eine bestimmte Person und wird ein Datensatz von Bewegungsprofilen von mehreren Tausend Menschen erworben, kann die jeweilige Behörde versuchen, das Bewegungsprofil der verdächtigen Person herauszufiltern. Wie in Anwendungsbeispiel 3 beschrieben, können auch automatisierte Verfahren verwendet werden, um auffällige Muster zu identifizieren. Bei einer solchen automatisierten Auswertung der Daten steigt die Wahrscheinlichkeit,

13 Werden aber von spezialisierten Firmen schon fertige Analysen eingekauft, die wiederum auf den oben beschriebenen Daten basieren, so liegt die große Streubreite des Eingriffs zwar nicht beim Nachrichtendienst vor, stattdessen sind diese ungezielten Grundrechtseingriffe aber vorgelagert bei der Verarbeitung durch das Unternehmen gegeben.

dass Personen, die sich nur rein zufällig in dieser Datensammlung befinden, Ziel von weiteren Ermittlungsmaßnahmen werden (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 212).

Wie schwer es gemeinhin ist, sich dieser Art der Datenverarbeitung zu entziehen, lässt sich daran erkennen, dass präzise Standortdaten und anderweitige sensible Informationen auch von hochrangigen politischen Akteuren und Militärangehörigen gekauft werden können (Ryan & Christl, 2023). Wenn also selbst dort, wo die nationale Sicherheit betroffen ist und sowohl die Organisationen als auch deren Beschäftigten den Schutz personenbezogener Daten priorisieren, schützenswerte Daten von Datenhändlern gekauft werden können, dann ist es für die Allgemeinheit sicher noch schwieriger, dieser Datenerfassung zu entgehen (van den Berg, 2024; Sherman et al., 2023).

3.3. Der Ankauf der Daten durch Nachrichtendienste erfolgt heimlich

Auch die Heimlichkeit einer Informationsbeschaffung wirkt sich verstärkend auf das Eingriffsgewicht aus. Nach der Rechtsprechung des BVerfG und des Europäischen Gerichtshof für Menschenrechte (EGMR) folgen aus der Heimlichkeit des Vorgehens auch höhere Anforderungen an die gesetzliche Grundlage (BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09 , Rn. 1-29 Rn. 104ff.; EGMR 02.08.1984, 8691/79 [Malone gg. das Vereinigte Königreich], 1984; EGMR 04.12.2015, 47143/06 [Roman Zakharov gg. Russland], 2015, Rn. 229; EGMR 25.05.2021 58170/13 u.a. [Big Brother Watch u.a. gg. das Vereinigte Königreich], 2021, Rn. 333) Das ist auch dann der Fall, wenn der Zugriff über einen privaten Intermediär erfolgt und den betroffenen Personen bekannt ist, dass das jeweilige Unternehmen über diese Daten verfügt (BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020, 1 BvR 1873/13 -, Rn. 1-275, Rn. 129).[14]

Wie bei der Bestandsdatenauskunft und auch der oben angesprochenen Vorratsdatenspeicherung erfolgt die Informationsbeschaffung beim Datenkauf durch die Nachrichtendienste heimlich. Während aber bei den Regelungen zur Bestandsdatenauskunft und der Vorratsdatenspeicherung immerhin gesetzlich vorgeschrieben war, welche Daten über Nutzer:innen gesammelt und den Behörden zugänglich gemacht werden müssen, ist beim Datenkauf für die Betroffenen einerseits de facto nicht nachvollziehbar, welche Daten über sie in den Händen privater Datenhändler liegen, und anderseits keine Rechtsgrundlage erkennbar, die den Kauf dieser Daten durch Nachrichtendienste in angemessener Weise regelt (siehe Kapitel 4).

14 Das hat das BVerfG bereits in einem Urteil zur gesetzlichen Grundlage der Bestandsdatenauskunft klargestellt. Diese ermöglicht es den Sicherheitsbehörden, unter bestimmten Voraussetzungen auf die Vertragsdaten von Telekommunikationsdienstleistern zuzugreifen.

Im Zusammenhang mit dem Datenkauf durch den BND betonte die Bundesregierung unlängst, dass die Betroffenen der „Erhebung und Weiterveräußerung dieser Daten durch die kommerziellen Anbieter“ zugestimmt hätten (Bundesregierung, 2023a, S. 43). Dadurch wird suggeriert, dass der Eingriff weniger schwer wiege. Dagegen spricht aber ein wichtiger Umstand: Die Wege der Datenerfassung und der Weiterveräußerung im Datenmarkt sind derart intransparent, dass eine allgemeine Zustimmung der Nutzer:innen diese zahlreichen Dimensionen sicher nicht bewusst umfasst hat. Die Berliner Landesdatenschutzbeauftragte stellte kürzlich fest, dass es für den Einzelnen schon mehr als herausfordernd sei, „die komplexe Struktur der beteiligten Akteure sowie die spezifischen Datenflüsse bei der Erteilung einer Einwilligung nachzuvollziehen“ (Dachwitz, 2023a). Dadurch werde eine „tatsächlich selbstbestimmte und informierte Einwilligung [...] praktisch unmöglich“ (Dachwitz, 2023a). Geradezu utopisch wirkt vor diesem Hintergrund die insinuierte Annahme der Bundesregierung, dass Nutzer:innen den Kauf ihrer Daten durch Sicherheitsbehörden bei ihrer Zustimmung berücksichtigen könnten, sie der sicherheitsbehördlichen Auswertung ihrer Daten so mittelbar zustimmen oder diese zumindest absehen könnten – und dass sich daraus ein verringertes Eingriffsgewicht ergebe (vgl. Sosna, 2024, S. 57 ff.).

Von dieser Frage abgesehen, verdeutlichen die in diesem Abschnitt erörterten Urteile zur Bestandsdatenauskunft und zur Vorratsdatenspeicherung, dass schon das verdeckte Zugreifen des Staates auf Daten, von denen der Öffentlichkeit bekannt ist, dass Unternehmen sie führen, ein schwerer Grundrechtseingriff ist. Für den Ankauf von Daten, die auf höchst intransparente Weise erfasst, verarbeitet und weiterveräußert werden, gilt das umso mehr.

3.4. Der Zugang für die Betroffenen zu effektivem Rechtsschutz ist beschränkt

Dass der Ankauf heimlich erfolgt und für das Individuum kaum nachvollziehbar ist, welche Interaktionen zwischen den datenerfassenden Unternehmen, Datenhändlern und Sicherheitsbehörden genau stattfinden, hat zur Folge, dass auch der Zugang zum Grundrecht auf einen effektiven Rechtsschutz gegen staatliche Grundrechtseingriffe de facto verstellt ist.[15]

15 Das Grundrecht auf effektiven Rechtsschutz schreibt fest: „Wird jemand durch die öffentliche Gewalt in seinen Rechten verletzt, so steht ihm der Rechtsweg offen“. Die Umsetzung dieses Anspruchs ist gerade im Bereich der Nachrichtendienste eine Herausforderung.Nachrichtendienstliche Arbeit erfolgt in aller Regel verdeckt. Einige Methoden der Datenerhebung sehen aber Benachrichtigungspflichten vor, die den Betroffenen ermöglicht, die rechtliche Zulässigkeit zu prüfen. Bei anderen Methoden ist eine Kontrolle durch eine unabhängige Stelle vorgesehen, um die Einschränkung dieses Grundrechts zu kompensieren.

In diesem Zusammenhang wird häufig darauf verwiesen, dass betroffene Personen Auskunftsrechte gegenüber den Unternehmen über die Verarbeitung ihrer Daten haben. Selbst wenn aber Betroffene bei einem datenverarbeitenden Unternehmen Auskunft darüber verlangen würden, wohin ihre personenbezogene Daten übermittelt wurden, können sie wohl kaum darauf hoffen, ein vollständiges Bild darüber zu erhalten, durch wen ihre Daten verarbeitet wurden. Denn für die Unternehmen selbst ist es in der Regel schon aus technischen Gründen nicht vollständig nachvollziehbar, an welche Stellen diese Daten direkt und mittelbar am Ende weiterveräußert wurden (Ryan & Christl, 2023, S. 6).

Unberührt vom rechtlichen Anspruch einer Person gegenüber dem Unternehmen, Auskunft darüber zu erlangen, an wen die eigenen Daten übermittelt wurden, bleibt das Recht, sich gegen die unrechtmäßige Datenerhebung des Staates zur Wehr setzen zu können.

Dieses Grundrecht auf effektiven Rechtsschutz gegen unrechtmäßige Grundrechtseingriffe wird im Falle von nachrichtendienstlichen Datenkäufen schon dadurch behindert, dass den meisten Personen das Bewusstsein der eigenen Betroffenheit fehlt. Das liegt unter anderem daran, dass – anders als beispielsweise bei der Fernmeldeaufklärung – dem geltenden Rechtsrahmen keine Informationen über die spezifische Befugnis der Nachrichtendienste zum Kauf von Daten aus Werbedatenbanken zu entnehmen sind (Siehe Kapitel 5.1).

Wollen Individuen eine potenzielle Grundrechtsverletzung prüfen, müssten sie für eine gerichtliche Beschwerde im Regelfall die hinreichende Wahrscheinlichkeit ihrer Betroffenheit nachweisen. Da über die Art und Weise des Vorgehens der Nachrichtendienste allerdings so gut wie nichts öffentlich bekannt ist, ist fraglich, wie ein solcher Nachweis aussehen sollte.

Dass den Betroffenen dieses Grundrecht de facto verwehrt ist, erhöht wiederum die Intensität des Eingriffs (Hornung, 2022, S. 33).

3.5. Diskriminierungs- und Manipulationsrisiken durch den Datenkauf

Zudem unterliegen die gekauften Daten einem erhöhten Risiko manipuliert zu werden oder diskriminierend verzerrt zu sein. Die Qualität der Daten ist oft nur schwer zu überprüfen. Werden Informationen erworben, für deren Genese andere Daten verwendet wurden, kann die Behörde in der Regel nicht sicherstellen, dass diese Informationen nicht auf Grundlage diskriminierender oder manipulierter Daten ermittelt wurden.

Daten von Kreditauskunfteien können hier zur Veranschaulichung dienen: Oft ist schwer einsehbar, wie Kreditwürdigkeitswerte ermittelt und welche Daten hierfür verwendet werden. Das Risiko, dass bei der Berechnungsweise oder der Datengrundlage diskriminierende Verzerrungen vorliegen, ist hoch. Ausgehend von den Resultaten, also den Kreditwürdigkeitseinstufungen, sind sie nicht mehr nachzuvollziehen. Werden auf dem Datenmarkt Informationen gekauft, können diese darüber hinaus auch willentlich durch interessierte Dritte verzerrt worden sein. Und auch abseits von absichtlichen Verzerrungen der Daten, durch die beispielsweise kriminelle Akteure oder andere Staaten Sicherheitsbehörden täuschen wollen, sind die auf dem Markt erhältlichen Daten oft unzuverlässig (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 212). Solche Informationen, deren Entstehung nicht gänzlich nachzuvollziehen ist, können die Grundlage bilden, auf der weitere grundrechtsrelevante Maßnahmen beschlossen werden. In diesem Fall besteht ein hohes Risiko für die unrechtmäßige Diskriminierung marginalisierter Gruppen (Steiner, 2024).

Gibt eine unzuverlässige Datenbasis den Ausschlag darüber, ob eine:r App-Nutzer:in eine Werbung angezeigt wird oder nicht, ist der Schaden begrenzt. Wenn diese Information aber darüber entscheidet, ob die Nutzer:in Ziel weiterer Überwachungsmaßnahmen durch Sicherheitsbehörden wird, ist das hochproblematisch und in Widerspruch zu verfassungsrechtlichen Schutznormen (siehe Kapitel 4).

Daraus folgt: Das Risiko der Unzuverlässigkeit von Daten erhöht zusätzlich das Eingriffsgewicht und erfordert besondere Sicherungsmaßnahmen (BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 - 1 BvR 2634/20, Rn. 1-178, Rn. 95).

3.6. Der Datenkauf begünstigt ein diffuses Überwachungsgefühl

Ein weiterer Aspekt begründet die Schwere der Grundrechtseingriffe, die mit dem Datenkauf durch Nachrichtendienste einhergehen: das Potenzial, ein allgemeines Überwachungsgefühl in der Bevölkerung zu erzeugen. In Urteilen zur Verfassungsmäßigkeit der Befugnisse zur Vorratsdatenspeicherung und aus dem Anti-Terror-Datei-Gesetz argumentierte das BVerfG wie folgt: Grundrechtseingriffen durch verdeckte Überwachungsmaßnahmen kommt dann eine besondere Schwere zu, wenn diese in der Lage sind, ein „diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann“ (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 212). Der Argumentation des Gerichts zufolge ist das Risiko hierfür insbesondere dann hoch, wenn der Eingriff von den Betroffenen un-

mittelbar nicht bemerkt wird und wenn er Kommunikationsvorgänge betrifft, die unter Vertraulichkeitserwartung geführt werden.

Wenn Nachrichtendienste Daten bei Händlern kaufen, wird dieser Grundrechtseingriff wie oben beschrieben von den Betroffenen in aller Regel ebenfalls nicht bemerkt. Auch mit größerer Anstrengung können sie im Nachhinein kaum ermitteln, wie ihre Daten in dem Geflecht der Datenhändler übermittelt und verarbeitet wurden. Und noch viel weniger, ob und wie diese die Nachrichtendienste erreichen.

Auch die Vertraulichkeitserwartung der Betroffenen scheint in vielen möglichen Konstellationen gegeben. Man muss nur an Beispiele denken wie die Internetrecherchen zu Symptomen psychischer Erkrankungen, den Besuch einer Abtreibungsklinik oder die regelmäßige Teilnahme an Selbsthilfegruppen für Suchtkranke. Alle diese Informationen ließen sich aus bei Datenhändlern verfügbaren Daten extrahieren. Und bei all diesen Aktivitäten besteht berechtigter Grund zur Annahme, dass die Betroffenen nicht wollen, dass andere davon erfahren.

Nun könnte argumentiert werden, dass die Nutzer:innen der Verarbeitung dieser Daten durch die Unternehmen zugestimmt hätten und daher keine Vertraulichkeitserwartung angenommen werden könne. Hier muss aber, wie bereits in Kapitel 3.3, auf den Einwand des Berliner Landesdatenschutzbeauftragten verwiesen werden. Der Datenmarkt ist derart komplex und unübersichtlich, dass eine „tatsächlich selbstbestimmte und informierte Einwilligung [...] praktisch unmöglich“ ist (Dachwitz, 2023a). Nutzer:innen, die annehmen, dass private Dienstleister über ihre Informationen verfügen, können außerdem nicht automatisch annehmen, dass auch staatliche Stellen hierauf Zugriff haben. Dass Nutzer:innen diesen Zugriff nicht absehen können, mag zunächst wie ein Widerspruch zu der Annahme wirken, dass der Kauf von Daten zu einem Gefühl des allgemeinen Beobachtetseins in der Bevölkerung führen kann. Aber genau diese Widersprüchlichkeit befördert diesen Zustand, in dem das Verfassungsgericht eine Gefahr für die Demokratie erkennt. Das BVerfG beschreibt das Gefühl wie folgt: „Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können“ (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 241).

Die Besonderheiten der nachrichtendienstlichen Arbeitsweise müssen hinsichtlich des Potenzials, ein solches allgemeines Gefühl des Beobachtetseins entstehen zu lassen, berücksichtigt werden. Einerseits wird das Gewicht der Grundrechtseingriffe durch Nachrichtendienste im Vergleich zu Polizeibehörden dadurch verringert, dass diese keine unmittelbaren Zwangsbefugnisse haben. Gleichzeitig betont das Karlsruher Gericht im Kontext der Vorratsdatenspeicherung aber, dass die Aktivitäten der Nachrichtendienste im Geheimen erfolgen und die Eingriffsbefugnisse deshalb in

besonderer Weise dazu geeignet seien, ein „Gefühl des unkontrollierbaren Beobachtetwerdens“ zu erzeugen und „dadurch nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung“ zu entfalten (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 233).

Die mit diesem Gefühl einhergehende mögliche Anpassung des Verhaltens kann die Wahrnehmung von Grundrechten in vielen Bereichen beeinträchtigen (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 212). Durch den Einschüchterungseffekt können Bürger:innen in weiteren Grundrechten eingeschränkt werden, beispielsweise in ihrem Recht auf die freie Persönlichkeitsentfaltung oder in ihrer Meinungs- und Versammlungsfreiheit. Bergen nachrichtendienstliche Maßnahmen die Gefahr, zu einem solchen Gefühl in der Bevölkerung beizutragen, erhöht das deren Eingriffsgewicht (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 233).

3.7. Zusammenfassung

Käuflich erwerbbare Daten können tiefe Einblicke in das Privatleben Betroffener ermöglichen, bis hin zur Erstellung umfassender Persönlichkeitsprofile. Kaufen Nachrichtendienste Datensätze mit personenbezogenen Daten, sind davon in der Regel eine Vielzahl von Menschen betroffen – auch solche, deren Verhalten keinerlei Anlass für die Erfassung gegeben hat. Weil der Datenmarkt komplex ist und Nachrichtendienste diese Datenkäufe heimlich durchführen, können Betroffene die Eingriffe kaum absehen. Die Möglichkeit der Betroffenen, ihr Grundrecht auf effektiven Rechtsschutz gegen solche Eingriffe wahrzunehmen, ist darüber hinaus stark begrenzt. Zudem droht durch den Zugriff der Nachrichtendienste auf die umfassenden, sensiblen und wenig zielgerichteten Datensammlungen ein allgemeines Überwachungsgefühl in der Bevölkerung, mit schwerwiegenden Auswirkungen auf individuelle Grundrechte und die demokratische Ordnung als Ganzes.

4. Ist die gesetzliche Grundlage für nachrichtendienstliche Datenkäufe mit verfassungsgerichtlichen Mindestanforderungen vereinbar?

Grundsätzlich gilt: Wenn der Staat in Grundrechte eingreift, darf er das nur mit einer ausreichend bestimmten gesetzlichen Grundlage. Zudem bedarf es einer effektiven und unabhängigen Kontrolle.

Das vorherige Kapitel hat die Gründe aufgezeigt, warum der nachrichtendienstliche Kauf von Daten sogar erhebliche Grundrechtseingriffe bewirken kann. Ist die Intensität der Eingriffe hoch, muss eine Reihe von Voraussetzungen erfüllt sein, damit staatliche Grundrechtseingriffe rechtmäßig sind. Was aber heißt das konkret? Wie muss der Rechtsrahmen ausgestaltet sein, damit nachrichtendienstliche Datenkäufe rechtmäßig sind? Und inwiefern werden die Anforderungen vom derzeitigen Rechtsrahmen erfüllt? Diese Fragen werden wir in diesem Kapitel aufgreifen.

4.1. Anforderungen an eine gesetzliche Grundlage für nachrichtendienstliche Datenkäufe

Die Anforderungen an den Rechtsrahmen für nachrichtendienstliche Datenkäufe ergeben sich aus verfassungs- und europarechtlichen Grundsätzen und der Anwendung einschlägiger Rechtsprechung des BVerfG.

4.1.1. Bedarf es einer einfachgesetzlichen Grundlage?

Zunächst stellt sich die Frage, ob nachrichtendienstliche Datenkäufe einer einfachgesetzlichen Grundlage bedürfen oder ob zur Legitimation dieser Überwachungstätigkeit eine allgemeine Befugnis der Nachrichtendienste zur Erhebung und Verarbeitung personenbezogener Daten ausreicht.

Grundsätzlich ist der Gesetzgeber verpflichtet, „in grundlegenden, normativen Bereichen alle wesentlichen Entscheidungen selbst zu treffen" – und er darf solche Abwägungen nicht an die ausführenden Behörden delegieren (BVerfG, Urteil des Zweiten Senats vom 19. September 2018, 2 BvF 1/15 -, Rn. 1-357, Rn. 191).[16] Das heißt, dass

16 Außerdem enthalten manche Grundrechte einen ausdrücklichen Gesetzesvorbehalt. Darunter zählen zum Beispiel das Fernmeldegeheimnis (Art. 10 Abs. 2 GG) und die Unverletzlichkeit der Wohnung (Art. 13 Abs. 2 GG). Um also auf diese Grundrechte staatlich einzuwirken, bedarf es zwingend einer spezifischen Gesetzesgrundlage.

grundlegende normative Bereiche des sicherheitsbehördlichen Handelns nicht allein von der Exekutive durch Dienstvorschriften reglementiert werden können, sondern, dass das Parlament dafür entsprechende Gesetzestexte zu verabschieden hat.

Daraus folgt nicht, dass jedwede vorstellbare Handlung der Sicherheitsbehörden mit nur geringfügiger Grundrechtsrelevanz in ein Gesetz gefasst werden muss. Das würde zu einem unübersichtlichen Konvolut an Gesetzestexten führen und die Effizienz der Sicherheitsvorsorge und der Kontrolle schmälern. Stattdessen verweist das BVerfG bei einer Abwägung, ob es einer einfachgesetzlichen Grundlage bedürfe, regelmäßig auf die Intensität des mit der staatlichen Überwachungsbefugnis einhergehenden Grundrechtseingriffs.

Nur dort, wo diese über ein bestimmtes Maß hinausgehen, ist eine spezifische Regelung notwendig. Im Grunde gilt hier: Je intensiver der Eingriff, desto dringender bedarf es einer formellen, vom Parlament beschlossenen spezifischen Gesetzesgrundlage (BVerfG, Urteil des Zweiten Senats vom 19. September 2018, 2 BvF 1/15 -, Rn. 1-357, Rn. 194).

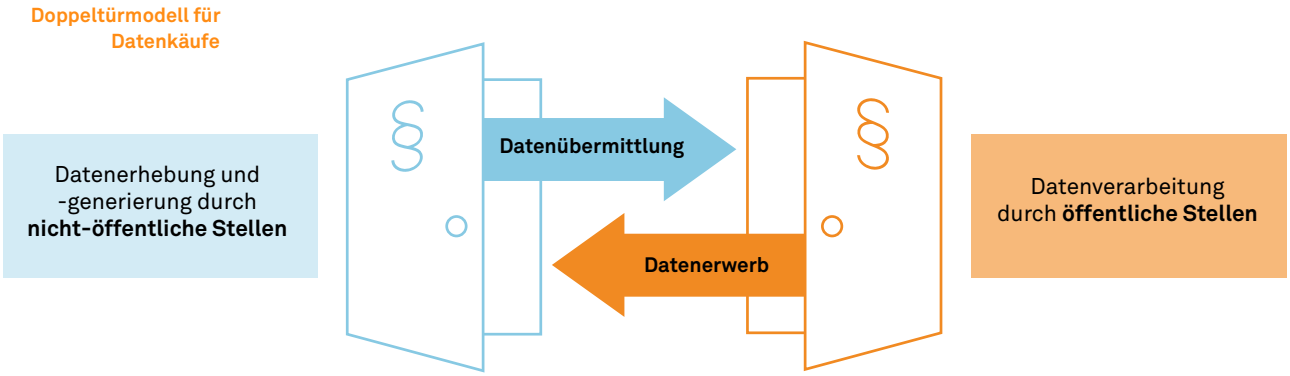
Beispielsweise urteilte das BVerfG, dass eine Kenntnisnahme öffentlich zugänglicher personenbezogener Informationen durch staatliche Stelle keinen ausreichenden Grundrechtseingriff darstellten und daher nicht grundsätzlich einer gesetzlichen Grundlage bedürften (Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07 -, Rn. 1-333, Rn. 308). Das könne sich jedoch ändern, sobald diese Informationen „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden“ (Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07 -, Rn. 1-333, Rn. 309).[17]

Zu bestimmen, wo genau die Grenze verläuft, ab der eine einfachgesetzliche Grundlage geboten ist, ist in der Praxis oft eine regulatorische Herausforderung. Die in Kapitel 3 dargelegten Eigenschaften des nachrichtendienstlichen Datenkaufs, wie die große Streubreite des Eingriffs und die Sensibilität der Informationen, die auf diese Weise erhoben werden können, sprechen unserer Meinung nach klar dafür, dass es Konstellationen geben kann, in denen bereits die Beschaffung dieser Daten ein hohes Eingriffsgewicht hat. Dieses hohe Eingriffsgewicht setzt sich auch dann fort oder verstärkt sich noch, wenn die Daten verarbeitet und möglicherweise mit Daten aus anderen Beschaffungsmethoden kombiniert werden. Eine einfachgesetzliche

17 Sosna diskutiert erstens, inwiefern diese im Zusammenhang mit Eingriffen in das Grundrecht nach Art. 10 GG angestellte Überlegung des BVerfG auch auf Eingriffe in das Recht auf informationelle Selbstbestimmt übertragbar ist und stellt gleichzeitig in Frage, ob diese Aussage angesichts der veränderten technischen Möglichkeiten der systematischen Erfassung von Inhalten im Internet heute noch als gültig angenommen werden kann (Sosna, 2024, S. 54 f.).

Grundlage für nachrichtendienstliche Datenkäufe ist unserer Auffassung nach deshalb dringend geboten.

Verdeutlicht wird die Notwendigkeit einer gesetzlichen Grundlage außerdem durch das unserer Meinung nach auch in diesem Fall anwendbare Doppeltürmodell. Dieses vom BVerfG im Zusammenhang mit den Urteilen zur Bestandsdatenauskunft entwickelte Modell besagt, dass es nicht nur einer Rechtsgrundlage bedarf, um der abgebenden Stelle die Übermittlung der Daten zu gestatten. Benötigt wird auch eine gesetzliche Grundlage für den Abruf der Daten durch die empfangende Stelle [18] (BVerfG, Beschluss des Ersten Senats vom 24. Januar 2012, 1 BvR 1299/05 -, Rn. 1-192, Rn. 123) – denn Übermittlung und Entgegennahme stellen jeweils eigene Grundrechtseingriffe dar (BVerfG, Urteil des Ersten Senats vom 24. April 2013, 1 BvR 1215/07 -, Rn. 1-233, Rn. 95). Dies gilt auch für die Fälle, in denen die übermittelnde Stelle ein Unternehmen ist.[19]



4.1.2. Welche Elemente muss eine gesetzliche Grundlage enthalten?

Wo das Eingriffsgewicht ein geringfügiges Maß überschreitet, ist der Gesetzgeber nach Karlsruher Rechtsprechung verpflichtet, eine Reihe von Mindestanforderungen an die Ausgestaltung der notwendigen gesetzlichen Grundlage zu beachten (BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 - 1 BvR 2634/20, Rn. 1-178, Rn. 104).

18 Zusätzlich sei an dieser Stelle erwähnt, dass auch erhebliche Zweifel an der Rechtmäßigkeit der Praxis der privaten Akteure besteht. Siehe hierfür auch Wetzling und Dietrich (2022, S. 19 ff).

19 Dieser Grundsatz wird auch vom BVerfG in seinem Urteil zur Bestandsdatenauskunft unterstrichen. Zudem bewog diese Anforderung das Gericht in seinem Urteil zum BayVSG von 2022 dazu, eine Norm als verfassungswidrig zu einzustufen, auf die gestützt die Landesverfassungsschutzbehörde Daten von privaten Stellen abrief (BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020, 1 BvR 1873/13 -, Rn. 1-275, Rn. 95; BVerfG, Urteil des Ersten Senats vom 26. April 2022, 1 BvR 1619/17 -, Rn. 1-407).

Normenklarheit und Bestimmtheit

Zunächst muss eine für nachrichtendienstliche Datenkäufe notwendige gesetzliche Grundlage den Grundsätzen der Normenklarheit und Bestimmtheit genügen (BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 -, Rn. 1-215; BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 137). Diese Mindestanforderung leitet das BVerfG aus dem Rechtsstaatsprinzip ab (Detterbeck, 2020, S. 227–228). Bei der heimlichen Erhebung und Verarbeitung von personenbezogenen Daten, wie beim Datenkauf durch Nachrichtendienste gegeben, müssen an diese Kriterien zudem noch gesteigerte Anforderungen gestellt werden (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 137). Konkret bedeutet das, dass in einer gesetzlichen Ermächtigung zum Datenkauf insbesondere die Anordnungsvoraussetzungen, legitime Verwendungszwecke und Grenzen des Eingriffs „bereichsspezifisch, präzise und normenklar festgelegt werden“ müssen (Durner et al., 2024, S. 176).

Das Zitiergebot nach Art. 19 Abs. 1 Satz 2 verlangt zudem, dass dort wo ein Gesetz eine Grundlage für Grundrechtseingriffe schafft, auch das betroffene Grundrecht ausdrücklich in der Befugnisnorm genannt werden muss. Der Zweck dieses Gebotes ist, dem Gesetzgeber die Grundrechtseingriffe bewusst zu machen und diesen so zu befähigen, die Folgen dieser Einschränkung in der Abwägung zu berücksichtigen. Das Zitiergebot gilt dabei nur für Grundrechte, zu deren Einschränkung der Gesetzgeber im Grundgesetz ausdrücklich ermächtigt wird (Bundesministerium der Justiz, 2008). Dazu gehört zwar nicht das Recht auf informationelle Selbstbestimmung, aber beispielsweise das Fernmeldegeheimnis, die Unverletzlichkeit der Wohnung und das Recht auf Versammlungsfreiheit.

Das Zitiergebot ist daher nicht auf alle Fälle des Datenkaufs anwendbar. Es gibt aber Konstellationen, wo der nachrichtendienstliche Datenkauf in die zuletzt genannten Grundrechte eingreift (siehe Anwendungsbeispiel 1) und deren notwendige gesetzliche Grundlage nur dann verfassungskonform wäre, wenn sie dem Zitiergebot entspräche.

Verhältnismäßigkeit

Grundrechtseingriffe des Staates müssen zudem verhältnismäßig sein. Nur mit einer hinreichend präzisen gesetzlichen Grundlage kann der Gesetzgeber die Voraussetzungen für die Einhaltung des Verhältnismäßigkeitsgebots schaffen. Demnach darf eine staatliche Maßnahme die betroffenen Bürger:innen nicht übermäßig benachteiligen („Übermaßverbot”) (Detterbeck, 2020, S. 229). Eine verhältnismäßige Maßnahme erhält ein ausgeglichenes Verhältnis zwischen dem angestrebten legitimen Zweck und dem Gewicht des Grundrechtseingriffes für die betroffene Person. Um dieses Verhältnis zu gewährleisten und willkürliche und

missbräuchliche Eingriffe zu verhindern, muss der Gesetzgeber bei erheblichen Grundrechtseingriffen Anforderungen für die Datenerhebung ebenso wie für die Datenverwendung definieren (vgl. BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 232). Dabei gilt zu beachten, dass sich bei heimlichen Maßnahmen besonders strenge Anforderungen an die Qualität der gesetzlichen Grundlage ergeben. Wo sich nämlich sonst Befugnisse „im Wechselspiel von behördlicher Einzelanordnung und gerichtlicher Kontrolle schrittweise konkretisieren können“ (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 137), bleiben die Eingriffe hier unbemerkt und die Betroffenen können sich kaum zur Wehr setzen.

Zum Schutz der Persönlichkeitsentfaltung können Bürger:innen zudem berechtigterweise erwarten, dass der intimste Bereich des Privatlebens, der sogenannte Kernbereich der privaten Lebensgestaltung, nicht überwacht wird. Aus der in Kapitel 3.1 dargelegten Wahrscheinlichkeit, dass durch den Kauf von Daten auch auf kernbereichsrelevante Informationen zugegriffen werden kann, folgt die Pflicht des Gesetzgebers, weitere Schutzmechanismen vorzusehen. Diesbezüglich hat das Verfassungsgericht unmissverständlich klargestellt: Für Methoden der Informationsbeschaffung, die „typischerweise zur Erhebung kernbereichsrelevanter Daten führen, muss der Gesetzgeber Regelungen schaffen, die einen wirksamen Schutz normenklar gewährleisten” (BVerfG, Urteil des Ersten Senats vom 26. April 2022, 1 BvR 1619/17 -, Rn. 1-407, Rn. 305).

Vorhersehbarkeit

Zudem gilt zu beachten, dass der notwendige Rechtsrahmen für nachrichtendienstliche Datenkäufe Betroffene ausreichend befähigen sollte, die wesentlichen Züge des staatlichen Handelns zu erkennen. Bürger:innen sollten abschätzen können, was der Staat darf und wie ihre Grundrechte davon betroffen sein können. Sie sollten in der Lage sein, mögliche rechtliche Konsequenzen ihres Handelns abzuschätzen und ihr Verhalten entsprechend anzupassen (EGMR 25.05.2021 58170/13 u.a. (Big Brother Watch u.a. gg. das Vereinigte Königreich), 2021, Rn. 333). Das heißt nicht zwingend, dass jede konkrete Maßnahme der Nachrichtendienste für sich genommen vorhersehbar sein muss. Es ist aber zumindest geboten, „dass die betroffene Person grundsätzlich erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist“ (BVerfG, Urteil des Ersten Senats vom 27. Juli 2005, 1 BvR 668/04 -, Rn. 1-166, Rn. 117). Betroffene sollen so zudem befähigt werden, die Maßnahmen öffentlich zur Debatte zu stellen und so einen demokratischen Abwägungsprozess ermöglichen (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 242).

Effektiver Rechtsschutz

Darüber hinaus haben von staatlichen Grundrechtseingriffen betroffene Personen ein Recht auf effektiven Rechtsschutz. Das heißt, dass ihnen die Möglichkeit eingeräumt werden muss, die Rechtmäßigkeit von Grundrechtseingriffen im Nachhinein unabhängig überprüfen zu lassen. Insbesondere verdeckte Maßnahmen zur Informationsbeschaffung sind nicht leicht mit dem Grundrecht auf effektiven Rechtsschutz in Einklang zu bringen.

Bei anderen Formen der verdeckten Erhebung personenbezogener Daten hat der Gesetzgeber deshalb Benachrichtigungspflichten explizit in den Rechtsrahmen mit aufgenommen.[20] Erst eine Benachrichtigung ermöglicht es den Betroffenen in der Regel, von ihrem Grundrecht Gebrauch zu machen und die Rechtmäßigkeit des Grundrechtseingriffs gerichtlich überprüfen zu lassen.

Nicht in jedem Fall sind solche Benachrichtigungspflichten für verdeckte Maßnahmen verfassungsrechtlich geboten. Wo auf die Benachrichtigungspflichten aber verzichtet wird, müssen Gesetzgeber sicherstellen, dass sich jede Person, die den Verdacht hat, von einer Überwachungsmaßnahme betroffen zu sein, an eine unabhängige Stelle wenden kann, die die Rechtmäßigkeit des potenziellen Eingriffs überprüfen kann (EGMR 25.05.2021 58170/13 (Big Brother Watch u.a. gg. das Vereinigte Königreich), 2021, Rn. 357ff.). Diese unabhängige Stelle muss dabei nicht zwingend richterlich besetzt sein. Dem Grundsatz eines fairen Verfahrens muss aber entsprochen werden, in dem ein kontradiktorisches Verfahren ermöglicht wird und die Entscheidungen begründet werden und bindende Wirkung haben (Steiner, 2024, S. 37).

4.1.3. Zwischenfazit

Die potenziell schwerwiegenden Grundrechtseingriffe durch nachrichtendienstliche Datenkäufe sind eine rechtsstaatliche Herausforderung: Es muss zwischen der Wahrung von Grund- und Menschenrechten einerseits und der Handlungsfähigkeit der Nachrichtendienste andererseits abgewogen werden. Orientierung dafür, wo regulatorisches Eingreifen notwendig ist, bietet die Anwendung des Gebots der Normenklarheit und Bestimmtheit durch das BVerfG im Zusammenhang mit anderen Methoden der nachrichtendienstlichen Informationsbeschaffung.

Eine ausreichend präzise gesetzliche Grundlage trägt in mehrfacher Hinsicht dazu bei, die Nachrichtendienste mit einem effektiven, rechtssicheren und grundrechtsschonenden Werkzeugkasten auszustatten. Sie trägt zur Wahrung der Ver-

20 Siehe beispielsweise die Mitteilungspflicht in §12 G10-Gesetz und die in § 13 G10-Gesetz genannte Möglichkeit, gegen eine Anordnung und den anschließenden Vollzug einer Überwachungsmaßnahme im Nachhinein gerichtlich vorzugehen.

hältnismäßigkeit der Maßnahmen bei, sie verbessert die Vorhersehbarkeit der Grundrechtseinschränkungen und ermöglicht den Zugang zu effektivem Rechtsschutz für Betroffene. Sie schafft zudem Rechtssicherheit für die Nachrichtendienste.

4.2. Genügt der aktuelle Rechtsrahmen für nachrichtendienstliche Datenkäufe den Mindestanforderungen?

Die zahlreichen im vorherigen Kapitel aufgeführten Anforderungen an die notwendige gesetzliche Grundlage für nachrichtendienstliche Datenkäufe werden von den aktuellen Regelungen im Nachrichtendienstrecht nicht im Ansatz erfüllt.

Mit dem käuflichen Erwerb von Daten gehen potenziell schwerwiegende Grundrechtseingriffe einher (Kapitel 3.1.). Daraus ergeben sich Mindestanforderungen an die gesetzliche Grundlage für diese Form der Informationsbeschaffung (Kapitel 4.1.). Um die Erhebung, die Speicherung, die Verarbeitung und die Übermittlung dieser Daten zu rechtfertigen, brauchen die jeweils mit diesen Schritten einhergehenden Grundrechtseingriffe eine spezifische Ermächtigungsgrundlage.

4.2.1. Die Generalklausel als einzige Grundlage für Kauf, Speicherung und Verarbeitung von Daten

Zur Rechtfertigung der Erhebung, Speicherung und Verarbeitung von Daten, die aus dem nachrichtendienstlichen Kauf hervorgehen, kann in Ermangelung ausreichend bestimmter Befugnisnormen lediglich die jeweilige Generalklausel der Dienste im Nachrichtendienstrecht herhalten. Für den BND ist dies beispielsweise §2 Abs. 1 BND-Gesetz,[21] wonach dieser die erforderlichen personenbezogenen Daten verarbeiten darf, um unter anderem Informationen über Vorgänge im Ausland zu erhalten, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik sind – sofern keine anderen Bestimmungen des BDSG oder des BNDG dem entgegenstehen.[22]

Für Grundrechtseingriffe von geringer Intensität ist es vertretbar, sich einzig auf die Generalklausel zu berufen. Für Grundrechtseingriffe von erhöhter Eingriffsschwere

21 Im BVerfSchG findet sich die vergleichbare Generalklausel in §8 Abs. 1 und im MADG in §1 Abs. 1.

22 Darüber hinaus gibt es noch qualifizierte Generalklauseln für den Einsatz nachrichtendienstlicher Methoden der Informationsbeschaffung, nämlich in §5 BNDG, §9 BVerfSchG und §5 MADG. Aus der Formulierung der Begründung zu §10a ergibt sich aber, dass der Datenkauf nach Auffassung des Gesetzgebers nicht zu den nachrichtendienstlichen Mitteln zählt. Die Grundvoraussetzungen der qualifizierten Generalklausel in §5 BNDG müssen hier also nicht erfüllt sein.

kann eine derart weitgefasste Befugnisgeneralklausel den im Kapitel 4.1. beschriebenen Mindestanforderungen nicht im Ansatz gerecht werden.[23]

Es fehlen unter anderem die notwendigen Vorgaben über Anordnungsvoraussetzungen, Eingriffsschwellen sowie weitere Verfahrensschritte zur Wahrung der Verhältnismäßigkeit. Wie in 4.1. beschrieben, ist es bei derart intensiven Grundrechtseingriffen nicht ausreichend, wichtige Vorgaben zur Wahrung des Grundrechteschutzes allein durch geheime Dienstvorschriften zu regeln. Es bedarf vielmehr einer spezifischen einfachgesetzlichen Grundlage.

Die weit gefassten Generalklauseln stehen einer effektiven legislativen Kontrolle und der Rechtssicherheit für die Dienste entgegen (Löffelmann & Zöller, 2022, S. 156).

Beim Blick auf die gesetzliche Grundlage anderer Formen der Datenerhebung mit erhöhter Grundrechtsrelevanz wird die bestehende Diskrepanz deutlich. Spezifische Normen für den ganzen Prozess der Datenverwendung gibt es im Nachrichtendienstrecht derzeit beispielsweise für die strategische Fernmeldeaufklärung. Der untenstehende Vergleich mit dem aktuellen Rechtsrahmen für den nachrichtendienstlichen Kauf von Daten verdeutlicht, wie unzureichend der Status Quo hier ist.

23 Das ergibt sich einerseits aus den deutschen verfassungsrechtlichen Grundsätzen des Bestimmtheitsgebots und der Wesentlichkeitstheorie und aus Art. 8 Abs. 2 der Europäischen Menschenrechtskonvention. Siehe auch (Hornung, 2022).

Tabelle: Rechtlicher Rahmen im Vergleich

Normen im BNDG zur Erfassung und Verwendung von Daten im Rahmen der strategischen Ausland-Fernmeldeaufklärung (A-FMA) im Vergleich zum Ankauf von Daten

Anordnungsvoraussetzungen			Verfahrensvorschriften		
	Strategische A-FMA	Ankauf von Daten		Strategische A-FMA	Ankauf von Daten
Legitime Zwecke	§19(1)	§2(1)[24]	Schriftliche Anordnung	§23	
Vorliegen tatsächlicher Anhaltspunkte für Aufklärungsrelevanz	§19(4)		Benachrichtigungspflichten	§59	
Vorliegen tatsächlicher Anhaltspunkte für den verfolgten Zweck	§19(4)		Löschfristen	§§19(7) & 27	§7
Begrenzung des Gesamtvolumens der Überwachung	§19 (8)		Filtervorgaben	§19(7)	
Vorab-Kontrollverfahren	§23 (4)		Kontinuierliche Prüfung der Relevanz der erhobenen Daten	§27	§7
			Kennzeichnungspflicht	§19(10)	
			Löschprotokollpflichten	§§ 21,22, 24 & 27	
			Kernbereichsschutz	§22	
			Schutz von Vertraulichkeitsbeziehungen	§21	
			Übermittlungsvorschriften	§§ 11 - 11g	§10a
			Spezifische Berichtspflicht an Bundeskanzleramt	§23(8)	

Legende

- Einfachgesetzliche Regelung vorhanden
- Keine einfachgesetzliche Regelung vorhanden

24 Dass gesetzliche Normen vorhanden sind, bedeutet nicht zwingend, dass diese unproblematisch sind. Wo aber überhaupt einfachgesetzliche Regelungen vorhanden sind, ermöglichen sie unter anderem eine öffentliche Auseinandersetzung mit den Regeln. Wenngleich es im Vergleich zum Datenkauf für die strategische Ausland-Fernmeldeaufklärung präzisere Regeln gibt, hat auch sie erhebliche Schwächen und genügt den Vorgaben des BVerfG nicht in Gänze.

4.2.2. Spezifische, aber ungenügende Grundlage für die Übermittlung von gekauften Daten

BND

Der Gesetzgeber hat im Zuge der Novellierung des Nachrichtendienstrechts im Oktober 2023 eine neue Regelung der Übermittlung von Daten aus „allgemein zugänglichen Quellen" in das BND-Gesetz eingefügt. Für die Übermittlung käuflich erworbener Daten werden hier dieselben Anforderungen gestellt wie an solche, die mit nachrichtendienstlichen Mitteln erhoben wurden.

> **§10a Übermittlung von personenbezogenen Daten aus allgemein zugänglichen Quellen**
> (1) Der Bundesnachrichtendienst darf personenbezogene Daten, die er aus allgemein zugänglichen Quellen erhoben hat, einer anderen Stelle übermitteln, wenn dies erforderlich ist
> 1. zur Erfüllung seiner Aufgaben oder
> 2. zur Erfüllung der Aufgaben der empfangenden Stelle.
> Eine automatisierte Übermittlung ist zulässig.
> (2) Absatz 1 gilt nicht für personenbezogene Daten, die aus allgemein zugänglichen Quellen systematisch erhoben oder zusammengeführt wurden. Die Übermittlung richtet sich in diesen Fällen nach den Unterabschnitten 3 und 4."

Während der Gesetzestext nur auf „personenbezogene[n] Daten, die [der BND] aus allgemein zugänglichen Quellen erhoben hat" abstellt, wird in dem Begründungstext klargestellt, dass diese Regelung auch für „Daten aus dem Ankauf z.B. von umfänglichen Werbedatenbanken und anderen Datenbanken mit vergleichbarer Eingriffsintensität" einschlägig ist (Bundesregierung, 2023a, S. 43). Dieser Einschub ist zunächst einmal zu begrüßen. Er verdeutlicht, dass die an der Gesetznovelle beteiligten Akteure nachrichtendienstliche Datenkäufe als relevante Praxis erachten, die beim Gesetzgebungsprozess mitberücksichtigt werden muss.

Allerdings besteht auch hier ein Klarheitsdefizit. Dass Absatz 2 des Paragrafen auch für gekaufte Daten gilt, ergibt sich nicht aus dem Gesetzestext selbst, sondern eben nur aus der Begründung. Außerdem lässt sich der zuvor genannte Satz zur Anwendbarkeit auf gekaufte Daten auch so interpretieren, dass nicht alle käuflich erworbene Daten unter diese Regelung fallen, sondern nur bestimmte mit hoher Eingriffsintensität. Das kann zwar sinnvoll sein, setzt aber eine Systematisierung voraus, um den Rechtsanwender:innen wie auch den Betroffenen Orientierung geben zu können.

BAMAD und BfV

Für BAMAD und BfV ist die Rechtslage noch unklarer. Im neu eingefügten §25d BVerfSchG, auf den auch §11 MADG verweist, heißt es:

> §25d Nicht nachrichtendienstlich erhobene personenbezogene Daten
>
> *„Personenbezogene Daten, die das Bundesamt für Verfassungsschutz nicht mit nachrichtendienstlichen Mitteln (§ 8 Absatz 2) erhoben hat, darf es abweichend von den §§ 19 bis 22 und 25a auch für sonstige erhebliche Zwecke der öffentlichen Sicherheit oder für sonstige erhebliche Interessen des Empfängers übermitteln, es sei denn der Übermittlung stehen besondere gesetzliche Verarbeitungsregelungen oder überwiegende schutzwürdige Interessen der betroffenen Person entgegen. Die §§ 23, 25 und 25c sind nicht anzuwenden.“*

Die in §8 Abs. 2 BVerfSchG genannten nachrichtendienstlichen Mittel werden dabei nur beispielhaft skizziert: „[...] Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden. In Individualrechte darf nur nach Maßgabe besonderer Befugnisse eingegriffen werden.“ Auch in der Begründung zu §25d wird nicht deutlicher, ob gekaufte Daten nun von den die Übermittlung regelnden Vorschriften §§19 bis 22 ausgenommen sind, oder nicht. Auch eine Berücksichtigung des potenziell hohen Eingriffsgewichts bei der Erfassung offen zugänglicher Informationen fehlt hier im Vergleich zu Begründung des §10a BNDG. Wird die Regelung in §25d BVerfSchG so ausgelegt, dass käuflich erworbene Daten als allgemein zugängliche Quellen anzusehen sind und der Kauf keine systematische Erhebung darstellt, können diese unter extrem niedrigen Voraussetzungen an andere inländische, ausländische, öffentliche und sogar private Stellen übermittelt werden.[25]

25 Darüber hinaus ist anzumerken, dass die einfache Unterscheidung bei Übermittlungsregelungen zwischen Informationen, die aus nachrichtendienstlichen und solchen, die mit anderen Mitteln beschafft wurden, nicht zulässig ist: „Denn durch die Betrachtung eines einzelnen, für sich genommen weniger eingriffsintensiven Datenerhebungsvorgangs würde die Grundrechtsbelastung, die von der breit angelegten, teils niederschwelligen Beobachtungstätigkeit nachrichtendienstlicher Behörden ausgeht, nicht in Gänze erfasst. Nachrichtendienstliche Behörden schöpfen ihre Erkenntnisse aus einer Fülle von Daten, die sie weit im Vorfeld konkreter Gefahren und operativer Tätigkeit erheben, miteinander und mit Erkenntnissen anderer Stellen verknüpfen und filtern, um daraus relevante Informationen zu gewinnen und auch weiterzugeben; dies ist eine Besonderheit ihrer Aufgabe“. (BVerfG, Urteil des Ersten Senats vom 26. April 2022, 1 BvR 1619/17 -, Rn. 1-407, Rn. 238ff.).

4.2.3. Zusammenfassung

Es ist positiv zu bewerten, dass der Gesetzgeber mit der Novelle des BNDG 2023 erstmals anerkannt hat, wie auch aus der Erhebung offen zugänglicher Daten eine „besondere Gefahrenlage für die Persönlichkeit des Betroffenen“ (Bundesregierung, 2023a, S. 42) entstehen kann. Gut, dass der Gesetzgeber dies auch für den Kauf von Daten anerkennt.

Die Bundesregierung sollte bei der angekündigten großen Reform des Nachrichtendienstrechts nun konsequenterweise eine ausreichend bestimmte gesetzliche Grundlage für die Erhebung, Speicherung und Verarbeitung dieser Daten schaffen. Denn aus verfassungsrechtlicher Perspektive ist klar: Um schwerwiegende Grundrechtseingriffe zu rechtfertigen, die aus dieser Praxis hervorgehen können, muss dringend eine normenklare und bestimmte gesetzliche Regelung geschaffen werden. Für die Erhebung, Speicherung und Verarbeitung sind die Generalklauseln die einzigen Normen, auf die sich die Dienste derzeit berufen können. Dass diese den Anforderungen, die in Kapitel 4.1. herausgearbeitet werden, nicht gerecht werden, haben wir verdeutlicht.

Aber auch für die Datenübermittlung besteht noch erheblicher Konkretisierungsbedarf. Während für den BND der Kauf von Daten immerhin im Begründungstext der Novelle genannt wird, ist das in der gesetzlichen Grundlage für BAMAD und BfV nicht der Fall. Auch im Bereich des Militärischen Nachrichtenwesens der Bundeswehr ist davon auszugehen, dass sie sich dieser Form der Informationsbeschaffung bedient. Sollte der Gesetzgeber im Zuge der anstehenden Reform also die überfällige, verfassungsrechtlich dringend gebotene gesetzliche Grundlage für die Überwachungsaktivitäten der Bundeswehr schaffen, sollte auch diese Form der Informationsbeschaffung dabei berücksichtigt werden (Ruckerbauer & Wetzling, 2023).

5. Anforderungen an die Kontrolle

Eine den vorgenannten Kriterien entsprechende Rechtsgrundlage ist eine notwendige, aber nicht hinreichende Voraussetzung für die Rechtmäßigkeit nachrichtendienstlicher Datenkäufe. Die Einhaltung gesetzlicher Vorgaben muss auch kontrolliert werden.

Was genau sollte das Kontrollmandat der Aufsichtsbehörden bezüglich der nachrichtendienstlichen Datenkäufe beinhalten? Welchen institutionellen Charakter sollte die Aufsichtsbehörde haben, die sich mit dieser Materie befasst? Bedarf es neben der parlamentarischen Kontrolle und der unabhängigen Datenschutzkontrolle durch den oder die Bundesbeauftragte:n für den Datenschutz und die Informationsfreiheit (BfDI) noch einer gerichtsähnlichen Kontrolle?

Diese Fragen stehen im Fokus dieses Kapitels. Zunächst erörtern wir, welche Anforderungen an die Kontrolle nachrichtendienstlicher Datenkäufe und die anschließende Nutzung der auf diese Weise erworbenen Informationen zu stellen sind. Anschließend prüfen wir, ob der aktuelle gesetzliche Rahmen für die Kontrolle und die Kontrollpraxis diesen Anforderungen genügen.

5.1. Die Intensität der Grundrechtseingriffe bestimmt auch die erforderliche Kontrolltiefe

Die Anforderungen an die Kontrolle lassen sich nicht einheitlich für alle Methoden der nachrichtendienstlichen Informationsbeschaffung bestimmen. Das liegt daran, dass die erforderlichen Kontrollvorgaben entscheidend von der jeweiligen Intensität der Grundrechtseingriffe der Überwachungsmaßnahmen bestimmt werden: Eine einzelne Erhebung öffentlich verfügbarer Daten ist in der Regel nicht so einschneidend für die Betroffenen wie eine Online-Durchsuchung. Im Allgemeinen gilt: Je intensiver der Grundrechtseingriff, desto strenger sollten sowohl die gesetzlich vorgeschriebene wie auch die tatsächlich praktizierte Kontrolltiefe sein.

Aber auch die nachrichtendienstlichen Datenkäufe sind in dieser Hinsicht nicht einheitlich zu bewerten. Je nach Anwendungsbeispiel (siehe Kapitel 2.3) können sie sehr unterschiedliche Grundrechtsrelevanz haben. Daher lassen sich dieser Methode nachrichtendienstlicher Informationsbeschaffung weder pauschal ein geringfügiges noch ein besonders tiefgreifendes Eingriffsgewicht zuschreiben. Da es Konstellationen geben kann, in denen bereits der Erwerb von Datensätzen – und erst recht deren anschließende Verarbeitung – einen starken Grundrechtseingriff darstellen, bedarf es für diese Fälle strengerer gesetzlicher Vorgaben (Kapitel 4.1.2) und weitergehender Anforderungen an die Kontrolle. Ein Fall, für den das sicherlich gilt, ist der in Anwendungsbeispiel 2 beschriebene massenhafte Kauf von Bewegungsdaten.

5.2. Ist eine gerichtsähnliche Vorabkontrolle für nachrichtendienstliche Datenkäufe nötig?

Ob und inwieweit Überwachungsmaßnahmen die Schwelle zu intensiven Grundrechtseingriffen überschreiten, entscheidet letztlich über die Frage, inwiefern die nötige Kontrolle allein von der parlamentarischen Nachrichtendienstkontrolle und der Kontrolle durch den BfDI gewährleistet werden kann. „Nach der Rechtsprechung des BVerfG kann bei Ermittlungsmaßnahmen, die einen schwerwiegenden Grundrechtseingriff bewirken, verfassungsrechtlich eine vorbeugende Kontrolle durch eine unabhängige Instanz geboten sein. Dies gilt insbesondere, wenn der Grundrechtseingriff heimlich erfolgt und für den Betroffenen unmittelbar nicht wahrnehmbar ist“ (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 248).

Unserer Auffassung nach wäre deshalb bei besonders grundrechtsrelevanten Fallkonstellationen des nachrichtendienstlichen Datenkaufs eine „gerichtsähnlich ausgestaltete Stelle“ (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 275) nötig. Sie sollte, wie auch bei der strategischen Ausland-Fernmeldeaufklärung durch den BND, „in formalisierten Verfahren schriftlich und abschließend mit Wirkung für Bundesregierung und Nachrichtendienst“ (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 275) entscheiden, ob ein zunächst zu beantragender Datenkauf genehmigt werden kann. Der Schwerpunkt dieser Kontrolle sollte auf der „Wahrung der Grundrechte der Betroffenen“ und „der Sicherung und praktischen Effektivierung der rechtlichen Grenzen der staatlichen Überwachungstätigkeit“ liegen (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 272).[26]

Das BVerfG hat unlängst unmissverständlich ausgeführt, dass für besonders grundrechtsintensive Methoden der nachrichtendienstlichen Informationsbeschaffung wie beispielsweise die Wohnraumüberwachung oder den Einsatz von verdeckten Ermittler:innen ein unabhängiges Verfahren zur Freigabe von Überwachungsmaßnahmen vor deren Vollzug notwendig ist (BVerfG, Urteil des Ersten Senats vom 26. April 2022, 1 BvR 1619/17 -, Rn. 1-407). In dem Urteil wurden nachrichtendienstliche Datenkäufe zwar nicht explizit als Mittel der Informationsbeschaffung genannt, die zukünftig einer Vorabkontrolle bedürfen. Aber die Erwägungen, die zu dieser Entscheidung geführt haben, lassen sich unserer Meinung nach auch auf diese Praxis anwenden (Wetzling & Vieth-Ditlmann, 2023).

26 Bei der parlamentarischen Kontrolle um die politische Richtungskontrolle und bei der Kontrolle durch den oder die BfDI geht es zudem um Datenschutz und Datensicherheit.

Wenn Datenkäufe also ähnlich schwer in Grundrechte eingreifen wie andere Formen der nachrichtendienstlichen Informationsbeschaffung, bei denen Genehmigungsverfahren und eine kontinuierliche Rechtskontrolle verfassungsrechtlich erforderlich sind, so sollte dies unserer Meinung nach auch hier der Fall sein.

5.3. Qualitätskriterien der Kontrolle

Zudem sind weitere allgemeine Qualitätskriterien der Kontrolle zu bedenken, die der Gesetzgeber zur Bestimmung der Angemessenheit und Leistungsfähigkeit der Kontrolle aus der deutschen und der europäischen Rechtsprechung entnehmen kann. Das betrifft einerseits die Unabhängigkeit der Kontrolle und andererseits deren Wirksamkeit. Darüber hinaus sollten die zentralen Aufgaben, Ressourcen und Prozesse der Kontrolle in einem vom Parlament verabschiedeten Gesetz festgeschrieben werden.

5.3.1. Unabhängigkeit

Der EGMR hat in einer Reihe von Urteilen wesentliche Kriterien für die Unabhängigkeit von Aufsichtsgremien identifiziert. Dabei konzentriert sich das Gericht auf funktionale Kriterien, wie den Prozess der Auswahl und der Benennung der Kontrollbeauftragten sowie deren Kontrollkompetenzen und -grenzen.

Dabei ist es weniger entscheidend, ob das Kontrollgremium als gerichtliche Instanz oder unabhängige Verwaltungseinrichtung fungiert. Relevant ist vielmehr seine Unabhängigkeit von der Exekutive (EGMR 16.05.1977, 7360/76 (Zand gg. Österreich), 1977) und seine Unvoreingenommenheit (EGMR 01.10.1982, 8692/7 (Piersack gg. Belgien), 1982). Die Unabhängigkeit eines Kontrollorgans zeigt sich unter anderem in dem Verfahren, nach dem seine Mitglieder ausgewählt und berufen werden. Es geht aber auch darum, inwiefern seine Mitglieder vor äußeren Einflüssen geschützt werden und ihre Unbefangenheit sichergestellt wird. Darüber hinaus ist wichtig, unter welchen Umständen Kontrollierende aus ihrem Amt entfernt werden können (EGMR 21.07.2009, 34197/02 (Luka gg. Rumänien), 2009).[27]

Auch das BVerfG betont, dass die Kontrollinstanzen über ein „eigenes Budget“ und eine „eigene Personalhoheit“ verfügen müssen und „in ihrer Arbeit von Einflussnahmen wirksam abgeschirmt“ sein sollten (BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332, Rn. 137).

27 Diese vorgenannten EGMR-Urteile wurden von Elspeth Guild in einem Beitrag auf aboutintel.eu zusammengetragen. Siehe Guild und Wetzling (2021).

5.3.2. Effektivität

Neben der Unabhängigkeit ist die Effektivität der Kontrolle ein entscheidendes Kriterium. Wie wirksam die Kontrollbefugnisse sind, hängt einerseits vom Zugang der Kontrollstellen zu den Informationssystemen und Datenbanken der Nachrichtendienste ab. Andererseits ist die technische Befähigung der Kontrollierenden dazu, Kontrollprogramme aufzusetzen, eine weitere Voraussetzung dafür, dass der Informationszugang auch sinnvoll genutzt werden kann. Zudem beeinflusst die Motivation der Kontrollierenden und deren Expertise in den zahlreichen rechtspraktischen und technologischen Fragen der Kontrolle deren Leistungsfähigkeit.

Kontrollgremien müssen über ausreichend Ressourcen und abschließende Entscheidungsbefugnisse verfügen. Angesichts der intensiven Kooperation von Nachrichtendiensten mit ausländischen und inländischen Diensten muss auch dafür Sorge getragen werden, dass die Kooperation der Aufsichtsgremien regelmäßig und ergebnisorientiert stattfindet. Dies ist wichtig, um zu verhindern, dass Kontrolldefizite entstehen. Häufig lassen sich die diversen Kooperationstätigkeiten der Dienste allein über die Kontrollpraxis der einen Seite nicht ausreichend einhegen. Es bedarf vielmehr gemeinsamer Kontrollstandards und Austauschmöglichkeiten der Kontrollgremien – insbesondere auch zu Methoden der nachrichtendienstlichen Informationsbeschaffung, die einige Aufsichtsgremien vielleicht noch nicht ausreichend verfolgen (de Ridder, 2019).

Die Anforderungen an den Zugang der Kontrollgremien zu Informationen und Daten der Nachrichtendienste hat die Sonderberichterstatterin der Vereinten Nationen für die Förderung und den Schutz der Menschenrechte im Rahmen der Bekämpfung des Terrorismus in ihrem Bericht an den Rat für Menschenrechte der Vereinten Nationen vom März 2023 gut zusammengefasst: Darin mahnt sie an, „dass den Aufsichtsgremien generell ein direkter Zugang zu den operativen Systemen der Nachrichtendienste gewährt wird und dass sie die Möglichkeit haben, gespeicherte Daten auf Eingabefehler zu überprüfen. Sie sollten auch in Überprüfungen der Datenminimierung einbezogen werden. Auf diese Weise wird die Kontrolle der nachrichtendienstlichen Protokollaufzeichnungen gewährleistet und es werden Methoden geschaffen, die eine Kontrolle ermöglichen, wenn die systematische Identifizierung von Mustern eine starke Überschneidung mit der illegalen und unangemessenen Nutzung nachrichtendienstlicher Datenbanken ergibt“ (Ní Aoláin, 2023, Rn. 50).

Bei nachrichtendienstlichen Datenkäufen kann es aufgrund des verdeckten Charakters der Informationsbeschaffung notwendig sein, das Grundrecht auf effektiven Rechtsschutz einzuschränken. Hier sollte diese Einschränkung, zumindest bei Fällen mit hoher Eingriffsintensität, ähnlich wie bei der strategischen Fernmeldeaufklärung des BND durch eine kontinuierlichen Rechtskontrolle kompensiert werden.

Eine ausreichende Kompensation wäre gemäß einer analogen Anwendung der Rechtsprechung des BVerfG aber nur dann gegeben, wenn eine „mit wirksamen Befugnissen ausgestattete Stelle“ (BVerfG, Urteil des Ersten Senats vom 26. April 2022, 1 BvR 1619/17 -, Rn. 1-407, Rn. 290) diese Datenkäufe und anschließende Datenverwendung kontrollieren könnte. Dafür bräuchte diese Kontrollinstanz zudem „Einblick in alle Überwachungsmaßnahmen, denen eine Person durch eine Behörde ausgesetzt ist“ (BVerfG, Urteil des Ersten Senats vom 26. April 2022, 1 BvR 1619/17 -, Rn. 1-407, Rn. 290), da die Verhältnismäßigkeit des Grundrechtseingriffs von der Gesamtwirkung aller auf die betroffene Person wirkende Maßnahmen abhängt.

5.3.3. Eigener Rechtsrahmen für die Kontrolle

Klare gesetzliche Standards sind nötig, um die Rechtmäßigkeit von Grundrechtseingriffen überprüfen zu können. Das betrifft auch den Rechtsrahmen für die Kontrolle. Entscheidend ist hier, dass wesentliche Informationen, beispielsweise zur institutionellen Ausgestaltung eines Aufsichtsgremiums, zur Bestellung seiner Mitglieder, zu seinem Kontrollmandat sowie zu seinen Kontrollrechten und -pflichten auch gesetzlich festgeschrieben sind.

5.4. Analyse und Bewertung des aktuellen Rechtsrahmens und der Praxis der Kontrolle

In diesem Abschnitt analysieren und bewerten wir anhand der genannten Kriterien den gegenwärtigen Rechtsrahmen für die Kontrolle nachrichtendienstlicher Datenkäufe und, sofern vorhanden und öffentlich erkennbar, die parlamentarische, datenschutzrechtliche und gerichtsähnliche Kontrollpraxis mit Bezug auf diese Form der nachrichtendienstlichen Informationserhebung.

5.4.1. Ausreichende Kontrollbefugnisse der Kontrollgremien?

Die zahlreichen Organe der Nachrichtendienstkontrolle in Deutschland entsprechen von ihrer institutionellen Ausgestaltung und ihrem allgemeinen gesetzlich festgeschriebenen Kontrollmandat[28] her in vielen Teilen den allgemeinen Anforderungen an die Unabhängigkeit und Effektivität der Kontrolle.[29] Vereinzelt gibt es aber auch hier

28 Hier sei auf das Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeiten des Bundes (PKGrG) und die öffentlich einsehbare Geschäftsordnung des Parlamentarischen Kontrollgremiums verwiesen. Ebenso auf die Vorgaben im Kapitel 4 des Bundesdatenschutzgesetzes (BDSG), insbesondere § 14 zu den Aufgaben und § 16 zu den Befugnissen des oder der BfDI und den Vorgaben zur G10-Kommission im Art. 10 Gesetz und zum Unabhängigen Kontrollrat im BND-Gesetz samt öffentlich einsehbarer Geschäftsordnung.

29 Siehe Wetzling (2024) zum Verbesserungsbedarf mit Blick auf die Effektivität und Unabhängigkeit des Unabhängigen Kontrollrats.

gewichtige Defizite: Im Kontext der anstehenden Reform des Nachrichtendienstrechts wäre es zum Beispiel wichtig, dem oder der BfDI verpflichtende Abhilfebefugnisse zu geben (Ruckerbauer, 2024). Zudem sollte der Unabhängige Kontrollrat als oberste Bundesbehörde einen eigenen und erweiterten Rechtsrahmen erhalten (Wetzling, 2024).[30]

Sind die einzelnen Kontrollinstanzen aber auch ausreichend mandatiert, um den nachrichtendienstlichen Datenkauf zu kontrollieren? Das wollen wir im Folgenden prüfen. Wir blicken zunächst auf die parlamentarische Kontrolle, gefolgt von der datenschutzrechtlichen und der gerichtsähnlichen Kontrolle.

5.4.1.1. Die parlamentarische Kontrolle könnte umfassend kontrollieren

Im Bereich der parlamentarischen Kontrolle spielt das Parlamentarische Kontrollgremium (PKGr) des Bundestages die entscheidende Rolle.[31] Es kontrolliert die Bundesregierung hinsichtlich der Tätigkeiten der drei Nachrichtendienste des Bundes (Deutscher Bundestag, 2024a, S. 3). Die Bundesregierung hat dem Gremium gegenüber eine Bringschuld: Sie unterrichtet das Gremium umfassend über die *allgemeine Tätigkeit* der Nachrichtendienste des Bundes und über *Vorgänge von besonderer Bedeutung*. Bei *sonstigen Vorgängen* hat das Gremium gegenüber der Bundesregierung eine Holschuld (siehe §4 PKGrG).

Laut der Anlage zu §4 der Geschäftsordnung des Parlamentarischen Kontrollgremiums hat der Gesetzgeber hier „bewusst unbestimmte und daher ausfüllungsbedürftige, verschiedenen Bewertungen zugängliche Rechtsbegriffe verwendet. Diese gestatten es, vielschichtige Konstellationen zu erfassen, ohne alle erdenklichen Sachverhalte antizipieren oder die Norm fortlaufend anpassen zu müssen“ (Deutscher Bundestag, 2016, S. 5).

Ob Datenkäufe von hoher Eingriffsintensität nun als Vorgang von besonderer Bedeutung, als allgemeine Tätigkeit oder aber als sonstiger Vorgang auszulegen sind, ist in der Regel eine „normative Einzelfallentscheidung“ (Deutscher Bundestag, 2016, S. 5). In der Anlage zur Geschäftsordnung werden *Vorgänge von besonderer Bedeutung* näher als „Geschehnisse oder Geschehensabläufe, die vom Routinegeschäft der

30 Das Mandat des UKRats (oberste Bundesbehörde) wird derzeit noch in einem Gesetz einer Bundesoberbehörde (BND) aufgeführt. Um klarer zu unterstreichen, dass der UKRat seine Kontrolltätigkeiten ohne Weisungsgebundenheit und Einflussnahme ausüben kann – auch wenn er formaljuristisch der Exekutive zugeordnet bleibt –, sollten die den UKRat betreffenden Vorschriften aus dem BND-Gesetz in ein eigenes UKR-Gesetz überführt werden.

31 Zudem sind das Vertrauensgremium nach § 10a Abs. 2 der Bundeshaushaltsordnung und das Art. 13-Gremium (vgl. Art. 13 Abs. 6 S.2 GG) zu nennen. Darüber greifen Ausschüsse des Deutschen Bundestages, z.B. der Innenausschuss und der Verteidigungsausschuss, aber auch Untersuchungsausschüsse regelmäßig Aspekte dem Politikfeldes Nachrichtendienste bzw. des Nachrichtendienstrechts auf. Außerdem stehen den einzelnen Mitgliedern des Bundestages zahlreiche Informationsrechte zu.

Nachrichtendienste (ND) abweichen und deren Kenntnis für eine effektive Kontrolle durch das Parlamentarische Kontrollgremium nach der Bewertung im Einzelfall unerlässlich ist“ (Deutscher Bundestag, 2016, S. 5) bezeichnet. Aus unserer Sicht stellt die von der Bundesregierung im Begründungstext zum 2023 neugefassten §10a BNDG erwähnte Praxis des Ankaufs von Daten aus Werbedatenbanken mit Blick auf deren hohe Grundrechtsrelevanz (aber auch aus Gründen der Datensicherheit und Datenqualität) durchaus eine Tätigkeit dar, über die das PKGr umfassend informiert werden sollte. Ob diese Praxis einen Vorgang von besonderer Bedeutung im Sinne des §4 PKGrG darstellt, ist hier nicht weiter entscheidend.[32] Viel wichtiger ist, dass diese Methode der nachrichtendienstlichen Informationsbeschaffung eine Praxis darstellt, die klar vom Kontrollrahmen des PKGr umfasst ist. Wesentliches Merkmal des PKGr ist ja, dass es „Zugriff auf einen dem Parlament ansonsten unzugänglichen Bereich der Exekutive“ (Deutscher Bundestag, 2024a, S. 4) hat.

Auch die Kontrollbefugnisse des PKGr scheinen hier zumindest der gesetzlichen Lage nach ausreichend: „Im Rahmen seiner Kontrollrechte kann das Kontrollgremium von der Bundesregierung bzw. den Nachrichtendiensten des Bundes verlangen, Akten oder andere in amtlicher Verwahrung befindliche Schriftstücke, gegebenenfalls auch im Original, herauszugeben und in Dateien gespeicherte Daten zu übermitteln sowie jederzeit Zutritt zu sämtlichen Dienststellen der Nachrichtendienste des Bundes zu erhalten (§5 Absatz 1 PKGrG). Das Kontrollgremium kann auch Bedienstete der Nachrichtendienste befragen oder von ihnen schriftliche Auskünfte einholen (§ 5 Abs. 2 PKGrG). Die Bundesregierung hat solchen Informationsverlangen des Kontrollgremiums unverzüglich zu entsprechen (§ 5 Abs. 3 PKGrG). Diese Befugnisse ermöglichen eine „frühzeitige und kontinuierliche Kontrolle“ (Deutscher Bundestag, 2024a, S. 4).

Ein Ständiger Bevollmächtigter unterstützt die Mitglieder des Kontrollgremiums durch „regelmäßige und einzelfallbezogene Untersuchungen“ (§ 5a Abs. 1 PKGrG). Zudem kann das Kontrollgremium mit der Mehrheit von zwei Dritteln seiner Mitglieder nach Anhörung der Bundesregierung im Einzelfall einen Sachverständigen oder eine Sachverständige beauftragen, zur Wahrnehmung seiner Kontrollaufgaben Untersuchungen durchzuführen (§ 7 Absatz 1 PKGrG).

32 Laut §4 Abs. 1 S. 2 Nr. 2 PKGrG können insbesondere „behördeninterne Vorgänge mit erheblicher Auswirkung auf die Aufgabenerfüllung“ einen besonderen Vorgang darstellen. Hier sei angemerkt, dass der Ankauf von Werbedatenbanken (ADINT) und das systematische Zusammenführen von öffentlich verfügbaren Daten (OSINT) in der nachrichtendienstlichen Praxis einen Paradigmenwechsel eingeleitet hat (Wetzling & Dietrich, 2022).

5.4.1.2. Der oder die BfDI könnte umfassend kontrollieren

Ähnlich wie bei der parlamentarischen Kontrolle durch das PKGr umfasst das Kontrollmandat der oder des BfDI grundsätzlich auch den nachrichtendienstlichen Datenkauf. Die allgemeine Kontrollbefugnis der oder des BfDI ergibt sich aus dem Bundesdatenschutzgesetz (siehe §16 Absatz 2 und 3 BDSG). Das Nachrichtendienstrecht erteilt dem oder der BfDI zudem einen expliziten Auftrag, die Einhaltung der Vorschriften über den Datenschutz zu überprüfen.[33] Der oder die BfDI hat im Bereich der Nachrichtendienste weitreichende Zugangs-, Auskunfts- und Einsichtsrechte (Sosna, 2022, S. 247), definiert werden diese in §28 Abs. 3 BVerfSchG. Im Ergebnis ist es so möglich, „einen Großteil der Tätigkeiten der Nachrichtendienste des Bundes zu kontrollieren, liegt doch der überwiegende Teil ihrer Tätigkeiten in der Verarbeitung personenbezogener Daten, also vor allem in der Erhebung und Speicherung, aber auch der Analyse und der Übermittlung an andere Stellen“ (Sosna, 2022, S. 247).

Das wichtigste Instrument des oder der BfDI, um Datenschutzmängel oder -verstöße abzustellen, ist die Beanstandung nach §16 Abs. 2 BDSG (Sosna, 2022, S. 248). Der oder die BfDI muss zudem angehört werden, wenn die Dienste eine Dateianordnung erlassen. Diese Anhörungspflicht bietet die Gelegenheit auf datenschutzrechtliche Bedenken hinzuweisen und verschafft dem oder der BfDI einen umfassenden Einblick in die Tätigkeiten der Nachrichtendienste. Denn solche „Dateianordnungen sind für jede automatisierte Datei zu erstellen“ (Sosna, 2022, S. 247).

5.4.1.3. Die G10-Kommission und der Unabhängige Kontrollrat bisher ohne Zuständigkeit

Im Gegensatz zur parlamentarischen und datenschutzrechtlichen Kontrolle lässt sich der Kompetenzkatalog des vom Bundestag bestellten Hilfsorgans zur quasi-richterlichen Kontrolle von Beschränkungsmaßnahmen nach dem Art. 10 Gesetz (G10-Kommission) nicht ohne eine Novellierung des Nachrichtendienstrechts auf nachrichtendienstliche Datenkäufe erstrecken. Gleiches gilt für den UK-Rat, der bis jetzt allein die Kontrolle der Rechtmäßigkeit der technischen Aufklärung nach Abschnitt 4 des BND-Gesetzes verantwortet.

Im Zuge der bundespolitischen Reaktion auf das Karlsruher Urteil zum BayVSG[34] wird ohnehin darüber nachgedacht, die Vorabkontrolle für weitere Maßnahmen der nachrichtendienstlichen Informationsbeschaffung einzuführen. Deshalb sollte die Umgestaltung der Kontrolllandschaft dazu genutzt werden, das bestehende Kontrolldefizit hinsichtlich des nachrichtendienstlichen Datenkaufs auszugleichen (siehe Kapitel 6).

33 Siehe Sosna (2022) mit weiterführenden Informationen zur Datenschutzaufsicht über die Nachrichtendienste des Bundes.

34 Bayrisches Verfassungsschutzgesetz

5.4.2. Ausreichende Kontrollpraxis?

Entscheidender als die Frage, ob die Kontrollinstanzen ausreichend mandatiert sind, um die Praxis nachrichtendienstlicher Datenkäufe zu kontrollieren, ist die Frage, ob sie ihre Befugnis auch nutzen. In diesem Abschnitt soll es daher darum gehen, ob, und wenn ja welche, Kontrollpraxis mit Blick auf die grundrechtsrelevanten nachrichtendienstlichen Datenkäufe zu erkennen ist.

Aufgrund der gebotenen Geheimhaltung stehen uns als Außenstehende hier nur bedingt belastbare Informationen zur Verfügung. Die folgenden Informationen stammen aus Gesprächen mit Mitgliedern der verschiedenen Aufsichtsgremien und dem Studium ihrer jeweiligen Tätigkeitsberichte.

5.4.2.1 Nachrichtendienstliche Datenkäufe: Bisher kein berichtenswerter Gegenstand der parlamentarischen Kontrolle

Was die parlamentarische Kontrollpraxis betrifft, so wissen wir beispielsweise nicht, ob diese Praxis der Informationsbeschaffung in den 47 Sitzungen des PKGr zwischen Oktober 2021 und September 2023 auf der Tagesordnung stand. Wir stellen aber fest, dass diese Form der nachrichtendienstlichen Informationsbeschaffung weder im letzten, noch in den vorherigen öffentlich einsehbaren Berichten des PKGr Erwähnung fand. Sachverständige haben dazu keine Untersuchungen geführt.

Laut PKGr-Bericht wurde der Ständige Bevollmächtigte „mit insgesamt neun strukturellen Untersuchungen beauftragt. Zudem wurden fünf Untersuchungen, mit denen der Ständige Bevollmächtigte in der 19. Wahlperiode beauftragt wurde, im Berichtszeitraum abgeschlossen“ (Deutscher Bundestag, 2024a, S. 12). Was genau Thema dieser Untersuchungen war, wissen wir nicht. Laut PKGr-Bericht gehören dazu „regelmäßig die Aufgaben und Zuständigkeiten des Nachrichtendienstes im untersuchungsgegenständlichen Bereich, Struktur und Kooperationen, Methodik und Einsatz nachrichtendienstlicher Mittel und eine fachliche Bewertung (§ 2 Abs. 5 S. 1 Anlage 2 zur GO-PKGr). Die fachliche Bewertung umfasst regelmäßig Aussagen zur Rechtmäßigkeit des Vorgehens, zur Geeignetheit der Prozesse und Strukturen, Ressourceneinsatz, Erfolgen und Optimierungspotenzial (§ 2 Abs. 5 S. 2 Anlage 2 zur GO-PKGr)“ (Deutscher Bundestag, 2024a, S. 12).

Falls unter den neun Untersuchungen des Ständigen Bevollmächtigten auch eine zur Methodik und zum Einsatz nachrichtendienstlicher Datenkäufe samt fachlicher Bewertung gewesen sein sollte, stellt sich die Frage, warum dies im PKGr-Bericht nicht weiter thematisiert wurde.

Mit Blick auf die Nutzung von Steuergeldern wäre es auch angezeigt, diese Praxis im Vertrauensgremium zu thematisieren. Diesem Gremium des Bundestages obliegt die Bewilligung von Ausgaben, die der Geheimhaltung unterliegen. Auch hier ist es uns nicht möglich, die tatsächliche Praxis des Vertrauensgremiums in dieser Frage zu beleuchten.

Für die nachrichtendienstlichen Tätigkeiten der Bundeswehr hat das PKGr keine Zuständigkeit. Der Verteidigungsausschuss ist zwar für die Kontrolle des Militärischen Nachrichtenwesens zuständig. Solange er sich aber nicht selbst als Untersuchungsausschuss einsetzt, ist der Zugang zu beispielsweise den Zentralen Dienstvorschriften in diesem Bereich und den Überwachungstätigkeiten extrem beschränkt. Der Verteidigungsausschuss sollte aber im Rahmen seiner Möglichkeiten auch die Praxis des Datenkaufs im Bereich des Militärischen Nachrichtenwesens beleuchten.[35]

5.4.2.2. Nachrichtendienstliche Datenkäufe: Bisher kein berichtenswerter Gegenstand der Kontrolle durch die oder den BfDI

Die Tätigkeitsberichte der oder des BfDI sind stets lesenswert und für Außenstehende deutlich informativer als die vergleichsweise spärlichen Berichte des PKGr. Mit Blick auf die hier zur Diskussion stehende Praxis geben aber auch sie keinen Hinweis darauf, ob die Nutzung käuflich erworbener Daten im Fokus der datenschutzrechtlichen Kontrolle stand.

Interessanterweise moniert die oder der BfDI in seinem 32. Tätigkeitsbericht – aus unserer Sicht völlig zurecht–, dass der Gesetzgeber keine „Rechtsgrundlage für die vorgelagerte Verarbeitung systematisch erhobener oder zusammengeführter personenbezogener Daten aus allgemein zugänglichen Quellen“ (Deutscher Bundestag, 2024b, S. 88) geschaffen habe. Als Außenstehende erfahren wir in seinem Tätigkeitsbericht aber nicht, inwiefern die von der systematischen Erhebung und Zusammenführung allgemein zugänglicher Quellen (OSINT) zu trennende Praxis der nachrichtendienstlichen Datenkäufe Teil der Kontrolltätigkeit der Kontrollpraxis der oder des BfDI war. Interessant sind in diesem Kontext auch die Ausführungen einer Referatsleiterin der Behörde, die es für denkbar hält, dass „sich Dritte, ohne dass weder [die betroffene Person] noch der jeweilige Betreiber etwas davon weiß, all diese faktisch zugänglichen Daten zusammensuchen, was auch als Scraping bezeichnet wird. Und die diese Datensätze gerne an Vierte verkaufen. Spätestens dann sucht man eine Rechtsgrundlage wohl vergebens“ (Sosna, 2024, S. 53).

35 Im Allgemeinen sollte auch der verfassungswidrige Zustand behoben werden, dass im Bereich des Militärischen Nachrichtenwesens ohne spezifische gesetzliche Grundlage schwer in Grundrechte eingegriffen werden kann. Auch das eklatante Kontrolldefizit sollte beseitigt werden (Ruckerbauer & Wetzling, 2023).

Damit die oder der BfDI die Nutzung von gekauften Daten durch die Nachrichtendienste effektiv kontrollieren kann, braucht sie oder er Einblick in die Verträge der Nachrichtendienste mit den Datenhändlern. Nach den Bestimmungen in §28 Abs. 3 BVerfSchG müssen die Dienste der oder dem BfDI diesen Einblick gewähren. Es wäre von öffentlichem Interesse zu erfahren, ob dies auch in der Praxis so gehandhabt wird. Etwaige Einwände der datenführenden Nachrichtendienste könnten wir zumindest als Außenstehende nicht nachvollziehen.

Eine Herausforderung in der Praxis besteht zudem in der fehlenden Befugnis der oder des BfDI, die Behebung eines beanstandeten Zustands verpflichtend anordnen zu können (Ruckerbauer, 2024). Zwar kann auch „die Fachaufsicht [...] den Nachrichtendienst dazu anhalten, diese Verstöße abzustellen, auch wenn der Nachrichtendienst anderer Meinung ist. In der Praxis ist [aber] feststellbar, dass die Fachaufsicht häufig die Rechtsauffassung des verantwortlichen Nachrichtendienstes teilt und keine Abhilfemaßnahmen veranlasst. Auffällig ist dies insbesondere dann, wenn eine Datenverarbeitung auf eine unzureichende Rechtsgrundlage gestützt wird“ (Sosna, 2022, S. 248). Wie sehr die fehlenden Befugnisse des oder der BfDI die Kontrollfähigkeit beeinträchtigen können verdeutlicht auch die jüngst angestrengte Klage der Behörde gegen den BND, weil der Kontrollbehörde die Einsicht in wesentliche Unterlagen verweigert werden (BfDI 2024).

5.5. Zwischenfazit: Unzureichende Kontrolle

Die Bedeutung von Datenkäufen als Methode nachrichtendienstlicher Informationsbeschaffung nimmt zu. Wie in Kapitel 3 beschrieben, kann diese Praxis mit schweren Grundrechtseingriffen verbunden sein. Unserer Auffassung nach ist es daher dringend geboten, diese Praxis intensiv zu kontrollieren. Die Tätigkeitsberichte des PKGr und des oder der BfDI geben bisher leider keine Auskunft darüber, inwiefern nachrichtendienstliche Datenkäufe Gegenstand der tatsächlich praktizierten Kontrolle waren. Wir bedauern zudem, dass die gesetzlich festgeschriebenen Kompetenzen der einzelnen Kontrollgremien nicht ausreichen, um die mit dieser Praxis verbundenen Grundrechtseingriffe gemäß den in Kapitel 4 und 5 beschriebenen Anforderungen entsprechend auf ihre Zulässigkeit und Notwendigkeit hin überprüfen zu können. Es fehlen vor allem ein Genehmigungsverfahren und ein Prozess der gerichtsähnlichen Kontrolle für den Kauf und die Verwendung von Daten mit besonderer Eingriffsintensität.

6. Handlungsempfehlungen

Dieses Papier hat Datenkäufe als Praxis der nachrichtendienstlichen Informationsbeschaffung in den Fokus genommen. In diesem Kapitel sprechen wir vier Handlungsempfehlungen aus, deren Umsetzung unserer Meinung nach dringend geboten ist. Vorher fassen wir kurz zusammen, warum gesetzgeberische und politische Veränderungen in Angriff zu nehmen sind.

6.1. Warum die Praxis nachrichtendienstlicher Datenkäufe grundlegende Veränderungen im Nachrichtendienstrecht und der Nachrichtendienstkontrolle erfordert

Auf dem Datenmarkt können Nachrichtendienste in vielerlei Art tätig werden: Sie können an Real-Time-Bidding-Auktionen teilnehmen und durch das Schalten von Werbeanzeigen in Apps eine Vielzahl personenbezogener Daten erheben. Sie können zudem über Datenhändler, die sich auf ihre Bedürfnisse spezialisiert haben, eine Reihe unterschiedlicher Datenprodukte erwerben (Brayne, 2020, S. 25; Tau, 2023).

Datenhändler ermöglichen den Zugang zu Listen von Personenprofilen mit Wohnadressen, Gesundheitsinformationen, politischen Überzeugungen, Interessenprofilen, Religionszugehörigkeit und anderen Informationen. In den Niederlanden ist es einem Rechercheteam gelungen, einen Datensatz mit Bewegungsdaten von vier Millionen niederländischen Telefonen zu erhalten – verbunden mit der jeweils einzigartigen Werbe-ID (Dachwitz & Meineck, 2024). Diese Daten sind alles andere als uninteressant für Nachrichtendienste: Wer genauere Informationen über Teilnehmende einer bestimmten Demonstration benötigt, kann so beispielsweise internetfähige Geräte, die sich zum Zeitpunkt der Versammlung in der Gegend befunden haben, identifizieren. In ähnlicher Weise ist es aufgrund der auf dem Datenmarkt erworbenen Bewegungsdaten möglich, Mobilgeräte in Grenzgebieten aufspüren (vgl. Ng, 2022). Auch ist es Nachrichtendiensten möglich, Softwarelösungen mit integrierten Datensätzen aus dem RTB-Markt zu kaufen, um Nutzer:innen von Apps dauerhaft zu tracken und Alarm zu schlagen, wenn das Bewegungsprofil einer Person oder deren Verhalten aus der Reihe fällt.

Auch in Deutschland ist davon auszugehen, dass Nachrichtendienste die zahlreichen Möglichkeiten des Datenmarktes nutzen, um Informationen einzukaufen. Während über einzelne Datenkäufe wenig bekannt ist, entnehmen wir der Begründung der BNDG-Novelle vom Herbst 2023, dass der BND sich auf dem Datenmarkt Informationen beschafft. Schließlich beschreibt die Bundesregierung dort im Zusammenhang mit §10a Abs. 1 BNDG, dass „spezielle Datenbanken“ genutzt werden, die auch „zahlungspflichtige Angebote“ sein können (Bundesregierung, 2023a, S. 42). Zu §10a Abs. 2 wird zudem erklärt, dass sich diese Regelung auch auf die „Übermittlung

von Daten aus dem Ankauf z.B. von umfänglichen Werbedatenbanken und anderen Datenbanken mit vergleichbarer Eingriffsintensität“ beziehen (Bundesregierung, 2023a, S. 43). Wir gehen davon aus, dass sich neben dem BND auch BAMAD und BfV dieser Praxis der Informationsbeschaffung bedienen.

Unbestritten ist, dass Datenkäufe derzeit einen enormen Vorteil für die Nachrichtendienste bieten: Diese Praxis kann zwar auch erhebliche Grundrechtseingriffe beinhalten (Kapitel 3), aber sie ist – anders als andere Formen der nachrichtendienstlichen Informationsbeschaffung – nicht an ein Genehmigungsverfahren gebunden. Die Verarbeitung von Daten aus dieser Methode ist gesetzlich auch deutlich weniger eingeschränkt. Unsere detaillierten Ausführungen zum Rechtsrahmen (Kapitel 4) und zur Kontrolle (Kapitel 5) haben vielmehr gezeigt, dass gesetzliche Vorgaben und öffentlich wahrnehmbare Kontrollpraxis hier geradezu rudimentär sind. Datenkäufe bieten daher nicht nur die Möglichkeit, die über andere Methoden erhobenen Informationen weiter anzureichern, sondern auch, an Informationen zu gelangen, deren Erhebung den Nachrichtendiensten über andere Mittel niemals gestattet wäre oder zumindest umfangreiche Genehmigungsverfahren voraussetzen würde (ODNI, 2022, S. 13). Der Kauf von Daten bietet derzeit also einen Weg, elementare rechtsstaatliche Anforderungen an Grundrechtseingriffe zu umgehen (Cameron, 2023; Tau, 2024b).

Weil der Kauf und die Verwendung der auf dem Datenmarkt erhältlichen Informationen einen schweren Eingriff in Grundrechte darstellen kann (siehe Kapitel 3), besteht aus unserer Sicht jetzt ein dringender gesetzgeberischer Handlungsbedarf: Diese Beschaffungsmethode sollte zukünftig besser geregelt werden. Um einen unverhältnismäßigen nachrichtendienstlichen Zugriff auf personenbezogene Daten und den daraus erwachsenden Missbrauchsgefahren vorzubeugen, muss der Datenkauf auf ein notwendiges Maß beschränkt werden. Diese Praxis sollte auch deutlicher im Fokus der Nachrichtendienstkontrolle stehen. Zur Wahrung der Rechtmäßigkeit bei besonders starken Grundrechtseingriffen gehören dazu auch ein unabhängiges Genehmigungsverfahren und die Vorabkontrolle durch ein gerichtsähnliches Aufsichtsgremium.

Im Rahmen der angekündigten Reform des Nachrichtendienstrechts bietet sich dem Gesetzgeber in den nächsten Monaten die Chance, die dringend benötigte und für den Sommer 2024 angekündigte „wertungskonsistente Systematisierung der Regelungen zur Informationsbeschaffung“ (Bundesregierung, 2023b, S. 1) in Angriff zu nehmen. Gravierende Defizite beim Rechtsrahmen und der Kontrolle sollten dabei nicht auf die lange Bank geschoben werden. Starke Grundrechtseingriffe sollten eine ähnliche Regelungs- und Kontrolldichte erfahren. Wie dieser Impuls mit Blick auf nachrichtendienstlichen Datenkäufe verdeutlicht hat, ist dies derzeit noch nicht ansatzweise der Fall.

6.2. Konkrete Handlungsempfehlungen

Wir glauben, dass die folgenden vier Kernforderungen an den Gesetzgeber geeignet sind, den Weg zu einer verfassungskonformen Praxis dieser nachrichtendienstlichen Beschaffungsmethode zu ebnen. Die Forderungen leiten sich aus unserer Sicht aus den vorgenannten Kapiteln ab, sie bedürfen aber noch der weiteren Präzisierung. Wir freuen uns daher über jedwede Kommentare und Kritik.

6.2.1. Nehmt eine Systematisierung der Grundrechtseingriffe beim Datenkauf vor

Wenn Nachrichtendienste Daten kaufen, kann das viele verschiedene denkbare Formen annehmen – mit ebenso vielfältigen möglichen Auswirkungen auf die Grundrechte der Betroffenen. Kauft ein Nachrichtendienst Informationen darüber, ob ein Individuum regelmäßig öffentliche Verkehrsmittel nutzt, liegt eine geringere Eingriffsintensität vor als wenn ein Nachrichtendienst, wie in Anwendungsbeispiel 2 beschrieben, massenhaft individualisierte Bewegungsdaten kauft. Diesen Unterschieden sollte auch der Rechtsrahmen Rechnung tragen.

Für die schweren grundrechtlichen Eingriffe ist dringend eine gesetzliche Grundlage notwendig, die strenge Sicherungsmechanismen vorsieht, um die Verhältnismäßigkeit der Eingriffe zu gewährleisten. Für solche Datenkäufe, die weniger schwerwiegend in Grundrechte eingreifen, können die Eingriffsschwellen niedriger ausgestaltet werden. Hierfür muss der Gesetzgeber aber eine Systematik entwickeln, die der jeweiligen grundrechtlichen Relevanz gerecht wird.

Die Aufgabe, die vielen für das Eingriffsgewicht relevanten Faktoren dabei in angemessener Weise miteinzubeziehen, ist sicher eine herausfordernde. Im Folgenden haben wir einige Denkanstöße, Eckpunkte und Fragen aufgeführt, die bei der Ausarbeitung eines wertungskonsistenteren Rechtsrahmens berücksichtigt werden sollten.

Grundlage für diese Systematisierung sollten die in der verfassungsgerichtlichen Rechtsprechung entwickelten Grundsätze zur Bestimmung des Eingriffsgewichts sein. Während in der Literatur ausführlich diskutiert wird, wie eine Systematisierung der Eingriffsintensität klassischer Überwachungsmethoden aussehen könnte, steht eine spezifische Diskussion der Grundrechtewirkung von Datenkäufen noch am Anfang. Hinsichtlich der Klassifizierung des Eingriffsgewichts wird meist zwischen drei oder vier Stufen von geringfügigen bis schwersten Grundrechtseingriffe differenziert (Sosna, 2024, S. 58). Derzeit erarbeitet das Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht im Auftrag der Bundesregierung eine Überwachungsgesamtrechnung. Die Erkenntnisse hieraus, insbesondere hinsichtlich der methodenübergreifenden Bestimmung des Eingriffsgewichts, könnten auch in diesem Kontext hilfreich sein.

Wir haben in Kapitel 3 bereits zentrale Kriterien zur Bestimmung des Eingriffsgewichts erörtert. Eine umfangreichere Liste stellt dabei unter anderem auf diese Faktoren ab:

→ „die Anzahl der unmittelbar betroffenen Grundrechtsträger,

→ die Möglichkeit der Anwendung gegenüber Berufsgeheimnisträgern,

→ der Schutz des Kernbereichs privater Lebensgestaltung, [...]

→ ihre ‚Streuwirkung',

→ ihre ‚Heimlichkeit', [...]

→ die Möglichkeit der Bildung von Verhaltens-, Kommunikations-, Bewegungs- oder Persönlichkeitsprofilen,

→ der Grad der ‚Beschädigung' des betroffenen Grundrechts, [...]

→ die Art und Weise der Datenerhebung und etwaiger sie vorbereitender Maßnahmen,

→ ob die Maßnahme durch den Staat selbst oder mithilfe privater Dritter durchgeführt wird, [...]

→ besondere Gefahren und weitere Konsequenzen für Betroffene,

→ die Möglichkeiten der weiteren Verwendung erhobener Daten, [...]

→ ob Betroffene selbst einen Anlass für den Eingriff geschaffen haben,

→ ob Schutzvorkehrungen gezielt unterlaufen werden, sowie

→ die gesamtgesellschaftlichen Auswirkungen auf das Verhalten potenzieller Betroffener" (Poscher et al., 2022, S. 20 mit Verweis auf Löffelmann GSZ 2019, 16 (19)).

Solche Kataloge intensitätsbestimmender Faktoren, die aus der Rechtsprechung des BVerfG abgeleitet sind, ließen sich nutzen, um unterschiedliche Kategorien mit unterschiedlichen Sicherungsmechanismen und Kontrollintensitäten zu versehen. Bei der Bestimmung der Eingriffsintensität der Datenkäufe bedarf es letztlich einer genauen Auseinandersetzung mit den angebotenen Produkten auf den Datenmarkt und mit der beabsichtigten und tatsächlichen Verwendung durch die Nachrichtendienste.

Noch ist wenig über die Umsetzung der Überwachungsgesamtrechnung bekannt. Bei der Arbeit an diesem Evaluierungswerkzeug für die bestehenden Überwachungsbefugnisse der Sicherheitskräfte sollten die zahlreichen informationstechnischen Befugnisse der Dienste, die sich derzeit hinter der Generalklausel verstecken, berücksichtigt werden. Das gilt sicher auch für nachrichtendienstliche Datenkäufe.

Ausgehend von der anwendungssicher gestalteten Unterscheidung zwischen Datenkäufen, die besonders schwer in Grundrechte eingreifen, und solchen, die eine

geringfügige Wirkung auf Grundrechte der Betroffenen haben, sollte der Gesetzgeber dann einen angemessenen gesetzlichen Rahmen schaffen.

6.2.2. Schafft Sicherungsmechanismen für Datenkäufe mit besonders schweren Auswirkungen auf Grundrechte

Wie in Kapitel 3 dargelegt, kann bereits der Kauf von personenbezogenen Daten schwer in Grundrechte eingreifen. Ganz grundsätzlich sollte eine Diskussion darüber stattfinden, welche Form der Datenkäufe überhaupt durch die Nachrichtendienste getätigt werden sollten und wo rote Linien verlaufen sollten. Für Eingriffe, die man den Nachrichtendiensten ermöglichen möchte, braucht es dann eine ausreichende rechtliche Legitimierung. Um unverhältnismäßige Auswirkungen auf die Betroffenen und die Gesellschaft als Ganzes vorzubeugen, sollte der Gesetzgeber die notwendigen Sicherungsmaßnahmen in einer gesetzlichen Grundlage verankern, die zentrale rechtsstaatliche Prinzipien gewährleistet. Ein Festhalten an der Praxis, ohne die gesetzliche Grundlage zu schaffen wäre, nicht mit dem Grundgesetz vereinbar.

Anordnungsvoraussetzungen. In einer gesetzlichen Grundlage für besonders eingriffsintensive Datenkäufe muss benannt werden, unter welchen Voraussetzungen ein solcher Kauf von Daten überhaupt zulässig sein soll.

Legitime Zwecke. Um die Verhältnismäßigkeit zu gewährleisten, müssen mindestens die legitimen Zwecke, deren Erfüllung der Datenerwerb dienen soll, in der Gesetzesgrundlage genannt werden. Orientieren könnte sich der Gesetzgeber hierfür am Katalog der zulässigen Zwecke für Maßnahmen der strategischen Fernmeldeaufklärung in §19 Abs. 4 BNDG. Zudem sollte hier festgelegt werden, dass tatsächliche Anhaltspunkte dafür vorliegen müssen, dass aus den zu erwerbenden Daten Erkenntnisse mit Bezug auf die Verfolgung der legitimen Zwecke gewonnen werden können.

Schriftliches Anordnungsverfahren. Zudem sollte festgelegt werden, wann Datenkäufen eine schriftliche Anordnung vorausgehen muss, in der ebenjene verfolgten Zwecke und der beabsichtigte Erkenntnisgewinn begründet werden.

Filtervorgaben. Um sicherzustellen, dass der Eingriff auf möglichst gezielte Weise erfolgt, sollten analog zu den Regelungen zur strategischen Auslands-Fernmeldeaufklärung auch Filtervorgaben gemacht werden. Dabei sollte die unmittelbare Löschung der für das Aufklärungsinteresse nicht relevanten Daten vorgeschrieben werden.

Relevanzprüfung und Löschpflichten. Auch für die in diesem initialen Filtervorgang nicht unmittelbar gelöschten Daten sollten Vorgaben zur kontinuierlichen Prüfung der Relevanz der erhobenen Daten und der Löschfristen festgelegt werden, die über die allgemeinen Vorgaben zur Datenverarbeitung der Nachrichtendienste hinaus gehen.

Zweckbindung und Kennzeichnungspflicht. Der Ankauf von großen Datensammlungen birgt das Risiko, dass Daten verfassungswidrig auf ‚Vorrat' zurückgehalten werden, um diese bei Bedarf später erneut und gegebenenfalls für andere Zwecke zu analysieren. Der Anlass für eine solche erneute Verwendung in der Vergangenheit erworbener und zurückgehaltener Daten können dabei neue Ermittlungsvorgänge sein – oder aber neue Möglichkeiten (oder Befugnisse) der Datenanalyse, die zuvor nicht mögliche Informationsextraktionen zulassen. Die Wiederverwendung erhobener Daten zu anderen Zwecken widerspricht aber dem Prinzip der Zweckbindung. Die zweckverändernde Verarbeitung von Daten darf deshalb nur unter bestimmten Umständen ermöglicht werden. Sie müssen dem verfassungsgerichtlichen Kriterium der hypothetischen Datenneuerhebung genügen. Um diese Prüfung der Zulässigkeit der Verwendung für einen anderen Zweck durchführen zu können, müssen diese Daten aber auch entsprechend gekennzeichnet werden. Der Gesetzgeber muss deshalb auch eine Kennzeichnungspflicht für gekaufte Daten vorschreiben.

Schutz von Berufsgeheimnisträger:innen. Der Gesetzgeber sollte zusätzliche Sicherungsmechanismen vorsehen, um dem besonderen Schutzniveau von Informationen, die Vertraulichkeitsbeziehungen von Berufsgeheimnisträger:innen betreffen, zu gewährleisten. Das betrifft beispielsweise Informationen, die Aufschluss über die Quellen von Journalist:innen oder die Beziehungen zwischen Gläubigen und Geistlichen geben können.

Schutz des Kernbereichs privater Lebensgestaltung. Auch der Kernbereich der privaten Lebensgestaltung muss bei einer Novellierung des Nachrichtendienstrechts und der Schaffung einfachgesetzlicher Grundlagen für eingriffsintensive Datenkäufe besonders geschützt werden. Wie auch bei der Fernmeldeaufklärung besteht beim Kauf der auf dem Datenmarkt erhältlichen Informationen ein hohes Risiko, in diese besonders geschützten Bereiche einzudringen (siehe Kapitel 3.1).

Kompensationsmechanismen für eingeschränkten Zugang zu effektivem Rechtsschutz. In Kapitel 4.1. wird beleuchtet, wie der Zugang für Betroffene zu ihrem Grundrecht auf effektiven Rechtsschutz dadurch beeinträchtigt wird, dass Nachrichtendienste beim Ankauf von Daten verdeckt vorgehen. Hieraus erwächst für den Gesetzgeber die Pflicht, entsprechende Kompensationsmechanismen vorzusehen. Eine Möglichkeit hierfür sind die Benachrichtigungspflichten für Betroffene. Doch ist schwer vorstellbar, wie eine Benachrichtigung aller in einem gekauften Datensatz erfassten Personen sinnvoll umsetzbar ist. Denn zum einen bestehen erhebliche

Zweifel an der technischen Durchführbarkeit und auch zum anderen ist fraglich, ob das im Interesse der Betroffenen wäre.[36] Eher sollte deshalb auf die Möglichkeit zurückgegriffen werden, fehlende Benachrichtigungspflichten durch die Vorabkontrolle einer unabhängigen Stelle zu kompensieren.

6.2.3. Schafft eine angemessene Kontrolle für nachrichtendienstliche Datenkäufe

In Kapitel 5 haben wir beleuchtet, dass die derzeitige Kontrollpraxis der grundrechtlichen Bedeutung der Datenkäufe durch Nachrichtendienste nicht ausreichend gerecht wird. Der Gesetzgeber sollte im Zuge der anstehenden Nachrichtdienstreform daher bessere Voraussetzungen für eine effektive Kontrollpraxis schaffen. Zudem würden wir uns wünschen, dass die Kontrollgremien ihre bestehenden Möglichkeiten intensiv nutzen. Wo möglich, sollten sie zudem der Öffentlichkeit detaillierter darüber berichten.

Unabhängiges Genehmigungsverfahren für besonders schwere Grundrechtseingriffe. Eine unabhängige vorbeugende Kontrolle ist hier nötig, denn die Grundrechtseingriffe können schwerwiegend sein und die Betroffenen können die Einschränkungen in aller Regel nicht wahrnehmen. Dass dadurch erhebliche negative Konsequenzen für Individuen und Demokratie erwachsen können, haben wir in Kapitel 3 dargelegt. Um die Verhältnismäßigkeit der Maßnahmen sicherzustellen und um den stark eingeschränkten Zugang zu effektivem Rechtsschutz zu kompensieren, sollte der Gesetzgeber in Zukunft auch diese Methode der Informationsbeschaffung in besonders schwerwiegenden Fällen einer Vorabkontrolle unterwerfen. Welcher gerichtsähnlichen Kontrollinstanz dieser Auftrag zukommen soll, müsste natürlich noch entschieden werden (Wetzling & Vieth-Ditlmann, 2023). Sollte der UKRat dieses Mandat bekommen, wären dort zunächst noch eine Reihe von Veränderungen vorzunehmen (Wetzling, 2024).

Parlamentarische Kontrolle intensivieren. Das Parlament sollte seine Kontrollkompetenzen in diesem Bereich nutzen und die Praxis des nachrichtendienstlichen Datenkaufs beleuchten. Das PKGr könnte den Ständigen Bevollmächtigten damit beauftragen, regelmäßig Untersuchungen durchzuführen. Zudem könnten auch Sachverständige beauftragt werden, für das Gremium Untersuchungen zu nachrichtendienstlichen Datenkäufen durchzuführen. Weil das PKGr hier nicht kontrollieren

36 Ein zu großer Aufwand allein ist jedoch noch kein hinreichendes Argument, um die verfassungsrechtlichen Anforderungen schlicht nicht einzuhalten. Aber die zur Benachrichtigung notwendigen datenverarbeitende Schritte können den Grundrechtseingriff in einem solchen Maß verstärken, dass aus datenschutzrechtlicher Sicht eine Nicht-Benachrichtigung zu bevorzugen ist. Das gilt beispielsweise dann, wenn die Daten der Betroffenen nur zufällig miterworben wurden, die Betroffenen nur unerheblich eingeschränkt werden und daher anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung haben (BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345, Rn. 245).

kann, sollte im Bereich des Militärischen Nachrichtenwesens zumindest der Verteidigungsausschuss in Erfahrung bringen, inwieweit diese Methoden der Informationsbeschaffung dort auch zum Einsatz kommen.

Kontrolle durch den oder die BfDI stärken. Der oder die BfDI kann im Rahmen seines oder ihres Mandats bereits alle datenverarbeitenden Tätigkeiten der Nachrichtendienste kontrollieren. Dazu gehören auch der Erwerb und die Verarbeitung von käuflich erhältlichen Daten. Bisher haben sich die Datenschutzbeauftragten in ihren Tätigkeitsberichten zu dieser Form der Informationsbeschaffung und ihren grundrechtlichen Auswirkungen nicht geäußert. Angesichts der hohen Relevanz des Themas und der neuen Herausforderungen, die damit einhergehen, wäre es zukünftig dringend geboten, dass diese Praxis einen zentraleren Stellenwert in der sicherheitsbehördlichen Kontrolltätigkeit des oder der BfDI einnimmt. Ein öffentliches Berichten über grundlegende Problematiken dieser Informationsbeschaffungsmethode muss dem oder der BfDI ermöglicht werden und Geheimhaltungsvorschriften sollten dem nicht entgegen stehen. Dafür muss sichergestellt werden, dass der oder die BfDI auch in der Praxis Einblick in die Kaufverträge zwischen Nachrichtendiensten und Unternehmen erhält. Um schwere datenschutzrechtliche Verstöße auch dann beheben zu können, wenn das zuständige Ministerium die Rechtsauffassung des oder der BfDI nicht teilt, sollte der oder die BfDI anders als bisher bindende Anordnungsbefugnisse erhalten (Ruckerbauer, 2024).

6.2.4. Definiert Mindestanforderungen auch für den Kauf von Daten mit geringerer Grundrechtsrelevanz

Nicht alle käuflich erworbenen Daten haben zwangsläufig eine so hohe Grundrechtsrelevanz, dass die in den vorangehenden Kapiteln genannten Anforderungen an die gesetzliche Grundlage und die Kontrolle erforderlich sind. Sollen an die Verarbeitung dieser weniger grundrechtsintensiven Daten niedrigere Voraussetzungen gestellt werden, müssen diese Fälle aber ausgehend von der in 6.2.1. beschriebenen Systematisierung dennoch klar definiert werden. Das ist wichtig, um keine Schlupflöcher zu bieten, diese Sicherungsmechanismen zu umgehen.

Denn viele der scheinbar harmlosen Daten können im Nachhinein einen tiefen Eingriff bewirken, zum Beispiel wenn diese weiterverarbeitet und mit Daten aus anderen nachrichtendienstlichen Beschaffungsmethoden verknüpft werden. Im Rahmen der Weiterverarbeitung können diese Daten beispielsweise deanonymisiert werden, und aus aggregierten Daten können neue Erkenntnisse über Individuen extrahiert werden, die für die Schaffung neuer Personenprofile genutzt werden könnten.

Wie im folgenden Kapitel diskutiert, finden in anderen Demokratien bereits intensive Diskussionen dazu statt, welche Daten in eine solche Kategorie fallen könnten, deren Erfassung und Verwendung andere Sicherungsmaßnahmen erforderlich macht. Auch bei diesen Datenkäufen sollte in einer gesetzlichen Grundlage definiert werden, wie diese Daten verwendet, wie sie weiterverarbeitet und mit welchen anderen Daten sie kombiniert werden dürfen. Denn dies kann je nach Verwendung erhebliche Auswirkungen auf die Grundrechtswirkung haben.

Darüber hinaus sollten angesichts des undurchsichtigen Datenmarktes grundsätzliche Mindeststandards für solche Transaktionen definiert werden. Nachrichtendienste müssen die Qualität der gekauften Daten prüfen. Dafür müssen sie nachvollziehen können, wie die gekauften Daten von den Unternehmen erhoben und verarbeitet wurden. Der Erwerb von Daten solcher Unternehmen, deren Datensammlungen offensichtlich gegen europäisches und nationales Datenschutzrecht verstoßen, sollten ausgeschlossen werden (Wetzling & Dietrich, 2022).

6.2.5. Tauscht Euch mit Euren Kolleg:innen in anderen Ländern aus

Deutschland ist nicht das einzige Land, das vor der großen Herausforderung steht, diese neuen Formen der Informationsbeschaffung in Einklang mit rechtsstaatlichen Standards zu bringen. Aufsichtsgremien in Norwegen und den Niederlanden haben öffentlich kritisiert, dass der von den Nachrichtendiensten in diesen Staaten praktizierte Einkauf von Daten ohne ausreichende gesetzliche Grundlage stattfindet. Dabei kritisieren sie, dass die grundrechtlichen Sicherungsmechanismen der Schwere der Eingriffe nicht gerecht wird (CTIVD, 2021; EOS-Committee, 2023, S. 15).

Auch in den USA setzen sich gerade öffentliche Stellen mit der Frage auseinander, wie bei der Nutzung solcher Informationen aus dem Datenmarkt sichergestellt werden kann, dass nicht unverhältnismäßig in Grundrechte eingegriffen wird. Für den Umgang mit *sensitive commmercially available information (CAI)* hat im Mai 2024 die amerikanische Regierung einen ersten Leitfaden veröffentlicht (ODNI, 2024). Zudem stehen weitergehende politische Forderungen nach zusätzlichen Schutzmechanismen im Raum. Zuletzt wurden diese im Rahmen der Diskussionen um den *Fourth Amendment Is Not For Sale Act* laut. In Großbritannien gibt es bereits seit 2016 umfassende Vorgaben zum Erwerb und zur Verarbeitung von *bulk personal datasets*, was auch kommerziell erworbene Daten umfasst.

Im Leitfaden zur Nutzung von sensitive CAI wird festgehalten, dass Datensammlungen in einer völlig neuen Größenordnung angefertigt werden und für die Nachrichtendienste zugänglich sind. Auf diese Weise sind laut ODNI-Informationen über nahezu jede:n erhältlich, deren direkte Erhebung den Sicherheitsbehörden niemals

gestattet wäre oder zumindest umfangreiche Genehmigungsverfahren zur Voraussetzung hätte. Für besonders sensible Datenkäufe schlägt der ODNI deshalb regierungsinterne Mechanismen vor, die einen ausreichenden Schutz der Privatsphäre sicherstellen sollen (ODNI, 2024). Diese sind zwar nur bedingt auf die deutsche Gesetzgebung übertragbar, weil auch diese Sicherungsmechanismen den Vorgaben des BVerfG für schwere Grundrechtseingriffe nicht gerecht würden. Wir empfehlen den an der Ausarbeitung der anstehenden Nachrichtendienstreform Beteiligten dennoch, sichmit diesen ersten Vorgaben auseinanderzusetzen.

Überlegungen werden in dem ODNI-Papier auch dazu angestellt, wie eine Systematisierung aussehen kann, die zwischen Daten mit hoher Grundrechtsrelevanz („Sensitive Commercially Available Informationen [=CAI]“) unterscheidet und solchen Daten, deren Erhebung und Verarbeitung nur geringfügig in Grundrechte eingreift.[37] Vorgegeben wird darin beispielsweise, dass „newspapers or other periodicals; weather reports; books, journal articles, or other published works; public filings or records; or similar documents or databases, whether accessed through a subscription or accessible free of cost” pauschal nicht als sensitve CAI einzustufen sind.

Unabhängig von der Wertigkeit dieser Einstufungen wäre eine Auflistung von Quellen-Typen auch für den deutschen Gesetzgeber eine sinnvolle Möglichkeit, weniger sensible Daten zunächst zu kategorisieren.

37 Auch im Vereinigten Königreicht findet derzeit eine Diskussion darüber statt, wie Datensätze, die erwartbar geringe Grundrechtswirkung entfalten können, definiert werden können. Siehe dazu (Lord Anderson, 2023).

7. Fazit

In anderen Staaten wird bereits darüber diskutiert, unter welchen Umständen Nachrichtendiensten Datenkäufe ermöglicht werden sollten und insbesondere welche Sicherheitsvorkehrungen dabei zu treffen sind. Kontrollgremien beleuchten dort zudem die Thematik und kritisieren die unzureichenden gesetzlichen Regelungen. Erste Regierungen veröffentlichen Leitlinien zur Frage, welche Standards hierbei gelten sollten (ODNI, 2024).

Im Gegensatz dazu sind die Bundesregierung und der Bundestag in dieser Sache bisher weitgehend untätig geblieben. Auch die Kontrolle, sofern sie überhaupt nachrichtendienstliche Datenkäufe in den Blick nimmt, ist öffentlich nicht wahrnehmbar.

Im Vorfeld der großen Reform des Nachrichtendienstrechts hoffen wir mit diesem Impuls eine Debatte darüber anzustoßen, inwieweit Nachrichtendienste beim kommerziellen Erwerb von Informationsprodukten strengeren Regeln und Kontrollen unterworfen werden sollten. Aktuell ist die Missbrauchsgefahr im weitgehend unregulierten und unkontrollierten Feld sehr hoch. Im Fokus sollte die Frage stehen, wie verhindert werden kann, dass wichtige Standards und Beschränkungen, die für andere nachrichtendienstliche Tätigkeiten gelten, über diese Praxis ausgehebelt beziehungsweise unterlaufen werden.

Wir haben in diesem Bericht einige Kernforderungen formuliert, um den Weg zu einer verfassungskonformen Praxis dieser nachrichtendienstlichen Beschaffungsmethode zu ebnen. Dazu gehört, dass eine Systematisierung der Grundrechtseingriffe beim Datenkauf vorgenommen wird. Zudem sollten Standards und Sicherungsmechanismen für Datenkäufe mit besonders schweren Auswirkungen auf Grundrechte geschaffen werden. Es ist aber auch wichtig, dass Mindestanforderungen für den Kauf von Daten mit geringerer Grundrechtsrelevanz definiert werden. Zudem sollte man den Austausch mit Akteuren der Nachrichtendienstführung und -kontrolle in anderen Demokratien suchen. Dadurch lassen sich sicher weitere wichtige Erkenntnisse für einen besseren regulatorischen Umgang mit nachrichtendienstlichen Datenkäufen gewinnen.

Bibliographie

van den Berg, E. (2024). Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'. Verfügbar unter: https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico

Boorstein, M. & Kelly, H. (2023). Catholic group spent millions on app data that tracked gay priests. Verfügbar unter: https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/

Brayne, S. (2020). Predict and Surveil: Data, Discretion, and the Future of Policing. Oxford: Oxford University Press.

BfDI. (2024). BfDI erhebt Klage gegen den Bundesnachrichtendienst. Verfügbar unter: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2024/05_Klage-BND.html

Bundesministerium der Justiz. (2008). Handbuch der Rechtsförmlichkeit. Verfügbar unter: https://hdr.bmj.de/vorwort.html

Bundesregierung. (2023a). Entwurf eines Gesetzes zur Änderung des BND-Gesetzes, Drucksache 20/8627. Verfügbar unter: https://dserver.bundestag.de/btd/20/086/2008627.pdf

Bundesregierung. (2023b). Entwurf eines Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts, Drucksache 20/8626 . Verfügbar unter: https://dserver.bundestag.de/btd/20/086/2008626.pdf

C, A. & Carter, R. J. (2023). Large Language Models and Intelligence Analysis. Verfügbar unter: https://cetas.turing.ac.uk/publications/large-language-models-and-intelligence-analysis

Cameron, D. (2023). The US Is Openly Stockpiling Dirt on All Its Citizens. Verfügbar unter: https://www.wired.com/story/odni-commercially-available-information-report/

Christl, W. & Toner, A. (2024). Pervasive identity surveillance for marketing purposes. Verfügbar unter: https://crackedlabs.org/dl/CrackedLabs_IdentitySurveillance_LiveRamp.pdf

CTIVD. (2021). Automated OSINT: tools and sources for open source investigation. Verfügbar unter: https://www.ctivd.nl/documenten/rapporten/2022/02/08/rapport-74

Dachwitz, I. (2023a). Wie deutsche Firmen am Geschäft mit unseren Daten verdienen. Verfügbar unter: https://netzpolitik.org/2023/adsquare_theadex_emetriq_werbetracking-wie-deutsche-firmen-am-geschaeft-mit-unseren-daten-verdienen/

Dachwitz, I. (2023b). Das sind 650.000 Kategorien, in die uns die Online-Werbeindustrie einsortiert. Verfügbar unter: https://netzpolitik.org/2023/microsofts-datenmarktplatz-xandr-das-sind-650-000-kategorien-in-die-uns-die-online-werbeindustrie-einsortiert/

Dachwitz, I. & Meineck, S. (2024). Datenhändler verticken Handy-Standorte von EU-Bürger*innen. Verfügbar unter: https://netzpolitik.org/2024/berliner-unternehmen-datenhaendler-verticken-handy-standorte-von-eu-buergerinnen/

Detterbeck, S. (2020). Allgemeines Verwaltungsrecht. C.H.BECK. Verfügbar unter: https://www.beck-elibrary.de/10.17104/9783406759659/allgemeines-verwaltungsrecht?page=1

Deutscher Bundestag. (2024a). Bericht über die Kontrolltätigkeit gemäß § 13 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes, Drucksache 20/10473 .

Deutscher Bundestag. (2024b). 32. Tätigkeitsbericht für den Datenschutz und die Informationssicherheit, Drucksache 20/10800. Verfügbar unter: https://dip.bundestag.de/vorgang/32-t%C3%A4tigkeitsbericht-f%C3%BCr-den-datenschutz-und-die-informationsfreiheit-t%C3%A4tigkeitsbericht-f%C3%BCr/310260

Durner, Dürig, Herzog & Scholz. (2024). GG Art. 10.

EOS-Committee. (2023). Annual Report 2022. Verfügbar unter: https://eos-utvalget.no/wp-content/uploads/2023/06/EOS-Committee-annual-report-2022.pdf

Forbrukerrådet. (2020). Out of Control: How consumers are exploited by the online advertising industry. Verfügbar unter: https://storage02.forbrukerradet.no/media/2020/01/2020-01-14-out-of-control-final-version.pdf

Guild, E. & Wetzling, T. (2021). Germany's BND Act & recent CJEU case law. about:intel. Zugriff am 15.5.2024. Verfügbar unter: https://aboutintel.eu/bnd-reform-cjeu/

Hornung, G. (2022). Künstliche Intelligenz zur Auswertung von Social Media Massendaten. Verfügbar unter: https://www.mohrsiebeck.com/10.1628/aoer-2022-0002

Lord Anderson, D. (2023). Independent Review of the Investigatory Powers Act 2016. Verfügbar unter: https://assets.publishing.service.gov.uk/media/649eaeb545b6a2000c3d460b/Independent_Review_of_the_Investigatory_Powers_Act_2016-FINAL.pdf

Löffelmann, M. & Zöller, M. A. (2022). Nachrichtendienstrecht. Baden-Baden: Nomos. Verfügbar unter: https://www.nomos-elibrary.de/index.php?doi=10.5771/9783748908456

Löffelmann, M. (2019): Der Schutz grundrechtssensibler Bereiche im Sicherheitsrecht. Zeitschrift für das gesamte Sicherheitsrecht 2019, S. 190–196

Ng, A. (2022). Homeland Security records show 'shocking' use of phone data, ACLU says. Verfügbar unter: https://www.politico.com/news/2022/07/18/dhs-location-data-aclu-00046208

Nießen, C (2024). Undurchsichtige Praktiken von Datenhändlern und damit verbundene Rechtsunsicherheiten: Eine rechtsvergleichende Betrachtung. Privacy in Germany 2024.

Ní Aoláin, F. (2023). Human rights implications of the development, use and transfer of new technologies in the context of counterterrorism and countering and preventing violent extremism. Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism No. A/HRC/52/39. UN Human Rights Council. Verfügbar unter: https://documents.un.org/doc/undoc/gen/g23/020/43/pdf/g2302043.pdf?token=bpCnjXn1XCqN05kGPb&fe=true

ODNI. (2022). Senior Advisory Group Panel on Commercially Available Information. Verfügbar unter: https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

ODNI. (2024). Intelligence Community Policy Framework For Commercially Available Information. Verfügbar unter: https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf

Poscher, R., Kilchling, M. & Landerer, L. (2022). Überwachungsbarometer für Deutschland - Ein Modellkonzept. Verfügbar unter: https://www.freiheit.org/sites/default/files/2023-08/analyse_ueberwachung_teil2_260122_final.pdf

Reviglio, U. (2022). The untamed and discreet role of data brokers in surveillance capitalism: a transnational and interdisciplinary overview. Verfügbar unter: https://policyreview.info/articles/analysis/untamed-and-discreet-role-data-brokers-surveillance-capitalism-transnational-and

Ruckerbauer, C. (2024). Die Stärkung des Datenschutzbeauftragten als Schlüssel zu einer effektiveren Nachrichtendienstkontrolle. Verfügbar unter: https://www.stiftung-nv.de/sites/default/files/snv-impuls-staerkung-des-bfdi-fuer-eine-effektivere-nachrichtendienstkontrolle.pdf

Ruckerbauer, C. & Wetzling, T. (2023). Zügellose Überwachung? Defizite der Kontrolle des Militärischen Nachrichtenwesens der Bundeswehr. Zugriff am 9.2.2024. Verfügbar unter: https://www.stiftung-nv.de/en/publication/defizite-der-kontrolle-des-militaerischen-nachrichtenwesens-der-bundeswehr

Ruschemeier, H. (2023). Data Brokers and European Digital Legislation. European Data Protection Law Review 2023. S. 27 – 38. Verfügbar unter: https://edpl.lexxion.eu/article/edpl/2023/1/7

Ryan, J. & Christl, W. (2023). Europe's hidden security crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors. Verfügbar unter: https://www.iccl.ie/digital-data/europes-hidden-security-crisis/

Sherman, J., Barton, H., Klein, A., Kruse, B. & Srinivasan, A. (2023). Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security. Verfügbar unter: https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/

Sosna, S. (2022). Der BfDI – ein Kontrollorgan unter dem Radar? Zeitschrift für das Gesamte Sicherheitsrecht, Heft 6, 245.

Sosna, S. (2024). „Fundgrube Internet" – vom tatsächlich möglichen und rechtlich zulässigen Sammeln der Nachrichtendienste im Netz. Zeitschrift für das Gesamte Sicherheitsrecht, (GSZ 2024, 53).

Sovereign Systems. (ohne Jahr). Patternz – National Security Pattern Detection. Verfügbar unter: https://web.archive.org/web/20231003181009/https:/sovsys.co/wp-content/uploads/2020/04/PATTERNZ-NATIONAL-SECURITY-PATTERN-DETECTION.pdf

Steiner, E. (2024). Big Brother Watch/Centrum för Rättvisa" - Die strategische Fernmeldeaufklärung des Bundesnachrichtendienstes im Spiegel der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte, Heft 1.

Süddeutsche Zeitung. (2024). Staatliches Hacking: Weiter Weg zur Reform. Dossier Digitalwende vom 16.05.

Tau, B. (2023). How Ads on Your Phone Can Aid Government Surveillance. Verfügbar unter: https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04?st=n7yjv4ugq7nk4ej&reflink=desktopwebshare_permalink

Tau, B. (2024a). Means of control (First edition.). New York: Crown.

Tau, B. (2024b). How the Pentagon Learned to Use Targeted Ads to Find Its Targets—and Vladimir Putin. Verfügbar unter: https://www.wired.com/story/how-pentagon-learned-targeted-ads-to-find-targets-and-vladimir-putin/

Twetman, H. & Bergmanis-Korats, G. (2021). Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data. Verfügbar unter: https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf

Vines, P., Roesner, F. & Kohno, T. (2017). Exploring ADINT: Using Ad Targeting for Surveillance on a Budget - or - How Alice Can Buy Ads to Track Bob. Verfügbar unter: https://dl.acm.org/doi/10.1145/3139550.3139567

Wetzling, T. (2024). Bedingt kontrollfähig: Warum der Unabhängige Kontrollrat einer Reform bedarf. Verfügbar unter: https://www.stiftung-nv.de/sites/default/files/snv_impuls_warum-der-unabhaengige-kontrollrat-einer-reform-bedarf.pdf

Wetzling, T. & Dietrich, C. (2022). Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform? Verfügbar unter: https://www.stiftung-nv.de/en/publication/disproportionate-use-commercially-and-publicly-available-data-europes-next-frontier

Wetzling, T. & Vieth-Ditlmann, K. (2023). Mehr Rechtskontrolle wagen. Verfügbar unter: https://www.stiftung-nv.de/de/publikation/mehr-rechtskontrolle-wagen-warum-das-mandat-des-unabhaengigen-kontrollrats-erweitert

Wyden, R. (2024). Letter to the Director of National Intelligence. Verfügbar unter: https://www.wyden.senate.gov/imo/media/doc/signed_wyden_letter_to_dni_re_nsa_purchase_of_domestic_metadata_and_ftc_order_on_data_brokers_with_attachments.pdf

Gesetzestexte

BDSG. *Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das zuletzt durch Artikel 7 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.*

BNDG. *Gesetz über den Bundesnachrichtendienst vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 4 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.*

BVerfSchG. *Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 2 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.*

G 10. Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), 2017 I 154), das zuletzt durch Artikel 4 des Gesetzes *vom 22. Dezember 2023 (BGBl. 2023 I Nr. 413) geändert worden ist.*

MADG. *MAD-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2977), das zuletzt durch Artikel 3 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist.*

PKGrG. *Kontrollgremiumgesetz vom 29. Juli 2009 (BGBl. I S. 2346), das zuletzt durch Artikel 10 des Gesetzes vom 19. April 2021 (BGBl. I S. 771) geändert worden ist*.

GO-PKGr. *Geschäftsordnung gemäß § 3 Abs. 1 Satz 2 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (Kontrollgremiumgesetz - PKGrG) vom 29. Juli 2009 (BGBl. I S. 2346), zuletzt geändert durch Gesetz vom 30. November 2016 (BGBl. I S. 2746).*

Rechtsprechung

BVerfG, Beschluss des Ersten Senats vom 24. Januar 2012, 1 BvR 1299/05 -, Rn. 1-192.

BVerfG, Beschluss des Ersten Senats vom 27. Mai 2020, 1 BvR 1873/13 -, Rn. 1-275.

BVerfG, Beschluss des Ersten Senats vom 28. September 2022, 1 BvR 2354/13 -, Rn. 1-167.

BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 -, Rn. 1-215.

BVerfG, Urteil des Ersten Senats vom 03. März 2004, 1 BvR 2378/98 -, Rn. 1-373.

BVerfG, Urteil des Ersten Senats vom 27. Juli 2005, 1 BvR 668/04 -, Rn. 1-166.

BVerfG, Urteil des Ersten Senats vom 27. Februar 2008, 1 BvR 370/07 -, Rn. 1-333.

BVerfG, Urteil des Ersten Senats vom 02. März 2010, 1 BvR 256/08 -, Rn. 1-345.

BVerfG, Urteil des Ersten Senats vom 24. April 2013, 1 BvR 1215/07 -, Rn. 1-233.

BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09 -, Rn. 1-29.

BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17 -, Rn. 1-332.

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

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

BVerfG, Urteil des Zweiten Senats vom 19. September 2018, 2 BvF 1/15 -, Rn. 1-357.

EGMR, 16.05.1977, 7360/76 (Zand gg. Österreich), 1977.

EGMR, 01.10.1982, 8692/7 (Piersack gg. Belgien), 1982.

EGMR, 02.08.1984, 8691/79 (Malone gg. das Vereinigte Königreich), 1984.

EGMR, 21.07.2009, 34197/02 (Luka gg. Rumänien), 2009.

EGMR, 04.12.2015, 47143/06 (Roman Zakharov gg. Russland), 2015.

EGMR, 25.05.2021 58170/13 u.a. (Big Brother Watch u.a. gg. das Vereinigte Königreich).

EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – Space-Net u.a.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autoren

Corbinian Ruckerbauer ist für die SNV im Bereich „Digitale Grundrechte, Überwachung & Demokratie“ tätig. Er koordiniert das European Intelligence Oversight Network (EION), das Nachrichtendienstkontrolleur:innen und anderen Expert:innen eine Plattform für regelmäßigen und strukturierten Austausch bietet. Er gehört zum Redaktionsteam von about:intel, einer Diskussionsplattform, die Expert:innen zu einem sektor- und länderübergreifenden Dialog zusammenbringt, um drängende Fragen an der Schnittstelle von Technologie, Überwachung und Demokratie zu diskutieren.

Kontakt
Corbinian Ruckerbauer
cruckerbauer@stiftung-nv.de

Dr. Thorsten Wetzling leitet das Themenfeld „Digitale Grundrechte, Überwachung & Demokratie“ in der Stiftung Neue Verantwortung. Dort stehen die verschiedenen Formen des sicherheitsbehördlichen Zugangs und der Verarbeitung von personenbezogenen Daten im Fokus unterschiedlicher Projektarbeiten. Dabei geht es häufig um rechtspraktische Fragen, ob und wie der Einsatz moderner Überwachungstechnologie vom Gesetzgeber rechtsstaatlich einzuhegen und von den unabhängigen Aufsichtsbehörden effektiv und umfassend zu kontrollieren ist.

Kontakt
Dr. Thorsten Wetzling
twetzling@stiftung-nv.de

Impressum

Stiftung Neue Verantwortung e. V.
Ebertstraße 2
10117 Berlin

T. +49(0)30 81 45 03 78 80
F. +49(0)30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Alina Siebert