Kapitel A: Einleitung

In den vergangenen Jahren haben sich sowohl die deutsche als auch die europäische Verfassungsrechtsprechung ausführlich mit verschiedenen staatlichen Überwachungsmaßnahmen im Bereich der Sicherheitsgewährleistung beschäftigt.

Seit dem Volkszählungsurteil,[1] in dem das Recht auf informationelle Selbstbestimmung entwickelt wurde, steht für das BVerfG fest, dass sämtliche staatliche Datenverarbeitungen *Informationseingriffe*[2] darstellen und somit als Grundrechtsbeeinträchtigungen gerechtfertigt werden müssen. Die Privatheit wird infolgedessen nicht mehr nur durch die grundrechtliche Abschirmung bestimmter Lebensbereiche, Art. 10 Abs. 1, Art. 13 Abs. 1 GG, sondern als eigenständiger Aspekt der Persönlichkeitsentfaltung i. S. d. Art. 2 Abs. 1 GG geschützt. Trotz einiger Kritik[3] an der Dogmatik der informationellen Selbstbestimmung hat sich dieser Ansatz zu einer ständigen Linie der Verfassungsrechtsprechung entwickelt und wird weithin akzeptiert.[4]

Das wohl bedeutendste Feld dieser Rechtsprechung lässt sich dabei im Bereich der staatlichen Sicherheitsgewährleistung ausmachen. Datenverarbeitungen finden zwar bei nahezu sämtlichen Verwaltungshandlungen statt, auch in ganz allgemeinen Bereichen der Leistungsverwaltung. Grundrechtssensibel sind solche alltäglichen Vorgänge aber nicht. Dementsprechend steht bei Datenverarbeitungen durch die Fach- bzw. Leistungsverwaltung nicht das Verfassungsrecht, sondern die einfachgesetzliche Ausgestaltung durch das Datenschutzrecht und dessen Anwendung im Zentrum der Debatte.

---

1 BVerfGE 65, 1 (43) – Volkszählung.

2 Begriff schon bei *Rogall,* Informationseingriff, 1992, S. 27 ff.

3 *Albers*, Informationelle Selbstbestimmung, 2005, S. 113 ff., 437 ff., *Dies*., in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (16 f.); *Vogelgesang,* Informationelle Selbstbestimmung, 1987, S. 139 ff.; *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (131 ff.); *Britz* in Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (566 ff.); *Placzek,* Informations- und Datenschutz, 2006, S. 80 f.; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Ladeur*, DÖV 2009, 45; *Trute*, JZ 1998, 822; *Hoffmann-Riem*, AöR 123 (1998), 513 (528); *J.-P. Schneider* in BeckOK Datenschutzrecht, Grundlagen Syst. B Rn. 25.1.

4 S.a. jüngst die Kritik bei *J. Franz Lindner/Unterreitmeier*, JZ 2022, 915.

Anderes gilt für Bestimmungen, die staatliche Sicherheitsbehörden zu Datenverarbeitungen auf den Gebieten der Gefahrenabwehr, Strafverfolgung und zur politischen Vorfeldaufklärung ermächtigen. Zu deren Verhältnismäßigkeit liegt mittlerweile eine ganze Reihe von Urteilen des BVerfG, EuGH und EGMR vor, die wissenschaftlich und gesellschaftlich intensiv begleitet werden. Aus diesen umfangreichen Urteilen hat sich mittlerweile ein komplexes System für die gesetzliche Ausgestaltung sicherheitsrechtlicher Informationseingriffe entwickelt (dazu Kap. B. III. 1).[5] Dieses Rechtsregime wird als *Sicherheits-* bzw. *Sicherheitsverfassungsrecht*[6] bezeichnet.

Anstatt bestimmte (Informations-)Eingriffe der Sicherheitsbehörden als pauschal unverhältnismäßig einzustufen, bringt insbesondere das BVerfG eine Je-Desto-Formel[7] zur Anwendung, im Rahmen derer – ausgehend von der schematisch bestimmten Intensität einer Ermächtigungsgrundlage[8] – die notwendigen materiellen, verfahrensrechtlichen und datenschutzspezifischen Anforderungen entwickelt werden.

Geprüft wird also im Ergebnis nur noch, ob der Gesetzgeber bei der Gestaltung eines Informationseingriffs die richtigen Einschränkungen und Anforderungen für die konkrete Maßnahme aus dem sicherheitsrechtlichen Baukasten ausgewählt hat. So dies nicht der Fall ist, fungieren die Urteile als *Handlungsanweisung* zur korrekten Ausgestaltung des jeweiligen Gesetzes.[9]

Der Grundsatz der Verhältnismäßigkeit kommt insofern nicht mehr in Form einer klassischen Rationalitätskontrolle zur Anwendung, sondern als hermeneutisches Werkzeug[10] zur Entwicklung konkreter Gewährleistungen aus den allgemein gehaltenen Schutzbereichen der Privatheitsgrundrechte.

---

5 Instruktiv BVerfGE 141, 220 – BKA-Gesetz.

6 Vgl. *Tanneberger,* Sicherheitsverfassung, 2014; *Dietrich/Gärditz* (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28

7 *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.; *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 116; früh schon *Vahle,* Aufklärung, 1983, S. 94 ff., 130.

8 *Löffelmann*, GSZ 2019, 16 (19); *Poscher/Kilchling/Landerer*, GSZ 2021, 225 (230 ff.);*F. Braun/F. Albrecht* VR 2017, 151 (152); *Hornung/Schnabel*, DVBl 2010, 824 (826).

9 Krit. insofern *Schluckebier* abw. Meinung BVerfGE 125, 260 (364 ff., 373); *Schoch* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 63 (66 ff.); *Wolff*, ZG 2016, 361 (366 f.).

10 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 77 ff.

Ein anderes Vorgehen kommt im informationellen Sicherheitsrecht – jedenfalls auf Gesetzesebene – kaum in Betracht. Informationserhebungen werden immer nur dann notwendig, wenn die Umstände eines Sachverhalts gerade nicht klar sind. Das Ausmaß der jeweiligen Sicherheitsbedrohung kann im Moment der datenverarbeitenden Maßnahme noch nicht bestimmt werden. Die ermächtigenden Gesetze, die im Voraus der konkreten Maßnahme vorliegen müssen, können also nicht auf eine bereits vorgenommene Güterabwägung aufbauen. Vielmehr muss durch die Ausgestaltung eines Gesetzes sichergestellt werden, dass die Maßnahme *effektiv*[11] bleibt, d. h. nur schonend und nur in solchen Fällen zur Anwendung kommt, in denen die Beeinträchtigung der Privatheit zu dem angestrebten Sicherheitszweck nicht außer Verhältnis steht.[12] Dabei kommen auch kompensatorische Effekte zum Tragen.

Die so behandelten Maßnahmen können in zwei Formen unterteilt werden: individuelle Überwachungsmaßnahmen auf der einen Seite sowie Massenüberwachungsmaßnahmen auf der anderen. Eingriffe, die konkret auf eine Person oder einen engen Personenkreis ausgerichtet werden, lassen sich als individuelle *Überwachungsmaßnahmen* bezeichnen. Hierzu zählt etwa die Überwachung eines bestimmten Telefonanschlusses (TKÜ) oder die Online-Durchsuchung des Endgeräts einer spezifischen Person. Diese Maßnahmen zeichnen sich dadurch aus, dass ein konkreter Anlass für das Vorgehen gegenüber dieser Person vorliegt. Insofern lässt sich insbesondere über eine gesetzliche Einschränkung des Anlasses eine grundrechtssensible Effektivität erzielen.[13] Die strafprozessuale TKÜ, § 100g StPO, die einen intensiven Grundrechtseingriff darstellt,[14] darf etwa nur zur Aufklärung bestimmter Straftaten eingesetzt werden, an denen ein besonders hohes gesellschaftliches Aufklärungsinteresse besteht. Der Anlass kann aber noch weiter eingegrenzt werden. So stellt das Sicherheitsrecht oft bestimmte Anforderungen an die Prognose, nach der die Maßnahme tatsächlich etwas

11 *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 242 ff.; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 82 f., 14 ff.; aus der Rspr etwa BVerfGE 155, 166 (197 f.); E 141, 220 (268 ff.) – BKA-Gesetz; allg.: „Realisierungsgrade" bei *N. Petersen,* Verhältnismäßigkeit, 2015, S. 65 ff.

12 Allg. zur Verhältnismäßigkeitsproblematik von Gesetzen *Schlink,* Abwägung, 1976, S. 134 ff.; *ders.*, FS 50 Jahre BVerfG, Bd. II, 2001, S. 445 (461 f.); *Jestaedt* in Jestaedt/Lepsius (Hrsg.), Verhältnismäßigkeit, 2021, S. 293 (293 ff.).

13 *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (127); *Tanneberger,* Sicherheitsverfassung, 2014, S. 353 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.).

14 BVerfGE 129, 208 (240); E 113, 348 (382).

zur angestrebten Sicherheitsgewährleistung beiträgt. § 100g StPO verlangt etwa das Vorliegen *bestimmter Tatsachen*, die darauf hindeuten, dass die betroffene Person eine der besagten schweren Straftaten tatsächlich begangen hat oder versucht hat, diese zu begehen.

Von diesen anlassbezogenen Maßnahmen unterscheiden sich die Phänomene der *Massenüberwachung*.[15] Diese zeichnen sich dadurch aus, dass immer auch Daten von solchen Personen mit dem Ziel der Sicherheitsgewährleistung verarbeitet werden, die im Moment der Datenverarbeitung keinen entsprechenden Anlass geliefert haben.

Solche Maßnahmen finden insbesondere bei nachrichtendienstlichen Tätigkeiten schon lange statt.[16] Sie wurden in den vergangenen Jahren jedoch ausgedehnt und nehmen nunmehr verschiedene Formen an. Bestimmte Daten werden nicht mehr nur anlasslos gerastert, sondern auf Anweisung des Staats auf Vorrat gehalten, da den jeweiligen Daten kategorisch ein potenzieller Nutzen für die Sicherheitsgewährleistung innewohnen soll. Eine solche *Vorratsdatenspeicherung* wurde insbesondere für Telekommunikationsverkehrs-[17] und Fluggastdaten[18] eingeführt, wobei es in beiden Fällen zu bedeutsamen Urteilen verschiedener Verfassungsgerichte kam (dazu Kap. C II. 1. & 2).

Bei der Behandlung der Massenüberwachungsmaßnahmen stellt sich in der grundrechtlichen Betrachtung ein spezifisches Problem ein. Mangels konkreten Anlasses ist ausgeschlossen, dass sich sämtliche Datenverarbeitungen mit angemessener Wahrscheinlichkeit tatsächlich positiv auf einen angemessenen Sicherheitszweck auswirken. Vielmehr steht von vor-

15 Krit. zum Begriff „Massenüberwachung" *B. Huber*, NVwZ-Beilage 2021, 3 (3).

16 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz) (G 10) vom 13.08.1968 (BGBl. I S. 949); dazu BVerfGE 30, 1 – Abhörurteil.

17 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. 2006 L 105/54; dazu EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

18 Richtlinie (EU) 2016/681 des europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. 2016, L 119/132); dazu EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)) = EuZW 2022, 706.

neherein fest, dass sich die absolute Mehrzahl[19] der Einzelvorgänge im Nachhinein als unnötig erweisen wird. Die Verhältnismäßigkeit lässt sich also nicht im Voraus durch effektivitätsgewährleistende Einschränkungen herstellen. Ebenso wenig kommt eine abstrakte Relation des Gesamtnutzens einer gesetzlichen Ermächtigung mit der Vielzahl der Einschränkungen in Betracht, da dann abstrakt die informationelle Selbstbestimmung der Gesellschaft mit dem Sicherheitsinteresse der Gesellschaft abgewogen werden müsste. Dieser Vorgang muss an der Inkommensurabilität[20] der Abwägungsgegenstände scheitern.

Die Rechtsprechung hat deswegen Wege gefunden, um auch Massenüberwachungsmaßnahmen im Rahmen des sicherheitsverfassungsrechtlichen Komplexes bewerten zu können (zum BVerfG Kap. B. III. 2., zum EuGH Kap. C. II.). Bei den Vorratsdatenspeicherungspflichten trennt sie etwa zwischen der Speicherung und dem Zugriff auf die Maßnahme. Da letzterer als Individualmaßnahme erfolgt, kann an dieser Stelle doch ein Anlass in die Ermächtigungsgrundlage einfließen, der zumindest die Verwendung nach der Speicherung effektiv eingrenzt. Nur die Speicherung bleibt also anlasslos, ist aber von den Grundrechtsberechtigten hinzunehmen.[21]

Darin kommt etwas Wichtiges zum Ausdruck. Den Informationseingriffen bzw. Datenverarbeitungen ist eine intensive Beeinträchtigung von Grundrechten nicht inhärent. Es ist in vielen Fällen schon nicht klar, wieso die Wahrnehmung und Verarbeitung bestimmter Informationen durch Dritte überhaupt einen Eingriff darstellen sollen, denn diese sind natürlicher Bestandteil einer kommunikativen und interagierenden Gesellschaft.[22] Die Problematik der Informationseingriffe besteht vielmehr darin, dass sie

19 Vgl. zur Häufigkeit der Verkehrsdatenabfrage *Albrecht/Kilchling/*Grafe, Forschungsbericht Telekommunikationsverbindungsdaten, S. 88 ff., abgedr. in BT-Drs. 16/8434; übersichtlich zur Empirie auch Moser-Knierim, Vorratsdatenspeicherung, 2014, S. 192 ff., krit. deshalb etwa *Gitter/Schnabel, MMR* 2007, 411 (414 f.); vgl. zur Kennzeichenkontrolle BW-LT-Drs. 16/5009, S. 5; *Engert* – Wie die Polizei Millionen Autofahrer mit einem System überwacht, das nicht funktioniert Buzzfeed.com vom 15.10.2018, https://www.buzzfeed.com/de/marcusengert/kennzeichenerfassung-der-polizei-funktioniert-nicht.

20 Vgl. *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 69; *Schlink,* Abwägung, 1976, S. 134 ff.

21 Jüngst EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 248 ff. = EuZW 2022, 706

22 *Albers* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (16 f.); *dies.,* Informationelle Selbstbestimmung, 2005, S. 113 ff., 437 ff.; *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (S. 136 ff.); *Placzek,* Informations- und Datenschutz, 2006, S. 92 ff.; *Trute* in Roßnagel (Hrsg.), Hdb. Datenschutz-

ein Glied in einer Kette verschiedener Handlungen darstellen, die sukzessive die Privatheit der Betroffenen beeinträchtigen.

Die Speicherung von Daten beispielweise ist an sich völlig unbedenklich. Über eine jede Person liegen bei etlichen staatlichen und privaten Stellen verschiedene Daten vor, die alle grundsätzlich im Rahmen von Ermittlungen erhoben und für verschiedene Zwecke verwendet werden können. Entscheidend für die kritische Betrachtung der Vorratsdatenspeicherung war deshalb nicht, dass Verkehrs- oder Fluggastdaten bei den jeweiligen Unternehmen überhaupt vorliegen, sondern dass diese im Rahmen der entsprechenden Gesetze final für die Sicherheitsbehörden aufgehoben und verfügbar gemacht wurden. Ohne diese Regelung wäre es gewissermaßen Zufall gewesen, ob die Daten aufgrund anderer gesetzlicher Vorschriften, etwa § 257 Abs. 4 HGB, noch vorgelegen hätten. Dieser Zufall sorgte zuvor für eine Form der Waffengleichheit gegenüber den Sicherheitsbehörden. Es ist dessen Wegfall, der die Vorratsdatenspeicherung zu einer strukturell bedenklichen Maßnahme macht.[23]

Vor dem Hintergrund dieser sicherheitsverfassungsrechtlichen Dogmatik soll in dieser Arbeit ein Gesetzeskomplex betrachtet werden, der sich ebenfalls als Phänomen der Massenüberwachung verstehen lässt, aber bislang neben den Telekommunikations- und Fluggastdaten ein Schattendasein führt: das Anti-Geldwäscherecht und die damit einhergehende Verarbeitung von Finanzdaten.

Zu den Finanzdaten zählen zunächst die Informationen über Verträge von Privatpersonen mit Finanzdienstleistern. Aus diesen *Bestandsdaten*[24] ergeben sich die jeweiligen Personendaten und die Umstände der in Anspruch genommenen Finanzleistung – also klassischerweise die Angaben zur Person, die Kontonummer und das Datum der Eröffnung eines Kontos, vgl. § 24c Abs. 1 Kreditwirtschaftsgesetz (KWG).

Zur Bevorratung und Verfügungstellung dieser Daten hat das BVerfG im Jahr 2007 geurteilt[25] – eine ganze Weile, bevor es sich mit der Spei-

---

recht, 2003, 2.5 Rn. 19; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121).

23 Vgl. *Szuba,* Vorratsdatenspeicherung, 2011, S. 196 ff.; *Grafe,* Verkehrsdaten, 2008, S. 13 ff.; *Puschke/Singelnstein*, NJW 2008, 113 (118); *Lisken*, ZRP 1994, 264 (267 f.).

24 Stattdessen häufig „Stammdaten" genannt, vgl. BVerfGE 118, 168, entsprechen aber der Definition der Bestandsdaten i. S. d., § 3 Nr. 6 TKG, s.a. *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 38; *Gnüchtel*, NVwZ 2016, 13 (16).

25 BVerfGE 118, 168 – Kontostammdaten.

cherung und Abfrage von Telekommunikationsbestandsdaten beschäftigt hat. Immerhin erregte dieses Urteil bzw. die automatisierte Abfrage der Konto*stammdaten* ein gewisses Interesse und wurde ausführlich auch von wissenschaftlicher Seite kommentiert.[26]

Deutlich brisanter, aber kaum im Kontext des Sicherheitsverfassungsrechts besprochen, ist die Überwachung auch von Konto*inhaltsdaten* im Rahmen des (Anti-)Geldwäscherechts.[27] Wenn über Vorratsdatenspeicherung geschrieben wird, findet sich – wenn überhaupt – lediglich eine Randnotiz zur Geldwäschegesetzgebung.[28] Dabei sehen die Vorschriften der Geldwäschebekämpfung recht offensichtlich sowohl eine massenhafte Analyse sämtlicher Kontotransaktionen als auch eine Bevorratung der dabei anfallenden Daten – also letztlich der Kontoauszüge – vor (Kap. D. III. 2). Diese beinhalten Datensätze von enormer persönlichkeitsrelevanter Aussagekraft.[29] Da die Zahlungsweise im Privatverkehr immer weiter digitalisiert wird und unbare Transaktionen den Alltag mittlerweile bestimmen[30], lassen sich aus Kontoauszügen weitreichende Persönlichkeitsprofile erstellen.[31]

Dass Kontoauszüge gespeichert werden, ergibt sich allerdings nicht nur aus dem Geldwäscherecht, sondern folgt aus etlichen Vorschriften des deutschen und europäischen Privat-, Handels- und Steuerrechts (Übersicht in Kap. D. II).

Das Anti-Geldwäscherecht unterscheidet sich insofern von der Vorratsdatenspeicherung von Telekommunikationsverkehrs- oder Fluggastdaten.

---

26 *Degen,* Geldwäsche, 2009, S. 273 ff.; *Samson/Langrock,* Gläserner Bankkunde, 2005, S. 17 ff., 57 ff., 78 ff., 85 ff.; *Zubrod*, WM 2003, 1210; *Herzog/Christmann*, WM 2003, 6 (12 f.); *Göres*, NJW 2005, 253 (256 f.); *Hamacher*, DStR 2006, 633 (637 f.); *ders.* Die Bank 09/2006, 40 *Widmaier*, WM 2006, 116 (118 ff.); Übersicht bei *Pfisterer*, JöR 2017, 393 (409 f.).

27 aus der jüngeren Lit.: Schindler, Geldwäschegesetzgebung, 2021, S. 296 ff.; Böszörmenyi/Schweighofer, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71 ff.); Milaj/C. Kaiser, Int. Data Privacy Law 7 (2017), 115; C. Kaiser, Privacy in Financial Transactions, 2018; B. Vogel in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (900 ff.); Bertrand/Maxwell/Vamparys, Int. Data Privacy Law 2021, 276.; zuvor *Werner,* Geldwäsche, 1996, S. 91 ff; 102 f.; *Herzog*, WM 1996, 1753 (1757 ff.); *ders*., WM 1999, 1905 (1910 ff.); *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 610 ff.

28 z. B. bei *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021 (117, Fn 1).

29 BVerfGE 120, 274 (347 f.) – Online-Durchsuchung.

30 *Deutsche Bundesbank,* Zahlungsverhalten in Deutschland, 2017.

31 *Pfisterer*, JöR 2017, 393 (400); *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (118 f.); *Westermeier*, Information, Communication & Society 23 (2020), 2047; *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 11.

Bei diesen kam es erst aufgrund spezieller Gesetze, die dem Sicherheitsrecht zuzurechnen sind, zu einer langfristigen Speicherung. Die geldwäscherechtlichen Vorschriften ließen sich hingegen wegdenken, ohne dass sich dadurch der faktisch gespeicherte Datenbestand verändern würde. Letztlich wird nur der Zweck der Speicherung ergänzt. Finanzdaten werden aufgrund des Geldwäscherechts *auch* zur Sicherheitsgewährleistung gespeichert.

Dieser Umstand wurde in den bisherigen Untersuchungen nicht hinreichend berücksichtigt – wie so viele Unterschiede des Anti-Geldwäscherechts zu den prominenteren Phänomenen der Massenüberwachung.

Dabei lässt sich die diffizile Betrachtung von Massenüberwachungsmaßnahmen gut an dem Beispiel illustrieren, da es zeigt, wie eng verknüpft einzelne Datenverarbeitungsschritte sein müssen, um tatsächlich eine grundrechtsproblematische Überwachungsthematik darzustellen (zum Begriff der Überwachung Kap. B. I).

Die Kritik an der Vorratsdatenspeicherung kann nicht darauf gestützt werden, dass massenhaft Daten gespeichert und später erhoben werden können. Denn dies entspricht letztlich nur dem allgemeinen Ermittlungsgrundsatz, wonach insbesondere die Strafverfolgungsbehörden grundsätzlich alle Informationen abrufen dürfen, soweit dies im Einzelnen angemessen ist.[32] Das Vorliegen massenhafter, aussagekräftiger Datenbestände ergibt sich in vielen Fällen nicht erst aus einer sicherheitsrechtlichen Speicheranordnung, sondern aus dem allgemeinen Rechtsverkehr. Dementsprechend finden praktisch andauernd „Vorratsdatenspeicherungen" statt.

Auch der Zugriff auf Kontoauszüge stellt ein altbekanntes, anerkanntes und praktisch bedeutsames Ermittlungswerkzeug der Staatsanwaltschaft dar[33] (zum Zugriff auf Kontodaten i. R. v. „klassischen Ermittlungen" s. Kap. E.). Diese Strafverfolgungsbehörden werden in der StPO zwar – anders als die Nachrichtendienste etwa nach § 8a Abs. 1 Nr. 2 BVerfSchG – gegenüber Privaten nicht zu verpflichtenden Auskunftsersuchen ermächtigt – ebenso wenig die allgemeinen Polizeibehörden.[34] In der Praxis kommen private Unternehmen schriftlichen Ersuchen nach Kontoinhaltsdaten von Sicherheitsbehörden aber stets nach. Denn sie wollen strafprozessuale Ope-

32 *F. Jansen,* Bankauskunftsersuchen, 2010; *Kahler,* Kundendaten, 2017; *Reichling*, JR 2011, 12; *Wonka*, NJW 2017, 3334.

33 *Masing*, NJW 2012, 2305 (2309); keine *„Wahrheitsfindung um jeden Preis"* BGHSt 14, 358 (365).

34 Zu diesen *Wonka*, NJW 2017, 3334 (3337 f.); OVG Koblenz, NVwZ 2002, 1529.

rativmaßnahmen, z. B. Durchsuchungen, abwenden. Man spricht daher auch von „Abwendungsauskünften".[35] Die Auskunftsersuchen der Staatsanwaltschaft werden aber, obwohl dabei auf massenhaft gespeicherte Daten zugegriffen wird, nicht als Phänomen der Massenüberwachung begriffen, und zwar zu Recht.

Die Maßnahmen der Massenüberwachung bzw. hier vor allem die Vorratsdatenspeicherung sind nicht deswegen von besonderer grundrechtlicher Brisanz, weil sie den Sicherheitsbehörden Zugriff auf eine Vielzahl gespeicherter Daten ermöglichen. Insoweit gehen sie eben nicht über die Standardmethoden der Ermittlung hinaus. Sie sind problematisch, weil sie eine Speicherung (oft bei Privaten) mit einem spezifischen, meist heimlichen, Zugriffsrecht verknüpfen[36] und somit bestimmte Daten mit dem Verdikt einer ständigen sicherheitsrechtlichen Potentialität belegen (zur rechtsstaatlichen Kritik s. Kap. B. III. 2. c.). Nur vor diesem Hintergrund kann das Anti-Geldwäscherecht als Massenüberwachungsform identifiziert werden, da es eben nicht nur (insbesondere nach § 8 Abs. 1 GwG) eine Speicherung veranlasst – diese wirkt sich ja faktisch gar nicht aus –, sondern eine ganze Reihe von Vorschriften zur heimlichen Nutzung dieser Daten durch Sicherheitsbehörden vorsieht.

Grundsätzlich ist das gesetzliche Anti-Geldwäschesystem proaktiv organisiert und wird deshalb als Unterfall der unternehmerischen Criminal Compliance besprochen.[37] Kreditinstitute und andere Verpflichtete sollen im Rahmen eines mehrstufigen Monitoring-Verfahrens erst automatisiert bestimmte *Auffälligkeiten* in den Transaktionen ihrer Kunden entdecken, diese dann (menschlich) überprüfen und bei erhärtetem Verdacht den Sicherheitsbehörden melden, § 43 Abs. 1 GwG. Früher ging diese Meldung direkt an vermeintlich zuständige Sicherheitsbehörden – meist die Landeskriminalämter. Seit der 3. Geldwäscherichtlinie müssen die EU-Mitgliedstaaten aber spezielle Zentralstellen einrichten: die *Financial Intelligence Units* (FIU). Diese nehmen die Meldungen entgegen, analysieren sie und leiten sie bei Erhärtung des Verdachts an andere Sicherheitsbehörden weiter.

35 *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 39 Rn. 40; *Reichling*, JR 2011, 12 (16).

36 Vgl. zur Definition *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021 (117).

37 Etwa *Vollmuth,* Geldwäscheprävention, 2020; *Hugger/Cappel* DB 2018, 1066.

Dieser proaktive, von den Privaten ausgehende Informationsweg wird ergänzt durch intensive Zugriffsrechte der FIU. Diese kann nach dem Gesetzeswortlaut ohne weitere Voraussetzungen heimlich bei sämtlichen geldwäscherechtlich Verpflichteten um umfangreiche Finanzinformationen ersuchen, § 30 Abs. 3 GwG. Außerdem können die Sicherheitsbehörden bei der FIU um solche Informationen ersuchen, worauf diese zur Übermittlung verpflichtet ist, § 32 Abs. 3 GwG. Das Geldwäscherecht sieht also verschiedene Richtungen für den Austausch von Finanzinformationen zwischen Privaten, FIU und verschiedenen Sicherheitsbehörden vor.[38]

Dieser Finanzfluss verbindet Elemente einer massenhaften Datenanalyse mit einer Vorratsdatenspeicherung. Das Geldwäscherecht lässt sich insofern gut mit dem System der Überwachung von Fluggastdaten (PNR) vergleichen. Auch dort werden massenhaft Daten analysiert und sodann für einen bestimmten Zeitraum aufbewahrt. Der einzige Unterschied besteht darin, dass die Aufbewahrung und Rasterung von Flugdaten vollständig von einer Zentralstelle (in Deutschland das BKA, § 1 Abs. 1 FluGDaG) durchgeführt wird. Die Airlines übermitteln nur (sämtliche) Flugdaten, nehmen selbst aber keine Speicherung oder Analyse vor. Diese Verarbeitungsschritte obliegen der Flugastdatenzentralstelle, §§ 4 ff. FluGDaG.

Die FIU hingegen ist erst einmal nur zur Analyse von Meldungen berufen. Die Auffindung auffälliger Sachverhalte per EDV-Monitoring aus dem Massenverkehr übernehmen die Privaten selbst, wodurch enorme Kosten ausgelagert werden.[39]

Trotz dieses Unterschieds im Verfahren ist die Finanzüberwachung im Rahmen der Bekämpfung von Geldwäsche und Terrorismusfinanzierung gut mit der Fluggastdatenüberwachung vergleichbar, weswegen das jüngst ergangene Urteil des EuGH zur PNR-Richtlinie[40] wegweisend bei der Beurteilung sein muss.

Mit dem Urteil wurden einige Grundsätze des EuGH zur Massenüberwachung revidiert, weshalb die bisherigen Besprechungen der Geldwäscherichtlinie nicht mehr aktuell sind. Diese leiden ohnehin an einer zu oberflächlichen Behandlung des Phänomens Massenüberwachung. Sowohl das BVerfG als auch der EuGH und, wenngleich schwächer ausgeprägt, der

38 Ausf. zum Informationsfluss im GwG *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (241 ff.).

39 *Saperstein/Sant/Ng*, Notre Dame Law Rev. Online 91 (2015), 1 (2 ff.).

40 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)) = EuZW 2022, 706.

EGMR (zu diesem Kap. C. III) überprüfen diese nicht im Rahmen einer Güterabwägung, sondern versuchen sich an einer *Prozeduralisierung*.[41]

Die Ausmaße dieses Ansatzes haben im PNR-Urteil ihren Höhepunkt erreicht. Hier ging der EuGH so weit, nicht mehr nur die konkreten Anforderungen an die gesetzliche Ausgestaltung vorzustellen und die Richtlinie aufzuheben, sofern sie hinter diesen Anforderungen zurückblieb. Er interpretierte stattdessen die notwendigen Anforderungen selbstständig in die Richtlinien hinein und zwar mehr oder minder losgelöst vom Wortlaut. An einigen Stellen handelt es sich dabei sogar um eine Auslegung *contra lege*.[42]

Bei der grundrechtlichen Bewertung der Anti-Geldwäschemaßnahmen als Massenüberwachungsphänomene soll diese Rechtsprechungslinie des EuGH – auch wenn man diese kritisch sieht – beachtet werden. Denn an einigen Stellen offenbaren sich Gestaltungslücken, die sich im Wege einer gezielt auf die Aufrechterhaltung des Gesetzes ausgerichteten Auslegung noch als verfassungsgemäß darstellen lassen. Diese Arbeit ist insofern nicht darauf angelegt, eine eigenständige bzw. persönliche verfassungsrechtliche Bewertung der Anti-Geldwäschemaßnahmen abzugeben. Vielmehr handelt es sich um einen Vorschlag, wie die Gerichte, basierend auf der bestehenden Rechtsprechungslinie, entscheiden könnten bzw. sollten.

Um diese Bewertung auch dogmatisch zu hinterlegen, wird die Rechtsprechung des BVerfG, des EuGH und des EGMR zu den Massenüberwachungsmaßnahmen in den ersten Kapiteln erläutert und analysiert werden (Kap. B. & C.). Die Hintergründe der grundrechtssensiblen Behandlung dieser Phänomene müssen zum Vorschein gebracht werden, um die Möglichkeit einer analogen Anwendung der gerichtlichen Feststellungen zur strategischen Überwachung und Vorratsdatenspeicherung von Telekommunikations- und Fluggastdaten zu fundieren.

Die wichtigste Erkenntnis ist dabei, dass erst aus einer Kombination verschiedener, final ausgerichteter Datenverarbeitungsschritte eine grundrechtssensible Überwachung entsteht. Nur das Vorliegen massenhafter Daten und die Möglichkeit des Zugriffs allein erklären noch nicht, wieso für verschiedene Formen der Massenüberwachung so strenge Anforderungen aufgestellt wurden, da sie sich insofern von der klassischen Ermittlung nicht unterscheiden. Massenüberwachungsmaßnahmen sind nur deshalb

41 *Tzanou/Karyda*, European Public Law 28 (2022), 123 (153 f.); s.a. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (104 ff.).

42 Dazu *Thönnes*, Die Verwaltung 2022, 527 (531 ff.); *ders.*, directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

problematisch, weil sie in Reaktion auf eine veränderte Sicherheitssituation von den Prinzipien der traditionellen Sicherheitsgewährleistung abrücken.

Deshalb wird in den nachfolgenden Kapiteln nicht nur das System der Geldwäschebekämpfung beschrieben (Kap. D.), sondern auch die außerhalb dieser Vorschriften bestehenden Möglichkeiten von Sicherheitsbehörden, auf Kontodaten zuzugreifen (Kap. E.). Dadurch soll gezeigt werden, dass sich das Geldwäscherecht von den im Sicherheitsrecht anerkannten Grundsätzen abgehoben hat und tatsächlich ein problematisches Phänomen von Massenüberwachung darstellt.

Anschließend sollen die bisherigen Versuche, diesen Komplex grundrechtlich zu bewerten, dargestellt werden (Kap. F.). Da diese an Oberflächlichkeit leiden und in den meisten Fällen auch noch nicht die entscheidende Rechtsprechung zu den PNR-Daten berücksichtigen, widmet sich die Arbeit dann final einem eigenen Versuch einer grundrechtlichen Bewertung des Geldwäscherechts (Kap. E.).