Sicherheit und Gesellschaft.
Freiburger Studien des Centre for Security and Society | 16

Lukas Martin Landerer

Massenüberwachung von Finanzdaten

Die Geldwäschebekämpfung unter der Sicherheitsverfassung

Nomos

Sicherheit und Gesellschaft.
Freiburger Studien des Centre for Security and Society

herausgegeben von
Prof. Dr. Hans-Helmuth Gander
Prof. Dr. Walter Perron
Prof. Dr. Ralf Poscher
Prof. Dr. Gisela Riescher
Prof. Dr. Thomas Würtenberger

Band 16

Lukas Martin Landerer

Massenüberwachung von Finanzdaten

Die Geldwäschebekämpfung unter der Sicherheitsverfassung

Nomos

Onlineversion
Nomos eLibrary

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Freiburg i. Br., Univ., Diss., 2024

u.d.T.: Massenüberwachung von Finanzdaten – Die Geldwäschebekämpfung unter der Sicherheitsverfassung

ISBN 978-3-7560-2415-5 (Print)

ISBN 978-3-7489-5290-9 (ePDF)

1. Auflage 2025

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2024/2025 von der Juristischen Fakultät der Albert-Ludwigs-Universität Freiburg als Dissertation angenommen.

Ich bedanke mich herzlichst bei Herrn Prof. Dr. Ralf Poscher für die Betreuung dieser Arbeit. Er hat meine Ausbildung über ein Jahrzehnt lang begleitet, gefördert und geprägt. Meine Begeisterung für das öffentliche Recht ist von ihm inspiriert. Bedanken möchte ich mich auch bei Herrn Prof. Dr. Jan Henrik Klement für die zügige Erstellung des Zweitgutachtens.

Besonders freue ich mich über die Aufnahme dieser Arbeit in die Schriftenreihe "Sicherheit und Gesellschaft. Freiburger Studien des Centre for Security and Society" im Nomos Verlag. Hierfür bedanke ich mich sehr bei den Herausgebern Prof. Dr. Hans-Helmuth Gander, Prof. Dr. Walter Perron, Prof. Dr. Ralf Poscher, Prof. Dr. Gisela Riescher und Prof. Dr. Thomas Würtenberger.

Mein weiterer Dank gilt der Max-Planck-Gesellschaft. Im Rahmen meiner Tätigkeit am Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht in Freiburg wurde mir die Erstellung dieser Arbeit ermöglicht. Die zahlreichen Diskussionsrunden, Konferenzen und Vorträge haben mir vertiefte Blicke in die Rechtswissenschaft und zusammenhängende Disziplinen gewährt. Hervorzuheben sind dabei die anregenden Gespräche mit Herrn Dr. Benjamin Vogel, dessen Expertise zum Geldwäscherecht mich sehr vorangebracht hat. Besonders bedanken möchte ich mich auch bei meinen tollen Kolleg*innen, die mich jederzeit unterstützt und deren kritische Gedanken zu meiner Arbeit mich stets bereichert haben: Manuel, Laura P., Daniel, Marc, Jakob M., Christian, Morten, Florian, Claudia, Svenja, Jakob H., Antonia, Laura W., Maja, Johanna und Rafael.

Zuletzt und vor Allem möchte ich meiner Familie und meinen Freunden – soweit sie nicht schon genannt wurden – danken. Ihre Unterstützung hat mit mir meine lange Ausbildung erst ermöglicht. Birgitta, Andreas, Bärbel, Anna, Max, Rita, Martin, Caro, Michael und Kim. Euch möchte ich diese Arbeit widmen.

Letzter Stand der inhaltlichen Bearbeitung ist der 31. August 2023. Zitierte Internet-Links wurden zuletzt am 12.01.2025 überprüft.

Inhaltsverzeichnis

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.).

Kapitel B: Massenüberwachung im Verfassungsrecht: Vorratsdatenspeicherung und strategische Aufklärung

Der staatliche Umgang mit Finanzdaten, insbesondere im Rahmen der Geldwäschebekämpfung, soll umfassend aus der Perspektive des Sicherheitsverfassungsrechts betrachtet und bewertet werden. Dazu bedarf es einer Darstellung dieses Konzepts, um die Geltung für das Geldwäscherecht zu begründen.

Um die Hintergründe der Rechtsprechung zu den Maßnahmen der Massenüberwachung zu erläutern, soll zunächst der Versuch einer Erklärung unternommen werden, was unter dem Begriff der *sicherheitsrechtlichen Massenüberwachung* überhaupt verstanden werden soll. Nicht nur muss hierzu das Rechtsgebiet des Sicherheits- bzw. des Sicherheitsverfassungsrechts näher umschrieben werden. Auch mit dem Terminus der Massenüberwachung bzw. dessen Notwendigkeit und Mehrwert soll vorab eine Auseinandersetzung stattfinden.

Im weiteren Verlauf soll sodann die Rechtsprechung zu solchen Maßnahmen erläutert werden, die sich nach den vorangegangenen Überlegungen als sicherheitsrechtliche Massenüberwachung identifizieren lassen. Das sind vornehmlich die Urteile des Europäischen Gerichtshofs (EuGH) und des Bundesverfassungsgerichts (BVerG) zur Vorratsdatenspeicherung und zur strategischen Aufklärung. Diese Rechtsprechung wird – ausgehend von den allgemeinen Anforderungen der Rechtsprechung an die Überwachungsmaßnahmen der Sicherheitsbehörden – den Rahmen vorgeben, anhand dessen im Zuge dieser Arbeit die Regeln zur Überwachung des Finanzverkehrs überprüft werden sollen.

I. Einführung: Der Begriff der (Massen)Überwachung

Der Begriff der (Massen-)Überwachung taucht im Zusammenhang mit dem digitalen Zeitalter spätestens seit der NSA-Affäre immer wieder als Schlagwort[43], fast schon als Kampfbegriff, auf, ohne dass dabei stets klar

43 Siehe nur *Čas/Bellanova/Burgess ua.* in Friedewald/Burgess/Čas ua. (Hrsg.), Surveillance, 2017 (1).

wird, welche konkreten Sachverhalte damit eigentlich gemeint sein sollen. In Verbindung mit Finanzdaten ist von einer Massenüberwachung nur selten die Rede.

I. Unzulänglichkeiten und Potential des Überwachungsbegriffs

Das Phänomen der *Überwachung* wird nicht nur im rechtswissenschaftlichen, sondern auch im sozialwissenschaftlichen Kontext besprochen – insbesondere in der Kriminologie. Dort bilden die sog. „surveillance studies"[44] mittlerweile ein eigenständiges Forschungsfeld, auf dem insbesondere um eine Definition des Überwachungsbegriffs gerungen wird.

a. Der Überwachungsbegriff der „surveillance studies"

Nach *Lyon*, einem Vorreiter der surveillance studies, lässt sich Überwachung definieren als *„gezielte, systematische und routinemäßige Betrachtung persönlicher Umstände für Zwecke der Einflussausübung, Management, Schutz oder Direktion."*[45] Aufgrund dieser weiten Beschreibung bemerkt er, dass *Überwachung* mit einer ausgesprochenen Ambiguität verbunden ist. Der Begriff umfasst eine Fülle an Verhaltensweisen, die – je nach Kontext – eine völlig unterschiedliche Bewertung sowohl im Rahmen einer sozialen als auch rechtlichen Betrachtungsweise erfahren müssen.[46] Es macht offensichtlich einen Unterschied, ob bspw. eine Mutter ihr Kind auf dem Spielplatz beobachtet oder ob ein Polizeibeamter die Telefongespräche eines Verdächtigen abhört. Selbstverständlich können diese beiden Fälle der *Überwachung* daher auch keinem gemeinsamen Normregime unterliegen.

44 Vgl. *Lyon,* Surveillance Studies, 2012; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18 *ders.,* The electronic Eye, 1994; *Zurawski* in Zurawski (Hrsg.), Surveillance Studies, 2007, S. 7; s.a. *Adensamer,* Hdb. Überwachung, 2020, S. 24 ff.

45 *Lyon,* Surveillance Studies, 2012, S. 14; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18 (19); *J. Pohle* FIfF-Kommunikation 2019(4), 37 (37).

46 *Lyon,* Surveillance Studies, 2012, S. 14; *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (73) *Adensamer,* Hdb. Überwachung, 2020, S. 24; *Kreissl/Norris/Krlic ua.* in Wright/Kreissl (Hrsg.), Surveillance, 2015, S. 150 (155 f.).

Für eine ergiebige wissenschaftliche Auseinandersetzung gleich welcher Disziplin muss also stets die konkrete Form bzw. die Maßnahmen bestimmt werden, in denen sich die Überwachung manifestiert.[47]

b. Der Überwachungsbegriff im Recht

Für die rechtliche Betrachtung ist es von erheblicher Bedeutung, durch wen die *Überwachung* erfolgt, und aus welchem Grund, da einerseits die Wirkung der Grundrechte – der äußersten Schicht des Schutzes vor Überwachung – von der Person des *Überwachenden* abhängig ist, Art 1 Abs. 3 GG, und andererseits das Datenschutzrecht zwischen öffentlichen und nicht-öffentlichen Stellen unterscheidet[48], §§ 23, 24 BDSG.

Trotzdem widmen weder das deutsche noch das europäische Recht dem Überwachungsbegriff eine eigene Definition, wenngleich diese Rechtsordnungen an einigen Stellen explizit von Überwachung sprechen.

So kennen wir etwa die Videoüberwachung, z. B. § 4 BDSG, die Telekommunikations*überwachung* (TKÜ), z. B. §§ 54 PolG BW, 51 BKAG, 100a StPO, die akustische Wohnraum*überwachung*, § 100c StPO, oder die Pflicht zur *Überwachung* von Geschäftsbeziehungen, Art. 13 Abs. 1 lit. d) der EU-Geldwäscherichtlinie (GWRL)[49]. An anderen Stellen wird hingegen auf die Bezeichnung als Überwachung verzichtet – etwa bei den automatisierten Kennzeichen*erfassungssystemen* (z. B. Art. 39 BayPAG).[50]

Dass das Recht den Überwachungsbegriff nicht ausreichend reflektiert, zeigt sich etwa in § 100a StPO – der Vorschrift über die strafprozessuale TKÜ. Dort heißt es, dass *auch ohne Wissen der Betroffenen die Telekommunikation überwacht und aufgezeichnet werden darf.*

Hier wird semantisch zwischen der *Überwachung* und der *Aufzeichnung* getrennt. Man könnte also meinen, dass diese Norm von einem Überwachungsbegriff ausgeht, der allein auf die staatliche Wahrnehmung bestimm-

47 Vgl. *Kreissl/Norris/ Krlic ua.* in Wright/Kreissl (Hrsg.), Surveillance, 2015, S. 150 (155 f.).

48 Dazu *Masing*, NJW 2012, 2305 (2306 ff.).

49 Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. 2018, L 156/43; konsolidierte Fassung der 4. und 5. GWRL, Dok. 02015L0849-20210630.

50 Das BVerfG spricht auch von „*Kennzeichenkontrolle*", siehe BVerfGE 150, 244 – Autom. Kennzeichenkontrolle II.

ter Informationen gerichtet ist. Aus Sicht des Betroffenen wird aber regelmäßig die Aufzeichnung das größere Problem darstellen, da die spätere Beweisführung gegen ihn gerade auf der Perpetuierung seiner Kommunikation beruht. Schon hier zeigt sich somit eine erste Unzulänglichkeit des allgemeinen Überwachungsbegriffs. Erblickte man dessen Fokus allein in der fremden Wahrnehmungshandlung, könnte nur in bestimmten Situationen erklärt werden, wieso eine Überwachung als negativ oder als Eingriff empfunden wird.

Der Betroffene kann die Wahrnehmung ihn betreffender Informationen schließlich nicht grundsätzlich kontrollieren und ist daher vielfach auf das Interesse beschränkt, über die reine (Fremd-)Wahrnehmung hinausgehende Handlungen in Bezug auf solche Informationen abzuwehren.[51] In der Literatur zu § 100a StPO wird der Befugnis zur *Aufzeichnung* deshalb zu Recht kein eigenständiger Wert beigemessen. Sie geht in der *Überwachung* schon deshalb mit auf, weil in den meisten Fällen keine Echtzeitabhörung der Kommunikation stattfindet, sondern allein eine technische Aufzeichnung, die später gesichtet wird.[52]

Somit zeigt sich, dass im Bereich staatlicher Maßnahmen weniger die Wahrnehmung bestimmter Sachverhalte für die Überwachung entscheidend ist, als die technischen Instrumente[53], mit denen sie erfolgt und manifestiert wird.

Auch im Datenschutzrecht sucht man vergeblich nach einer Definition der Überwachung. Der Begriff scheint in diesem Rechtsgebiet nur beiläufig vorzukommen, etwa in § 4 BDSG, der die private Video*überwachung* reglementiert. Im Kern hängt sich das (europäische) Datenschutzrecht stattdessen am Begriff der „Datenverarbeitung" auf, unter dem sämtliche informationsbezogenen Handlungen zusammengefasst werden.

Dabei muss genau genommen zwischen Informationen und Daten unterschieden werden, wobei jeweils verschiedene Definitionen bzw. Abgren-

51 *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. Datenschutzrecht, 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).

52 *Günther* in MüKo StPO, § 100a Rn. 86.

53 Zum Begriff des "Instruments" in Bezug auf Maßnahmen der Geldwäscheprävention vgl. *Favarel-Garrigues/Godefroy/Lascoumes* in Svedberg Helgesson/Mörth (Hrsg.), Securitization, 2012, S. 88 (91 ff.).

zungen vorgeschlagen werden.[54] Für die in dieser Arbeit behandelten Fragen reicht es allerdings völlig aus, Daten als *zeichenhafte Darstellung von Informationen* zu verstehen.[55]

Auch der Anwendungsbereich der DSGVO, die „Daten" mit „Informationen" in Art. 4 Abs. 1 Nr. 1 gleichsetzt, ist nach Art. 1 Abs. 1 nur eröffnet, wenn personenbezogene Informationen verarbeitet werden, was wiederum irgendeine Verkörperung dieser Informationen voraussetzt.[56]

Verarbeitung in diesem Sinne meint nach Art. 4 Nr. 2 DSGVO *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung"*. Jeder Einzelne dieser Vorgänge muss für sich stets den datenschutzrechtlichen Anforderungen entsprechen, Art. 5, 6 DSGVO.

Für das über der DSGVO stehende europäische Primärrecht, insbesondere Art. 7, 8 der EU-Charter, sind die Begriffsbestimmungen des Datenschutzrechts aber selbstverständlich nicht abschließend, da auch auf europäischer Ebene gilt, dass das einfache Recht nicht den Inhalt des Primärrechts abschließend bestimmen kann.[57] Für Eingriffe in die Grundrechte auf Privatleben und Datenschutz nach Art. 7, 8 EU-Charter muss der EuGH daher nicht die Begriffsbestimmung des Art. 4 Nr. 2 DSGVO bemühen. Er kann unmittelbar anhand des Schutzbereichs der Grundrechte prüfen, ob eine Maßnahme einen Eingriff in diese darstellt.[58] Die Datenverarbeitungs-

54 Übersicht bei *Albers,* Informationelle Selbstbestimmung, 2005, S. 87 ff.; *Placzek,* Informations- und Datenschutz, 2006, S. 92 f.

55 Siehe nur *Sieber*, NJW 1989, 2569 (2572); *Albers* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (23); *Bäcker*, Der Staat 2012, 91 (92); *Trute* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, 2.5 Rn. 17

56 *Karg* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 1 Rn. 25.

57 Vgl. *J.-P. Schneider*, Die Verwaltung 2011, 499 (515) mit Verweis auf EuGH, Urteil v. 20.5.2003, C-138/01, C-139/01 (Österreichischer Rundfunk), Rn. 68 ff = EuR 2004, 276.

58 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 = NJW 2017, 717 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 121 ff. – PNR Canada = ZD 2018, 23

schritte der DSGVO taugen dem Gerichtshof jedoch als Ansatzpunkt.[59] Da die DSGVO letztlich dem Schutz der Grundrechte aus Art. 7, 8 der EU-Charter dient[60], liegt jedenfalls immer dann ein Eingriff in diese Rechte vor, wenn eine grundrechtsgebundene Stelle eine Datenverarbeitung i. S. d. Art. 4 Nr. 2 DSGVO vornimmt.[61]

Jedenfalls aber kennt auch der EuGH keinen Überwachungstatbestand per se, sondern beschreibt stets – wie auch die DSGVO – einzelne Verhaltensweisen als konkrete Eingriffe bzw. Datenverwendungstatbestände, anstatt einheitlich von einer *Überwachung* zu sprechen.[62]

c. Überwachung als final ausgerichtete Kombination verschiedener Datenverarbeitungsschritte

Es scheint somit, als ob der Überwachungsbegriff nicht von eigenständiger rechtlicher Bedeutung ist, da die einzelnen Maßnahmen, die die jeweilige *Überwachung* konstituieren, Datenverarbeitungsmaßnahmen darstellen und daher dem Datenschutzrecht unterfallen – dem Verfassungsrecht sowieso.

Es lässt sich aber nicht leugnen, dass dem Begriff eine gewisse Konnotation inhärent ist, die greifbar gemacht werden muss. Eine Definition der *Überwachung* für den Kontext des Rechts könnte es erlauben, komplexere Sachverhalte abzugrenzen und miteinander zu vergleichen. Die einzelnen Datenverarbeitungsvorgänge sind nämlich mitnichten unabhängig voneinander, sondern eng verknüpft.[63] Sie können sich gegenseitig bedingen und vielgestaltig so kombiniert werden, dass die einzelnen Verarbeitungsschrit-

59 Etwa EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 = NJW 2021, 531; siehe dazu *Marsch,* Datenschutzgrundrecht, 2018, S. 130 f.; *Schiedermair* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO, Einl. Rn. 169 ff.

60 Erwägungsgrund 1, DSGVO; *Schantz* in BeckOK Datenschutzrecht, DSGVO Art. 1 Rn. 5; *Sydow* in Sydow DSGVO, Einl. Rn. 7.

61 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 13.

62 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 134 ff. = NJW 2021, 531; EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 154 ff. – PNR Canada = ZD 2018, 23; siehe auch BVerfGE 125, 260 (310 ff.) – Vorratsdatenspeicherung.

63 *Albers,* Informationelle Selbstbestimmung, 2005, S. 125 f.

te auf die Auswirkungen der jeweils anderen intensivierend wirken. So geht etwa das BVerfG bei Datenerhebungen durch Sicherheitsbehörden davon aus, dass allein die Möglichkeit der Weitergabe bereits die Intensität der ursprünglichen Erhebung erhöht.[64] Durch die Betrachtung bestimmter Handlungen als Verknüpfung von Datenverarbeitungsvorgängen lässt sich darstellen, weshalb manche *Überwachungs*phänomene in Bezug auf persönliche Daten von besonderer, auch rechtlicher, Problematik sind.

Ausgehend von diesem Verständnis lässt sich aus dem Begriff der (Massen)Überwachung ein Mehrwert für die rechtliche Beurteilung ziehen. Mit ihm lassen sich bestimmte Kombinationen von Datenverarbeitungsschritten bzw. den dahinterstehenden rechtlichen Grundlagen beschreiben, deren individuelle rechtliche Relevanz bzw. Eingriffsintensität sich gerade danach bestimmt, dass sie Teil einer solchen Kombination sind. Der Überwachungsbegriff befreit also nicht davon, einzelne Datenverarbeitungsschritte grundsätzlich als eigenständige Grundrechtseingriffe zu begreifen. Er kann aber für die jeweilige Bewertung der einzelnen Verarbeitungen ausschlaggebend sein.

Um dieses Begriffsverständnis zu erläutern, kann auf die Rechtsprechung zur Vorratsdatenspeicherung zurückgegriffen werden – eines der Phänomene, die hier als Form der Massenüberwachung vorgestellt werden sollen.

Unter einer Vorratsdatenspeicherung kann man allgemein die Kombination aus einer Verpflichtung zur Datenerhebung und Speicherung einerseits und Befugnisnormen zum Abruf der gespeicherten Daten andererseits verstehen.[65] Zwar belasten diese Schritte den Betroffenen nur teilweise auch tatsächlich. Die Intensität jeder einzelnen Beeinträchtigung ergibt sich aber daraus, dass sie Teil einer Kombination von aufeinanderfolgenden Datenverarbeitungspflichten und -rechten ist.

Mängel in der Regelung bzw. gesetzlichen Gestaltung eines Datenverarbeitungsschritts können deshalb auf weitere Datenverarbeitungsschritte durchschlagen und deren Verhältnismäßigkeit beeinflussen, obwohl jede Verarbeitung einen eigenen Grundrechtseingriff darstellt und deswegen separat geprüft werden könnte.

64 BVerfGE 100, 313 (384) – strategische Fernaufklärung.; BVerfGE 110, 33 (70); dazu *Löffelmann*, GSZ 2019, 16 (18 f.).

65 Vgl. *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 117; *dies.* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (80 ff.) vgl. auch *Europäische Kommission,* Informationsgesellschaft, KOM(890) endg, 26.01.2001, S. 20.

Schon die Speicherung bestimmter Daten kann daher eine erhebliche Rechtsverletzung darstellen, wenn die Voraussetzungen des Zugriffs unzureichend geregelt worden sind.[66] Die Verhältnismäßigkeit des Zugriffs hängt wiederum davon ab, ob damit umfassende Übermittlungspflichten einhergehen, und ob auf Daten zugegriffen wird, deren Speicherung schon einen erheblichen Grundrechtseingriff darstellt.

Zwischen sämtlichen Datenverarbeitungsschritten, die Teil eines Überwachungskomplexes sind, besteht also eine *synergetische Wechselwirkung*. Die Verhältnismäßigkeit kann zwar für jeden Eingriff bzw. Datenverarbeitungsschritt separat geprüft, aber ohne Betrachtung der übrigen Eingriffe nicht in ihrer rechtlichen Bedeutung erfasst werden.

2. Elemente staatlicher (Massen)Überwachung

Für einen rechtlich tragfähigen Begriff der Überwachung kommt es also weniger darauf an, dass überhaupt verschiedene Datenverarbeitungsschritte kombiniert werden – dies findet andauernd statt –, sondern auf die konkreten Wirkungen und Hintergründe dieser Kombination. Insofern kommt die von *Lyon* im Rahmen der surveillance studies angesprochene Ambiguität erneut zum Tragen.[67]

Im rechtlichen Kontext muss es darauf ankommen, konkret jene Formen herauszuarbeiten, die einer besonderen rechtlichen Würdigung bedürfen.[68] Dabei kann auf bestimmte Überwachungskomponenten oder -elemente[69] zurückgegriffen werden, die hier kurz vorgestellt werden sollen.

66 BVerfGE 125, 260 (327 ff.) – Vorratsdatenspeicherung; dazu *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 159; EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 = NJW 2014, 2169; dazu *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.); s.a. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 97 ff. = EuZW 2022, 706; dazu auch VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI, Rn. 73 „funktionale Einheit".

67 *Lyon,* Surveillance Studies, 2012, S. 14.

68 Ähnlich *Timan/Galič/Koops* in Brownsword/Scotford/Yeung (Hrsg.), Oxford Hdb. Law Regulation Tech, 2017, S. 731 (744 ff.).

69 Vgl. In Bezug auf die strategische Kommunikationsüberwachung insbesondere EGMR, Urt. v. 25.5.2021 – Nr. 58170/13, 62322/14, 24960/15, Big Brother Watch ua/ Vereinigtes Königreich, Rn. 325 = NVwZ-Beilage 2021, 11

a. Beobachten als Datenerhebung und Datenerfassung

Am Anfang jeder Überwachungshandlung steht eine finale Beobachtung, die sich (datenschutz-)rechtlich zur „Datenerhebung und -Erfassung" i. S. d. Art. 4 Nr. 2 DSGVO transkribieren lässt. Diese eng miteinander verbundenen Datenverarbeitungsvorgänge beziehen sich auf den Moment, in dem eine Information erstmals wahrgenommen und mindestens für einen Augenblick verkörpert wird.[70]

Die Auftrennung von Erhebung und Erfassung wirkt dabei oft künstlich, denn die Datenerhebung, d. h. eine Erstellung von Daten ohne anschließende, wenigstens kurzfristige Speicherung, ist als separat verstandener Vorgang praktisch irrelevant.

Aus grundrechtlicher Sicht ist die Differenzierung von Erhebung und Erfassung auch nicht von Belang. Einzelne Verarbeitungsschritte einer Überwachungsmaßnahme können als einheitlicher Eingriff verstanden werden, wenn die Vorgänge einen einheitlichen Lebenssachverhalt bilden. So hat etwa der EuGH die Speicherung von Verkehrsdaten und den Zugriff jeweils als eigenständigen Eingriff bewertet, ohne auf die datenschutzrechtliche Einteilung dieser Vorgänge jeweils einzugehen.[71] Auch im Rahmen seines Gutachtens zum geplanten Abkommen der EU mit Kanada über die Verwendung von Fluggastdaten (PNR-Abkommen[72]) wird nur zwischen den Schritten „Speicherung, Analyse und Verwendung" unterschieden,[73] obwohl der Vorgang der Speicherung zwingend verschiedene Datenverarbeitungsschritte i. S. d. Art. 4 Nr. 2 DSGVO beinhaltet.

Anders mutet insofern nur die dritte Entscheidung des EuGH zur TK-Vorratsdatenspeicherung an, *La Quadrature du Net*[74]. In diesem Urteil, in dem es auch um die automatisierte Analyse von Verkehrsdaten ging, identi-

70 *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 15 f.

71 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; vgl. auch Vgl. BVerfGE 150, 244 (265 ff.) – Automatische Kennzeichenkontrolle II.

72 Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR), COM(2013) 529 final, 2013/0251 (NLE).

73 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 154 ff. – PNR Canada = ZD 2018, 23; detailleirt EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 92 ff. = EuZW 2022, 706.

74 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531.

fizierte der Gerichtshof den Eingriff ausdrücklich ausgehend vom Begriff der *Datenverwendung* i. S. d. Art. 4 Nr. 2 DSGVO.[75]

Einen solchen Rückgriff auf die DSGVO im Rahmen der Prüfung eines Grundrechts mag man normhierarchisch kritisch beäugen.[76] Eine gewisse Einheitlichkeit des Eingriffstatbestands i. R. d. Art. 7, 8 EU-Charter und des Datenverarbeitungsbegriffs des Art. 4 Nr. 2 DSGVO, dem die grundrechtlichen Bestimmungen ja zugrunde liegen, ist aber durchaus praktikabel. Insbesondere hinsichtlich des ersten Schritts jeder Datenverarbeitung, der Erhebung und Erfassung, sind kaum Alternativen zu der datenschutzrechtlichen Definition denkbar. Es ergibt daher Sinn, auch für den grundrechtlichen Bereich, das *Beobachten* im Sinne einer gezielten Wahrnehmung mit der *Datenerhebung und -Erfassung* i. S. d. Art. 4 Nr. 2 DSGVO gleichzusetzen.

b. Analyse und/oder Speicherung erhobener Daten

Dass eine Überwachung zwangsläufig mit einer Beobachtung im Sinne einer Datenerhebung bzw. -erfassung beginnt, ist nun aber nicht viel mehr als eine Selbstverständlichkeit. Entscheidend ist, dass es nicht bei der Erhebung bestimmter Daten bleibt, sondern diese mit weiteren Verarbeitungsschritten kombiniert wird. Zwei Anschlussprozesse kommen hier in Betracht. Zum einen können die erhobenen Daten gespeichert werden, d. h. länger als für den Augenblick der Erhebung aufbewahrt werden, oder sie können analysiert werden.

Die Kombinationsmöglichkeiten sind vielfältig. So kann sich eine Analyse unmittelbar an die Erhebung anschließen und eine Speicherung oder Weiterleitung vom Ergebnis der Analyse abhängig gemacht werden, wie es etwa bei der Kennzeichenkontrolle[77] oder der strategischen Fernmeldeaufklärung[78] der Fall ist. Oder aber es erfolgt erst eine Speicherung und die Analyse wird erst später im Rahmen einer periodischen Datenspeicherrasterung vorgenommen. So arbeiten in den meisten Fällen die digitalen

75 Idem, Rn. 172.; s.a. *Kingreen* in Callies/Ruffert EUV/AEUV, EU-Charter Art. 8 Rn. 13.
76 *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 31.
77 Vgl. BVerfGE 150, 244 – Automatische Kennzeichenkontrolle II.
78 Vgl. BVerfGE 100, 313 (384) – Strategische Fernaufklärung.

Monitoringsysteme der Banken[79] (dazu Kap. D. III. 2. aa. (2)). Denkbar ist es aber natürlich auch, dass die Daten ausschließlich gespeichert werden, ohne dass unmittelbar weitere Vorgänge eingeleitet werden. In diesen Fällen werden die Speicherpflichten von Zugriffsvorschriften flankiert. Man spricht von der Vorrats(daten)speicherung.[80]

Auch den Vorgängen *Analyse* und *Speicherung* lassen sich verschiedene Datenverarbeitungsschritte i. S. d. Art. 4 Nr. 2 DSGVO zuordnen.

Das Speichern etwa ist als eigenständige Form der Datenverarbeitung explizit genannt und kann als *Aufnehmen* oder *Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung* definiert werden.[81]

Die Analyse von Datensätzen dürfte regelmäßig einen *Abgleich* i. S. d. Art. 4 Nr. 2 DSGVO darstellen, da hierunter nicht nur der Vergleich verschiedener Datensätze fällt, sondern auch das Durchsuchen von Datensätzen nach bestimmten Merkmalen.[82] Es ließe sich jedoch auch als *Auslesen* begreifen, wenn man diesen Verarbeitungsschritt als den Vorgang begreift, *ein auf einem Datenträger gespeichertes Datum zielgerichtet konkret zur Kenntnis zu nehmen*.[83] Jedenfalls aber wird eine Analyse als *Verwendung* gelten[84], die insofern als Auffangtatbestand fungiert.[85]

Weniger die Begrifflichkeiten sind entscheidend als der Inhalt der einzelnen Maßnahme. Damit bestimmte Vorgänge eine Informationsverarbeitung zur *Überwachung* machen, müssen von ihnen bestimmte Effekte ausgehen.

---

79 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 56; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (455 f.).

80 Siehe nur *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021 (117).

81 OVG Hamburg, NZI 2021, 191 (193); *Schild* in BeckOK Datenschutzrecht, DSGVO Art. 4 Rn. 42; *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 19.

82 *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 27; aA. wohl *Ernst* in Paal/Pauly DSGVO/BDSG, DSGVO Art. 4 Rn. 31; *Schild* in BeckOK Datenschutzrecht, DSGVO Art. 4 Rn. 52.

83 *Reimer* in Sydow DSGVO, Art. 4 Rn. 63; ähnlich *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 22 mit Verweis auf den englischen Begriff „retrieval".

84 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 = NJW 2021, 531.

85 *Schild* in BeckOK Datenschutzrecht, DSGVO Art. 4 Rn. 48; *Ernst* in Paal/Pauly DSGVO/BDSG, DSGVO Art. 4 Rn. 29; *Roßnagel* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO Art. 4 Nr. 2 Rn. 24; aA. *Reimer* in Sydow DSGVO, Art. 4 Rn. 67.

Dabei muss man sich stets vor Augen halten, dass Datenverarbeitungsvorgänge in der modernen Kommunikationsgesellschaft alltäglich sind. Sie finden universell statt – sowohl im sozialen als auch im wirtschaftlichen und öffentlichen (Verwaltungs-)Bereich. Es ist daher illusorisch, wenn man meint, stets selbst über deren Verwendung bestimmen zu können.[86] Dass aus den Grundrechten trotzdem ein Verdikt der Datensparsamkeit[87] abgeleitet wird, ja überhaupt ein Bestimmungsrecht über bestimmte Informationen entwickelt wurde, lässt sich weniger mit dem Schutz der Daten an sich, als aus den Risiken erklären, die die Datenverarbeitung mit sich bringen kann. Schon das BVerfG hatte dies im Volkszählungsurteil erkannt und auf diesen Verwendungszusammenhang hingewiesen.[88] Dennoch hat es grundsätzlich eine Linie eingeschlagen, die das Recht auf informationelle Selbstbestimmung als eigentumsähnliche Entscheidungsbefugnis über Preisgabe *und* Verwendung persönlicher Daten propagiert (s. unten II.2.).[89] Wie man sich eine solche Hoheit vorstellen soll, hat das Gericht aber nie überzeugend klären können.[90]

Um staatliche Überwachung daher als eigenständiges rechtliches Phänomen zu begreifen, muss die Bewertung verschiedener Datenverarbeitungskonstellationen vom Ende hergedacht werden, mithin vom Verwendungszweck der Maßnahmen.

86 *Schlink*, Der Staat 1986, 233 (243); *Hoffmann-Riem*, AöR 123 (1998), 513 (527 ff.); *Ladeur*, DÖV 2009, 45 (48 f.) *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121).

87 Vgl. *Schantz* in BeckOK Datenschutzrecht, DSGVO Art. 5 Rn. 24 ff.

88 BVerfGE 65, 1 – Volkszählung.

89 Vgl. Idem, (45 f.).; dazu *Vogelgesang,* Informationelle Selbstbestimmung, 1987, S. 139 ff. *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (132 f.); *Trute*, JZ 1998, 822 (825); aA. *Albers,* Informationelle Selbstbestimmung, 2005, 158 f., die eine solche Intention des BVerfG nicht erkennen mag; Übersicht bei *Placzek,* Informations- und Datenschutz, 2006, S. 80 ff.

90 Insbesondere *Albers,* Informationelle Selbstbestimmung, 2005, S. 236 ff; 280 ff.; s.a. *Hoffmann-Riem*, AöR 123 (1998), 513 (527 ff.); *Ladeur*, DÖV 2009, 45; *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (131 ff.).; zum internationalen Kontext *Fairfield/Engel* in Miller (Hrsg.), Privacy and Power, 2017, S. 95 (104 ff.).

c. „Sicherheitsrechtliche" Zwecke als Kern des Überwachungsbegriffs

Der maßgebliche Zweck einer jeden Überwachung im sozialwissenschaftlichen Sinn[91] hängt zunächst von der Person des Überwachenden ab. Die zeitgenössische Auseinandersetzung mit Überwachung betrifft nicht nur staatliche Überwachungsmaßnahmen, sondern adressiert immer mehr die *Überwachung* durch Private, insbesondere Internetkonzerne, die ihrer Natur nach auf eine große Menge persönlicher Daten Zugriff haben. Diese Form der Überwachung dürfte vornehmlich wirtschaftlichen Zwecken dienen.[92] Sie steht daher nicht im Fokus dieser Arbeit.

Staatliche Überwachungsmaßnahmen können verschiedene Zwecke verfolgen, insbesondere aber den Schutz der äußeren und inneren Sicherheit.[93] Es sind diese *sicherheitsrechtlichen* Fälle der Gewinnung, Vorhaltung und Analyse von Daten, die hier als eigenständiges Phänomen rechtlich gewürdigt werden sollen. Um sie von anderen Formen der Datenverarbeitung, insbesondere im Rahmen der Fachverwaltung, abzugrenzen, ist es sinnvoll, einen eigenen Terminus mit einer sensiblen Konnotation zu nutzen. Wenn hier von *Überwachung* die Rede ist, ist also allein die sicherheitsrechtliche Überwachung gemeint. Sie kann als Einzelmaßnahme erfolgen, wenn ein individueller Anlass vorliegt, oder systemisch ohne Anlass. In letzterem Fall kann von Massenüberwachung gesprochen werden. Was kein Gesetz vorsieht – und wegen des Willkürverbots auch nicht vorsehen dürfte – wäre eine individuell ausgerichtete Maßnahme ohne entsprechend konkreten Anlass. Wenn aber *sicherheitsrechtliche* Zwecke ausschlaggebend für die Bewertung bestimmter Kombinationen staatlicher Datenverarbeitungsvorgänge als Überwachung sind, sollte der Begriff des Sicherheitsrechts auch definiert werden.

Von diesem Rechtsgebiet ist – auch in dieser Arbeit – immer öfter die Rede, weshalb verschiedene Autoren sich jüngst nicht nur um eine Begriffs-

91 *Lyon,* Surveillance Studies, 2012, S. 14; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18 (19).

92 Dazu *Picot/Berchtold/Neuburger* in Kolany-Raiser/Heil/Orwat ua. (Hrsg.), Big Data & Gesellschaft, 2018, S. 309; *Skyrius/Giriūnienė/Katin ua.* in Srinivasan (Hrsg.), Big Data, 2018, S. 451; *Amnesty International,* Surveillance Giants, 2019, S. 8 ff.

93 Zum staatsrechtlichen Sicherheitsbegriff *Möstl,* Öfftl. Sicherheit, 2002, S. 3 ff., 126 ff.; *Tanneberger,* Sicherheitsverfassung, 2014, S. 11 ff.; *Bantlin,* Nachrichtendienste, 2021, S. 25 ff.

bestimmung bemüht haben, sondern auch um eine Erklärung, weshalb eine solche Definition notwendig ist.[94]

Einigkeit besteht darin, dass unter dem Begriff *Sicherheitsrecht* das Recht der Polizei, der Nachrichtendienste sowie das spezielle Ordnungsrecht, etwa das Versammlungs-, Melde- und Waffenrecht, zu subsumieren sind.[95] Korrekterweise ist aber auch das Straf- und Strafverfahrensrecht, das immer stärker mit dem Polizeirecht verzahnt wird, zum Sicherheitsrecht zu zählen.[96]

Von den verschiedenen Unterfangen zur Bestimmung des Sicherheitsrechts soll hier insbesondere jenes von *Gusy* kurz herausgestellt werden.[97] Nach ihm setzt sich das Sicherheitsrecht als Rechtsgebiet zusammen aus der *„Summe der Gesetze, welche Organisation und Handeln staatlicher oder privater Akteure auf dem Gebiet der Sicherheitsgewährleistung regeln"*.[98]

Der Begriff sei eine Sammelbezeichnung, über die ein Streit nicht lohne, da ein besserer Begriff noch nicht gefunden sei.[99] Gewinnbringend sei die Begriffsbestimmung nur dann, wenn aus der Einteilung bestimmter Normen in ein Rechtsgebiet auch etwas folge.[100]

Ob das für die hier angestrengte Untersuchung des Überwachungsbegriffs der Fall ist, könnte man zunächst bezweifeln, da von der Begriffsbestimmung wiederum nur die Begrifflichkeit der *Überwachung* abhängt, die selbst ja gerade nicht für die Sensibilität der hiermit beschriebenen Grundrechtsbeeinträchtigung ausschlaggebend ist. Die Notwendigkeit eines eigenen Begriffs der Überwachung ist gerade umgekehrt dem Bedürfnis einer semantischen Zusammenfassung verschiedener kritischer Verhaltensweisen geschuldet. Mit anderen Worten: Die TK-Vorratsdatenspeicherung wäre auch dann ein erheblicher Grundrechtseingriff, wenn man sie nicht als

94 *Graulich*, DVBl 2013, 1210; *Gärditz*, GSZ 2017, 1; *Gusy* in Dietrich/Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019, S. 9.

95 *Graulich*, DVBl 2013, 1210.

96 *Danne,* Prävention und Repression, 2022, S. 21 ff.; *Dietrich* in Dietrich/Fahrner/Gazeas ua. (Hrsg.), Hdb. Sicherheits- und StaatsschutzR, 2022, § 6 Rn. 49; *Götz* in Isensee/Kirchhof (Hrsg.), HdB StR Bd. IV, 3. Aufl. 2006, § 85 Rn. 5 f. *Gärditz*, GSZ 2017, 1 (2) mit Verweis in Fn 12 auf *Bäcker,* Kriminalpräventionsrecht, 2015; *Zöller,* Informationssysteme, 2002; aA *Graulich*, DVBl 2013, 1210, der allein auf den Zuständigkeitsbereich des 6. Senats des Bundesverwaltungsgerichts abstellt.

97 *Gusy* in Dietrich/Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019, S. 9.

98 Idem, (11).

99 Ibid.

100 Idem, (12 ff.).

Überwachung bezeichnete, und sie könnte mit der Fluggastdatenspeicherung auch dann verglichen werden, wenn man diese Maßnahmen nicht *a priori* einem einheitlichen Rechtsgebiet zugeordnet hätte. Im Gegenteil: Aus der Ähnlichkeit folgt letztlich die einheitliche Zuordnung.

Die Begriffsdiskussion um den Bereich des Sicherheitsrechts zur Klärung des Überwachungsbegriffs erscheint tautologisch, wenn man die sicherheitsrechtliche Relevanz zu dessen Komponente erhebt. Durch die gemeinsame Bezeichnung etwa verschiedener Maßnahmen als *Überwachung* kann aber doch eine gewisse Vorstellung über die Gemeinsamkeiten provoziert werden.

Auch Gusy sieht den Mehrwert der Einteilung von Rechtsnormen in Rechtsgebiete darin, dass sie den Vergleich verschiedener Normenkomplexe erleichtert.[101] Er schlägt drei Konzepte vor, nach denen sich Rechtsgebiete einteilen lassen könnten – darunter ein „deskriptives", das den gerade angestellten Überlegungen am ehesten Rechnung trägt. Danach bestimmt nicht das Rechtgebiet den Gegenstand, sondern der Gegenstand das Rechtsgebiet.[102] Es entstünden deskriptiv Perspektiven auf Vergleichbares und Unvergleichbares, was vor Verallgemeinerung schütze.[103] Das Sicherheitsrecht könne so der Vielfalt der ihm zugeordneten Rechtsnormen Rechnung tragen. Allerdings bleibe damit der Erkenntnisgewinn der Rechtseinteilung stets limitiert, da sich die entsprechenden Erkenntnisse unmittelbar auch aus den jeweiligen Gegenständen ableiten lassen könnten.[104]

Darin besteht aber kein Nachteil, wenn man den Nutzen der Rechtsgebietszuteilung in der Herstellung einer, auch semantischen, Ordnung erkennt[105] – gewissermaßen als sprachliche Indikation, mit der gewisse Erkenntnisse von vorneherein aufgedrängt werden.[106] Solche Erkenntnisse sind hier etwa, dass der sicherheitsrechtlich geprägte Überwachungsbegriff sowohl die Fachverwaltung als auch privatwirtschaftliche Datenverarbeitungsvorgänge ausschließt. Es muss nicht mehr im Einzelnen erläutert werden, wieso die gefahrenabwehrrechtliche Telekommunikationsüberwa-

101 Idem, (13 f.).
102 Idem, (17 ff).
103 Idem, (19).
104 Idem, (20).
105 Vgl. *Tanneberger,* Sicherheitsverfassung, 2014, S. 12; allg. *Schmidt-Aßmann,* Verwaltungsrecht, 2. Aufl. 2006, S. 8 f.
106 Ähnlich den Familienähnlichkeiten von *Wittgenstein,* Philosophische Untersuchungen, 1971, S. 56 ff; lfd. Nr. 65 ff.; dazu *Wennerberg* in Savigny (Hrsg.), Wittgenstein's PU, 2. Aufl. 2011, S. 33.

chung mit jener der Strafverfolgungsbehörden oder der Zollfahndung vergleichbar ist und rechtlich entsprechend gewürdigt werden kann, während sie sich von der Speicherung i. R. d. Wirtschafts- oder (Fach-)Verwaltung unterscheidet. Die Vergleichbarkeit wird durch die einheitliche Zuordnung stipuliert und kann von dem Adressaten der Aussage notfalls überprüft werden.

3. Zusammenfassung

Wenn der Begriff der Überwachung als Umschreibung verschiedener, rechtlich besonderes relevanter Kombinationen von Datenverarbeitungsschritten verwendet werden soll, muss er stets bestimmte Elemente enthalten. Dies ist notwendig, da *Überwachung* als sozialwissenschaftliches Phänomen eine Vielzahl verschiedener Lebenssachverhalte beschreiben kann, die keiner einheitlichen rechtlichen Betrachtung unterliegen. So unterscheiden sich private Überwachungsmaßnahmen großer Unternehmen grundlegend von jenen der staatlichen Sicherheitsapparate. Natürlich geht es in beiden Fällen darum, wer was über wen weiß, doch die Vorstellung, den gesellschaftlichen Informationsfluss einheitlich verrechtlichen zu können, ist schon im Grundsatz illusorisch.[107] Die verschiedenen Datenverarbeitungsvorgänge sind daher nach ihrem Zweck zu trennen, um sie dann im Rahmen der jeweiligen Rechtsgebiete würdigen zu können.

Die sicherheitsrechtlich motivierte Datenerhebung mit anschließender Analyse und/oder Speicherung der gewonnenen Daten muss daher als eigenständige Überwachungsform behandelt werden. Der Begriff des Sicherheitsrechts ist dabei deskriptiv zu verstehen.[108] Ob eine Maßnahme ihren sicherheitsrechtlichen Zweck verfolgt, ergibt sich nicht daraus, dass die dahinterstehende gesetzliche Regelung a priori dem Sicherheitsrecht zugeordnet wird, sondern aus der Ähnlichkeit und der damit einhergehenden Vergleichbarkeit zu anderen sicherheitsrechtlichen Maßnahmen. Dazu zählen insbesondere das Recht der Nachrichtendienste, das Polizeirecht und das Strafverfahrensrecht, deren Überwachungsmaßnahmen sich diese Arbeit widmet.

---

107 Vgl. *Hoffmann-Riem*, AöR 123 (1998), 513 (527 ff.); *Ladeur*, DÖV 2009, 45 (48 f.) *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 45 ff.; *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (121) .

108 *Gusy* in Dietrich/Gärditz (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019, S. 9 (S. 17 ff.).

II. Kurzübersicht: Schutz vor Überwachung im Grundgesetz

Sicherheitsrechtliche Überwachungsmaßnahmen sind heute als eine grundrechtsrelevante Form der Eingriffsverwaltung vollständig anerkannt. Es steht nicht infrage, ob sie in Grundrechte eingreifen, sondern in welche.

Da das Grundgesetz die Privatheit per se nicht ausdrücklich schützt, hat das BVerfG in seiner Rechtsprechung erst herausarbeiten müssen, inwiefern die Grundrechte vor Überwachung schützen. Dabei hat sich eine zweigeteilte Systematik entwickelt, die aus einem bereichsspezifischen und einem allgemeinen Schutz vor Informationseingriffen besteht.[109]

1. Bereichsspezifischer Überwachungsschutz: Art. 10 Abs. 1 GG, 13 Abs. 1 GG und das „IT-Grundrecht"

Beziehen sich Überwachungsmaßnahmen auf bestimmte Informationen bzw. Lebensbereiche, die eigens von den Grundrechten geschützt sind, kann von einem bereichsspezifischen Überwachungsschutz gesprochen werden. Der Grundrechtsschutz bezieht sich hier nicht unmittelbar auf Informationen, sondern auf die Sphäre, in der die Informationen offenbart werden.

Zum bereichsspezifischen Überwachungsschutz zählen das Brief-, Post- und Fernmeldegeheimnis nach Art. 10 Abs. 1 GG, die Wohnung nach Art. 13 Abs.1 GG[110]und die Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (im Folgenden „IT-Grundrecht").[111]

109 *Bäcker*, Der Staat 2012, 91 (94 ff.).

110 „spezielle Gewährleistung der Privatsphäre" BVerfG, NJW 2016, 3508 (3511 Rn. 42); zur Verbindung in dieser Hinsicht von Art. 10 Abs.1 und Art. 13 Abs. 1 GG *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 19 Rn. 965; s.a. *Albers,* Informationelle Selbstbestimmung, 2005, 370 ff.

111 So *Bäcker* in Rensen/Brink (Hrsg.), Leitlinien BVerfG, 2009, S. 99 (118 ff.); *Hauser,* IT-Grundrecht, 2015; s.a. *Dreier* in Dreier GG, Art. 2 Abs. 1 Rn. 82, Fn 386 mwN; krit. zum Begriff *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 22.

a. Allgemeine Reichweite des bereichsspezifischen Überwachungsschutzes

Art. 10 Abs. 1 GG schützt die zwischenmenschliche Kommunikation unter Abwesenden.[112] Grund des Schutzes ist also nicht unmittelbar das Interesse der Betroffenen an der Privatheit des Kommunikationsinhalts, wenngleich dieser natürlich subsidiär mitgeschützt wird, sondern das Vertrauen auf die Integrität des technisch unterstützten Kommunikationsvorgangs bzw. -mediums.[113] Geschützt werden alle tatsächlichen Teilnehmer des Kommunikationsvorgangs.[114]

Dabei handelt es sich beim Brief-, Post- und Fernmeldegeheimnis nach herrschender Auffassung nicht um ein Grundrecht, sondern drei nebeneinander bestehende Grundrechte mit jeweils eigenem Schutzbereich, die aber eng miteinander verwandt sind.[115] Sie alle haben gemeinsam, dass allein die Kommunikationsübertragung geschützt wird.

Die Schutzbereiche zeichnen sich also durch ein zeitliches Element aus. Der Schutz beginnt in dem Moment, in dem das Kommunikationsobjekt den Herrschaftsbereich des Absenders verlässt, und endet, sobald er sich gesichert im Herrschaftsbereich des Empfängers befindet.[116] Bei der Eingriffsbestimmung stellt das BVerfG allerdings allein darauf ab, dass sich der Eingriff auf Informationen bezieht, die im Rahmen der Übertragung angefallen sind, auch wenn sich seine Folgen erst nach der Übertragung verwirklichen.[117] Die Abfrage von Telekommunikationsdaten beim Dienstеanbieter stellt daher stets einen Eingriff in Art. 10 Abs. 1 GG dar.[118]

Eine weitere Form bereichsspezifischen Schutzes vor Überwachung gewährleistet Art. 13Abs. 1 GG, der die Unverletzlichkeit der Wohnung sta-

112 *Gusy* in v. Mangoldt/Klein/Starck GG, Art. 18 Rn. 44; *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 10 Rn. 1.

113 BVerfGE 100, 313 (358 f.) – Strategische Fernmeldeaufklärung; *Hermes* in Dreier GG, Art. 10 Rn. 33; *Albers,* Informationelle Selbstbestimmung, 2005, S. 371.

114 OVG Münster, NJW 1975, 1335; *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 129.

115 *Gusy* in v. Mangoldt/Klein/Starck GG, Art. 10 Rn. 45; *Hermes* in Dreier GG, Art. 10 Rn. 25 mwN; aA. *Schoch* JURA 2011, 194 (195).

116 Vgl. BVerfGE 115, 166 (183); Problematisch insbesondere bei Emails, dazu *Graf* in BeckOK StPO, § 100a Rn. 51 ff.; *Brodowski*, JR 2009, 402.

117 BVerfGE 120, 274 (307 f.) – Online-Durchsuchung; *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 85.

118 BVerfGE 107, 299 (313 f.); E 125, 260 (309 ff.) – Vorratsdatenspeicherung *Sieber/Brodowski* in Hoeren/Sieber/Holznagel (Hrsg.), Hdb. Multimedia-Recht, 2020, Teil 19.3 Rn. 120 mwN.

tuiert. Auch hier handelt es sich nicht unmittelbar um den Schutz von Informationen, sondern um einen speziellen Bereich, in den grundsätzlich nicht zur Gewinnung von Informationen eingedrungen werden soll, eine Art „räumlicher Privatsphäre".[119]

b. Überwachungsschutz von Finanzinformationen i. R. d. bereichsspezifischen Überwachungsschutzes

Für die hier untersuchten Finanzinformationen sind Art. 10 Abs. 1, Art. 13 Abs. 1 GG und das IT-Grundrecht von geringer Bedeutung, da diese gerade nicht den allgemeinen Datenschutz, sondern nur konkrete Übertragungswege und die Wohnung bzw. IT-Geräte als räumliche Sphäre schützen.

Die Unverletzlichkeit der Wohnung ist denkbar nur betroffen, wenn verkörperte Finanzdaten, etwa Kontoauszüge in Papierform, oder digitale Speichermedien aus einem nach Art. 13 Abs. 1 GG geschützten Raum beschlagnahmt werden. Dazu zählen auch die nicht allgemein zugänglichen Geschäftsräume, solange sich dort Menschen regelmäßig aufhalten. Beschlagnahmungen bzw. Durchsuchungen bei einer Bank beeinträchtigen das Bankunternehmen also in Art. 13 Abs. 1 GG (i. V. m. Art. 19 Abs. 3 GG)[120] – nicht jedoch den (mit)betroffenen Kunden. Bei Bankschließfächern handelt es sich von vorneherein nicht um Wohnungen, da es am regelmäßigen Aufenthalt fehlt.[121]

Vor der Einführung des Rechts auf die Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme (dazu gleich) war noch umstritten, ob Art. 13 Abs. 1 GG auch vor einem technischen Zugriff auf sich in der Wohnung befindende Speichermedien schützt.[122] Das BVerfG hat dies abgelehnt.[123] Digitale Kontodaten, die sich auf einem Medium in einer Wohnung befinden, können also nur über Art. 13 Abs. 1 GG Schutz

119 BVerfGE 65, 1 (40) – Volkszählung; E 109, 279 (309, 325) – Großer Lauschangriff; *Papier* in Dürig/Herzog/Scholz GG, Art. 13 Rn. 4; *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 22 Rn. 1086.

120 Vgl. *Krepold/Zahrte* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 8 Rn. 231 ff.

121 BVerfG, Beschl. v. 16.10.2002 - 2 BvR 1306/02.

122 So etwa *Rux*, JZ 2007, 285 (292 ff.); *Kutscha*, NJW 2007, 1169 (1170 ff.) *Buermeyer*, HRRS 2007, 329 (332 ff.); *Hornung*, JZ 2007, 828; aA. *Germann,* Internet, 2000, S. 540 ff.; *Beulke/Meininghaus*, StV 2007, 60 (64).

123 BVerfGE 120, 274 (310 f.) – Online-Durchsuchung.

erfahren, wenn das körperliche Medium aus der Wohnung beschlagnahmt wird.

Wenn mittels einer Online-Durchsuchung auf gespeicherte Finanzinformationen zugegriffen wird, liegt ein Eingriff in das IT-Grundrecht vor. Aufgrund der hohen Anforderungen hat die Online-Durchsuchung in diesem Bereich aber keine große praktische Bedeutung. Stattdessen werden die Daten direkt von den kontoführenden Finanzdienstleistern abgegriffen, was mit deutlich weniger strengen Maßnahmen möglich ist[124] (dazu unten Kap. E.).

Nur geringe Spielräume bestehen auch für eine Anwendung des Art. 10 Abs. 1 GG in Bezug auf Kontodaten. Werden diese postalisch an den Kunden versandt, kommt eine Verletzung des Briefgeheimnisses in Betracht, wenn der Brief abgefangen und geöffnet wird oder beim Boten oder dem Absender Auskünfte über die Sendungen eingeholt werden. Auch aufgrund der immer stärkeren Verwendung von Online-Banking[125] dürften postalisch versandte Kontoauszüge aber eine immer geringere Rolle spielen und sind auch schwierig abzufangen.

Da die Finanzinformationen stets beim Absender verbleiben, ist ein Datenzugriff ohnehin stets auch unmittelbar bei den Instituten möglich. Die dortigen Dateibestände bestehen unabhängig von der Übermittlung an die Kunden und sind daher nach herrschender Auffassung nicht durch das Fernmeldegeheimnis geschützt.[126]

Das muss man nicht zwingend für überzeugend halten. Man könnte durchaus Speicherpflichten über den Zahlungsverkehr und damit einhergehende staatliche Zugriffe als Eingriff in das Fernmeldegeheimnis deuten, wenn man Zahlungen grundsätzlich als (geschützte Fern-)Kommunikation begreifen würde.[127]

Eine Überweisung ist nichts anderes als eine Reihe kommunikativer Vorgänge, die im digitalen Zahlungsverkehr über Signale abgewickelt wer-

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

125 Vgl. *Deutsche Bundesbank,* Zahlungsverhalten in Deutschland, 2017, S. 8 ff.; *Borges* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 11 Rn. 6.

126 Vgl. BVerfG, NJW 2009, 1405.

127 So für das Online-Banking *Singelnstein*, NStZ 2012, 593 (594 f.); aA. *Böckenförde*, JZ 2008, 925 (937 f.).

den.[128] Bei einer Kartenzahlung vor Ort weist bspw. der Zahler seine Bank an, eine Überweisung an ein bestimmtes Institut zu einem gewissen Zweck zu tätigen. Dabei müssen zwangsweise persönliche Informationen wie der Name von Zahler und Begünstigte sowie der Verwendungszweck, Datum etc. übermittelt werden (zur EU-ZahlungsdiensteRL[129], GeldtransferVO[130] und der SEPA-VO[131] siehe Kap. D. II. 2.). Die Überweisung zwischen den Banken ist ebenfalls ein kommunikativer Akt, bei dem Informationen über die jeweils zwischen den Banken bestehenden Salden ausgetauscht werden.[132] Auch Bareinzahlungen an einem Automaten sind ein kommunikativer Akt, bei dem der Kunde sein Institut anweist, einen gewissen Betrag seinem Konto gutzuschreiben. Dass es sich hierbei vor allem um wirtschaftlich relevante Informationen handelt, spielt für den inhaltsindifferenten Art. 10 GG keine Rolle.[133]

Im Ergebnis dürfte der Rechtsprechung, die digitale Bankvorgänge nicht unter den Schutz des Art. 10 Abs. 1 GG stellt, jedoch zuzustimmen sein. Der automatisierte Zahlungsprozess ist gerade dazu gedacht, eigentlich notwendige Kommunikation obsolet zu machen. Anstatt dem Bankmitarbeiter mitzuteilen, er solle eine Zahlung an das Konto einer bestimmten Person „X" mit dem Verwendungszweck „Y" veranlassen, reicht es, diese Informationen in ein technisches Zahlungssystem einzugeben und den

128 *Köndgen*, JuS 2011, 481; *Korff* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 45 Rn. 11 ff.

129 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG, ABl. 2007 L 319/1; neu gefasst durch Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/E, ABl. 2015, L337/35.

130 Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006, Abl. 2015, L 141/1.

131 Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009, ABl. 2012 L 94/22.

132 *Korff* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 45 Rn. 69 ff.

133 BVerfGE 67, 157 (172) – G-10; *Hermes* in Dreier GG, Art. 10 Rn. 41.

Informationsaustausch den Rechnern zu überlassen.[134] Man befindet sich also in einem Zwischenbereich von menschlicher Kommunikation und automatisierter Datenverarbeitung.[135]

Informationen sind dabei stets das Ergebnis von Kommunikation.[136] Auch verschiedene Speicherpflichten betreffen Informationen, die die jeweiligen Institute durch einen kommunikativen Akt erhalten, etwa eine Kontoeröffnung oder ein Telefonvertragsschluss, die beide eine Speicherung der Vertragsdaten nach sich ziehen. Geschieht dies nun unter Abwesenden könnte man auch hier das Fernmeldegeheimnis in Stellung bringen, denn verarbeitet werden zwangsweise die (fern-)kommunizierten Daten.

Das BVerfG ist diesen Weg zu Recht nicht gegangen[137], denn er ließe eine Abgrenzung von reinem Informationsschutz und spezifischem Kommunikationsschutz kaum mehr zu. Dem Versuch, jedwede Information auf ihren Ursprung als Kommunikationsergebnis zu rekonstruieren, um den Schutzbereich des Art. 10 Abs. 1 zu eröffnen, muss man widerstehen. Jede Speicherpflicht ließe sich ansonsten als Verarbeitung eines Kommunikationsumstands oder -inhalts darstellen. Der damit einhergehende universale Kommunikationsschutz würde den Schutzzweck des Fernmeldegeheimnisses sprengen. Art. 10 Abs. 1 GG schützt das Vertrauen in die Integrität bestimmter Kommunikationsvorgänge und nicht allgemein vor dem medialen Festhalten bestimmter alltäglicher Vorgänge, auch wenn sich diese als digitale Kommunikationsakte darstellen lassen. [138] Speicherpflichten über Zahlungsvorgänge oder Kontoeröffnungen sind daher nicht dem Schutz des Fernmeldegeheimnisses zu unterstellen, auch wenn sie mit digitalen Mitteln vollzogen werden.

134 Zum Kartenzahlungssystem *S. Kröger* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 47 Rn. 17 ff.

135 *Singelnstein*, NStZ 2012, 593 (594 f.).

136 *Albers,* Informationelle Selbstbestimmung, 2005, S. 87 f.

137 BVerfGE 118, 168 (183 ff.) – Kontostammdaten; E 130, 151 (181 f.) – Bestandsdatenauskunft I; E 155, 119 (168 f.) – Bestandsdatenauskunft II; *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 113.

138 *Böckenförde*, JZ 2008, 925 (937 f.).

2. Allgemeiner Überwachungsschutz: Die informationelle Selbstbestimmung

Allgemeinen Schutz vor Überwachung bietet das Recht auf informationelle Selbstbestimmung, bei dem es sich um einen Unterfall[139] des Allgemeinen Persönlichkeitsrechts (APR) aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1[140] GG handelt.

Das APR ist ein Rahmenrecht, das verschiedene (Teil-)Gewährleistungen umfasst.[141] Zusammenfassend lässt es sich als Recht der Grundrechtsträger beschreiben, ihre Persönlichkeit möglichst frei zu entfalten. Hierfür ist ein Rückzugsraum und die Möglichkeit, „für sich zu sein"[142] unerlässlich (Privatheitsschutz).[143] Außerdem sollen die Grundrechtsträger selbstbestimmt über die öffentliche Darstellung ihrer Persönlichkeit entscheiden können (Selbstdarstellungsschutz).[144]

Im Volkszählungsurteil[145] hat das BVerfG diesen Aspekt der Selbstbestimmung auf Daten erweitert und wie folgt argumentiert. Moderne Datenverarbeitungssysteme beherbergten die Gefahr, persönliche Daten so zu kumulieren, dass umfangreiche Persönlichkeitsprofile erstellt werden könnten. Solche Profile öffneten der Manipulation Tür und Tor, die faktisch ein selbstbestimmtes Leben vereitelten. Insofern käme es zu einem typischen Übergang[146] von Selbstdarstellung zu Selbstbestimmung[147]. Die (psychologischen) Effekte der Fremdwahrnehmung durch Datenverarbeitung beeinträchtigten die Freiheit zum selbstbestimmten Handeln.

---

139 BVerfGE 65, 1 (41 ff.) – Volkszählung.

140 Zur Verortung krit. *Lorenz*, JZ 2005, 1121 (1124 f.); *Kube* in Isensee/Kirchhof (Hrsg.), Hdb. StR Bd. VII, 3. Aufl. 2009, § 148 Rn. 31 ff. *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 52 mwN; nach *Dreier* in Dreier GG, Art. 2 Rn. 69 Fungiert Art. 1 Abs. 1 GG als „programmatische Leit- und Auslegungsrichtlinie"; ähnlich *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 89.

141 *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 147 f.; *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 53; *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 8 Rn. 511 ff.

142 *Kube* in Isensee/Kirchhof (Hrsg.), Hdb. StR Bd. VII, 3. Aufl. 2009, § 148 Rn. 129.

143 BVerfGE 27, 1 (6) – Mikrozensus; E 54, 148 (153 f.); *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 58 f.; „Recht der Selbstbewahrung" bei *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 8 Rn. 512 ff.

144 BVerfGE 35, 202 (220 ff.); *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 166 ff.

145 BVerfGE 65, 1 (41 ff.) – Volkszählung.

146 Vgl. *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 148.

147 Ausf. zum Zusammenhang von Selbstdarstellung und -Entfaltung *Britz,* Entfaltung durch Selbstdarstellung, 2007.

Um sich hiervor zu schützen, muss dem Betroffenen grundsätzlich das Recht zugestanden werden, „*selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*".[148] Ein Eingriff liegt deshalb immer vor, wenn staatliche Stellen persönliche Daten *verarbeiten,* also *erheben*, *speichern*, *verwenden* oder *weitergeben*,[149] wobei jeder Datenverarbeitungsschritt einen eigenständigen Eingriff darstellt (s. o.).[150]

Diese Konzeption der informationellen Selbstbestimmung wird von Teilen der Literatur aufgrund der angedeuteten Verfügungshoheit als Analogie zum Eigentumsrecht verstanden und entsprechend kritisiert.[151] Das BVerfG strebe eine Selbstbestimmung über persönliche Informationen an, die es aber naturgemäß gar nicht geben könne.[152] Informationen entstünden erst durch Kommunikation, weshalb eine Verfügungsgewalt über das Wissen Anderer – auch im Hinblick auf die Informationen über den Betroffenen – illusorisch sei.[153]

148 BVerfGE 65, 1 (43) – Volkszählung; aus der jüngeren Rspr: E 156, 11 (39) – Antiterrordatei II; *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 175 mwN; *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 17 jeweils mwN.

149 BVerfGE 115, 320 (341) – Rasterfahndung; E 130, 151 (183 f.) – Bestandsdatenauskunft I jeweils mwN; s.a. *Kunig/Kämmerer* in v. Münch/Künig GG, Art. 2 Rn. 76; als Ansatzpunkt kann der Verarbeitungsbegriff aus Art. 4 Nr. 2 DSGVO dienen; vgl. *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 18; *Schoch* JURA 2008, 352 (356) (zu § 3 BDSG a.F.); zum Verhältnis von Art. 4 Nr. 2 DSGVO und Art. 8 EU-Charter: *Kingreen* in Callies/Ruffert EUV/AEUV, EU-Charter Art. 8 Rn. 13.

150 BVerfGE 150, 244 (265 f.) – Autom. Kennzeichenkontrolle II; ebenso EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 124 – PNR Canada = ZD 2018, 23; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR) = EuZW 2022, 706.

151 *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; keine Eigentumsanalogie erkennt *Albers,* Informationelle Selbstbestimmung, 2005, S. 158 f.

152 *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. Datenschutzrecht, 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).

153 *Albers* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (16 f.); *dies.,* Informationelle Selbstbestimmung, 2005, S. 113 ff., 437 ff.; *Placzek,* Informations- und Datenschutz, 2006, S. 92 ff.; *Poscher* in Miller (Hrsg.),

Der Versuch, eine allgemeine Informationshoheit zu etablieren, führe in der Konsequenz dazu, dass das Datenschutzrecht als Datenverarbeitungsverbot mit Erlaubnisvorbehalt[154] konzipiert werden muss. Da die Verarbeitung von Informationen den Gegenstand jeglicher Kommunikation darstellt, würde letztlich nur der Alltag verrechtlicht und kein Grundrecht geschützt.[155]

Ausgehend von dieser Kritik werden verschiedene Alternativen zum Verständnis der informationellen Selbstbestimmung vorgeschlagen. Allen Konzeptionen gemein ist ihr Ziel, grundrechtlichen Schutz vor staatlichen Überwachungsmaßnahmen zu gewährleisten. Die Ansätze unterscheiden sich nur in der Konstruktion der Grundrechtseingriffe, kommen aber doch stets zu dem Ergebnis, dass die Grundrechte vor staatlichen Informationseingriffen schützen sollen.[156]

Auch im Ergebnis haben sich die Rechtsprechung und Literatur, soweit dort die informationelle Selbstbestimmung als systematischer Gewährleistungskomplex verstanden wird, angenähert. Das BVerfG bestimmt zwar weiterhin den Eingriff als solchen danach, ob Daten überhaupt verarbeitet werden und die Eingriffsintensität danach, welche und wie viele Daten verarbeitet werden (siehe unten III. 2. B.).[157] Es versteht aber die Verhältnismäßigkeitsprüfung nicht mehr als schlichte Rationalitätskontrolle, sondern zur konkreten Ausarbeitung formeller und materieller Voraussetzungen und anderer gesetzlicher Schutzvorkehrungen.[158] Im Rahmen dieser „Handlungsanleitungen"[159] für den Gesetzgeber manifestiert sich letztlich die Vorstellung, dass die informationelle Selbstbestimmung keine Informa-

---

Privacy and Power, 2017, S. 129 (S. 136 ff.); *Britz* in Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (566 ff.); *Trute* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 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); *Schlink*, Der Staat 1986, 233 (243).

154 *Bull,* Netzpolitik, 2013, S. 136 ff.; *Weichert*, DuD 2013, 246; „zum einfachrechtlichen Verbot mit Erlaubnisvorbehalt" *Buchner/Petri* in Kühling/Buchner DSGVO/BDSG, DSGVO Art. 6 Rn. 1; krit. dazu *Roßnagel*, NJW 2019, 1; *Albers/Veit* in BeckOK Datenschutzrecht, DSGVO Art. 6 Rn. 11.

155 *Hoffmann-Riem*, AöR 123 (1998), 513 (528); *Bull,* Netzpolitik, 2013, 136 ff.

156 Im Ergebnis auch *Thiel,* Entgrenzung, 2012, S. 264 ff.

157 Siehe nur BVerfGE 118, 168 (196) – Kontostammdaten mwN. aus der Rspr.

158 Siehe nur *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *ders.*, Die Verwaltung 2008, 345; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84; *Gurlit*, NJW 2010, 1035 (1037 ff.).

159 *Schluckebier* abw. Meinung BVerfGE 125, 260 (373).

tionshoheit realisiert, sondern einen gewissen Standard der Art und Weise staatlicher Informationsverarbeitung gewährleistet.[160]

Unabhängig vom weiterhin geführten Streit um die Dogmatik der informationellen Selbstbestimmung gilt also, dass die sicherheitsrechtliche Verwendung von Finanzdaten bestimmten Grenzen unterliegen muss, die sich kohärent aus der bestehenden Rechtsprechung zu vergleichbaren Überwachungsmaßnahmen ableiten lassen müssen.

III. Überwachungsmaßnahmen in der Rechtsprechung des BVerfG

Diesen grundgesetzlichen Überwachungsschutz hat das BVerfG in den letzten Jahren ausführlich elaboriert. Es liegt nunmehr eine ganze Reihe an Urteilen vor, in denen konkrete Maßnahmen und ganze Gesetzespakete zur Regelung der Überwachungsbefugnisse von Sicherheitsbehörden umfassend überprüft wurden. In diesen Urteilen hat das BVerfG nicht nur grundsätzliche Aussagen zur sicherheitsrechtlichen Überwachung aufgestellt, sondern im Rahmen der Verhältnismäßigkeitsprüfung ein nuanciertes Anforderungssystem für verschiedene Maßnahmen ersonnen.[161]

In jüngerer Zeit sind einige Versuche unternommen worden, die Rechtsprechung des BVerfG zu den verschiedenen Teilbereichen des Sicherheitsrechts als kohärentes System darzustellen.[162] Die Anforderungen des Gerichts – insbesondere an die materiellen Eingriffsschwellen in den einzelnen Gesetzen der Sicherheitsbehörden – legen in der Tat nahe, dass das Gericht ein einheitliches „Baukastensystem" für die Entwicklung der Sicherheitsgesetzgebung etablieren will.

160 Vgl. *Albers,* Informationelle Selbstbestimmung, 2005, 447 ff.; *dies.* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11 (26 ff.).

161 Siehe nur *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *ders.*, Die Verwaltung 2008, 345; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84; *Gurlit*, NJW 2010, 1035 (1037 ff.).

162 *Tanneberger,* Sicherheitsverfassung, 2014, S. 362 ff.

1. Grundlinien zu Überwachungsmaßnahmen in der Rechtsprechung des BVerfG

Bei der Bewertung der rechtlichen Zulässigkeit bestimmter Maßnahmen ist das BVerfG davon abgerückt, grundsätzliche Aussagen zu treffen. Anstatt den verschiedenen Sicherheitsbehörden aufgrund einer vermeintlichen Unverhältnismäßigkeit einzelne Befugnisse zu verbieten, ist das Gericht dazu übergegangen, aus dem Grundsatz der Verhältnismäßigkeit konkrete Schwellen und andere Anforderungen für die einzelnen Eingriffe abzuleiten.[163]

Das BVerfG hat in den letzten Jahren einen ganzen Katalog an Eigenschaften herausgearbeitet, die die Intensität einer Überwachungsmaßnahme beeinflussen.[164] Auf dessen Grundlage werden Eingriffe sodann mittels einer recht gefestigten Kasuistik in ein Stufenmodell eingeordnet.[165] Am unteren Ende stehen die „geringfügigen Eingriffe".[166] In der Mitte finden sich die Eingriffe „von erheblichem Gewicht"[167] und am schwersten wiegen die „tiefgreifenden"[168] Eingriffe bzw. Eingriffe von „hoher Intensität."[169]

---

163 Insbesondere BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 353 ff.; *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84: "Operationalisierung der Verhältnismäßigkeit"; *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff.); *Volkmann*, NVwZ 2022, 1408 (1411): „Steuerungsmodell"; *Trute*, Die Verwaltung 2009, 85 (85 ff; 96 ff.); *Schoch*, Der Staat 2004, 347; *Groß* KJ 2002, 1 (9 ff.) allg. *Bumke* in Hoffmann-Riem (Hrsg.), Innovationen im Recht, 2016, S. 115 (133 ff.); *ders.,* Grundrechtsvorbehalt, 1998, 100 ff., 235 ff.; allg. krit. zur „Maßstabssetzung" des BVerfG *Lepsius* in Jestaedt/Lepsius/Möllers ua. (Hrsg.), Entgrenztes Gericht, 2011, S. 159.

164 Übersichtlich *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 89 ff.; *Poscher/Kilchling/Landerer*, GSZ 2021, 225 (230 ff.); *Löffelmann*, GSZ 2019, 16 (19); *F. Braun/F. Albrecht* VR 2017, 151 (152); *Hornung/Schnabel*, DVBl 2010, 824 (826).

165 Dreistufiges Modell nach *Rusteberg*, KritV 2017, 24 (29 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 89 ff. erkennt vier Intensitätsstufen; krit. zur Aussagekraft der Nomenklatur *Tanneberger,* Sicherheitsverfassung, 2014, S. 234 f.

166 BVerfGE 67, 157 (179) – G-10; siehe auch VGH Mannheim, NVwZ-RR 2011, 231 (233)

167 BVerfGE 150, 244 (283) – Autom. Kennzeichenkontrolle II.

168 BVerfGE 141, 220 (267 ff.) – BKA-Gesetz.

169 BVerfGE 120, 274 (322) – Online-Durchsuchung.

Primäre Intensitätsaspekte sind die verarbeitete Datenmenge und -qualität, Heimlichkeit und Streubreite einer Maßnahme.[170] Es ist ein Erfordernis des Verhältnismäßigkeitsgrundsatzes, dass diesen intensivierenden Merkmalen durch kompensierende Vorkehrungen begegnet wird. Je intensiver sich eine Maßnahme nach den beschriebenen Merkmalen darstellt, desto stärker müssen die Kompensationsvorkehrungen sein.[171]

Dieser Ansatz des BVerfG hat dazu geführt, dass die Urteile[172] zu den jüngsten Novellierungen der Sicherheitsgesetze immer umfassender geworden sind, da das Gericht letztlich die Tatbestandsvoraussetzungen einzelner Eingriffsmaßnahmen selbstständig neu aufsetzt. Anstatt sich mit der für den Einzelfall konstruierten Rationalitätskontrolle abzumühen, versteht es den Verhältnismäßigkeitsgrundsatz bzw. die Angemessenheit im Sicherheitsrechts als Auftrag zur interpretatorischen Fortentwicklung rechtlicher Überwachungsmaßstäbe.[173]

Eine rein auf die Verwerfung oder Aufrechterhaltung von Gesetzen gerichtete Vorgehensweise wäre auch nicht praktikabel. Die Anforderungen an die Ausgestaltung der sicherheitsrechtlichen Überwachungsmaßnahmen sind mittlerweile so fein, dass der Gesetzgeber etliche Anläufe bräuchte. Schon deshalb muss das BVerfG die Anforderungen, die es jeweils für eine angemessene Ausgestaltung als notwendig erachtet, konkret benennen.[174] Dies führt zwar in der Tat dazu, dass das BVerfG dem Gesetzgeber letztlich „Handlungsanleitungen" zur Gesetzgebung im Sicherheitsrecht vorlegt,

170 Übersichtlich *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 89 ff.; *Poscher/Kilchling/Landerer*, GSZ 2021, 225 (230 ff.); *Löffelmann*, GSZ 2019, 16 (19); *F. Braun/F. Albrecht* VR 2017, 151 (152); *Hornung/Schnabel*, DVBl 2010, 824 (826).

171 *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.

172 Jüngst etwa; BVerfGE 154, 152 – Ausland-Ausland-Fernmeldeaufklärung; E 155, 119 – Bestandsdatenauskunft II; BVerfG, NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz;
NJW 2023, 1196 – Polizeiliche Datenanalyse.

173 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82.

174 *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. D Rn. 253; mit Verweis zur Gegenmeinung bei *Schöndorf-Haubold*, Sicherheit und Freiheit im Polizeirecht, 2014 (noch nicht veröffentlicht).

was durchaus an „judicial activism" grenzt.[175] Eine bessere Lösung, die rechtsstaatlich gebotene Abwägung von Sicherheit und Freiheit (vor Überwachung) praktikabel vorzunehmen, ist aber trotz aller Kritik noch nicht gefunden.[176]

Die „Handlungsanleitungen" drücken sich für Informationserhebungen als ausdifferenzierte Je-Desto-Formel[177] aus und sind somit eine Vorwegnahme der dem Gericht zugewiesenen Verhältnismäßigkeitsprüfung. Ausgehend von der systematisch bestimmten Intensitätsstufe einer Maßnahme wird – teilweise recht pauschal – eine Vielzahl spezifischer Anforderungen als Ergebnis der Verhältnismäßigkeitsprüfung entwickelt. So dürfen „besonders schwerwiegende Maßnahmen" nur bei konkretisierter Gefahr bzw. spezifischem Verdacht einer schweren Straftat und nur unter Richtervorbehalt angeordnet werden. Ebenso wie es Art. 13 Abs. 4 GG für den großen Lauschangriff vorsieht. Letztlich zeichnet das BVerfG also die Idee unmittelbar geltender Eingriffsanforderungen in der Verfassung nach und stützt sich bei dieser Fortbildung auf den Grundsatz der Verhältnismäßigkeit.

Eine solche Fortentwicklung ist auch für die Übermittlung von Informationen aus sicherheitsrechtlichen Überwachungsmaßnahmen erkennbar. Ausgangspunkt ist der Grundsatz, dass eine zweckändernde Datenübermittlung einen rechtfertigungsbedürftigen Grundrechtseingriff darstellt. Anstatt einer Rationalitätskontrolle im Einzelfall gelten aber auch hier konkretisiert pauschale Vorgaben durch das informationelle Trennungsprinzip und den Grundsatz der hypothetischen Datenneuerhebung, die insofern den Verhältnismäßigkeitsgrundsatz operationalisierbar machen.[178]

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

176 So auch *Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 192; ähnlich positives Fazit bei *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 184 ff.

177 *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.

178 *F. Schneider*, GSZ 2022, 1 (1) Zum Grundsatz der hypothetischen Datenneuerhebung; für diesen Aspekt zum informationellen Trennungsprinzip: *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (191); *Unterreitmeier*, DÖV 2021, 659 (660 ff.); *Poscher/Rusteberg* KJ 2014, 57 (68 f.); *dies.* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Reform der Nachrichtendienste, 2020, S. 145 (S. 152 ff.).

2. Massenüberwachung und Verfassungsrecht

In vielen Fällen befasste sich die Rechtsprechung[179] primär mit individuellen Überwachungsmaßnahmen, die zwar auch bei Finanzdaten eine große praktische Rolle spielen (s. Kap. E.), sich allerdings in der Funktionsweise deutlich von den Phänomenen der Massenüberwachung dadurch unterscheiden, dass kein Datenverarbeitungsschritt vorgenommen wird, bevor ein sicherheitsrechtlicher Anlass vorliegt.

Da sich diese Arbeit vornehmlich den geldwäscherechtlichen Massenüberwachungstatbeständen widmen will, soll im Folgenden dargestellt werden, wie sich die aufgestellten Grundsätze des BVerfG auf solche Maßnahmen der Massenüberwachung auswirken.

a. Formen der Massenüberwachung

Die Typisierung in der Individual- und Massenüberwachung hängt davon ab, ob die Überwachung in jedem konkret betroffenen Fall anlassbezogen erfolgt oder nicht. Es liegt in der Natur der Massenüberwachung, dass ihre Effektivität gerade davon abhängt, dass gezielt auch solche persönlichen Daten verarbeitet werden, bei denen im Moment der Verarbeitung noch nicht klar sein kann, ob sie für den verfolgten sicherheitsrechtlichen Zweck dienlich sind. Die Massenüberwachung kann insofern als Versuch des Staates verstanden werden, sich der allgemeinen Problematik des sicherheitsrechtlichen Vorfeldbereichs[180] zu widmen.

Diese besteht darin, dass gewisse Gefahren, deren Verursacher – etwa im Bereich Terrorismus[181] – gänzlich unbekannt sind, schon deshalb als stets gegenwärtig betrachtet werden müssen, da sich das Gegenteil nie beweisen ließe. Der Staat könnte letztlich immer einen Anlass zur für- bzw. vorsorglichen Überwachung vorbringen. Aufgrund dieser „stetigen Verhält-

179 Etwa BVerfGE 120, 274 – Online-Durchsuchung; E 113, 348 – TKÜ; mehrheitlich auch E 141, 220 – BKA-Gesetz; BVerfG, NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz.

180 Zur Vorfeldproblematik siehe *Albers,* Determination, 2001, S. 112 ff., 215 ff., 252 ff.; *Zöller,* Informationssysteme, 2002, S. 319 ff.; *Thiel,* Entgrenzung, 2012, S. 81 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Hoppe,* Vorfeldermittlungen, 1999; *Poscher*, Die Verwaltung 2008, 345 (348 ff.); *Wolff*, DÖV 2009, 597 (604).

181 *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (26 ff., 42).

nismäßigkeit“[182] stößt die Abwägungsrechtsprechung bei der Behandlung von Überwachungsmaßnahmen an ihre Grenzen.[183] Als Eingriffe, die der Gewinnung von Informationen dienen, setzen sie sinnvollerweise voraus, dass ein Informationsdefizit besteht. Die materiellen Anforderungen an ihre Zulässigkeit können daher naturgemäß nur in begrenztem Rahmen an das Vorliegen bestehender Information geknüpft werden. Stattdessen stehen prognostische Elemente im Vordergrund.[184]

Eine Überwachung ist folglich regelmäßig schon im erweiterten Vorfeld einer Gefahr zweckmäßig oder im strafprozessualen Kontext, wenn die Verwirklichung einer schweren Straftat zwar gesichert erscheint, aber noch völlig unklar ist, wer Täter sein könnte, etwa in Fällen der organisierten Kriminalität oder des Terrorismus.[185]

Aufgrund der bestehenden Anonymität kommen Individualüberwachungsmaßnahmen bei diesen Sachverhalten nicht in Betracht. Der Staat ist darauf angewiesen, die für solche Maßnahmen notwendigen Verdachtsmomente erst zu gewinnen[186] und die Voraussetzungen für die dann stattfindenden Ermittlungen zu gewährleisten. Dementsprechend haben sich zwei Formen der Massenüberwachung entwickelt: die Vorratsdatenspeicherung und die Datenanalyse. Letztere wiederum tritt in unterschiedlichen Gestaltungsformen auf: der Rasterfahndung und dem strategischen Abgleich.[187] Auch eine Kombination dieser Maßnahmen ist möglich, wenn die massenhaft gesammelten Daten nicht nur analysiert, sondern unabhängig vom Analyseergebnis vorratsmäßig gespeichert werden, wie es etwa im Rahmen der Fluggastdatenspeicherung der Fall ist.

Um einen Vergleich der Geldwäschebekämpfung mit den bereits von der Rechtsprechung behandelten Überwachungsmaßnahmen vorzunehmen,

182 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82 mit Verweis auf *Enders* in Enders/Wiederin/Pitschas ua. (Hrsg.), VVDStRL 64 (2004), 2005, S. 7 (45 f.).

183 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *ders.*, Die Verwaltung 2008, 345; s.a. *Volkmann*, JZ 2006, 918 (918 f.); *Lepsius* Leviathan 2004, 64 (78 ff.); *ders.* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23.

184 *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 223 ff.; *Bonin,* Kompensation, 2014, S. 217 ff.; allg. zu Wahrscheinlichkeit im Gefahrenabwehrrecht *Poscher*, Die Verwaltung 2008, 345 (S. 352 ff.).

185 *Albers,* Determination, 2001, 111 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 35 ff.; *Lisken*, ZRP 1994, 264.

186 Vgl. zur „Verdachtsgewinnung“ schon *Bull*, FS Selmer, 2004, S. 29.

187 zur Unterscheidung vgl. *Kahler,* Kundendaten, 2017, S. 37 f.; *Petri*, StV 2007, 266.

sollen die Grundzüge der bekannten Formen von Massenüberwachungsmaßnahmen nachgezogen werden, um strukturelle Parallelen der entsprechenden Normkomplexe aufzuzeigen.

aa. Vorratsdatenspeicherung

Eine schlichte Form der Massenüberwachung stellt dabei zunächst die sogenannte Vorratsdatenspeicherung dar, bei der bestimmte Daten für einen retrograden Zugriff der Sicherheitsbehörden vorgehalten werden.

Dabei dreht sich die grundrechtliche Problematik im Kern um die Verknüpfung von Speicherpflicht und (sicherheitsrechtlicher) Zugriffsberechtigung. Allgemein nämlich stellen Speicherpflichten, bei denen die spätere Notwendigkeit der Daten im Moment der Speicherung noch nicht hinreichend bekannt ist, keine Besonderheit dar.[188] Sie finden sich an verschiedenen Orten der Rechtsordnung – etwa in behördlichen Registern[189] oder den Buchhaltungspflichten von Kaufleuten, bspw. § 147 AO, § 257 HGB.[190] Allein die Speicherung ohne jeden erkennbaren gegenwärtigen oder zukünftigen Zweck ist stets rechtswidrig.[191]

Die Diskussion um die *Vorratsdatenspeicherung* betraf vor diesem Hintergrund also weniger das Konzept *vorrätiger* Daten als solches, sondern spezifisch die universelle Speicherung von TK-Verkehrsdaten zur späteren Nutzung durch Sicherheitsbehörden.[192] Erst nachdem durch das PNR-Abkommen mit Kanada und später durch den Erlass der PNR-RL auch die Speicherung von Fluggastdaten zur Verbrechensbekämpfung etabliert wurde, wurde der Begriff der Vorratsdatenspeicherung außerhalb der Telekommunikationsdaten intensiver diskutiert.[193]

Beiden Maßnahmen ist gemein, dass der Staat eine Bevorratung von Daten – selbst oder durch Dritte – vornimmt, deren primärer Zweck

188 Vgl. BVerfGE 130, 151 (189 f.) – Bestandsdatenauskunft I; zur Schufa z.B. s. VG Wiesbaden, ZD 2022, 706.
189 *Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 174 f.
190 Übersichtlich *Schober*, BC 2013, 528.
191 So schon BVerfGE 65, 1 (46) – Volkszählung.
192 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 139; vgl. auch *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 117 (117 f.).
193 *EDPS,* Stellungnahme 05/2015, PNR, 24.09.2015; *Arzt*, DÖV 2017, 1023; *A. Knierim* ZD 2011, 17.

zunächst in der Verfügbarkeit besteht.[194] Im Moment der Speicherung ist ein sicherheitsrechtlicher Anlass noch nicht vorhanden. Da der Daten-Art aber allgemein vom Staat ein hoher Nutzen für die Sicherheitsbehörden attestiert wird, werden die jeweiligen Datensätze für den Fall vorgehalten, dass die Zweckerforderlichkeit nachträglich eintritt.

Prägnant an der *Vorratsdatenspeicherung* ist also nicht der Zugriff auf retrograde Daten, denn Informationen müssen immer erst bestehen, damit sie verwendet werden können, sondern dass der Staat gewissermaßen das Vertrauen in die sicherheitsrechtliche Irrelevanz eines jeden Bürgers ablegt (dazu unten). Hingegen ist die Vorstellung fehlgeleitet, dass erst die Vorratsdatenspeicherung es dem Staat ermöglicht, Informationen abzugreifen, die vor Eintreten des sicherheitsrechtlichen Anlasses entstanden sind. Eine solche Anonymität vor Beginn der Ermittlungen existiert nicht, da es sowohl dem Staat als auch den Privaten unbenommen ist, verschiedenste Daten aus verschiedensten Gründen unter Berücksichtigung des allgemeinen Datenschutzrechts ohnehin zu speichern. Die Vorratsdatenspeicherung ist insofern nur eine Reaktion des Staates auf den Umstand, dass bestimmte Daten in der Praxis ihre ursprüngliche Zweckerforderlichkeit verlieren und deshalb eigentlich zu löschen wären, Art. 17 Abs. 1 lit. A), 5 Abs. 1 lit. B, c, e DSGVO.[195] So wurden (und werden teilweise[196]) die TK-Verkehrsdaten vor Einführung der „Flatrate-Verträge" von den Providern ohnehin aus Abrechnungszwecken für eine längere Zeit vorgehalten und im Rahmen der Ermittlungstätigkeit auch den Sicherheitsbehörden zugänglich gemacht.[197]

Bei den Finanzdaten lässt sich dies gut beobachten (dazu unten Kap. E.). Obwohl die geldwäscherechtlichen Aufbewahrungspflichten recht offensichtlich eine Vorratsdatenspeicherung vorsehen (dazu Kap. D. III. 2. D.), findet eine intensivere Diskussion weder in der deutschsprachigen Rechtswissenschaft noch in der Öffentlichkeit statt (Übersicht zur Diskussion in Kap. F.). Dieses überschaubare Interesse lässt sich angesichts der Sensibilität – gerade der Kontoinhaltsdaten – wohl nur damit begründen,

194 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 140.

195 *Wolff* in BeckOK Datenschutzrecht, Syst. A Rn. 51.

196 Vgl. *BfJ,* Statistik Verkehrsdatenerhebung, 2020, S. 4 f., https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_Verkehrsdaten_2020.pdf?__blob=publicationFile&v=4, zuletzt aufgerufen am 12.01.2025; LG Landshut, Beschluss v. 16.01.2013 - 6 Qs 309/12; LG Mannheim, ZD 2018, 223; dazu *Bär* in BeckOK StPO, TTDSG § 9 Rn. 16; *J.-D. Braun* in Geppert/Schütz Beck'scher TKG Kommentar, TKG § 96 Rn. 21.

197 *Breyer,* Vorratsspeicherung, 2005, S. 12 ff.

dass ein Zugriff auf Kontoinhalte eine seit Jahren etablierte Praxis der Staatsanwaltschaften[198] darstellt, da die Daten aus verschiedenen Gründen (Kap. D. II.) ohnehin vorliegen.

Das Bemerkenswerte an der Vorratsdatenspeicherung ist die Kombination aus Speicherung und Zugriff. Jeder dieser Datenverarbeitungsschritte stellt zwar einen eigenständigen Eingriff dar, die Bewertung hängt jedoch gerade davon ab, dass die Schritte aufeinander zugerichtet sind und absichtlich kombiniert wurden. Bei der Verhältnismäßigkeit jedes Verarbeitungsschrittes ist also die Verhältnismäßigkeit der anderen Schritte zu beachten. Sie verhalten sich insofern wechselwirkend bzw. synergetisch.

Der Staat belegt eine bestimmte Datenform mit dem Verdikt, dass diese Daten in Zukunft für Sicherheitsbehörden relevant werden können. Damit kehrt er die Grundannahme, dass Daten nur gespeichert werden sollen, wenn ihre zukünftige Nutzung für bestimmte Zwecke absehbar ist, und dann für andere Zwecke bloß zufällig vorliegen und ermittelt werden können, in das Gegenteil um.[199]

Diese Zufälligkeit bzw. Unkontrollierbarkeit der Datenverfügbarkeit stellt normalerweise ein natürliches Abwehrmittel gegen staatliche Ermittlungsmaßnahmen dar. Dieses wird dem Bürger geraubt, wenn der Staat bestimmte Daten für die Eventualität, dass sie tatsächlich für Ermittlungen notwendig werden, vorsorglich aus dem Bereich des Unkontrollierbaren herausnimmt.

bb. Datenanalyse: strategische Aufklärung und Rasterfahndung

Die zweite Form der Massenüberwachung stellen die strategischen Aufklärungsmaßnahmen und die Rasterfahndung dar, die sich dadurch auszeichnen, dass größere Datenmengen technisch analysiert werden, um dadurch Verdachtsmomente gegenüber bestimmten oder bestimmbaren Personen zu gewinnen.

Bei der Rasterfahndung erfolgt dies durch den fortlaufenden Abgleich verschiedener Datensätze, indem stets nur die Überschneidungen in den folgenden Schritten ausgewertet werden, um einen immer enger werdenden

198 Siehe nur *F. Jansen,* Bankauskunftsersuchen, 2010; *Kahler,* Kundendaten, 2017, S. 31 ff.; *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 8 Rn. 31 ff.; *Reichling*, JR 2011, 12.

199 Krit. insofern *Szuba,* Vorratsdatenspeicherung, 2011, 192 ff.

Personenkreis zu identifizieren.[200] Da sich ein vergleichbares Instrument in der Überwachung von Finanzdaten nicht finden lässt – auch die „Operation Mikado"[201] (unten Kap. E. I. 1. C. bb.) stellte keine Rasterfahndung dar[202] –, soll diese Maßnahme hier aber nicht näher erläutert werden.[203] Von größerem Interesse ist hier das Durchleuchten einzelner Datensätze nach bestimmten Suchelementen, das mangels Abgleich verschiedener Datensätze gerade nicht als Rasterfahndung zu qualifizieren ist,[204] sondern als strategische Aufklärung bezeichnet werden kann.

Eine strategische Aufklärungsmaßnahme im hier verstandenen Sinne liegt vor, wenn auf eine massenhafte Datensammlung innerhalb eines bestimmten räumlichen und/oder zeitlichen Bereichs ein unmittelbarer Abgleich der erhobenen Daten mit einem bestimmten Datensatz erfolgt. So werden beispielsweise bei der automatisierten Kennzeichenerfassung sämtliche KFZ-Kennzeichen erfasst, die an einem gewissen Streckenabschnitt vorbeikommen, und in einem automatisierten Prozess mit einer Liste gesuchter KFZ-Kennzeichen abgeglichen.[205] Nur bei einem „Treffer" finden die Daten weitere Verwendung durch die jeweiligen Sicherheitsbehörden. „Nichttreffer" werden umgehend gelöscht.

Ein anderes Beispiel ist die strategische Fernmeldeaufklärung. Bei dieser werden große Mengen von Telekommunikationsinhalten, die auf zuvor bestimmten Telekommunikationswegen stattfinden, erhoben und auf bestimmte „Selektoren" hin durchleuchtet. Diese Selektoren können formalen Charakters sein, etwa eine bestimmte Adresse oder Anschlusskennung, oder inhaltlicher Natur, etwa bestimmte Begriffe oder Sätze.[206]

---

200 BVerfGE 115, 320 (321) – Rasterfahndung; *Gerhold* in BeckOK StPO, § 98a Rn. 9 ff.

201 BVerfG, NJW 2009, 1405

202 Idem, (1406 f.); AG Halle, DuD 2007, 464 (467); zust. *Kahler,* Kundendaten, 2017, S. 37 f.; *Petri*, StV 2007, 266, die aber eine Anwendung des § 161 Abs. 1 S. 1 Hs. 2 StPO iE. ablehnen; aA. *Schnabel*, DuD 2007, 426 (427 f.): „mittelbare Rasterfahndung"; *Brodowski*, JR 2010, 543 (547 f.).

203 Allerdings enthält auch die vorzeitige PNR-Analyse Elemente der Rasterfahndung vgl. *Arzt*, DÖV 2017, 1023 (1026 ff.).

204 Vgl. BVerfG, NJW 2009, 1405 (1406 f.); OLG Stuttgart, NStZ 2001, 158 (159); OLG Köln, NStZ-RR 2001, 31 (32); *Köhler* in Meyer-Goßner/Schmitt StPO, § 98a Rn. 8.

205 Zur Funktionsweise siehe nur *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 970; *Roggan*, NStZ 2022, 19 (21).

206 Bspe. bei *B. Huber*, NJW 2013, 2572 (2573); umfassend zu den formalen Selektoren aus der Zusammenarbeit BND-NSA *Graulich*, (1. UA des 18. Deutschen Bundestags), Fernmeldeaufklärung mit Selektoren, MAT A SV-11/2, zu A-Drs. 404, 23.10.2015, S. 23 ff., 98 ff.

Wie die Vorratsdatenspeicherung zeichnen sich die strategischen Aufklärungsmaßnahmen dadurch aus, dass von der Datenverarbeitung stets auch solche Personen betroffen sind, die im Moment der Verarbeitung keinerlei Anlass für eine sicherheitsrechtliche Überwachung geliefert haben. Ausgangspunkt ist abermals, dass der Staat, etwa aufgrund der (Omni-)Präsenz organisierter Kriminalität, allgemein davon ausgeht, dass sich aus den Informationen der Abgleichsdatensätze sicherheitsrelevante Sachverhalte ergeben könnten.[207] Je nachdem, wie spezifisch diese Daten sind, steigert sich jedoch die Eingriffsschwelle für den Abgleich. Durch die Eingrenzung der Suchbegriffe soll gewährleistet werden, dass der Abgleich nur spezifische Verdachtsmomente hervorbringt, die dem Anlass entsprechen.[208]

Die strategische Aufklärung unterscheidet sich in struktureller Hinsicht erheblich von der Vorratsdatenspeicherung. Bei der Vorratsdatenspeicherung tritt der Anlass, der die Nutzung der gespeicherten Daten erforderlich werden lässt, extrinsisch ein. Die Daten selbst werden erst bei Eintreten eines Anlasses wiederaufgegriffen, und nicht proaktiv – bevor es zu einem Verdachtsmoment gekommen ist – zur Einleitung von Ermittlungen genutzt. Gerade so verhält es sich hingegen bei den strategischen Aufklärungsmaßnahmen. Zwar stehen auch hier extrinsische Gründe hinter der Aufnahme bestimmter Selektoren in die Abgleichsdatensätze. Die Maßnahmen sollen aber unmittelbar zu weiteren Ermittlungs- oder auch Exekutivmaßnahmen führen, weshalb eine Speicherung in Nichttrefferfällen ausbleibt. Die strategische Aufklärung dient also, wie auch die Rasterfahndung[209] oder der Abgleich von PNR-Daten[210], der Gewinnung bzw. Verdichtung von vorab konkretisierten Verdachtsmomenten[211] und nicht der Förderung später (eventuell) erforderlich werdender Ermittlungen der Sicherheitsbehörden.

b. Aspekte der Intensitätsbewertung

Beide Formen der Massenüberwachung weisen verschiedene vom BVerfG entwickelte Intensitätsmerkmale auf. Sowohl bei der Vorratsdatenspeiche-

207 *Bäcker*, Kriminalpräventionsrecht, 2015, S. 53 ff.
208 BVerfGE 150, 244 (281 ff.) – Autom. Kennzeichenkontrolle II.
209 BVerfGE 115, 320 (107) – Rasterfahndung.
210 *Arzt*, DÖV 2017, 1023 (1028).
211 BVerfGE 154, 152 (245 ff.) – Ausland-Ausland-Fernmeldeaufklärung; *Roggan*, NStZ 2022, 19 (20).

rung als auch bei der strategischen Kontrolle werden die Daten einer großen Zahl von Menschen zur Förderung sicherheitsrechtlicher Ziele verarbeitet, ohne dass dies den Betroffenen im Moment der Verarbeitung stets gewahr wird.

aa. Anlasslosigkeit und Streubreite

Gerade die Betroffenheit einer Vielzahl von Personen steht sinnbildlich und namensgebend für das Phänomen der Massenüberwachung. Eine hohe „*Streubreite*" wirkt sich steigernd auf die Intensität der Grundrechtsbeeinträchtigung aus.

Bei Individualmaßnahmen sind zwar ebenfalls Dritte mitbetroffen, etwa die Kontaktpersonen einer Person, deren Telekommunikation überwacht wird. Bei solchen Maßnahmen stellt die Streubreite aber kein entscheidendes Merkmal der Intensitätsbewertung dar, sondern spielt eine untergeordnete Rolle.[212] Im Vordergrund der Individualmaßnahmen steht vielmehr, wie tief in die Privatsphäre der final betroffenen Person eingegriffen wird. Allerdings kann es hier vergleichsweise stringent gelingen, mittels Eingriffsschwellen zu gewährleisten, dass der Eingriff nur dann vorgenommen wird, wenn die Chancen auf eine sicherheitsrechtliche Relevanz der Informationen hochstehen. Die gesetzliche Grundlage der Maßnahme gewinnt hierdurch an Effektivität und wird somit *verhältnismäßig*.[213]

Bei Maßnahmen der Massenüberwachung verhält es sich umgekehrt. Sie kommen prinzipiell in Situationen zur Anwendung, bei denen gerade erst die Bewahrung oder Gewinnung von relevanten Informationen im Raum stehen. Es liegt insofern in ihrer Natur, dass sie nicht effektiv, nicht zielgerichtet, sondern universell ausgerichtet sind.

Da Massenüberwachungsmaßnahmen zwangsläufig breit streuen, sind sie nach der Bewertungsmatrix des BVerfG *stets* besonders eingriffsinten-

212 Vgl. allerdings BVerfGE 113, 348 (383) – TKÜ.

213 *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 82; *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff., 127).

siv.[214] Dieser Intensität müssten nach der Je-Desto-Formel[215] (s. o. III. 1.) nun eigentlich hohe Eingriffsschwellen gegenüberstehen und damit insbesondere ein rechtfertigender Anlass. Die Anlasslosigkeit ist aber gerade die Wurzel der hohen Streubreite. Die verfassungsgerichtliche Dogmatik führt zu dem paradoxen Ergebnis, dass eigentlich gerade für solche Maßnahmen ein rechtfertigender Anlass bestehen müsste, die sinnvollerweise nur anlasslos erfolgen können.[216]

Das BVerfG steht insofern vor einem Dilemma. Zur Operationalisierung des Verhältnismäßigkeitsgrundsatzes muss das Gericht – wenn es seine Rechtsprechung im Sicherheitsrecht stringent halten will – auch für anlasslose Maßnahmen bestimmte Anforderungen aufstellen, ohne gleichzeitig deren Nutzen zu versperren.[217] Im Rahmen der Vorratsdatenspeicherung konnte es sich insofern noch mit der Trennung von Speicherung und Zugriff behelfen. Der Zugriff stellt eine Individualmaßnahme dar. Er kann daher mittels bestimmter Eingriffsschwellen eingegrenzt werden. Nach dem BVerfG kann es ergo zulässig sein, eine universale Speicherpflicht bestimmter Datenkategorien einzuführen, wenn die tatsächliche Nutzung dieser Daten durch die Behörden auf bestimmte Fälle beschränkt bleibt. Die Bewertung der Speicherung hängt somit (auch) von der Ausgestaltung der Zugriffsvorschriften ab.[218]

Bei Maßnahmen der massenhaften Datenanalyse kommt diese Möglichkeit nicht in Betracht, da die Erhebung der Daten unmittelbar durch die Sicherheitsbehörden erfolgt. Hier kam das BVerfG daher nicht umhin, schon für den ersten Verarbeitungsschritt der Überwachungsmaßnahmen bestimmte Beschränkungen aufzustellen. So muss etwa die strategische Fernmeldekontrolle auf eine begrenzte Zahl von Telekommunikationswe-

214 So schon BVerfGE 100, 313 (376, 392) – Strategische Fernmeldeaufklärung; E 115, 320 (354) – Rasterfahndung; E 150, 244 (283 f.) – Autom. Kennzeichenkontrolle II.

215 Siehe nur *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.; *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 116.

216 Vgl. *Volkmann*, NVwZ 2022, 1408 (1411).

217 Insofern krit. *Möstl*, GSZ 2019, 101 (106 ff.).

218 BVerfGE 125, 260 (320 ff.) – Vorratsdatenspeicherung; aA. der EuGH, der schon die Speicherpflicht von bestimmten Umständen abhängig macht, siehe EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.) = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135.

gen beschränkt werden[219], für die eine sicherheitsrechtliche Relevanz begründet werden muss und von denen wiederum nur eine begrenzte Zahl der Kommunikationsinhalte ausgelesen werden darf, §§ 5, 10 Abs. 4,5 G-10; §§ 10 Abs. 2, 8 BNDG (s. o.)).

Auch *anlasslose* Maßnahmen – in dem Sinne, dass sie gezielt auch eine große Menge sicherheitsrechtlich nicht relevanter Sachverhalte bzw. Personen erfassen – sind damit nicht gänzlich ohne Erfüllung bestimmter Voraussetzungen zulässig.

Dass das BVerfG insofern eine grundsätzlich kritische Position gegenüber Massenüberwachungsmaßnahmen eingenommen hat, wird nicht nur positiv gesehen.[220] Dem BVerfG lässt sich durchaus vorwerfen, selbstreferentiell vorzugehen, da es die hohe Intensität maßgeblich von der jeweils enormen Streubreite der Maßnahmen ableitet. Dass die Streubreite einer Maßnahme aber überhaupt intensivierend wirkt, ist keine sich aufdrängende extrinsische Erkenntnis, sondern eine (begründungsbedürftige) Feststellung des Gerichts. An dieser hält es auch bislang strikt fest. Die intensivierende Wirkung der Streubreite wird gewissermaßen als Axiom behandelt,[221] obwohl die dogmatischen Begründungen durchaus kritisiert werden.[222]

Im Ergebnis verdient das BVerfG aber Zustimmung. Das Gericht nimmt letztlich eine objektive Betrachtungsposition ein, indem es die jeweiligen Ermächtigungsgrundlagen auf ihre gesellschaftlichen Auswirkungen hin untersucht. Dogmatisch kann dieses quantitative Element als Ausprägung der objektiv-verfassungsrechtlichen Gesetzeskontrolle verstanden werden.[223]

---

219 BVerfGE 100, 313 (376 ff.) – Strategische Fernmeldeaufklärung; E 154, 152 (250 ff.) – Ausland-Ausland-Fernmeldeaufklärung

220 *Haas* abw. Meinung zu BVerfGE 115, 320 (371); *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 98 ff.; *Würtenberger*, FS Schröder, 2012, S. 285 (299 f.); *Löffelmann* – "Kaum betroffen" FAZ Online vom 29.04.2015, https://www.faz.net/aktuell/politik/staat-und-recht/gastbeitrag-kaum-betroffen-13566596-p2.html?service=printPreview, zuletzt aufgerufen am 12.01.2025; auch krit. aber iE zustimmend *Möstl* in BeckO PolR Bayern, Syst. Vorb. Rn. 41, 48.

221 Vgl. BVerfGE 154, 152 (242) – Ausland-Ausland-Fernmeldeaufklärung.

222 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 ff.; *Nettesheim* in Nettesheim/Diggelmann/Lege ua. (Hrsg.), VVDStRL 70, 2011, S. 7 (28 f.); *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 98 ff.; *ders.* in Möllers/van Ooyen (Hrsg.), BVerfG Öfftl. Sicherheit I, 2. Aufl. 2012, S. 65 (87 f.); *Trute*, Die Verwaltung 2009, 85 (98 ff.); differenziert *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.

223 So *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.; *Breckwoldt,* Grundrechtskombinationen, 2014, S. 195 ff.; *Klement*, AöR 2009, 35 (45 ff.); *Brade*, DÖV 2019, 853.

bb. Heimlichkeit

Auch deren Heimlichkeit wird bei allen Maßnahmen der Massenüberwachung als intensivierendes Element von der ständigen Rechtsprechung berücksichtigt.[224] Die intensivierende Wirkung der Heimlichkeit lässt sich sowohl mit der Unterdrückung des Rechtsschutzes im Sinne eines Abwägungsverbundes[225] der Privatheitsgrundrechte mit Art. 19 Abs. 4 GG oder einschüchternden Effekten erklären.[226] In letzterem Falle darf man aber, wie auch bei der Streubreite darauf verwiesen, den Eingriff durch das Gesetz nicht unmittelbar in der konkreten Maßnahme, die durch das Gesetz ermöglicht wird, erblicken. Stattdessen muss man auf die mittelbar-faktischen Wirkungen abstellen, die sich bei den Betroffenen durch das Wissen um die gesetzliche Maßnahme und die technischen Möglichkeiten der Sicherheitsbehörden einstellen.[227]

Trotz dieser noch offenen dogmatischen Fragen ist die intensivierende Wirkung in der Rechtsprechung etabliert und wird auch von der Rechtswissenschaft nicht mehr erkennbar angezweifelt. Es stellt sich jedoch heraus, dass die Definition der Heimlichkeit des BVerfG nicht differenziert genug ist, da es die Überwachungsmaßnahmen einheitlich begreift und nicht auf die einzelnen Datenverarbeitungsschritte abstellt. So zeichnen sich Vorratsdatenspeicherungen aufgrund ihrer Universalität ja gerade dadurch aus, dass die Speicherung nicht ohne Kenntnis des Betroffenen erfolgt, sondern diesem schon durch die Verabschiedung der gesetzlichen Grundlage bekannt wird bzw. bekannt werden kann.[228]

Auch der eventuell folgende Zugriff geschieht nicht zwangsläufig ohne Kenntnisnahme. Zwar soll der Betroffene von diesem nach der gesetzlichen Gestaltung nichts erfahren, jedenfalls bei den manuellen Zugriffsverfahren erhalten Dritte aber zwangsläufig Kenntnis von der Abfrage. Diese wiederum könnten grundsätzlich den Betroffenen informieren, etwa wenn sie

224 BVerfGE 154, 152 (241) – Ausland-Ausland-Fernmeldeaufklärung; E 150, 244 (283) – Autom. Kennzeichenkontrolle II.

225 *Breckwoldt,* Grundrechtskombinationen, 2014, S. 132 ff.; *Spielmann,* Konkurrenz, 2008, S. 173 ff.; krit. gegenüber solchen Verbundsbetrachtungen: *Kahl,* Schutzergänzung, 2000, S. 25 mwN.; Übersicht bei *Heß,* Grundrechtskonkurrenzen, 2000, S. 82 ff.

226 BVerfGE 125, 260 (320) – Vorratsdatenspeicherung.

227 Dazu Eingriffen *Oermann/Staben*, Der Staat 2013, 630 (640 ff.); krit. *Klement* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. III, 2. Aufl. 2022, § 80 Rn. 59.

228 *Schluckebier* abw. Meinung BVerfGE 125, 260 (366).

sich aufgrund eines vertraglichen Verhältnisses zu dessen Schutz verpflichtet fühlen.[229]

cc. Exkurs: Mitwirkung Privater bei der öffentlichen Sicherheitsgewährleistung

Überhaupt ist die Einbeziehung Privater in sicherheitsrechtliche Aufgaben ein Phänomen, das insbesondere bei den Maßnahmen der Massenüberwachung Bedeutung erlangt. Zwar sind auch manche Individualmaßnahmen, etwa die TKÜ, nicht ohne die Mithilfe Privater denkbar.[230] Hier reduziert sich deren Kooperationspflicht aber meist auf technische Aspekte der Datenerhebung.

Im Rahmen der Massenüberwachung nimmt die Mithilfe Privater eine neue Qualität an. Die Regelungen der TK-Vorratsdatenspeicherung nach § 176 TKG sowie die Bestandsdatenspeicherungspflichten der §§ 174 ff. TKG und §§ 24c KWG, 93b, 93 Abs. 7. 8 AO beruhen primär auf der Vorhaltung und Bereitstellung enormer Datenmengen durch Private. Auch bei der Geldwäschebekämpfung stehen Private an der Spitze. Sie müssen Kontotransaktionen überwachen und etliche Daten vorhalten (dazu Kap. D. III.).

Da die Sicherheitsgewährleistung prinzipiell dem Staat obliegt, stellt sich bei diesen Überwachungskomplexen die Frage, ob die Ausgliederung bestimmter Maßnahmen auf die grundrechtliche Bewertung einen Einfluss hat.

(1) Indienstnahme Privater und „Criminal Compliance“

Das allgemeine Phänomen, dass Private – insbesondere Wirtschaftsunternehmen – durch spezifische Pflichten in die Verhinderung von Straftaten miteingebunden werden, hat sich in den letzten Jahrzehnten immer stärker entwickelt und wird mittlerweile gar als eigenes Rechtsgebiet der „Criminal Compliance“ behandelt. Im Vordergrund der Criminal Compliance steht

229 Für Banken etwa *Reichling*, JR 2011, 12 (16); *Krepold/Zahrte* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 8 Rn. 261.

230 *Rückert* in MüKo StPO, §100a Rn. 237.

grundsätzlich das Misstrauen[231] des Gesetzgebers gegenüber den Unternehmen selbst aufgrund deren originärer Nähe zu bestimmten Delikten. Primäres Anliegen der Criminal Compliance ist es mithin, bestimmte Unternehmen bzw. deren Mitarbeiter durch gesetzliche Pflichten von strafbarem Verhalten abzuhalten oder dieses aufzudecken[232]. Es handelt sich um eine Form der *regulierten Selbstregulierung*.[233]

Versteht man jedes strafbarkeitsvermeidende oder -aufdeckende Verhalten als Criminal Compliance[234], können selbst solche wirtschaftsrechtlichen Pflichten noch mit dem Begriff umschrieben werden, die allein auf die Mithilfe bei der Durchsetzung von Sicherheitsinteressen gegenüber Dritten ausgerichtet sind. Da insofern aber der für den Begriff wichtige Aspekt der regulierten Selbstregulierung in den Hintergrund tritt, überrascht es nicht, dass die Mitwirkungspflichten bei der Vorrats- oder Bestandsdatenspeicherung nicht unter dem Schlagwort der Criminal Compliance diskutiert werden, sondern meist nur unter dem verfassungsrechtlichen Topos der *Indienstnahme Privater*.[235]

Anders verhält es sich bei solchen Normkomplexen, die eine aktive Mithilfe bei der Erlangung sicherheitsrechtlich relevanter Informationen über Dritte vorsehen, bei denen die jeweiligen Produkte der Unternehmen in einem engen Zusammenhang mit den verfolgten Delikten stehen. Hier sind etwa das Anti-Geldwäscherecht und das Netzwerkdurchsetzungsgesetz (NetzDG)[236] zu nennen. Diese Regelungsmaterien zeichnen sich dadurch aus, dass bestimmte strafbare Verhaltensweisen Dritter ohne die Angebote der jeweils verpflichteten Privaten kaum ausgeübt werden könnten.

231 *Schünemann*, GA 2013, 191 (196); aA *Kölbel*, ZStW 2014, 499, der die Criminal Compliance als Vertrauensvorschuss deutet.

232 Vgl. *Rotsch* in Rotsch (Hrsg.), Criminal Compliance, 2015, § 1 Rn. 42 ff., 50; *ders.* in Rotsch (Hrsg.), Compliance Zukunft, 2013, S. 3 (9 f.); *Bock,* Criminal Compliance, 2011, S. 23 ff.

233 *Kölbel*, ZStW 2014, 499 (507 ff.); *Sieber*, FS Tiedemann, 2008, S. 449 (460 f.); allg. zum Konzept *Ayres/Braithwaite,* Regulation, 1995, S. 101 ff.

234 Vgl. *Hilgendorf* in Rotsch (Hrsg.), Compliance Zukunft, 2013, S. 19 (21).

235 Etwa *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 306 ff.; *F. Braun*, K&R 2009, 386; *Schoch* in Schoch/Schneider, VerwR, VwVfG § 1 Rn. 175; allg. BVerfGE 30, 292 (311); *Ibler* in Dürig/Herzog/Scholz GG, Art. 86 Rn. 120; *Manssen* in v. Mangoldt/Klein/Starck GG, Art. 12 Rn. 202.

236 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) vom 01. September 2017 (BGBl. I S. 3352), zuletzt geändert durch Gesetz vom 21. Juli 2022 (BGBl. I S. 1182); dazu *Adelberg,* Netzwerke, 2020, S. 128 mwN.; *Wimmers/Heymann*, AfP 2017, 93 (S. 97 f.).

Bei diesen Normkomplexen wird vonseiten der Gesetzgebung gern argumentiert, dass es auch hier letztlich um Selbstschutz der Unternehmen geht.[237] Diese würden sonst regelmäßig in den Verdacht einer Beihilfestrafbarkeit gelangen[238] oder aufgrund der einschlägigen Delikte wirtschaftliche Nachteile erleiden. Im Erwägungsgrund Nr. 2 der 4. GeldwäscheRL[239] wird beispielsweise ausdrücklich darauf hingewiesen, dass die Verpflichteten durch ihre Mithilfe bei der Geldwäschebekämpfung *die Solidität, Integrität und Stabilität der Kreditinstitute und Finanzinstitute sowie das Vertrauen in das Finanzsystem* – also letztlich sich – behüten.

(2) Auswirkungen der Einbeziehung Privater auf die Grundrechtsprüfung

Für die grundrechtliche Bewertung spielt die begriffliche Abgrenzung der *Indienstnahme Privater* von der *Criminal Compliance* kaum eine Rolle. Sie sind aus wissenschaftlicher Perspektive allenfalls als „Schlüsselbegriffe"[240] interessant, da sich die jeweiligen Diskurse in Abhängigkeit von den Oberbegriffen durchaus unterscheiden.

Dass eine grundrechtsbeeinträchtigende, informationelle Maßnahme zur Sicherheitsgewährleistung nicht unmittelbar durch einen staatlichen Akteur ausgeübt wird, sondern aufgrund einer Verpflichtung durch einen Privaten, kann sich auf die Intensität der Maßnahme zwar mildernd auswirken, etwa wenn bei einer verpflichtenden Speicherung durch die Indienstnahme weitere Hürden geschaffen und Dezentralität gewährleistet werden.[241] Der Eingriff wird durch die Ausgliederung an Private aber nicht prinzipiell

237 BT-Drs. 14/8739, S. 11 „Einsparungen durch bessere Sicherheitslage"; vgl. auch *Findeisen*, wistra 1997, 121 (125); *ders.* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (113 ff.); *Bergles/Eul*, BKR 2002, 556 (562 f.).

238 Zur Geldwäschestrafbarkeit von Banken etc. *Boerger* in Momsen/Grützner (Hrsg.), Hdb. Wirtschafts- & Steuerstrafr, 2. Auflage 2020, § 38 Rn. 160 ff.

239 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. 2015, L 141/73.

240 Vgl. *Voßkuhle* in Grimm (Hrsg.), Selbstregulierung, 2001, S. 197 (198).

241 BVerfGE 125, 260 (320 ff.) – Vorratsdatenspeicherung.

intensiviert.[242] Eine verpflichtende Indienstnahme ist dem Staat weiterhin als eigener Eingriff zuzurechnen und ändert daher nicht grundsätzlich den Charakter der Maßnahme[243].

Im Urteil zur Kontostammdatenauskunft hatte das BVerfG sogar noch angenommen, dass den betroffenen Kontoinhabern praktische Nachteile dadurch entstehen könnten, dass die Institute von den Abfragen erfahren würden, da diese auf die Ermittlungsmaßnahmen proaktiv mit Kontoschließungen reagieren könnten.[244] Aus diesem Umstand leitete es ab, dass sich vollständig heimliche, weil technisch automatisierte Zugriffe von Sicherheitsbehörden bei Privatunternehmen weniger intensiv auf die Rechte der Betroffenen auswirkten, da schon mit dem Bekanntwerden von Ermittlungen bei Dritten eine Reputationsgefährdung einherginge.

Diese Auffassung hat das BVerfG allerdings in jüngeren Urteilen nicht mehr wiederholt. Sie ist auch nicht mit dem hier vorgestellten Verständnis der Heimlichkeit in Einklang zu bringen. Datenerhebungen bei Dritten, die auch dem Dritten verborgen bleiben, weisen eine maximal ausgeprägte Heimlichkeit auf, da faktisch keine Möglichkeit der Kenntnisnahme besteht. Zwar ist sicher richtig, dass die Kenntnis des Dritten über die Ermittlungen zu faktischen Nachteilen führen könnte, etwa durch die vorzeitige Kündigung von Vertragsverhältnissen. Diesen Gefahren kann aber auf entsprechender Ebene begegnet werden. So können beispielsweise Bankkunden die Ablehnung eines Antrags auf Eröffnung eines Basiskontos nach §§, 49, 50 ZKG rechtlich prüfen lassen. Wird eine Basiskontoeröffnung wegen einer Geldwäscheverdachtsmeldung abgelehnt, muss die Ablehnung nachträglich aufgehoben werden, wenn sich der Verdacht nicht erhärtet.[245]

Die *absolute* Heimlichkeit einer Maßnahme – in dem Sinne, dass kein Dritter von ihr erfährt – wirkt sich also nicht positiv, sondern eher negativ auf den Betroffenen aus, da ohne sie zumindest die Möglichkeit des Dritten bestünde, den Betroffenen über die Maßnahme zu informieren. Eine solche

242 aA. *Szuba,* Vorratsdatenspeicherung, 2011, S. 194 ff.; *Grafe,* Verkehrsdaten, 2008, S. 18 f.; *Herzog*, WM 1996, 1753 (1762).

243 Idem (310); *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff. mwN.; aA. *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 30.

244 BVerfGE 118, 168 (194 f.) – Kontostammdaten.

245 OLG Frankfurt, BKR 2021, 380 (382); zur Kündigung von Girokonten wegen Geldwäscheverdachts vgl. OLG Jena, Urt. v. 29.09.2020 – 5 U 165/19.

Informierung kann in Abwesenheit von Sanktionsvorschriften sogar eine vertragliche Pflicht darstellen.[246]

Es ist also zu begrüßen, dass das BVerfG nicht mehr versucht hat, die Kenntnisnahmemöglichkeit Dritter intensitäts*steigernd* zu berücksichtigen. Seiner nunmehr neutralen Haltung in dieser Frage ist beizupflichten.[247]

c. Schlussbemerkung: Massenüberwachung als Problem objektiven Grundrechtsschutzes und Rechtsstaatlichkeit

Die Maßnahmen der Massenüberwachung fallen dadurch auf, dass sie natürlicherweise die verschiedenen vom BVerfG identifizierten intensitätssteigernden Merkmale in sich vereinen. Dies wirft angesichts bestehender dogmatischer Ungereimtheiten die Frage auf, ob die intensitätssteigernden Überwachungsmerkmale nicht letztlich vom Ende her gedacht wurden.

Das BVerfG erblickt offenbar in den Massenüberwachungsmaßnahmen eine intrinsische Gefährlichkeit für die informationelle Selbstbestimmung der Gesellschaft. Es besteht der Verdacht, dass es Massenüberwachungen nicht für besonders intensiv hält, weil sie heimlich sind und eine hohe Streubreite aufweisen. Vielmehr scheint das BVerfG die Heimlichkeit und die Streubreite als intensivierende Merkmale einzustufen, weil sie für Massenüberwachungsmaßnahmen typisch sind.

Nach dieser Überlegung stellen Massenüberwachungsmaßnahmen primär ein rechtsstaatliches Problem dar, das im System der traditionellen Grundrechtsdogmatik über die Schöpfung von Intensitätsmerkmalen individuell rekonstruiert wurde.

aa. Totalüberwachung und Überwachungsgesamtrechnung

Noch auf grundrechtlicher Ebene bedürfte es einer solchen individuellen Rekonstruktion gar nicht, wenn man die Massenhaftigkeit bestimmter Überwachungsmaßnahmen nicht aus einer individuellen Grundrechtsper-

246 Für eine Informationspflicht aus dem Bankvertrag *Reichling*, JR 2011, 12 (16) mwN zum Streitstand; aA. *Krepold/Zahrte* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 8 Rn. 261.

247 BVerfGE 125, 260 (311 f.) – Vorratsdatenspeicherung; zust. *Durner* in Dürig/Herzog/Scholz GG, Art. 10 Rn. 154; ebenso EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169.

spektive betrachtet, sondern die Grundrechte als objektiven Gesellschaftsschutz versteht.[248]

Diesen Gedanken legen die Aussagen des BVerfG zum Verbot der (gesellschaftlichen)[249] Totalüberwachung aus dem Urteil zur Vorratsdatenspeicherung nahe. Danach dürfe die Einführung der Speicherung von Verkehrsdaten, die das Gericht grundsätzlich für zulässig erachtete, *„nicht als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. (…). Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland.“*[250]

Dieses *obiter Dictum* wurde von Teilen der Rechtswissenschaft[251] und der Politik[252] zum Anlass genommen, eine „Überwachungsgesamtrechnung“ zu fordern, nach der für die Legalität einzelner Überwachungsgesetze nicht nur deren individuelle Verhältnismäßigkeit ausschlaggebend sei. Stets müsse man sich obendrein fragen, ob sämtliche Überwachungsgesetze in einer Gesamtschau dazu führen könnten, dass ein von der Gesellschaft nicht mehr zu akzeptierendes Überwachungsniveau erreicht wird.

Im Koalitionsvertrag der „Ampel-Koalition“ 2021 wurde die Durchführung einer solchen Überwachungsgesamtrechnung beschlossen.[253] Derzeit

248 *Breckwoldt,* Grundrechtskombinationen, 2014, S. 196 ff.; *Klement*, AöR 2009, 35 (45 ff.); *Brade*, DÖV 2019, 853 (856 f.); s.a. *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 177 Fn 58; *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f. Fn 158.

249 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 236 ff.; *Löffelmann,* Überwachungsgesamtrechnung, 2022, S. 14; zur Abgrenzung von gesellschaftlicher Totalüberwachung („Überwachungsgesamtrechnung“, Begriff geprägt von *Roßnagel*, NJW 2010, 1238 (1242)) und Additiver Grundrechtseingriff siehe *Starnecker,* Videoüberwachung zur Risikovorsorge, 2016, S. 365 ff.; zu letzterem s. nur *Hornung* in Albers/Weinzierl (Hrsg.), Sicherheitspolitik, 2010, S. 65 (65 ff.); *Winkler*, JA 2014, 881.

250 BVerfGE 125, 260 (323 f.) – Vorratsdatenspeicherung.

251 Zuerst *Roßnagel*, NJW 2010, 1238; früher Umsetzungsversuch in Österreich durch *Tschohl et al.,* HEAT – Handbuch zur Evaluation der-Anti-Terror-Gesetze, 2016, https://epicenter.works/sites/default/files/heat_v1.2.pdf, zuletzt aufgerufen am 12.01.2025; krit. *Bieker/Bremert/Hagendorff* in Roßnagel/Friedewald/Hansen (Hrsg.), Fortentwicklung des Datenschutzes, 2018, S. 139; *Bieker/Bremert* FIfF-Kommunikation 2019(4), 34; *J. Pohle* FIfF-Kommunikation 2019(4), 37.

252 BT-Drs. 19/23695.

253 *SPD/Bündnis 90/Die Grünen/FDP,* Koalitionsvertrag "Mehr Fortschritt wagen", 2021, S. 85 f., https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

werden Vorschläge zusammengetragen, ob und wie eine solche *Rechnung* operationalisiert werden könnte.[254]

Die Debatte verdeutlicht, dass die Betrachtung massenhafter Überwachungsmaßnahmen nicht allein von individuell-grundrechtlichen Aspekten, sondern einer objektiven, politischen Skepsis gegenüber sicherheitsrechtlicher Dauerüberwachung der Gesamtbevölkerung geprägt ist.[255] Diese Skepsis wiederum besteht gewissermaßen *a priori*. Ihre praktischen Gründe ermittelt weniger die Grundrechtstheorie als die Sozialwissenschaft im Rahmen der *surveillance studies* (s. o.).[256]

Das BVerfG hat sich zu diesem Blickwinkel bzw. dieser objektiv-politischen Grundüberzeugung allerdings nicht ausdrücklich bekannt.[257] Es versucht stattdessen, aus der massenhaften Betroffenheit ein individuell intensivierendes Merkmal abzuleiten, indem es auf die Anlasslosigkeit und – aus der Gesetzesexistenz resultierende –Einschüchterungseffekte rekurriert. Massenhafte Überwachungsmaßnahmen sollen deshalb auch für den Einzelnen schwer wirken.

Auf die Kritik[258] an seiner Erklärung ist das Gericht bislang nicht eingegangen. Stattdessen behandelt es insbesondere die Gewichtung der Streubreite als sicherheitsrechtliches Axiom und geht somit letztlich selbstreferentiell[259] vor: Massenhafte Überwachungsmaßnahmen beeinträchtigen Grundrechte massiv, da sie breit streuen. Die Streubreite wiederum stellt eine Intensivierung dar, weil sie zu Einschüchterungseffekten führt und bewirkt, dass es immer auch zu anlasslosen Überwachungen kommt.

254 *Löffelmann,* Überwachungsgesamtrechnung, 2022; *Poscher/Kilchling/Landerer*, GSZ 2021, 225; *dies*., (Friedrich-Naumann-Stiftung für die Freiheit), Überwachungsbarometer, 2022; *Gerson* KriPoZ 2022, 404; *Gemmin*, DÖV 2022, 789; krit. *J. Franz Lindner/Unterreitmeier*, JZ 2022, 915.

255 *Kostov*, GSZ 2022, 267 (270).

256 Etwa *Adensamer,* Hdb. Überwachung, 2020, S. 24 ff.; *Kreissl/Norris/ Krlic Marija ua.* in Wright/Kreissl (Hrsg.), Surveillance, 2015, S. 150 (154 ff.); *Čas/Bellanova/Burgess ua.* in Friedewald/Burgess/Čas ua. (Hrsg.), Surveillance, 2017, S. 1; *Lemieux,* Surveillance, 2019; allg. *Lyon,* The electronic Eye, 1994; *ders.* in Monahan/Wood (Hrsg.), Surveillance Studies, 2018, S. 18.

257 Vgl. aber BVerfGE 115, 320 (357) – Rasterfahndung.

258 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 142 ff; S. 176 ff.; *Nettesheim* in Nettesheim/Diggelmann/Lege ua. (Hrsg.), VVDStRL 70, 2011, S. 7 (28); *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 98 ff.; *ders.* in Möllers/van Ooyen (Hrsg.), BVerfG Öfftl. Sicherheit I, 2. Aufl. 2012, S. 65 (87 f.); *Trute*, Die Verwaltung 2009, 85 (98 ff.).

259 Dazu allg. krit. *Rusteberg*, KritV 2017, 24 (26 f.).

Auf dieser Begründungsebene treten aber Probleme auf. Die Einschüchterungseffekte sind eine mittelbare Folge der Gesetzesexistenz und keine unmittelbare Konsequenz der Ausübung der entsprechenden Maßnahme.[260] Überdies sind sie empirisch kaum zu belegen.[261]

Auch die Anlasslosigkeit ist nur schwer als Argument für eine Erhöhung der Eingriffsintensität in Stellung zu bringen. Die in den Überwachungsgesetzen festgelegten Schutzgüter und spezifische Eingriffsschwellen gewährleisten die Effektivität des Eingriffs, indem sie ihn auf bestimmte relevante Szenarien begrenzen. Faktisch sind die unmittelbaren Nachteile einer Überwachung aber stets dieselben. Die Tiefe, mit dem das Recht „*selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*"[262] gebrochen wird, ist von der konkreten Begründung erst einmal unabhängig. Dieser Aspekt betrifft allein die Rechtfertigungsseite. Da auch auf Gesetzesebene der Eingriff grundsätzlich nach den Nachteilen der tatsächlichen Durchführung bestimmt wird, lässt sich die Anlasslosigkeit als Grundlage der intensivierenden Wirkung mit der Datenherrschaftstheorie des BVerfG also kaum in Einklang bringen.[263]

Politisch bzw. gesellschaftlich lässt sich die kritische Betrachtung der Massenüberwachung durch das BVerfG sicher befürworten. Aus einer dogmatischen Perspektive wäre es aber wünschenswert, dass das BVerfG die Schwierigkeiten einer individuell-rekonstruierten Erklärung der intensiven Grundrechtsbelastung anerkennt. Mehrere Autoren haben festgestellt, dass die gesellschaftliche bzw. sicherheitspolitische Brisanz mit der objektivrechtlichen Dimension der Grundrechte eingefangen werden kann.[264] Es bedarf weder der Verfassungsidentität noch einer Erheblichkeit des Eingriffs aus der individuellen Perspektive, um die hohen Anforderungen an die Rechtfertigung massenhafter Überwachungsmaßnahmen zu begründen. Ausreichend wäre es, die Zahl der durch eine Maßnahme

260 Vgl. *Klement* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. III, 2. Aufl. 2022, § 80 Rn. 59.

261 *Rath* in *Kritische Justiz* (Hrsg.), 60 Jahre GG, 2009, S. 65 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 f.; *J. Franz Lindner/Unterreitmeier*, JZ 2022, 915 (918).

262 Jüngst wieder BVerfGE 156, 11 (39) – Antiterrordatei II.

263 *Tanneberger,* Sicherheitsverfassung, 2014, S. 243 f.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 272 f.; vgl. auch *Bull* in Möllers/van Ooyen (Hrsg.), BVerfG Öfftl. Sicherheit I, 2. Aufl. 2012, S. 65 (87 Fn 117); *ders.* in van Ooyen/Möllers (Hrsg.), Hdb. BVerfG, 2015, S. 627 (642 f.); *Möstl*, GSZ 2019, 101.

264 *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.; *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f.; *Breckwoldt,* Grundrechtskombinationen, 2014, S. 195 ff.; *Klement*, AöR 2009, 35 (45 ff.); *Brade*, DÖV 2019, 853.

betroffenen Grundrechtsträger im Rahmen einer objektiv dimensionierten Grundrechtsprüfung als intensivierendes Merkmal anzuerkennen. Dieses Vorgehen entspricht der Funktion der Verfassungsbeschwerde als objektive Kontrolle[265] von gesellschaftspolitisch brisanten, weil breitenwirksamen, Grundrechtbeeinträchtigungen.[266]

Gerade weil sich individuelle Beeinträchtigungen in vielen Fällen nur schlecht mit Kollektivinteressen abwägen lassen,[267] sollte das BVerfG von der tradierten Individualperspektive – jedenfalls in Fällen wie der sicherheitsrechtlichen Massenüberwachung – Abstand nehmen, um den gesellschaftlichen Implikationen solcher Maßnahmen Ausdruck zu verleihen.

Es ist also richtig, dass Massenüberwachungsmaßnahmen grundsätzlich eine intensive Grundrechtsbeeinträchtigung darstellen. Aber nicht, weil sie den Einzelnen schwer treffen, sondern weil sie eine Vielzahl von Personen und somit die „*Freiheitlichkeit der Gesellschaft insgesamt*"[268] beeinträchtigen.

bb. Vertrauensbruch als Abkehr von traditioneller Sicherheitsgewährleistung

Die Rechtsprechung des BVerfG tritt staatlicher Massenüberwachung im Ergebnis zurecht kritisch gegenüber. Damit steht das Gericht auch nicht allein. Die Rechtsprechung spiegelt letztlich eine in Politik, Gesellschaft und Wissenschaft weit verbreitete Skepsis wider.

Nun wurde gerade festgestellt, dass sich diese Aversion schon auf grundrechtlicher Ebene im Rahmen einer objektiven Betrachtung damit erklären lässt, dass die Eingriffe eine Vielzahl von Grundrechtsträgern betreffen. Die entsprechenden Vorschläge beschreiben diese horizontale Kumulation allerdings gewissermaßen als Automatismus, weshalb die Übertragung des Konzepts auf Eingriffsgesetze außerhalb des Rechts elektronischer Da-

265 *Gusy* in van Ooyen/Möllers (Hrsg.), Hdb. BVerfG, 2015, S. 333 (344 ff.); *Schlaich/Korioth,* BVerfG, 12. Aufl. 2021, Rn. 205; *E. Klein*, DÖV 1982, 797 (803 ff.).

266 Vgl. zu den Pandemiemaßnahmen *Murswiek*, NVwZ-Extra 5/2021 (6); zust. *Schoch*, NVwZ 2022, 1 (6 f.).

267 *Lepsius* in Jestaedt/Lepsius (Hrsg.), Verhältnismäßigkeit, 2021, S. 1 (34); *ders.* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (34 f.); *Gusy* in Weber-Dürler/Kokott/Vesting (Hrsg.), VVDStRL 63, 2004, S. 153 (176 f.); *Rusteberg* in *Junge Wissenschaft Öffentlichen Recht e.V.* (Hrsg.), Kollektivität, 2012, S. 13 (19 ff.).

268 BVerfGE 150, 244 (284) – Autom. Kennzeichenkontrolle II.

tenverarbeitung (zur Sicherheitsgewährleistung) noch skeptisch betrachtet wird.[269]

Daneben existieren allerdings auch zwei – eng verwandte – rechtsstaatliche Ansätze, mit denen die grundrechtliche Sensitivität erklärt werden könnte. Aus dem Umstand, dass breit streuende Überwachungsmaßnahmen zwingenderweise auch solche Personen betreffen, ergibt sich einerseits ein allgemeiner Vertrauensbruch des Staates gegenüber dem Bürger und weiter eine Umgehung des traditionellen Reaktionismus des Sicherheitsrechts.

(1) Rechtstreue des Bürgers und Prävention

Massenüberwachungsmaßnahmen begründen sich letztlich mit der Allgegenwärtigkeit kaum individualisierbarer Bedrohungen und der deshalb ständig notwendigen Prävention.[270] Sie sind daher eng verknüpft mit dem allgemein sicherheitsrechtlichen Phänomen der Vorfeldverlagerung, die gerade zur Terrorismusbekämpfung auch im materiellen Strafrecht beobachtet werden kann.[271]

Die strafrechtliche Entwicklung hat zur Abstrahierung bestimmter Rechtsgutverletzung. Geführt. Bei den sog. „Präventionsstraftaten" wird beispielsweise schon in einer Mitgliedschaft, etwa § 129a Abs. 1 S. 1 Alt. 2 StGB, die Begründung einer Gefährdungssituation gesehen und pönalisiert.[272] Der Gesetzgeber spekuliert insofern, dass durch die Mitgliedschaft das Risiko einer tatsächlichen Rechtsgutverletzung signifikant erhöht wird.

Solche Spekulationen liegen auch den Massenüberwachungsmaßnahmen zugrunde. Bei den strategisch überwachten Lebenssachverhalten wird

269 *Breckwoldt,* Grundrechtskombinationen, 2014, S. 200 f.; vgl. zu Pandemiemaßnahmen allerdings *Murswiek*, NVwZ-Extra 5/2021 (6); zust. *Schoch*, NVwZ 2022, 1 (6 f.).

270 *Albers,* Determination, 2001, S. 112 ff., 215 ff., 252 ff.; *Zöller,* Informationssysteme, 2002, S. 319 ff.; *Thiel,* Entgrenzung, 2012, S. 81 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Hoppe,* Vorfeldermittlungen, 1999 ; *Poscher*, Die Verwaltung 2008, 345 (348 ff.); *Wolff*, DÖV 2009, 597 (604).; allg. zur Tendenz präventiven (Sicherheits-)Rechts statt vieler *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 391 ff.; *Denninger* in Huster/Rudolph (Hrsg.), Präventionsstaat, 2008, S. 85 (88 ff.) und die übrigen Beiträge dort; übersichtlich *Volkmann*, NVwZ 2022, 1408 (1410 f.).

271 Dazu nur *Hawickhorst,* Terrorismusbekämpfung, 2011, S. 18 ff.; *Sieber*, NStZ 2009, 353 (356 ff.); *Weißer*, JZ 2008, 388 (390 ff.); *Jakobs*, ZStW 2006, 839.

272 BT-Drs. 10/6635, S. 4; OLG München, NJW 2007, 2786 (2787); ausf. *Hawickhorst,* Terrorismusbekämpfung, 2011, S. 98 ff.

aufgrund allgemeiner Annahmen davon ausgegangen, dass konkrete Verdachtslagen aus der Überwachung bestimmter Bereiche extrahiert werden können.[273] Bei Maßnahmen der Vorratsdatenspeicherung wird allgemein aufgrund der Daten-Art angenommen, dass zumindest die Möglichkeit einer zukünftigen Relevanz für sicherheitsrechtliche Übermittlungen entsteht.[274]

Mit dieser spekulativen Betrachtung unmittelbar nicht sicherheitsrelevanter Verhaltensweisen bringt der Staat Misstrauen gegenüber den Grundrechtsträgern zum Ausdruck. Dieses gilt es grundsätzlich zu rechtfertigen, wenn sich der Staat nicht dem Vorwurf der Willkür aussetzen will.

Im materiellen Strafrecht lässt sich diese Rechtfertigung noch ganz gut darstellen. So sprechen gute Gründe für die Annahme, dass eine Mitgliedschaft in einer terroristischen Vereinigung eine nicht mehr zu duldende Rechtsgutgefährdung darstellt. Durch die Anknüpfung an bestimmte Tatsachen wird dem Delikt die Willkürhaftigkeit genommen und somit aus verfassungsrechtlicher Perspektive entschärft.[275] Problematisch sind spekulative Annahmen des Gesetzgebers aber, wenn sie einem Generalverdacht[276] gleichkommen. Dann nämlich wird zum Ausdruck gebracht, dass der Staat den Grundrechtsträgern nicht grundsätzlich zutraut, dass diese sich nicht ausschließlich rechtmäßig verhalten.[277] Bestimmte Freiheiten werden somit unter Rechtfertigungslast gesetzt.[278] Die Frage ist dann, ob es ein solches Grundvertrauen ähnlich der Unschuldsvermutung überhaupt geben muss[279] und dieses universellen Überwachungsmaßnahmen entgegen-

273 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 53 ff.; zur PNR-Analyse *Arzt*, DÖV 2017, 1023 (1025); *Ders.* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap G Rn. 1330.

274 *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 140; *Bull* in van Ooyen/Möllers (Hrsg.), Hdb. BVerfG, 2015, S. 627 (643).

275 OLG München, NJW 2007, 2786 (2787 f.) mwN.; krit. *Hawickhorst,* Terrorismusbekämpfung, 2011, S. 262 ff.

276 Vgl. Zur Vorratsdatenspeicherung *Orantek* NJ 2010, 193 (195).

277 *Breyer*, StV 2007, 214 (217).; *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 493 ff.; *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (31 f.); vgl. auch *B. Hirsch* in Huster/Rudolph (Hrsg.), Präventionsstaat, 2008, S. 164 (166 ff.), der die Vorratsdatenspeicherung in die Nähe des „Feindstrafrechts rückt.

278 *Masing*, JZ 2011, 753 (756 f.).

279 Für eine solche Annahme *Weßlau,* Vorfeldermittlungen, 1989, S. 300 ff.; *Dencker*, FS Dünnebier, 1982, S. 447 (459 f.) *Lisken*, NVwZ 1998, 22 (24); s.a. BayVGH ZD 2019, 515 (521).

steht[280], oder ob dem Staat aufgrund der Existenz bestimmter Kriminalitätsformen nicht doch ein niedrigschwelliger Generalverdacht zugestanden werden muss, der bestimmte anlasslose Datenverarbeitungen unter Umständen zulässig macht.

(2) Reaktivität der Sicherheitsgewährleitung als staatsrechtlicher Grundsatz?

Mit dem Verlust des Vertrauens in die Rechtstreue der Grundrechtsträger geht also die Abkehr vom Prinzip der Reaktivität des Sicherheitsrechts einher. Der Staat will nicht länger abwarten, dass für jede einzelne Person, die Ziel einer Datenverarbeitung werden soll, sicherheitsrechtlich relevante Tatsachen bekannt oder vermutet werden.

Traditionell sind in der Bundesrepublik die operativen Sicherheitsrechtsbereiche, das Polizeirecht und das Strafverfolgungsrecht zwar funktional getrennt. Das Polizeirecht dient als Gefahrenabwehr der Verhinderung konkreter Gefahren für die öffentliche Sicherheit, während das Strafverfahrensrecht der Durchsetzung des Strafrechts gilt. Beiden Rechtsbereichen gemein ist aber, dass sie grundsätzlich reaktiv ausgestaltet sind.[281]

Als Mindestanforderung gilt stets, dass grundrechtsbeeinträchtigende Maßnahmen erst dann vorgenommen werden können, wenn bestimmte Informationen die Erforderlichkeit ihres Handelns nahelegen. Das ergibt sich aus der rechtsstaatlichen Unschuldsvermutung, die auch für das Strafprozessrecht gelten soll.[282]

Für die Strafverfolgungsbehörden kommt dieser Grundsatz in § 152 Abs. 2 StPO zum Ausdruck, der für jede Ermittlungen mindestens einen Anfangsverdacht voraussetzt.[283] Ermittlungen, die dazu dienen sollen, erst einen Anfangsverdacht zu schaffen, sind den Behörden prinzipiell untersagt.[284]

280 So *Puschke/Singelnstein*, NJW 2008, 113 (118); *Szuba,* Vorratsdatenspeicherung, 2011, S. 196 ff. mit Bezug zum Rechstaatsprinzip (dazu unten).

281 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 51 ff., 122 ff.; *Gärditz* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. II, 2. Aufl. 2022, § 22 Rn. 60 ff.

282 *Schünemann*, FS 25 Jahre DAV, 2009, S. 827 (829 ff.).

283 BVerfG, NStZ-RR 2004, 143 (143)

284 Sog. „Vorfeldermittlungen" dazu *Rogall*, ZStW 1991, 907 (945 ff.); *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 152 Rn. 4b; *S. Peters* in MüKo StPO, § 152 Rn. 62;s.a.

Analog verhält es sich im Polizeirecht, das ein Tätigwerden mit operativem Eingriffscharakter stets vom Vorliegen einer konkreten Gefahr abhängig macht. Zwar sind Maßnahmen zur Gefahrenerforschung[285] grundsätzlich nicht unzulässig, diese dienen aber wie die staatsanwaltschaftlichen „Vorermittlungen" allein der Prüfung, ob bestimmte Erkenntnisse tatsächlich einen Eingriffsanlass konstituieren. Erforschungsmaßnahmen „ins Blaue hinein", die der proaktiven Besorgung solcher Erkenntnisse dienen sollen, verbieten sich.[286]

Von diesem Grundsatz der Reaktivität wird bei den anlasslosen Überwachungsmaßnahmen jedenfalls durch einzelne Datenverarbeitungsvorgänge abgerückt.[287] Sie dienen der Verdachtsgewinnung bzw. der Informationsvorsorge. Der Staat reagiert auf den Umstand, dass seine Sicherheitsbehörden angesichts der Universalität moderner Bedrohungen bei der Wahrung ihrer Aufgaben stets einen Schritt hintendran sind.[288]

Es stellt sich hier die allgemein staatsrechtliche Frage, ob dem Prinzip der reaktiven Sicherheitsgewährleitung überhaupt Verfassungsrang zukommt, etwa als Ausfluss der Menschenwürde[289] oder des Rechtsstaatsprinzips bzw. der Unschuldsvermutung[290], oder ob es sich schlicht um eine gesetzgeberische Entscheidung handelt.[291]

Das BVerfG hat im Urteil zur BKAG – jedenfalls für den Bereich der Gefahrenabwehr, festgestellt –, dass der Gesetzgeber nicht bei jeder sicherheitsrechtlichen Aufgabenwahrnehmung Eingriffstatbestände vorsehen

---

Zöller, Informationssysteme, 2002, S. 127 ff., der allerdings nicht zwischen „Vorermittlungen" und „Vorfeldermittlungen" unterscheidet.

285 Dazu nur *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. Dn Rn. 103 ff.; *Schenke*, JuS 2018, 505 (508 ff.).

286 Jüngst BVerfG, NJW 2023, 1196 (1212, Rn. 158) – Autom. Datenanalyse.; BVerfGE 115, 320 (361) – rasterfahndung.

287 *Puschke/Singelnstein*, NJW 2008, 113 (118); *Lisken*, ZRP 1994, 264 (267 f.).

288 *Albers,* Determination, 2001, 111 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 35 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (S. 253 ff.); *ders.*, Die Verwaltung 2008, 345 (345 ff.).

289 *Hund*, NJW 1992, 2118 (2119).

290 *Puschke/Singelnstein*, NJW 2008, 113 (118); *Szuba,* Vorratsdatenspeicherung, 2011, S. 196 ff. in diese Richtung auch *Lisken*, ZRP 1990, 15 (17 ff.); *ders.*, ZRP 1994, 264 (267 f.); übersichtlich *K. Weber,* Polizeirecht, 2011, S. 79 ff.

291 *Möstl* in Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer, 2008, S. 239 (242 ff.); *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.).; iE. auch BVerfGE 125, 260 (316 ff.) – Vorratsdatenspeicherung; E 150, 244 (282) – Autom. Kennzeichenkontrolle II.

muss, *„die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen."*[292]

Dabei ging es zwar konkret nicht um die Zulässigkeit anlassloser Massenüberwachungen, sondern um die Zulässigkeit individueller Maßnahmen bei „drohender Gefahr". Es ist aber bemerkenswert, dass sich das Gericht hier mit der tradierten Vorstellung reaktiver Sicherheitsgewährleistung grundsätzlich auseinandersetzt.

Ein Anknüpfungspunkt für einen *Grundsatz der Reaktivität im Sicherheitsrecht* außerhalb der Grundrechte müsste tatsächlich erst gefunden oder konstruiert werden. Insofern ist es verständlich, dass das BVerfG sich bei der Festlegung verfassungsrechtlicher Grenzen für sicherheitsrechtliche Überwachungsmaßnahmen vordergründig allein auf die grundrechtliche Verhältnismäßigkeitsprüfung verlässt und rechtsstaatliche Fragen als Intensitätskriterien verkleidet.

Vorzugswürdig scheint es aber, das Phänomen der Massenüberwachung als besonderes Verfassungsproblem zu begreifen. Man könnte dem Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG durchaus ein Prinzip entnehmen, wonach die Sicherheitsgewährleistung reaktiv zu erfolgen hat. Primär das Rechtsstaatsprinzip stünde der strukturell proaktiven[293] Massenüberwachung dann entgegen. Der Versuch des BVerfG, aus der Verfassungsidentität ein Verbot gesellschaftlicher Totalüberwachung abzuleiten, ging in diese Richtung, blieb bislang aber einmalig und wurde nie tatsächlich zur Anwendung gebracht.

3. Zusammenfassung

Staatliche bzw. sicherheitsrechtliche Überwachungsmaßnahmen haben also eine prominente Rolle in der Rechtsprechung des BVerfG eingenommen. Etliche Urteile zu überarbeiteten Sicherheitsgesetzen setzten sich überwiegend mit den jeweiligen Datenverarbeitungs- und -Übermittlungsrechten auseinander.[294]

Datenverarbeitende Handlungen der Sicherheitsbehörden greifen in Recht das Recht auf informationelle Selbstbestimmung, das Telekommuni-

292 BVerfGE 141, 220 (272) – BKA-Gesetz.

293 Vgl. *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 68 f.; Albers, Determination, 2001, S. 112 ff.

294 Insbesondere BVerfGE 141, 220 – BKA-Gesetz; NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz; ähnlich schon E 110, 33 – Außenwirtschaftsgesetz.

kationsgeheimnis und das Recht auf Vertraulichkeit und Integrität informationstechnischer Geräte ein. Bei der Verhältnismäßigkeitsprüfung durch des BVerfG hat sich aber eine Methode etabliert, die die Unterschiede der einzelnen Grundrechte verwischt.

a. Vorfeldüberwachung und Verhältnismäßigkeit

Die Überwachungsmaßnahmen haben dem BVerfG die Grenzen des Grundsatzes der Verhältnismäßigkeit aufgezeigt. Schon lange wird die Anwendung des Verhältnismäßigkeitsgrundsatzes bei Gesetzen kritisiert, da dieser mit seiner Kosten-Nutzen-Relation genuin auf den Einzelfall zugeschnitten ist.[295] Insbesondere Eingriffsgesetze regeln aber nicht den Einzelfall, sondern abstrakte Situationen und müssen entsprechend flexibel sein. Daher muss die konkrete Gestaltung des Gesetzes daraufhin geprüft werden, wie effektiv bzw. wie erfolgsversprechend die jeweilige Maßnahme zur Förderung des Gesetzeszweckes führt.[296]

Die Informationsgewinnung im Sicherheitsrecht betrifft den immer wichtiger gewordenen[297] Vorfeldbereich.[298] Sie findet also statt, bevor eine konkrete Gefahr erkennbar wird oder nur vermutet werden kann, bzw. vor dem Auftreten eines Anfangsverdachts. Das Ausmaß der Gefährdung eines Rechtsguts ist hier nicht bestimmbar, da die Zahl der möglichen Kausalverläufe immer größer wird, je weiter man sich von der tatsächlichen Rechtsgutverletzung wegbewegt.[299] Damit geht einher, dass der denklogi-

295 *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.).

296 *Hillgruber* in Isensee/Kirchhof (Hrsg.), Hdb StR Bd. IX, 3. Aufl. 2011, § 210 Rn. 76; *Stern,* StaatsR Bd. III/2, 1994, S. 836; speziell zum Sicherheitsrecht *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.

297 *Albers,* Determination, 2001, S. 112 ff., 215 ff., 252 ff.; *Zöller,* Informationssysteme, 2002, S. 319 ff.; *Thiel,* Entgrenzung, 2012, S. 81 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Hoppe,* Vorfeldermittlungen, 1999 ; *Poscher*, Die Verwaltung 2008, 345 (348 ff.); *Wolff*, DÖV 2009, 597 (604).

298 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Möstl* in Spiecker gen. Döhmann/Collin (Hrsg.), Generierung und Transfer, 2008, S. 239 (240 ff.); *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.).

299 Vgl. BVerfGE 113, 348 (378 ff.) – TKÜ; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 242; *Thiel,* Entgrenzung, 2012, S. 91 ff. mit Vergleich zum Umwelt-

sche Nutzen einer Überwachung mit der Verlagerung in den Vorfeldbereich zum Maximum strebt,[300] während der grundrechtliche Nachteil, die Preisgabe der Datenherrschaft[301], immer gleichbleibt. Überwachungsmaßnahmen im Vorfeld sind demnach *stets verhältnismäßig,* wenn sie möglichst früh ansetzen, und führen so die klassische Rationalitätskontrolle der Verhältnismäßigkeitsprüfung *ad absurdum*.[302]

Das BVerfG nutzt den Verhältnismäßigkeitsgrundsatz weniger zur Rationalitätskontrolle und mehr als Mittel zur Rechtsfortbildung.[303] Es verleiht ihm Ausdruck, indem es per Auslegung bestimmte materielle und formelle Zulässigkeitsvoraussetzungen sowie Kompensationsanforderungen für sicherheitsrechtliche Überwachungsmaßnahmen herausarbeitet.[304] Dieser Anforderungskomplex wird als *Sicherheitsverfassungsrecht* bezeichnet.[305]

---

recht; s.a. *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. D Rn. 255 ff.; *ders.,* Kriminalpräventionsrecht, 2015, S. 194 ff.

300 *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 f.); *Volkmann*, JZ 2006, 918 (919); allgemeiner. *Grimm* in Hassemer/Starzacher (Hrsg.), Organisierte Kriminalität, 1993, S. 28 (33 ff.); *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (S. 39 ff.).

301 BVerfGE 65, 1 (43) – Volkszählung; E 156, 11 (39) – Antiterrordatei II; krit. dazu etwa *Albers,* Informationelle Selbstbestimmung, 2005; *dies.* in Friedewald/Lamla/Roßnagel (Hrsg.), Informationelle Selbstbestimmung, 2017, S. 11; *Poscher* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 167; *ders.* in Miller (Hrsg.), Privacy and Power, 2017, S. 129; *Britz* in Hoffmann-Riem (Hrsg.), Offene Rechtswissenschaft, 2010, S. 561 (566 ff.).

302 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82 mit Verweis auf *Enders* in Enders/Wiederin/Pitschas ua. (Hrsg.), VVDStRL 64 (2004), 2005, S. 7 (45 f.); ähnlich *Hassemer* in *30. Strafverteidigertag* (Hrsg.), Sicherheit Freiheit, 2007, S. 9 (27 f.).

303 *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82.

304 BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 353 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84.; krit. *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.).

305 Vgl. *Tanneberger,* Sicherheitsverfassung, 2014; *Dietrich/Gärditz* (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245.

Das Verhältnismäßigkeitsprinzip kommt dabei in einer Je-desto-Formel[306] zum Ausdruck. Je intensiver die Überwachungsmaßnahme, desto strenger müssen die Zulässigkeitsvoraussetzungen sein und desto mehr Kompensations- und Kontrollmechanismen müssen etabliert werden. Dabei hält das BVerfG einen ganzen Katalog[307] an Merkmalen bereit, nach dem sich die Intensität der jeweiligen Überwachungsmaßnahmen bestimmen lässt. Ausgehend von diesen Merkmalen werden dann ebenfalls streng schematisch spezifische Anforderungen, gar Formulierungen hergeleitet, die das entsprechende Gesetz vorsehen muss.[308]

b. Grundrechtsintensität der Massenüberwachung

Maßnahmen der Massenüberwachung werden nach dieser Judikatur besonders kritisch gesehen, da sie ihrer Natur nach mehrere bedeutsame Intensitätsmerkmale in sich vereinen.[309] Ihre Anlasslosigkeit geht natürlicherweise mit einer extraordinären Streubreite einher.

Um die intensivierende Wirkung einer hohen Streubreite erklären zu können, sollte aber der Blickwinkel geändert werden. Statt aus einer individuellen Grundrechtsbetrachtung, erklärt sich die intensive Grundrechtsbeeinträchtigung aus einer objektiven. Schon die Menge der betroffenen Grundrechtsträger – jedenfalls im Rahmen der Bewertung von Überwachungsgesetzen – stellt per se einen intensivierenden Umstand dar, ohne dass sich dies erst durch die Wirkung auf den Einzelnen erklärt.[310]

306 *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.

307 *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).

308 instruktiv BVerfGE 141, 220 – BKA-Gesetz; NJW 2022, 1583 – Bayerisches Verfassungsschutzgesetz; zu den „Eingriffsschwellen" *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff.).

309 Vgl. BVerfGE 100, 313 (376 ff.) – Strategische Fernmeldeaufklärung; E 115, 320 (347 ff.) – Rasterfahndung; E 120, 378 (401 ff.) – Autom. Kennzeichenkontrolle I; E 125, 260 (318 ff.) – Vorratsdatenspeicherung; E 152, 216 (283 ff.) – Autom. Kennzeichenkontrolle II; E 154, 152 (241 ff.) – Ausland-Ausland-Fernmeldeaufklärung

310 *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 176 ff.; *Tanneberger,* Sicherheitsverfassung, 2014, S. 250 f.; *Klement*, AöR 2009, 35 (45 ff.); *Breckwoldt,* Grundrechtskombinationen, 2014, S. 196 ff.; *Brade*, DÖV 2019, 853 (856 f.); Übertra-

Für eine solche horizontale Kumulation lassen sich allgemeine Verfassungsgrundsätze ins Feld führen, die – so lässt sich spekulieren – bei der Meinungsbildung des BVerfG eine Rolle spielten. Anlasslose Massenüberwachungen brechen mit der Idee, dass der Staat seinen Bürgen generell Vertrauen entgegenbringt.[311] In deren Grundrechte wird aufgrund neuartiger, universeller Bedrohungslagen eingegriffen, obwohl von Beginn an feststeht, dass das Gros dieser Beeinträchtigungen nichts zum sicherheitsrechtlichen Ziel beitragen kann. Faktisch werden die Grundrechtsträger bei anlasslosen Datenverarbeitungen also unter Generalverdacht gestellt. [312] Damit einher geht eine Abkehr von der Idee, dass das Sicherheitsrecht grundsätzlich reaktiv ausgestaltet sein sollte. Eine solche Reaktivität schreibt die Verfassung zwar nicht vor, sie drängt sich aber als rechtsstaatlicher Grundgedanke durchaus auf.[313]

gung auf Maßnahmen außerhalb der Informationseingriffe *Murswiek*, NVwZ-Extra 5/2021 (6); zust. *Schoch*, NVwZ 2022, 1 (6 f.).

311 *Weßlau,* Vorfeldermittlungen, 1989, S. 300 ff.; *Dencker*, FS Dünnebier, 1982, S. 447 (459 f.) *Lisken*, NVwZ 1998, 22 (24); s.a. BayVGH, ZD 2019, 515 (521).

312 *Orantek* NJ 2010, 193 (195); *Breyer*, StV 2007, 214 (217).; *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 493 ff.; *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (31 f.); *Masing*, JZ 2011, 753 (756 f.).

313 *Puschke/Singelnstein*, NJW 2008, 113 (118); *Lisken*, ZRP 1990, 15 (17 ff.); *ders.*, ZRP 1994, 264 (267 f.); *Hund*, NJW 1992, 2118 (2119); zur „Dammbruchtheorie" *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 181 ff.

Kapitel C: Massenüberwachung im Europarecht

Staatliche Überwachungsmaßnahmen kollidieren nicht nur mit den deutschen Grundrechten, sondern auch mit europäischem Primär-, Sekundär- und Konventionsrecht. Auch in diesem findet sich allerdings keine eigenständige Begrifflichkeit der *Überwachung*. Stattdessen wird ebenfalls im Rahmen der Eingriffsbestimmung auf die einzelnen Datenverarbeitungsschritte abgestellt, wobei abermals die Intensitätsbewertung nicht isoliert, sondern im Rahmen einer Gesamtbetrachtung erfolgt, die auf die Wechselwirkung der einzelnen Verarbeitungsschritte abstellt.[314]

Der EuGH hat sich insbesondere mit seiner Rechtsprechung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten („TK-Verkehrsdaten") profiliert. In einer ganzen Reihe von Urteilen hat er nicht nur die unionsrechtliche Verpflichtung zur universellen Verkehrs- und Standortdatenspeicherung in Form der (TK-)VDS-RL[315] aufgehoben[316], sondern auch eigenständig erarbeitete nationale Regelungen der Mitgliedsstaaten für unionsrechtswidrig erklärt.[317]

Auch zur Speicherung und sicherheitsbehördlichen Verwendung von TK-Bestands-[318] sowie von Fluggastdaten[319] hat sich der EuGH geäußert

314 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 59 ff. = NJW 2014, 2169; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 97 ff. = EuZW 2022, 706; dazu auch VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI, Rn. 73 „funktionale Einheit".

315 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.

316 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

317 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.) = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531; Urteil v. 2.3.2021, C-746/18 (Prokuratuur) = NJW 2021, 2103; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135.

318 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal) = NJW 2019, 655.

319 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)) = EuZW 2022, 706; Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) = ZD 2018, 23.

und dabei die Erkenntnisse aus den Urteilen zur Vorratsdatenspeicherung übertragen und weiterentwickelt.

Mit der Speicherung und Analyse von Finanzinhaltsdaten sowie dem Zugriff auf solche Daten durch Sicherheitsbehörden hat sich der EuGH bislang noch nicht auseinandergesetzt. Dem Verfasser sind im September 2023 keine anhängigen Verfahren bekannt. Lediglich bestimmte Transparenzregeln der 4./5. Geldwäscherichtlinie (GWRL) über Vermögensberechtigte hat der Gerichtshof auf Verstöße mit Unionsgrundrechten und Datenschutzrecht hin überprüft und aufgehoben.[320] Ein Urteil, das sich allgemein mit den Maßnahmen zur Geldwäschebekämpfung beschäftigt, steht noch aus.

Der unionsrechtliche Rahmen für staatliche (Massen-)Überwachungsmaßnahmen soll in diesem Kapitel anhand der soeben genannten Urteile dargestellt werden, bevor später die in den folgenden Kapiteln thematisierten Maßnahmen auf ihre Vereinbarkeit mit dem Unionsrecht überprüft werden. Dabei soll auch kurz erläutert werden, inwiefern das Unionsrecht für Maßnahmen deutscher Sicherheitsbehörden überhaupt einschlägig ist.

I. Kurzübersicht: Europarechtlicher Schutz vor Überwachung

Wie auch das Grundgesetz hält das Unionsrecht bestimmte Vorschriften bereit, die die Privatheit, insbesondere im Rahmen von Kommunikation, schützen. Sie finden sich nicht nur primärrechtlich in der EU-Grundrechtecharta (EU-GRC)[321], sondern auch in der EMRK und im Unionssekundärrecht, dort in der Datenschutzgrundverordnung (DSGVO)[322], der Richt-

320 EuGH, Urt. v. 22.11.2022 – C-37/20, C-601/20 (WM ua/Luxembourg Business Registers) = NJW 2023, 199.

321 Charta der Grundrechte der Europäischen Union, Abl. 2012 C 326/02.

322 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl. 2016 L 119/1.

linie über den Datenschutz bei Sicherheitsbehörden (JI-RL)[323] und der Datenschutzrichtlinie für elektronische Kommunikation (e-Privacy-RL)[324].

1. Unionsgrundrechte: Art. 7, 8 EU-GRC, Art. 16 Abs. 1 AEUV

Im Europäischen Primärrecht schützen insbesondere die Art. 7, 8 EU-GRC und Art. 16 Abs. 1 AEUV vor staatlichen Überwachungsmaßnahmen.

Nach Art. 7 EU-GRC hat *jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation*. Art. 8 Abs. 1 EU-GRC bestimmt, dass jeder Person ein Recht auf *Schutz der sie betreffenden personenbezogenen Daten* zusteht. Nach Art. 8 Abs. 2 EU-GRC dürfen solche *Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten, legitimen Grundlage verarbeitet werden*. Jede Person hat danach weiter das Recht, *Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.*

Identisch zu Art. 8 Abs. 1 EU-GRC ist Art. 16 Abs. 1 AEUV formuliert. Das ist problematisch, da nach Art. 52 Abs. 2 EU-GRC die subjektiven Rechte der Verträge (EUV/AEUV) vorrangig anwendbar sind und die in der Charta enthaltenen Schranken insofern nicht unmittelbar gelten können.[325] Da Art. 16 Abs. 1 AEUV anders als Art. 8 EU-GRC keine Schranken beinhaltet, liefen die Schranken des Art. 8 Abs. 2, 3 EU-GRC dem Wortlaut nach leer. Dieses Ergebnis wird als offenkundiges Redaktionsversehen aufgefasst, für das verschiedene Lösungsvorschläge angeboten werden. Alle laufen im Ergebnis darauf hinaus, dass die doppelte Niederschrift des Datenschutzrechts keine inhaltlichen Auswirkungen hat und den Schranken des Art. 8

323 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, Abl. 2016, L 119/89.

324 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Abl. 2002 L 201/37.

325 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 52 Rn. 11 mwN; aA. *Jarass* in Jarass EU-GRC Art. 52 Rn. 54.

Abs. 2, 3 EU-GRC volle Geltung zukommt.[326] Im Folgenden wird daher das Datenschutzgrundrecht allein anhand des Art. 8 EU-GRC behandelt.

Art. 7 und 8 EU-GRC ließen sich, ähnlich der grundgesetzlichen Konstruktion (s. o. Kap. B. II.), als bereichsspezifisches Privatheits- und allgemeines Datenschutzrecht verstehen, die als eigenständige Grundrechte mit Spezialitätsvorrang behandelt werden könnten.[327] Art. 7 EU-GRC schütze nach dieser in Deutschland gängigen Lesart das Privatleben als solches, während Art. 8 EU-GRC spezifisch solche Daten schützt, die nicht in Zusammenhang mit dem Privatleben stehen.[328]

Der EuGH nahm in seiner früheren Rechtsprechung eine solche getrennte Betrachtungsweise aber nicht vor, sondern behandelte Art. 7, 8 EU-GRC letztlich als einheitlichen Schutz solcher Daten, die das Privatleben betreffen.[329] Erst seit den Urteilen zur Vorratsdatenspeicherung hat ein differenziertes Verständnis Eingang in die Rechtsprechung gefunden, wobei aber weiterhin keine völlig klare Trennung der Grundrechte vorgenommen wird.[330]

Während das BVerfG etwa die TK-Vorratsdatenspeicherung wegen dessen Spezialität allein als Eingriff in das Telekommunikationsgeheimnis i. S. d. Art. 10 Abs. 1 GG bewertete[331], prüfte der EuGH hinsichtlich der unionsrechtlichen und nationalen Regelungen zur TK-Vorratsdatenspeicherung

326 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada), Rn. 120 = ZD 2018, 23; übersichtlich *Wolff* in Frankfurter Kommentar, AEUV Art. 16 Rn. 11 f.; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 30.

327 Ausf. zum Verhältnis *Marsch,* Datenschutzgrundrecht, 2018, S. 203 ff.; *J. Kokott/Sobotta*, Int. Data Privacy Law 3 (2013), 222; *Gellert/Gutwirth,* Computer Law & Security Review 29 (2013), 522 (524 ff.); *W. Michl*, DuD 2017, 349.

328 *Generalanwalt Villalón*, Schlussantrag v. 12.12.2013, C-293/12, Rn. 62 ff. – Digital Right Ireland; *Schiedermair,* Schutz des Privaten, 2012, S. 349; *Jarass* in Jarass EU-GRC Art. 8 Rn. 4; *Streinz* in Streinz EUV/AEUV, EU-GRC Art. 8 Rn. 7; *Guckelberger*, EuZW 2011, 126 (128).

329 Vgl. EuGH, Urteil v. 17.10.2013, C-291/12 (Schwarz/Bochum), Rn. 24 ff. = NVwZ 2014, 435; Urteil v. 09.11. 2010, C 92/09, C 93/09 (Schecke u Eifert/Hessen), Rn. 52; Urteil v. 09.01.2008, C–275/06 (Promusicae/Telefónica), Rn. 64; *González Fuster,* Data Protection, 2013, S. 234 ff.; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 52; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 23, 31 f.; *Streinz* in Streinz EUV/AEUV, EU-GRC Art. 8 Rn. 7; *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 2; zu den Vorteilen dieser Rspr. *Marsch,* Datenschutzgrundrecht, 2018, S. 217 ff.; *W. Michl*, DuD 2017, 349 (353), der aber auch eine vorrangige Anwendung nur des Art. 8 EU-GRC als lex specialis für vertretbar hält.

330 *Marsch,* Datenschutzgrundrecht, 2018, S. 203 f.

331 BVerfGE 125, 260 (309 ff.) – Vorratsdatenspeicherung.

und PNR-Überwachung eine Verletzung „der sich aus *Art. 7, 8 EU-GRC ergebenden (Grund-)Rechte*".[332]

Der EuGH geht mithin offenbar davon aus, dass es sich grundsätzlich um zwei verschiedene Schutzbereiche handelt. Vor allem in *Digital Rights Ireland* und *Ligue des droits humains (PNR)* kommt diese Trennung von Art. 7 und 8 EU-GRC durch eine separate Schutzbereichsbestimmung deutlich zum Ausdruck.[333] Für die Bewertung der geprüften Maßnahmen spielt aber die Dualität der verschiedenen Grundrechte weiterhin keine Rolle. Ähnlich dem BVerfG[334] bewertet der EuGH die Intensität der Eingriffe nicht in Abhängigkeit von den konkret betroffenen Grundrechten, sondern anhand von Maßstäben (dazu unten), die einem einheitlichen Privatheitsschutz entsprechen, und begründet dies mit der *besonderen Bedeutung des Datenschutzes für die Privatheit.*[335] Auf der Prüfungsebene des Schutzbereichs kann daher von einer *parallelen*[336] statt einheitlichen Prüfung der Art. 7 und 8 EU-GRC gesprochen werden.

Der Datenschutz i. S. d. Art. 8 Abs. 1 EU-GRC ist dabei denkbar weit ausgerichtet. Er umfasst sämtliche Informationen über eine identifizierte oder identifizierbare natürliche Person[337] und spiegelt sich insofern in Art. 4 Nr. 1 DSGVO wider.[338] Überhaupt scheint der EuGH die grundrechtliche Ebene mit der einfachgesetzlichen Ausgestaltung zu verknüpfen. Er definiert Eingriffe in Art. 8 Abs. 1 EU-GRC neuerdings anhand Art. 4 Nr. 2 DSGVO

332 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), 100 = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), 115 = NJW 2021, 531; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 96 ff. = EuZW 2022, 706; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), 79 = NJW 2022, 3135.

333 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 96 ff. = EuZW 2022, 706.

334 Dazu *Gusy*, KritV 2000, 52 (53 ff.); *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 88 f., Fn 470 mwN; S. 165; eindrücklich am Bsp. von BVerfGE 141, 220 – BKA-Gesetz: *Rusteberg*, KritV 2017, 24 (27 ff.).

335 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 53 = NJW 2014, 2169.

336 *Kühling*, NVwZ 2014, 681 (682); *Jarass* in Jarass EU-GRC Art. 8 Rn. 4; *Johlen* in Stern/Sachs EU-GRC Art. 28 Rn. 24, Fn 51.

337 EuGH, Urteil v. 09.11. 2010, C 92/09, C 93/09 (Schecke u Eifert/Hessen), Rn. 52.

338 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art.8 Rn. 10; *Jarass* in Jarass EU-GRC Art. 8 Rn. 6.

gleich.[339] Jeder einzelne Verarbeitungsschritt i. S. d. Art. 4 Nr. 2 DSGVO stellt einen Eingriff in Art. 8 Abs. 1, 2 EU-GRC dar.[340]

Der EuGH versteht Art. 8 Abs. 1, 2 EU damit als (Quasi-)Herrschaftsrecht[341] über persönliche Daten, also als Recht einer Person, andere von der Verarbeitung ihrer Daten auszuschließen.[342] Das entspricht der Rechtsprechung des BVerfG zum Recht auf informationelle Selbstbestimmung. Trotz der Kritik an diesem Verständnis, ist im Ergebnis unstreitig, dass sicherheitsrechtliche Überwachungsgesetze konkreten grundrechtlichen Anforderungen unterliegen. Diese werden von der Rechtsprechung des EUGH laufend spezifiziert.

2. Konventionsrecht: Art. 8 EMRK und die Datenschutzkonvention

Den Schutz vor staatlicher Überwachung gewährleistet in Europa nicht nur das Unionsrecht, sondern auch die Europäische Menschenrechtskonvention – EMRK.[343]

Wie bereits erwähnt, orientiert sich Art. 7 EU-GRC stark an Art. 8 Abs. 1 EMRK, wonach *jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz hat.* Ein eigenständiges Datenschutzrecht wie Art. 8 EU-GRC sieht die EMRK nicht vor, weshalb der EGMR bei der Behandlung staatlicher Datenverarbeitungen auf den Privatheitsschutz verwiesen war und ist.

Dabei stellte er schon 1987 hinsichtlich eines Polizeiregisters recht pauschal fest, dass die Speicherung und Freigabe persönlicher Informationen

339 Etwa EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 = NJW 2021, 531; zum Verhältnis der DSGVO zu Art. 7, 8 EU-GRC: *Marsch,* Datenschutzgrundrecht, 2018, S. 130 f.; *Schiedermair* in Simitis/Hornung/Spieker Datenschutzrecht, DSGVO, Einl. Rn. 169 ff.

340 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 13.

341 *Lynskey*, Int. & Comp. Law Quarterly 63 (2014), 569 (589 ff.); *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art.8 Rn. 10.

342 Vgl. EuGH, Urteil v. 17.10.2013, C-291/12 (Schwarz/Bochum), Rn. 24 ff. = NVwZ 2014, 435.; krit. *González Fuster/Gutwirth*, Computer Law & Security Review 29 (2013), 531 (537); übersichtlich *Marsch,* Datenschutzgrundrecht, 2018, S. 127 ff.; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 50 f.

343 Europäische Menschenrechtskonvention (Konvetion zum Schutze der Menschenrechte und Grundfreiheiten) vom 04.11.1950, zuletzt geändert durch Protokoll Nr. 15 vom 24.6.2013.

einen Eingriff in das von Art. 8 Abs. 1 EMRK garantierte Recht auf Privatleben darstellen[344] und entwickelte von diesem Ausgangspunkt einen konventionsrechtlichen Datenschutz als Ausprägung der Privatheit.[345] Wie stark dieser Schutz ausgeprägt ist, wird allerdings unterschiedlich beurteilt.[346]

Auffällig an der Rechtsprechung des EGMR zu Art. 8 Abs. 1 EMRK ist die streng kasuistische Vorgehensweise. Bis heute hat der EGMR keine klare Begriffsdefinition des *Privatlebens* bereitgestellt, sondern entscheidet stets im Einzelfall, ob der staatliche (Informations-)Eingriff einen Eingriff in dieses darstellt.[347] Dabei werden zwei Rechtsprechungslinien[348] ausgemacht, wovon eine bei der Schutzbereichsbestimmung an die – weit auszulegende –Persönlichkeitsrelevanz der jeweiligen Daten anknüpft[349] und die andere auf das Ausmaß bzw. die Systematik der Datensammlung abstellt.[350] Aus letzter ließe sich ableiten, dass der EGMR bei Art. 8 Abs. 1 EMRK nicht mehr zwischen Datenschutz und Privatheit trennt, sondern wie das BVerfG jede Datenverarbeitung als Grundrechtseingriff behandelt und somit letztlich ebenfalls ein Recht auf informationelle Selbstbestimmung anerkennt.[351] Als Argument hierfür wurde der Erlass der Datenschutzkonvention[352] durch den Europarat im Jahr 1981 angeführt, die allerdings bis zur Vorlage des Protokolls im Jahr 2018[353] nur für automatisierte Verarbeitungen gilt

344 EGMR, Urt. v. 26.03.1987, 9248/81 (Leander/Schweden), Rn. 47.

345 *Schiedermair,* Schutz des Privaten, 2012, S. 239 ff.; *Marsch,* Datenschutzgrundrecht, 2018, S. 8 ff.

346 Übersichtlich *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 14 ff.; ein „Grundrecht auf Datenschutz" erkennt *Schiedermair,* Schutz des Privaten, 2012, S. 242; ähnlich *Böhringer/Marauhn* in Konkordanzkommentar, Kap. 16 Rn. 29; aA *Marsch,* Datenschutzgrundrecht, 2018, S. 12 ff.

347 Vgl. etwa EGMR, Urt. 25.09.2001, Nr. 44787/98 (PG u. JH/Vereinigtes Königreich), Rn. 57.; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 14 mwN.

348 So *Gellert/Gutwirth*, Computer Law & Security Review 29 (2013), 522 (526); *Marsch,* Datenschutzgrundrecht, 2018, S. 9 ff.

349 EGMR, Urt. v. 16.2.2000, Nr. 27798/95 (Amann/Schweiz), Rn. 65 ff.

350 EGMR, Urt. v. 04.05.2000, Nr. 28341/95 (Rotaru/Rumänien), Rn. 43 ff.

351 *Schiedermair,* Schutz des Privaten, 2012, 242 ff.; *Böhringer/Marauhn* in Konkordanzkommentar, Kap. 16 Rn. 29.

352 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Sammlung Europäischer Verträge - Nr. 108).

353 Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Sammlung Europäischer Verträge - Nr. 223).

und grundsätzlich keine individuellen Rechte beinhaltet[354], allerdings zum Ausdruck bringen könnte, dass schon damals ein grundrechtlicher Datenschutz anerkannt wurde.[355]

Gegen einen prinzipiellen konventionsrechtlichen Datenschutz sprechen laut den insofern skeptischen Autoren[356] aber jüngere Urteile des EGMR, die weiterhin staatliche Datenverarbeitungsmaßnahmen nur unter bestimmten Voraussetzungen als Eingriff ansehen wollen. Es soll auf den Kontext und das Ausmaß der Maßnahme[357] oder die Privatheitserwartungen der Betroffenen ankommen.[358]

Sind Daten von einer staatlichen Maßnahme betroffen, die der *Wohnung* oder der *Korrespondenz* zugeordnet werden können, ist die Zuordnung zum Privatleben vom Gesetzestext vorgegeben. Anders als im Grundgesetz besteht kein exklusives Spezialitätsverhältnis zwischen einem bereichsspezifischen und einem allgemeinen Privatheitsschutz, wenngleich der Begriff des Privatlebens als Lückenfüller verwendet wird.[359] Vielmehr handelt es sich bei der Wohnung und der Korrespondenz um anerkannte Teilbereiche des Privatlebens.[360] Der EMRK bemüht sich daher nicht um eine eindeutige Abgrenzung, sondern stellt etwa bei Dokumentenbeschlagnahmen schlicht fest, dass durch die Beschlagnahme (auch) von Korrespondenzdokumenten ein Eingriff in das Recht auf Schutz des Privatlebens vorliegt.[361]

Mit „Korrespondenz" war ursprünglich nur der Briefverkehr gemeint, der Begriff wurde vom EGMR jedoch sukzessive erweitert und umfasst heute sämtliche Mittel der Fernkommunikation[362], wobei nicht nur die

354 *Kübler,* Säulen der Europäischen Union, 2002, S. 37 ff.; *Johlen* in Stern/Sachs EU-GRC, Art. 8 Rn. 18 Fn 32.

355 *Schiedermair,* Schutz des Privaten, 2012, S. 242 ff.; s.a. EGMR, Urt. 04.05.2000, Nr. 28341/95 (Rotaru/Rumänien), Rn. 43 ff.

356 *Marsch,* Datenschutzgrundrecht, 2018, S. 12 ff.; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 15; ähnlich *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 54 f.

357 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 67 = EuGRZ 2009, 299.

358 EGMR Urt. 25.09.2001, Nr. 44787/98 (PG u. JH/Vereinigtes Königreich), Rn. 57.

359 *Schiedermair,* Schutz des Privaten, 2012, S. 232 ff.

360 *Gaede* in MüKo StPO, EMRK Art. 8 Rn. 1 "Oberbegriff".

361 Vgl. EGMR, Urt. v. 16.12.1992, Nr. 13710/88 (Niemitz/Deutschland), Rn. 27 ff; dazu krit. *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022.

362 EGMR, Urt. v. 06.09. 1978, Nr. 5029/71 (Klass u.a./Deutschland), Rn. 41 = NJW 1979, 1755; Urt. v. 05.09.2017, Nr. 61496/08 (Bărbulescu/Rumänien), Rn. 72.

Inhalte, sondern auch die Kommunikationsumstände geschützt werden.[363] Art. 8 Abs. 1 EMRK garantiert also ebenso wie der diesem nachgebildete Art. 7 EU-GRC einen umfassenden Kommunikationsschutz.[364] Im Vergleich zu Art. 10 GG ist der Schutz sogar erweitert, da Art. 8 Abs. 1 EMRK auch vor Kommunikationsverboten, -unterbrechungen und -verzögerungen schützt[365] und ferner auch dann noch gilt, wenn das Kommunikationsmedium sich im Herrschaftsbereich des Empfängers befindet und dort aufbewahrt wird.[366]

II. Massenüberwachung in der Rechtsprechung des EuGH

Soweit staatliche Überwachungsmaßnahmen ihre Grundlage im EU-Recht finden, spielt das Sekundärrecht eine geringe Rolle, da dieses nur einen Rahmen der Verarbeitung vorgibt und sich gegenüber gesetzlichen Ermächtigungen und Abweichungen offen zeigt. Maßgeblich für die Gestaltung sind also weniger die DSGVO und JI-Rl als die Art. 7, 8 EU-GRC bzw. die hierzu ergangene Rechtsprechung des EuGH, die im Folgenden erläutert werden soll. Ganz ähnlich dem BVerfG hat der Gerichtshof in einer Reihe prominenter Urteile spezifische Anforderungen an staatliche Überwachungsmaßnahmen – insbesondere zur Vorratsdatenspeicherung und Datenanalyse – aus dem Grundsatz der Verhältnismäßigkeit entwickelt.

1. Telekommunikationsdaten

Die bislang wohl wirkmächtigsten Urteile des EuGH zu sicherheitsrechtlichen Überwachungsmaßnahmen befassen sich mit Telekommunikationsdaten.

---

363 EGMR Urt. v. 03.04.2007, Nr. 62617/00 (Copland/Vereinigtes Königreich), Rn. 41 = MMR 2007, 431.

364 *Gersdorf* in BeckOK Informations-/MedienR, EU-GRC Art. 8 Rn. 41; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 39.

365 *Hermes* in Dreier GG Art. 10 Rn. 7; *Böhringer/Marauhn* in Konkordanzkommentar, Kap. 16 Rn. 67.

366 Vgl. EGMR, Urt. v. 16.12.1992, Nr. 13710/88 (Niemitz/Deutschland), Rn. 27 ff.; *Böhringer/Marauhn* in Konkordanzkommentar Kap. 16 Rn. 61 mwN.

a. TK-Verkehrsdaten

Insbesondere mit den Urteilen zur Vorratsdatenspeicherung von TK-Verkehrsdaten hat sich der Gerichtshof als bedeutende Institution auf dem Gebiet des Sicherheitsverfassungsrechts etabliert. Diese Rechtsprechung nahm ihren Ausgang im Jahr 2006 mit dem Erlass der VDS-RL[367] durch die EU.[368]

Mit dieser Richtlinie wollte die EU sicherstellen, dass bestimmte Daten *zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen*, Art. 1 Abs. 1 VDS-RL.

Nach Art. 3, 5 der VDS-RL sollten die Mitgliedstaaten deshalb vorsehen, dass Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste bzw. Betreiber eines öffentlichen Kommunikationsnetzes die bei ihnen anfallenden Telekommunikationsverkehrs- und Standortdaten[369] speichern und zwar nach Art. 6 der Richtlinie für mindestens sechs Monate.

Diese Daten sollten den *zuständigen Behörden* nach Maßgabe mitgliedstaatlicher Vorschriften zugänglich sein, wobei die Ausgestaltung, d. h. das „Wie" dieser Zugangsregeln, vollständig den Mitgliedstaaten überlassen wurde, Art. 4 VDS-RL. Einzig die Umschreibung des Anwendungsbereichs in Art. 1 Abs. 1 der Richtlinie begrenzte die Ausgestaltungsmöglichkeiten, da hiernach die Vorratsdatenspeicherung nur zur Bekämpfung *schwerer* Straftaten vorgesehen war. Es blieb allerdings den Mitgliedstaaten überlassen, zu bestimmen, welche Delikte der nationalen Straftatbestände als schwere Kriminalität in diesem Sinne gelten sollten.[370]

---

367 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.

368 Übersichtlich zum Inhalt *Westphal*, EuR 2006, 706; zur Historie statt vieler *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 148 ff. mit umfg. Übersicht zur Lit.; *Szuba,* Vorratsdatenspeicherung, 2011, S. 48 ff.; *Grabowska-Moroz* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 3 (3 ff.); *Bignami* Chicago J. of Int. Law 2007, 233 (238 ff.).

369 Vgl. heute § 3 Nr. 70, § 176 TKG; *Moser-Knierim*, Vorratsdatenspeicherung, 2014, S. 141; manchmal auch „Metadaten" vgl. Art. 4 Abs. 3 Lit a) b) c) e-Privacy-VO (Vorschlag der EU Kommission, COM(2017) 10 final - 2017/0003 (COD)); zu den Begriffen auch *Schramm/Shvets*, MMR 2019, 568 (569 (Fn. 24)).

370 Hierzu früh krit. *Breyer*, StV 2007, 214 (217 f.).

aa. Unionsrechtswidrigkeit der VDS-RL: *Digital Rights Ireland*

Gegen die VDS-RL erhoben die NGO *Digital Rights Ireland* vor dem Irischen High Court sowie die Kärntner Landesregierung gemeinsam mit über 11.000 Personen vor dem österreichischen Verfassungsgerichtshof Klagen, die jeweils zu Vorabentscheidungsverfahren am EuGH führten und dort zusammengefasst behandelt wurden.[371]

Der EuGH sollte insbesondere prüfen, ob die VDS-RL mit Unionsprimärrecht, insbesondere dem Recht auf Privatheit nach Art. 7 und dem Recht auf Datenschutz nach Art. 8 EU-GRC, sowie mit dem eng verwandten (s.o. I. 1. a.) Recht auf Privatheit nach Art. 8 EMRK vereinbar ist.

(1) Formelle Rechtswidrigkeit mangels Kompetenz der EU?

Dabei wurde bereits vor der Entscheidung an der formellen Rechtmäßigkeit der Richtlinie gezweifelt, da die Kompetenz der EU fraglich erschien.[372] Der EU-Gesetzgeber stütze die VDS-RL auf Art. 95 Abs. 1 EG[373] (heute 114 Abs. 1 AEUV). Dieser räumte der EU die Kompetenz zur Angleichung von Rechtsnormen ein, *die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.* Die Kommission argumentierte, dass aufgrund der bisherigen Rechtslage unterschiedliche Regelungen einer sicherheitsrechtlichen Vorratsdatenspeicherung möglich seien und deshalb eine Harmonisierung erforderlich sei.[374] Tatsächlich dürfte die Wahl der Kompetenzgrundlage aber schlicht auf einer politischen Notwendigkeit beruht haben, da auf Art. 95 Abs. 1 EG gestützte Richtlinien anders als Rahmenbeschlüsse i. S. d. Art. 34 Abs. 2 EG[375] (Art. 29 EUV) lediglich eine qualifizierte Mehrheit im Rat erforderten, Art. 251 Abs. 2 EG.[376]

371 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 17 ff. = NJW 2014, 2169; *Tracol*, Computer Law & Security Review 30 (2014), 736 (737).

372 BT-Drs. 16/1622, S. 4 ff.; *Westphal*, EuR 2006, 706 (712 f.); *Gitter/Schnabel*, MMR 2007, 411 (412 f.); *Breyer*, StV 2007, 214 (215 f.); *Flynn* UC Dublin Law Rev. 8 (2008), 1.

373 Vertrag zur Gründung der Europäischen Gemeinschaft, Konsolidierte Fassung 2002, Abl. 2002, C 325/1.

374 Erwägungsgründe Nr. 1, 5, 6 VDS-RL.

375 Vertrag über die Europäische Union, Konsolidierte Fassung 2002, Abl. 2002, C 325/1.

376 *Wissenschaftliche Dienste des Bundestags,* Vorratsdatenspeicherung, 2006, S. 8.

Zuvor war der EuGH hinsichtlich der bilateral vertraglich eingeführten Verpflichtung von Airlines, Fluggastdaten an US-Sicherheitsbehörden weiterzugeben (dazu unten II. 2.)[377], zu dem Ergebnis gelangt, dass eine solche Datenverarbeitung zu Sicherheitszwecken nicht in den Anwendungsbereich des Europäischen Datenschutzrechts fiel. Mangels einer solchen Verbindung der Regelung zum Unionsrecht komme Art. 95 Abs. 1 EG als Kompetenznorm nicht infrage. Die Verpflichtung zur Weitergabe von Fluggastdaten per Rahmenbeschluss hielt der Gerichtshof daher für rechtswidrig.[378]

Da die VDS-RL ebenfalls Private zu Datenverarbeitungen verpflichtete, die *schwerpunktmäßig*[379] sicherheitsrechtlichen Pflichten dienen sollten, wurde eine Übertragung dieser Rechtsprechung erwartet.[380] Die Republik Irland, unterstützt von weiteren Mitgliedstaaten, erhob denn auch noch im Jahr 2006 Nichtigkeitsklage und rügte die fehlende Kompetenz der Union.

Der EuGH wies diese Klage zurück.[381] Die VDS-RL betreffe unmittelbar keine Datenverarbeitung zum Schutz der öffentlichen Sicherheit. Sie adressiere unmittelbar nur die (privatwirtschaftlichen) Anbieter von Telekommunikationsdiensten im Binnenmarkt, da die Umstände, unter denen die Sicherheitsbehörden der Mitgliedstaaten auf die zu speichernden Daten zugreifen könnten, in der Richtlinie nicht geregelt seien.[382] Bei der Weiterleitung von Fluggastdaten an die US-Sicherheitsbehörden habe der Fall anders gelegen, da dort unmittelbar eine Verarbeitung durch die Sicherheitsbehörden der Mitgliedstaaten vorgesehen sei.[383]

377 Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security, ABl. 2004, L 183/83.

378 EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA) = NJW 2006, 2029; dazu *Simitis*, NJW 2006, 2011.

379 Zur „Schwerpunktheorie" EuGH, Urteil vom 30.01.2001, C-36/98 (Spanien/Rat), Rn. 59 = EuZW 2001, 208; Urt. v. 11.06.1991, C-300/89 (Titanoum Dioxid); *Terhechte* in Frankfurter Kommentar, AEUV Art. 114 Rn. 33; gegen die Anwendung bei vertikalen Konflikten *Tietje* in Grabitz/Hilf/Nettesheim Recht der EU, AEUV Art. 114 Rn. 125.

380 *Flynn* UC Dublin Law Rev. 8 (2008), 1 (11 f.); *Westphal*, EuR 2006, 706 (712 f.); *Gitter/Schnabel, MMR* 2007, 411 (412 f.); *Breyer*, StV 2007, 214 (215 f.).

381 EuGH, Urt. v. 10.2.2009, C-301/06 (Irland / Parlament und Rat) = MMR 2009, 244.; krit. *Ambos*, JZ 2009, 466 (470 f.).

382 Idem, Rn. 91.

383 Ibid.

(2) Unvereinbarkeit mit Primärrecht wegen unverhältnismäßiger Beschränkung der Art. 7, 8 EU-GRC

Erfolgreicher als der irische Staat war die Gruppe *Digital Rights Ireland* mit ihrer Grundrechtsklage bzw. dem daraus folgenden Vorabentscheidungsverfahren.

(a) (Schutzbereichs-)Parallelität von Art. 7 und 8 EU-GRC und Eingriffskomplex

Bei dieser Entscheidung war zunächst bemerkenswert, dass der EuGH die Möglichkeit eines Eingriffs hinsichtlich Art. 7 und 8 EU-GRC separat prüfte. Bislang hatte der Gerichtshof nicht zwischen diesen Grundrechten differenziert, sondern diese als Einheit geprüft (s.o.).[384] Nun stellte er klar, dass die Pflicht der Telekommunikationsanbieter, Verkehrsdaten universell zu speichern sowohl in den Schutzbereich des Art. 7 EU-GRC[385] als auch in jenen des Art. 8 EU-GRC[386] eingreife.

Darüber hinaus trennte er nicht nur zwischen den Schutzbereichen von Art. 7 und 8 EU-GRC, sondern auch zwischen den verschiedenen Datenverarbeitungsschritten, zu denen die Richtlinie verpflichtete.[387] Der EuGH erkannte, dass sowohl die verpflichtende Speicherung der Verkehrsdaten als auch deren Abruf durch die Sicherheitsbehörden jeweils einen eigenständigen Eingriff darstellten, die allerdings als Einheit geprüft werden müssten, da sich die Intensität der einzelnen Eingriffe nur aus der Gesamtschau ergebe.[388] Das Urteil zur Vorratsdatenspeicherung bringt damit das oben beschriebene Verständnis von Massenüberwachungsmaßnahmen zum Aus-

384 Vgl. EuGH, Urteil v. 17.10.2013, C-291/12 (Schwarz/Bochum), Rn. 24 ff. = NVwZ 2014, 435; Urteil v. 09.11. 2010, C 92/09, C 93/09 (Schecke u Eifert/Hessen), Rn. 52; Urteil v. 09.01.2008, C–275/06 (Promusicae/Telefónica), Rn. 64; dazu *Marsch,* Datenschutzgrundrecht, 2018, S. 203 ff.; *González Fuster,* Data Protection, 2013, S. 234 ff.; *J. Kokott/Sobotta*, Int. Data Privacy Law 3 (2013), 222; *Gellert/Gutwirth*, Computer Law & Security Review 29 (2013), 522 (524 ff.); *W. Michl*, DuD 2017, 349; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 52; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 23, 31 f.

385 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 38 ff. = NJW 2014, 2169.

386 Idem, Rn. 36.

387 Idem, Rn. 34 ff.

388 Idem, Rn. 54 ff.

druck, deren grundrechtliche Sensibilität sich daraus ergibt, dass mehrere aufeinander abgestimmte Datenverarbeitungsschritte kombiniert werden (s. o. Kap. B. I. 1. c.).

Im Ausgangspunkt stellte der EuGH also fest, dass die Richtlinie zwei Eingriffe umfasste, die jeweils zwei Grundrechte betrafen, wobei die Eingriffe nicht als Einheit,[389] sondern korrekterweise als Komplex behandelt wurden. Entsprechend wäre eine separate und umfassende Prüfung von Art. 7 sowie Art. 8 EU-GRC „der Reihe nach"[390] zu erwarten gewesen.

Eine solche Trennung der Grundrechte fand sich im Rahmen der Rechtfertigungsebene allerdings nur in der (Vorab-)Prüfung des unantastbaren Wesensgehalts der beiden Grundrechte i. S. d. Art. 52 Abs. 1 EU-GRC.[391] Für die Verhältnismäßigkeit spielte diese Parallelität[392] dann plötzlich keine Rolle mehr. Dort war nur noch von einem (einheitlichen) *Eingriff in die Rechte des Art. 7, 8 EU-GRC* die Rede.[393] Im Rahmen der Verhältnismäßigkeit scheint der EuGH demnach weiterhin von einer möglichen Kombination[394] der Grundrechte aus Art. 7 und 8 EU-GRC auszugehen.

(b) Verhältnismäßigkeit: Normenklarheit als Erforderlichkeitsgewährleistung

Bei der Prüfung stand die Verhältnismäßigkeit im Fokus, also die Frage, ob der Eingriffskomplex der Vorratsdatenspeicherung für die in der Richtlinie genannten Ziele geeignet, erforderlich und angemessen war.[395] An der Eignung zweifelte der EuGH nicht. Auch eine vorratsmäßige Speicherung nur

389 *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139).

390 Vgl. zur entsprechenden Methodik im GG *Dreier* in Dreier GG, Vorb. Art. 1 Rn. 155; *Stern,* StaatsR Bd. III/2, 1994, S. 1366 ff.

391 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 39 ff. = NJW 2014, 2169.

392 *Jarass* in Jarass EU-GRC, Art. 8 Rn. 4; *Johlen* in Stern/Sachs EU-GRC, Art. 28 Rn. 24, Fn 51.

393 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 45 ff., angedeutet schon in der Überschrift von Rn. 38 ff. "Rechtfertigung des Eingriffs" = NJW 2014, 2169.

394 *Marsch,* Datenschutzgrundrecht, 2018, S. 217 ff.; *W. Michl*, DuD 2017, 349 (353); allg zu Grundrechtskombinationen *Breckwoldt,* Grundrechtskombinationen, 2014; Spielmann*,* Konkurrenz, 2008, S. 190 ff.; *Heß,* Grundrechtskonkurrenzen, 2000, S. 84 f.

395 Der EuGH nimmt traditionell eine (manchmal unsystematische) dreiteilige Verhältnismäßigkeitsprüfung vor, da das (legitime)Gemeinwohlziel eigenständig in Art. 52

bestimmter Daten – hier TK-Verkehrsdaten – sei prinzipiell nützlich für strafrechtliche Ermittlungen.[396]

Die Erforderlichkeit hingegen zweifelte der EuGH an. Dabei stellte er zunächst fest, dass man aus der Dringlichkeit des Ziels der Richtlinie nicht automatisch auf deren Erforderlichkeit schließen könne. Die Erforderlichkeit i. S. d. Art. 52 Abs. 1 S. 2 EU-GRC verlange vielmehr, dass nur solche grundrechtsbeschränkenden Maßnahmen erlassen werden, die zur Förderung des Ziels *absolut notwendig* sind.

Dies erfordere zunächst, dass die Tragweite der Maßnahme durch *klare und präzise Regeln* bestimmt wird, *sodass die Personen, deren Daten auf Vorrat gespeichert wurden, über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen*.[397] Der Gerichtshof versteht insofern das, was in Deutschland als Bestimmtheitsgrundsatz bekannt ist, als Teil der Erforderlichkeit.[398] Das ergibt insofern Sinn, als nur durch eine ausreichende Normenklarheit eine Überwachungsermächtigung auf das *absolut Notwendige* beschränkt werden kann. Analog zu dieser Idee verhält sich die frühe Rechtsprechung des BVerfG zu Überwachungsmaßnahmen, in der die Notwendigkeit von Eingriffsschwellen noch aus dem Bestimmtheitsgrundsatz abgeleitet wurde.[399]

Die entscheidenden Ausführungen des EuGH verstehen sich also als Erforderlichkeits- und damit als Teil der europarechtlichen Verhältnismäßigkeitsprüfung.[400] Der Generalanwalt hingegen hatte die Anforderungen an die Ausgestaltung der Zugriffsregeln zur Einhegung der Eingriffsintensität als Problem der „Gesetzesqualität" i. S. d. Art. 52 Abs. 1 EU-GRC diskutiert.[401]

Abs. 1 EU-GRC genannt wird, vgl. *Schwerdtfeger* in Meyer/Hölscheidt EU-GRC, Rn. 52 Rn. 35 ff.; *Pache* in Frankfurter Kommentar, EU-GRC Art. 52 Rn. 24.

396 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 49 = NJW 2014, 2169.

397 Idem, Rn. 54.

398 *Schwerdtfeger* in Meyer/Hölscheidt EU-GRC Art. 52 Rn. 31.

399 BVerfGE 110, 33 (55 ff.) – Außenwirtschaftsgesetz.

400 Vgl. *Granger/Irion*, Eur. Law Rev. 2014, 834 (841 f.); *Tracol*, Computer Law & Security Review 30 (2014), 736 (742).

401 *Generalanwalt Villalón*, Schlussantrag v. 12.12.2013, C-293/12, Rn. 108 ff. – Digital Right Ireland.

Das Vorgehen des EuGH entspricht inhaltlich jenem des BVerfG. Zwar liegt der Fokus anders als beim BVerfG[402] nicht ausdrücklich auf der Angemessenheit, sondern der Erforderlichkeit. Schon hier werden jedoch abwägende Elemente eingebaut, sofern die Intensität der Maßnahme mit den vorgesehenen Zugriffseinschränkungen abgeglichen wird. Die Prüfung vermengt also Aspekte von Erforderlichkeit und Angemessenheit, wie sie in der deutschen Grundrechtslehre verstanden würde.[403]

(c) Intensitätsbestimmung

Der EuGH beginnt damit, intensivierende Aspekte der Vorratsdatenspeicherung hervorzuheben, wobei er sich in bemerkenswerter Weise an der Rechtsprechung des EGMR orientiert und diesen immer wieder zitiert.[404]

Schon zu Abschluss der Eingriffsdarstellung hatte der EuGH festgestellt, dass die heimliche Aufbewahrung der Verkehrsdaten geeignet ist, bei den Betroffenen ein Gefühl ständiger Überwachung auszulösen und schon deshalb besonders schwer wiege.[405] Wie auch das BVerfG[406] (s. o.) berücksichtigt der EuGH also Einschüchterungseffekte, die weniger auf der konkreten Speicherung beruhen als auf der abstrakten Gesetzesexistenz bzw. dem Wissen der Grundrechtsträger um die gesetzliche Obliegenheit der Speicherung. Was der EuGH dabei nicht bespricht, ist die Tatsache, dass eine gesetzlich obligatorische Speicherung jedenfalls diesen Teil der Überwachung gerade nicht zu einem heimlichen macht.[407] Soweit die Ein-

402 Vgl. BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; NJW 2022, 1583 (1585 Rn. 152 ff.) – Bayerisches Verfassungsschutzgesetz; dazu *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 39.

403 *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 52 Rn. 69.

404 Insbesondere EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich) = EuGRZ 2009, 299; zur Bezugnahme auf den EGMR durch den EuGH in *Digital Rights Ireland*: *Grabenwarter* in Stumpf/Kainer/Baldus (Hrsg.), Privatrecht Wirtschaftsrecht Verfassungsrecht, 2015, S. 1386 (1392 f.); *Boehm/Cole* ZD 2014, 553; s.a. *Boehm/Andrees*, CR 2016, 146.

405 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 37 = NJW 2014, 2169.

406 BVerfGE 65, 1 (43) – Volkszählung; E 120, 378 (402) – Autom. Kennzeichenkontrolle I; E 125, 260 (332) – Vorratsdatenspeicherung; krit. hierzu *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011; *J. Franz Lindner/Unterreitmeier*, JZ 2022, 915 (918 f.); Nachweise zur Rspr. und Übersicht zur Kritik bei *Bäcker,* Kriminalpräventionsrecht, 2015, S. 270 f.

407 *Schluckebier* abw. Meinung BVerfGE 125, 260 (366).

schüchterungseffekte mit der Heimlichkeit begründet werden, kann korrekterweise also nur auf die jederzeitige Zugriffsmöglichkeit abgestellt werden. Wie auch das BVerfG lässt der Gerichtshof eine tiefergehende Auseinandersetzung mit den empirischen[408] und theoretischen Schwächen der auf den Einschüchterungseffekten aufbauenden Argumentation vermissen.

Ebenfalls knapp wendet sich der EuGH dem Ausmaß des Grundrechtseingriffs zu. Er stellt fest, dass die Speicherung sämtlicher Verkehrsdaten verschiedenster technischer Kommunikationsgeräte aufgrund deren weiteren Verbreitung im Alltag letztlich einen Eingriff in die Grundrechte der gesamten europäischen Bevölkerung darstellt.[409] Der EuGH zieht die Menge der Grundrechtsbetroffenen also in die Intensitätsbestimmung mit ein.

Dabei ergibt sich aus den Ausführungen, dass der EuGH, ganz ähnlich dem BVerfG, die große Menge der Grundrechtsbetroffenen mit der damit natürlicherweise einhergehenden Anlasslosigkeit in Verbindung bringt. Aufgrund der Universalität der Speicherung würden auch Daten von Personen zur später eventuellen Nutzung durch die Sicherheitsbehörden verarbeitet, die im Moment der Speicherung überhaupt keinen Anlass zur Strafverfolgung gegeben hätten.[410] So wäre es etwa denkbar gewesen, die Speicherung nur auf bestimmte Personenkreise, Zeiten oder Orte zu beschränken, bei denen eine erhöhte Wahrscheinlichkeit gegeben wäre, auch solche Daten zu speichern, die später tatsächlich notwendig würden.[411]

(d) Ergebnis und Zusammenfassung

Aufgrund der geringen Regelungsdichte der Richtlinie befand der EuGH somit letztlich, dass der Eingriff in die Privatheitsgrundrechte nicht auf das Notwendige beschränkt sei, und erklärte die Richtlinie für primärrechtswidrig und nichtig.

Anders als das BVerfG, das den Grad der Regelungsdichte aus der Angemessenheit heraus entwickelt, stützt sich der EuGH auf die Erforderlichkeit, ausgeprägt durch den Bestimmtheitsgrundsatz. Im Ergebnis beurteilt aber auch der Gerichtshof die Grundrechtskonformität nach dem Effekti-

408 Zu diesen insbesondere *Rath* in *Kritische Justiz* (Hrsg.), 60 Jahre GG, 2009, S. 65.
409 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 56 = NJW 2014, 2169.
410 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 58 = NJW 2014, 2169.
411 Idem, Rn. 59.

vitätsgrad der Überwachungsmaßnahme. Methodisch scheint dieser Weg überzeugend, da sich die Erforderlichkeitsprüfung als Standort für Effektivitätsfragen durchaus aufdrängt. Das Vorgehen des BVerfG entspricht jedoch dessen mittlerweile eingeübten Priorisierung der Angemessenheit.[412]

Für die Speicherpflicht verlangte der Gerichtshof insofern eine Beschränkung *auf einen bestimmten Zeitraum und/oder ein bestimmtes geografisches Gebiet und/oder einen bestimmten Personenkreis, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, bzw. auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Verhütung, Feststellung oder Verfolgung schwerer Straftaten beitragen könnten.*[413] Die Speicherpflicht dürfe zudem nicht auf ein Minimum von sechs und Maximum von 24 Monaten festgelegt werden.[414]

Weiter verlangte der EuGH eine Beschränkung des Zugriffs auf das absolut Notwendige in materieller und formeller Hinsicht. Die entsprechenden Vorschriften müssten voraussetzen, dass auf die betroffenen Daten nur zugegriffen werden dürfe, wenn dies die Verhütung, Feststellung oder strafrechtliche Verfolgung genau abgegrenzter Straftaten (tatsächlich) bezwecke.[415] Außerdem verlangte er, dass der Zugriff nur auf Antrag zulässig sein solle, der einer unabhängigen Vorabkontrolle unterzogen wurde.[416]

Letztlich formulierte der EuGH spezifische Anforderungen an die Datensicherheit und -transparenz, wobei er jedoch den Diensteanbietern einen gewissen Spielraum beließ.[417]

Mit der Entscheidung hat sich der EuGH dennoch als entscheidende Stelle bei der Bewertung sicherheitsrechtlicher Überwachungsmaßnahmen, ja als aktives Grundrechtsgericht überhaupt etabliert.[418] Das Vorgehen gleicht jenem des BVerfG darin, dass aus denselben Intensitätsmaßstäben

412 dazu *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 39.

413 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 59 = NJW 2014, 2169.

414 Idem, Rn. 63 f.

415 Idem, Rn. 61 f.

416 Idem, Rn. 62.

417 Idem, Rn. 66 ff.

418 *Kühling*, NVwZ 2014, 681 (684 f.); *Granger/Irion*, Eur. Law Rev. 2014, 834 (844 ff.); *Wendel,* Wider die Mär vom Grundrechtsblinden, 09.04.2014, https://verfassungsblog.de/wider-maer-vom-grundrechtsblinden-eugh-und-vorratsdatenspeicherung/, zuletzt aufgerufen am 12.01.2025; *Prantl* – Ende der Maßlosigkeit SZ vom 08.04.2014, https://www.sueddeutsche.de/politik/urteil-zur-vorratsdatenspeicherung-ende-der-masslosigkeit-1.1932057, zuletzt aufgerufen am 12.01.2025.

letztlich Anforderungen an die Regelungsdichte abgeleitet werden, deren Zweck eine möglichst effektive Massenüberwachung darstellt. Es soll also mit möglichst wenigen und geringen Eingriffen ein relatives Maximum an Sicherheitsgewährleistung erzielt werden. Dies kann nur durch materielle Eingriffsschwellen und Verfahrens- sowie Datenschutzvorschriften erzielt werden.

bb. Unionsrechtswidrigkeit nationaler Vorratsdatenspeicherung

Mit der Nichtigkeitserklärung der VDS-RL durch *Digital Rights Ireland* war die Rechtsprechung des EuGH zur anlasslosen Speicherung von TK-Verkehrsdaten aber nicht am Ende. Sie nahm hierdurch erst ihren Anfang.

In den verschiedenen Mitgliedstaaten wurde unterschiedlich auf das Urteil des EuGH reagiert.[419] Weitgehende Einigkeit bestand – auch in der Literatur – dahingehend, dass aufgrund der spezifischen Regelung in Art. 15 Abs. 1 S. 2 e-Privacy-RL ein Anwendungsfeld des EU-Rechts, jedenfalls im Sinne der Rechtsprechung des EuGH[420], vorliegt und nationale Regelungen folglich mit den Anforderungen der Art. 7, 8 EU-GRC in der Auslegung des Gerichtshofs in Einklang stehen müssten.[421]

Nur einige Mitgliedstaaten änderten ihre bestehenden Regelungen aber proaktiv ab. Andere bestanden darauf, die Anwendung der vom EuGH postulierten Grundsätze durch die nationalen Gerichte abzuwarten. Drittens gab es auch noch eine Gruppe an Mitgliedstaaten, darunter die Bundesrepublik Deutschland, die das Urteil als Anlass nahmen, von der Implementation einer vorratsmäßigen Verkehrsdatenspeicherung erst einmal ganz abzusehen.[422]

419 Übersichtlich *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (268 ff.); *Vainio/Miettinen*, Int. J. of Law and Information Technology 23 (2015), 290 (299 ff.).

420 EuGH Urt. v. 26.2.2013, C-617/10 (Åkerberg Fransson), Rn. 17 ff. =NVwZ 2013, 561; Urt. v. 10.7.2014, C-198/13 (Hernández), Rn. 41 = EuZW 2014, 795; dazu *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 51 Rn. 8 ff.; *Hancox*, Common Market Law Rev. 50 (2013), 1411.

421 *Boehm/Cole*, ZD 2014, 553 (555); *Granger/Irion*, Eur. Law Rev. 2014, 834 (848); *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (267); aA. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.); für eine selbstständige Primärrechtswidrigkeit des Art. 15 Abs. 1 S. 2 e-Privacy-RL: *Sandhu*, EuR 2017, 453 (462 ff.).

422 *Roßnagel*, NJW 2016, 533 (534 f.).

Diese unterschiedlichen Reaktionen basierten auf der Unklarheit[423], ob durch *Digital Rights Ireland* die anlasslose Vorratsdatenspeicherung generell unzulässig[424] oder nur von der konkreten Ausgestaltung insbesondere der Zugriffsregelungen abhängig geworden war.[425]

(1) *Tele2Sverige/Watson*: Keine nationale Vorratsdatenspeicherung zur Verbrechensbekämpfung.

Diese Fragen hatte der EuGH im Urteil *Tele2Sverige/Watson*[426] erstmals zu beantworten, in dem er zusammengefasst über Vorabentscheidungsvorlagen aus Schweden und dem Vereinigten Königreich entschied. Beide (damals noch) Mitgliedstaaten hatten nach der Nichtigkeitserklärung der VDS-RL weiterhin Normen implementiert, die eine Vorratsdatenspeicherung von TK-Verkehrsdaten vorsahen. Das britische Modell unterschied sich vom schwedischen jedoch insoweit, dass im Vereinigten Königreich keine generelle Pflicht zur Speicherung bestand, sondern eine solche gegenüber einzelnen Betreibern vom Innenministerium erst angeordnet werden musste und mit verschiedenen Einschränkungen versehen werden konnte.[427]

Hinsichtlich des schwedischen Rechts stand also die Frage im Raum, ob eine gesetzlich universelle Pflicht zur Vorratsdatenspeicherung von Verkehrsdaten – in diesem Falle erneut für mindestens sechs Monate – durch nationale Gesetzgebung mit Europäischem Recht vereinbar war. Insofern entsprach die Ausgangslage hinsichtlich des schwedischen Verfahrens ganz jener aus dem Urteil *Digital Rights Ireland*.

423 Vgl. GA *Saugmandsgaard Øe*, Schlussantrag v. 16.07.2016, C-203/15,C-698/15 (Tele2Sverige/Watson ua.), Rn. 192 ff.

424 *Leutheusser-Schnarrenberger*, DuD 2014, 589 (592); ähnlich *Nachbaur*, ZRP 2015, 215 (216).

425 etwa England and Wales Court of Appeal, 20.11.2015 (Secretary of State for the Home Department v Davis MP c Ors) [2015] EWCA Civ 1185, Rn. 48 mit Verweis auf das Instanzgericht.; dazu *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.); zuvor schon BVerfGE 125, 260 (347 ff.) – Vorratsdatenspeicherung.

426 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.) = NJW 2017, 717.

427 Idem, Rn. 15 ff. (schwedisches Recht), Rn. 29 ff. (Recht des Vereinigten Königreichs); übersichtlich *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (268 ff.).

(a) Geltung der Art. 15 Abs. 1 e-Privacy-RL und Art. 7, 8 EU-GRC für nationale Vorratsdatenspeicherungsregime?

Dabei stellte der EuGH zunächst fest, dass solche nationalen Regelungen den Anwendungsbereich des Unionsrechts i. S. d. Art. 51 Abs. 1 EU-GRC betrafen, da die Einführung sicherheitsrechtlicher Vorratsdatenspeicherung als Einschränkung der sich aus Art. 5 e-privacy-RL ergebenden Rechte in Art. 15 Abs. 1 S. 1, 2 e-Privacy-RL spezifisch determiniert wurde.[428] Dass Art. 1 Abs. 3 e-Privacy-RL *Tätigkeiten im Bereich der öffentlichen Sicherheit und der Strafverfolgung* vom Anwendungsbereich dieser Richtlinie generell ausnahm, stand mit diesem Ergebnis zwar auf den ersten Blick im Widerspruch. Dieses Spannungsverhältnis[429] zwischen Art. 15 Abs. 1 S. 1, 2 und Art. 1 Abs. 3 e-Privacy-RL löste der EuGH aber auf, indem er Art. 1 Abs. 3 e-Privacy-RL eng auslegte und damit nur solche sicherheitsrechtlichen Datenverarbeitungen vom Anwendungsbereich ausnahm, die unmittelbar durch die zuständigen (Sicherheits-)Behörden erfolgten. Andernfalls käme Art. 15 Abs. 1 S. 1, 2 e-Privacy-RL kein Anwendungsbereich mehr zu.[430]

Es oblag dem EuGH daher zu entscheiden, inwieweit Art. 15 Abs. 1 S. 2 e-Privacy-RL der nationalstaatlichen Einführung einer TK-Vorratsdatenspeicherung entgegensteht. Die Norm selbst bleibt insofern vage. Art. 15 Abs. 1 S. 1 e-Privacy-RL statuiert lediglich einen Verhältnismäßigkeitsvorbehalt von sicherheitsrechtlichen Eingriffen in die von der Richtlinie garantierten Rechte, also der Vertraulichkeit elektronischer Kommunikation. Art. 15 Abs. 1 S. 2 e-Privacy-RL nennt als Beispiel für einen solchen Eingriff, *dass Daten während einer begrenzten Zeit aufbewahrt werden*.

Um konkrete Anforderungen an die Verhältnismäßigkeit von Vorratsdatenspeicherungsregimen herauszuarbeiten, bemühte der EuGH eine Auslegung des Art. 15 Abs. 1 S. 1 e-Privacy-RL im Lichte der Art. 7, 8 EU-GRC. Nationalstaatliche Eingriffe in die Telekommunikationsvertraulichkeit wären danach von Art. 15 Abs. 1 S. 2 e-Privacy-RL untersagt, soweit sie unverhältnismäßig in Art. 7, 8 EU-GRC eingriffen. Ausgangspunkt dieser Prüfung waren wiederum die Maßstäbe, die der Gerichtshof in *Digital Right Ireland* aufgestellt hatte.

428 *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.); dazu auch *M. W. Müller/Schwabenbauer*, NJW 2021, 2079 (2080 f.).

429 *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

430 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; s.a. *Boehm/Cole* ZD 2014, 553 (555); *Granger/Irion*, Eur. Law Rev. 2014, 834 (848); *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (267).

(b) Verhältnismäßigkeitsprüfung

Die Intensitätsfestlegung begann der EuGH in der Folge aber nicht mehr mit der Hervorhebung der Streubreite und Anlasslosigkeit, sondern stellte die Sensibilität von Verkehrsdaten heraus.[431] Die Speicherung solcher Daten sei schon deshalb ein besonders schwerwiegender Eingriff.[432]

Als mögliche Rechtfertigung dieses Eingriffs komme nur die Bekämpfung schwerer Straftaten in Betracht. Hierfür aber sei eine universelle Speicherpflicht nicht erforderlich, da sie das *absolut Notwendige* überschreite. Es würden zu viele Daten erhoben, die sich aufgrund der Anlasslosigkeit letztlich als für das Maßnahmenziel völlig unbrauchbar erwiesen .[433]

Der EuGH elaborierte ausführlich, dass Speicherpflichten, die auf der Grundlage spezifischer Erkenntnisse zeitlich und örtlich begrenzt seien, ebenso geeignet seien.[434] Unabhängig von den Zugriffsrechten komme eine universelle Pflicht der Telekommunikationsdienstleister zur Vorhaltung von TK-Verkehrsdaten also nicht in Betracht.

Damit war die erste Frage des Oberverwaltungsgerichts Stockholm beantwortet und die Diskussion um die Möglichkeit allgemeiner Vorratsdatenspeicherungen bei ausreichender Limitierung der Zugriffsmöglichkeiten (eigentlich) entschieden (dazu gleich unten).

Der EuGH widmete sich nun den Fragen aus Schweden und dem Vereinigten Königreich hinsichtlich der Ausgestaltung der Zugriffsregeln. Wie bereits dargelegt unterfielen auch diese dem Anwendungsbereich des EU-Rechts i. S. d. Art. 51 Abs. 1 EU-GRC, da der Gerichtshof die Vorratsdatenspeicherung zu Recht als Maßnahmenkomplex begreift und Art. 15 Abs. 1 e-Privacy-RL deshalb dahingehend auslegt, dass dieser auch die Zugriffsebene reglementiert.[435]

Auch für die Zugriffsregeln müssten die Mitgliedstaaten sicherstellen, dass sie verhältnismäßig sind, was wiederum nur dann möglich sei, wenn sie der Bekämpfung schwerer Kriminalität dienten und insofern erforderlich seien.[436] Der EuGH begrenzte also nicht nur selbstständig die Spei-

431 Dazu *Brkan*, German Law Journal 20 (2019), 864 (872 f.).
432 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 = NJW 2017, 717.
433 Idem, Rn. 106.
434 Idem, Rn. 108 ff.
435 Idem, Rn. 118; aA. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).
436 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 113 ff. = NJW 2017, 717.

cherpflichten, sondern auch den Zugriff, da Speicherung und Zugriff nur zusammengedacht werden können.[437] Er erteilte somit der Überlegung, dass eine allgemeine Speicherpflicht verhältnismäßig sein könnte, wenn nur der Zugriff ausreichend limitiert würde, eine recht deutliche Absage.[438]

Die materiellen Anforderungen an die Zugriffsregeln konkretisierte der EuGH noch etwas näher und schuf insbesondere eine neue Ausnahmekonstellation. Die Mitgliedstaaten müssten den Zugang zu vorratsmäßig gespeicherten Daten grundsätzlich auf solche Fälle beschränken, in denen bei der betroffenen Person ein Verdacht auf die Begehung einer schweren Straftat vorliegt. Abweichungen hiervon seien nur denkbar, wenn sich der Mitgliedstaat in einer Situation befindet, in der *vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind*.[439]

In formeller Hinsicht forderte der EuGH weiterhin, dass der Zugriff auf Vorratsdaten nur auf Antrag zulässig sein sollte, der vorab einer unabhängigen Prüfung durch eine Kontrollstelle unterzogen wurde.[440] Insofern ergab sich aus dem Urteil gegenüber der vorherigen Rechtsprechung nichts Neues. Dasselbe lässt sich über die abermals formulierten Anforderungen an die Datensicherheit und -transparenz sagen.[441]

(2) *La Quadrature du Net*: Ein Schritt zurück?

Die Hauptleistung von *Tele2Sverige/Watson* wurde überwiegend in der Übertragung der Rechtsprechung aus *Digital Rights Ireland* auf die nationalen Regeln erblickt, da die Unterschiede zu diesem Urteil in der Sache bei

437 *Mitsilegas/Guild/Kuskonmaz ua*., European Law Journal 2022 (online preprint), 1 (4).

438 Vgl. *Grabowska-Moroz* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 3 (8 ff.); *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (142 f.); *Roßnagel*, NJW 2017, 696 (697 ff.); *Priebe*, EuZW 2017, 136-130 (138).

439 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717.

440 Idem, Rn. 120 mit Verweis auf EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 62 = NJW 2014, 2169.

441 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 122 f. = NJW 2017, 717 mit Verweis auf Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 66 ff. = NJW 2014, 2169.

einer strengen Lesart eher gering ausfielen.[442] Jedenfalls bestand nun kein Zweifel mehr daran, dass universelle TK-Vorratsdatenspeicherungspflichten kaum mit den Unionsgrundrechten vereinbart werden konnten und laxe Zugriffsregelungen ohnehin nicht.

In den darauffolgenden Entscheidungen und deren Umsetzung durch nationale Gerichte sollte jedoch vor allem der in *Tele2Sverige/Watson* erstmals formulierten Ausnahmeregelung für besondere Bedrohungssituationen Bedeutung zukommen. Diese wurde in dem Urteil *La Quadrature du Net (ua.)* über die französischen und belgischen Regeln zur retrograden und zukunftsgerichteten Vorratsdatenspeicherung noch weiter ausdifferenziert.[443] Der EuGH bewegte sich damit weg vom absoluten Verbot der Vorratsdatenspeicherung und hin zu einer detaillierten *Prozeduralisierung*[444] im Sinne einer rechtsfortbildenden Verhältnismäßigkeitsprüfung.[445]

(a) Geltung der e-Privacy-RL bei Tätigkeit für Nachrichtendienste?

Anders als in den vorherigen Urteilen richteten sich die in *La Quadrature du Net* besprochenen Überwachungsmaßnahmen allerdings nicht auf die Strafverfolgung, sondern etablierten Datenverarbeitungspflichten der Telekommunikationsdienstleister für die Nachrichtendienste. Sowohl das französische als auch das belgische Recht sahen weiterhin vor, dass TK-Provider zur universellen Speicherung von Verkehrsdaten verpflichtet werden konnten, die dann u. a. den Nachrichtendiensten zur Verfügung gestellt werden mussten. Das französische Recht enthielt darüber hinaus die Ermächtigung der Nachrichtendienste, sich von den Anbietern spezifische Verkehrsdaten in Echtzeit übermitteln zu lassen. Außerdem wurden die Anbieter verpflichtet, ihre gespeicherten Daten mittels Datenanalyse nach

442 *Kipker/Schefferski/Stelter* ZD 2017, 124 (131 f.); vgl. auch *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (99 f.); s.a. die Nachweise zu (teils sehr) krit. Reaktionen bei *Grabowska-Moroz* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 3 (12).

443 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531.

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

445 Vgl. (zum BVerfG) *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82.

terrorismusverdächtigen Verbindungen zu durchsuchen und Treffer an die Nachrichtendienste zu übermitteln.[446]

Der sicherheitsrechtliche Zweck wurde zur Grundlage genommen, um abermals den Anwendungsbereich des Unionsrechts anzuzweifeln.[447] Ausgangspunkt hierfür war Art. 4 Abs. 2 S. 3 EUV, wonach die *nationale Sicherheit*, unter die insbesondere das Recht der Nachrichtendienste fällt[448], im alleinigen Verantwortungsbereich der Mitgliedstaaten verbleiben soll.

Der EuGH räumte diese Bedenken aus, indem er abermals eine Unterscheidung zwischen unmittelbar staatlicher Datenverarbeitung bzw. Überwachungstätigkeit und der entsprechenden Inpflichtnahme Privater vornahm.[449] Wie schon hinsichtlich des Spannungsverhältnisses zu Art. 1 Abs. 3 e-Privacy-RL[450] bemerkte er, dass Art. 15 Abs. 1 e-Privacy-RL zwangsläufig eine unionsrechtliche Determination für das Sicherheitsrecht herbeiführe. Es entspreche der gefestigten Rechtsprechung des Gerichtshofs, dass eine nationale Maßnahme nicht schon deshalb aus dem Anwendungsbereich des Unionsrechts falle, weil sie der nationalen Sicherheit diene.[451] Wie auch Art. 1 Abs. 3 e-Privacy-RL legte der EuGH also Art. 4 Abs. 2 S. 3 EUV letztlich eng aus und begrenzte dessen Zuständigkeitsabgrenzung auf staatliche Maßnahmen, an denen keine Private beteiligt sind.[452] Dazu verwies er insbesondere auch auf den mittlerweile in Kraft getretenen Art. 23 Abs. 1 lit. d) DSGVO, aus dem sich ebenfalls ergebe, dass private Datenverarbeitungen im Rahmen staatlicher Sicherheitsinteressen dem europäischen Datenschutz unterlägen.[453]

---

446 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 31 ff. = NJW 2021, 531.

447 Idem, Rn. 89; Vgl. *Sandhu*, EuZW 2021, 209 (221); GA *Campos Sánchez-Bordona*, Schlussantrag v. 15.01.2020, C-511/18, C-512/18 (la Qudadrature du Net ua.), Rn. 77 ff.

448 *Sule* in Dietrich/Sule (Hrsg.), Intelligence Europe, 2019, Chapt. 2 Rn. 19 ff.; s.a. *Cameron*, Int. J. of Intelligence and CounterIntelligence 33 (2020), 452 (454 ff.); *Karpenstein/Sangi*, GSZ 2020, 162 (167).

449 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 91 ff. = NJW 2021, 531.

450 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 99 = NJW 2017, 717; krit. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

451 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 91 ff. = NJW 2021, 531.

452 Ebenso, GA *Campos Sánchez-Bordona*, Schlussantrag v. 15.01.2020, C-511/18, C-512/18 (la Qudadrature du Net ua.) Rn. 77 ff.; dazu krit. *Cameron*, Int. J. of Intelligence and CounterIntelligence 33 (2020), 452 (459).

453 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 102 = NJW 2021, 531.

(b) Ausnahme vom Verbot der Vorratsdatenspeicherung in nationalen Bedrohungssituationen

Abermals stand daher infrage, ob die zu prüfenden nationalstaatlichen Regelungen nach Art. 15 Abs. 1 e-Privacy-RL, ausgelegt im Lichte der Art. 7, 8 EU-GRC, zulässig waren.

Einen bedeutenden Unterschied zu den vorher entschiedenen Fällen zur Vorratsdatenspeicherung erkannte der EuGH hier in der Zielsetzung von Vorratsdatenspeicherungsregimen, die der *nationalen Sicherheit* i. S. d. Art. 4 Abs. 2 EUV dienen. Diese gehe über die konkreteren in Art. 15 Abs. 1 e-Privacy-RL genannten Sicherheitszwecke, wie etwa der Bekämpfung von (auch schwerer) Kriminalität, hinaus.[454] Wie auch das BVerfG[455] geht der EuGH also von einer abstrakteren, gesamtheitlichen Sicherheitsgewährleistung der Nachrichtendienste aus, die den Staat in seiner Integrität schützt[456] und intendiert damit – ebenfalls gleich dem BVerfG–, dass für Überwachungsmaßnahmen zum Schutz der nationalen Sicherheit i. S. d. Art. 4 Abs. 2 EUV geringere Anforderungen gelten, wenngleich das BVerfG stets daran erinnert, dass sich die erweiterten Vorfeldbefugnisse der Nachrichtendienste nur rechtfertigen lassen, weil ihnen operative Möglichkeiten fehlen.[457] Dies ist in anderen EU-Ländern nicht zwingend der Fall.

Auch in formal-methodischer Hinsicht schlägt das Urteil eine etwas andere Richtung ein. Stand bei *Digital Rights Ireland* und *Tele2Sverige/Watson* noch der Grundsatz der Erforderlichkeit im Sinne *absoluter Notwendigkeit* im Vordergrund, erklärte der EuGH nunmehr, dass die schwere Beeinträchtigung der Art. 7, 8 EU-GRC zu den verfolgten Sicherheitsinteressen der Bevölkerung, wie sie in verschiedenen Rechten zum Ausdruck kommen[458], in einem *strikt angemessenen Verhältnis* stehen müsse. Neben der Beschränkung auf das absolut Notwendige müsse *darüber hinaus auch eine ausge-*

454 Idem, Rn. 136 f.

455 Vgl. BVerfGE 156, 11 (51 f.) – Antiterrordatei II; E 133, 277 (325 f.) – Antiterrordatei I; *Poscher/Rusteberg* KJ 2014, 57 (62 f.).

456 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 135 f. = NJW 2021, 531; so schon ausf. *Sule* in Dietrich/Sule (Hrsg.), Intelligence Europe, 2019, Chapt. 2 Rn. 19 ff., insbesondere Rn. 69 ff.

457 BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.);, NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Gusy*, GA 1999, 319 (327) *Gärditz*, JZ 2013, 633 (634); *Gusy*, GA 1999, 319 (327).

458 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 123 ff. = NJW 2021, 531.

wogene Gewichtung der dem Gemeinwohl dienenden Zielsetzung und der fraglichen Rechte vorgenommen werden.[459]

Im Ergebnis wirkte sich die Neuausrichtung auf den Angemessenheitsaspekt nicht aus. Weiterhin nutzte der EuGH die Verhältnismäßigkeitsprüfung dazu, die Effektivität[460] der Überwachung (dazu oben) zu gewährleisten, indem die Zulässigkeit der einzelnen Datenverarbeitungsschritte von bestimmten Anforderungen abhängig gemacht und damit eine Verknüpfung zum verfolgten Zweck hergestellt wurde.[461]

Solch eine ausreichende Verknüpfung zum Schutz der nationalen Sicherheit sah der EuGH grundsätzlich auch bei der Anordnung einer universellen Vorratsdatenspeicherungen gegeben. Anders als im Rahmen der Strafverfolgung oder der Gewährleistung der öffentlichen Sicherheit stünde Art. 15 Abs. 1 e-Privacy-RL hier nicht unbedingt entgegen. Voraussetzung sei jedoch, dass *hinreichend konkrete Umstände die Annahme zuließen, dass sich der betreffende Mitgliedstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersähe.*[462] Die in solchen Situationen gespeicherten Daten dürften auch automatisch analysiert werden (näher zur Datenanalyse unten II. 2. b. & c.).[463]

Über das Vorliegen einer solchen Bedrohung müsse vorab aber ein Gericht oder eine unabhängige Verwaltungsstelle entscheiden.[464]

Eine solche Ausnahme vom grundsätzlichen Verbot der Vorratsdatenspeicherung bei akuten, die nationale Sicherheit betreffenden Bedrohungslagen hatte der EuGH zwar schon in *Tele2Sverige/Watson* angedeutet.[465]

459 Idem, Rn. 129 f. mit Verweis auf EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 55 = NJW 2019, 655.

460 Vgl. zum Effektivitätsaspekt bei der Verhältnismäßigkeit von Überwachungsmaßnahmen *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 242 ff.; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 82 f., 14 ff.; *Stern,* StaatsR Bd. III/2, 1994, S. 836; aus der Rspr etwa BVerfGE 115, 166 (197 f.); insbesondere aber BVerfGE 141, 220 (268 ff.) – BKA-Gesetz.

461 Vgl. *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (148).

462 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 137 ff. = NJW 2021, 531.

463 Idem, Rn. 178.; s.a. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 176 ff. = EuZW 2022, 706.

464 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 139 = NJW 2021, 531.

465 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717.

Dass er damit nun ernst machte und mit dieser Möglichkeit das bisher verteidigte absolute Verbot der anlasslosen Vorratsdatenspeicherung von TK-Verkehrsdaten aufweichte, wurde in der Literatur dennoch mit einiger Ernüchterung aufgenommen[466] und teilweise auf politischen Druck der Mitgliedstaaten zurückgeführt.[467]

(c) Möglichkeiten bei der Kriminalitätsbekämpfung: anlasslose IP-Adressen-Speicherung, „Targeted Retention" und „Quick Freeze"

Was die Ziele der Verhütung und Verfolgung schwerer Straftaten anbelangte, verblieb der EuGH bei seiner bisherigen Einschätzung, dass eine universelle Vorratsdatenspeicherung von TK-Verkehrsdaten nicht angeordnet werden dürfe. Nur die „targeted retention"[468], also eine zielgerichtet persönliche und/oder zeitlich bzw. örtlich begrenzte Anordnung, könnte sich insofern im Rahmen des absolut Notwendigen bewegen. Für diese Feststellung zog er sämtliche in den vorherigen Urteilen aufgestellten Intensitätsparameter heran, stellte also sowohl auf die Datenqualität im Sinne der Möglichkeit eines Profiling als auch auf die Menge der betroffenen Grundrechtsträger und die damit verbundene Anlasslosigkeit ab.[469]

Auch hier differenzierte der EuGH nun aber weiter und schuf erstmals eine Ausnahme von den genannten Grundsätzen für die vorratsmäßige Speicherung der IP-Adressen von Internetnutzern im Rahmen der Bekämpfung schwerer Kriminalität.

Zwar seien auch diese als Verkehrsdaten zu qualifizieren, obwohl sich aus den Adressen lediglich ergebe, welches Endgerät bzw. welcher Nutzer eine Internetkommunikation über den jeweiligen Provider aufgebaut habe. Insofern handele es sich um weniger sensible Daten.[470] Mittelbar ergebe sich aus dieser Zuordnung allerdings die Möglichkeit nachzuvollziehen, welche Internetadressen ein Nutzer aufgebaut hat (etwa, weil die zugreifenden

466 *Ogorek*, NJW 2021, 531 (547): „Pyrrhussieg"; *Sandhu*, EuZW 2021, 209 (222); differenziert *Tzanou/Karyda*, European Public Law 28 (2022), 123.

467 *Zalnieriute*, Modern Law Rev. 85 (2022), 198 (213 ff.).

468 Vgl. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (101); *Cameron*, Common Market Law Rev. 58 (2021), 1433 (1449); *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (149).

469 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 140 ff. = NJW 2021, 531.

470 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 152, 157 = NJW 2021, 531.

IP-Adressen von den jeweiligen Servern protokolliert werden[471]). Auch die IP-Adressen könnten demnach zur Erstellung von Persönlichkeitsprofilen verwendet werden.[472]

Da jedoch die Bekämpfung bestimmter, mit dem Internet untrennbar verbundener Kriminalitätsformen, etwa der Kinderpornografie, unmöglich würde, wenn die IP-Adressen nicht gespeichert würden, sah der EuGH eine universelle Vorratsdatenspeicherung als verhältnismäßig an, wenn nur der Zugriff strikt genug ausgestaltet würde.[473]

Ebenfalls äußerte sich der EuGH zur zukunftsgerichteten Verkehrsdatenspeicherung in Echtzeit, dem sogenannten „Quick-Freeze"[474]. Bei Vorliegen bestimmter Anhaltspunkte dürften die Mitgliedstaaten Anordnungen regeln, die den Providern auferlegen, die aktuell vorhandenen und in Zukunft anfallenden Verkehrsdaten einer oder mehrerer Personen zu speichern, wenn dies zur Bekämpfung schwerer Kriminalität oder dem Schutz der nationalen Sicherheit notwendig ist.[475] Betroffen von solch einer Maßnahme dürfe nicht nur der jeweils Verdächtige sein, sondern auch Personen in dessen *sozialem oder beruflichem Umfeld oder in bestimmten geografischen Zonen, etwa an den Orten, wo die fragliche Straftat oder Beeinträchtigung der nationalen Sicherheit begangen oder vorbereitet wurde*.[476]

471 Dazu EuGH, Urteil vom 19.10.2016, C-582/14 (Breyer/Deutschland) = NJW 2016, 3579; zum Unterschied der IP-Abfrage und der Nutzung der IP in Folgeermittlungen vgl. *Kamp/Ebeling* in BeckOK POR NRW, PolG NRW § 20a Rn. 50 ff.; dazu auch BVerfGE 130, 151 (198 f.) – Bestandsdatenauskunft I.

472 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 153 = NJW 2021, 531.

473 Idem, Rn. 155 ff.

474 Dazu *Juszczak/Sason*, eucrim 2021, 238 (247); zur Rechtslage in der StPO: *Rückert* in MüKo StPO, § 100g Rn. 116; mittlerweile liegt allerdings ein Referentenentwurf des *BMJ* vor https://kripoz.de/wp-content/uploads/2022/10/refE-quick-freeze.pdf, zuletzt aufgerufen am 12.01.2025.

475 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 163 ff. = NJW 2021, 531.

476 Idem, Rn. 165.

(3) *Spacenet/Telekom*: Das (vorläufige) Aus der Vorratsdatenspeicherung in Deutschland

Die Grundsätze des EuGH aus *La Quadrature du Net* wurden jüngst hinsichtlich der deutschen Regelung zur Vorratsdatenspeicherung bestätigt.[477]

Die Bundesrepublik hatte Ende 2015 die Wiedereinführung der Vorratsdatenspeicherung überraschend[478] beschlossen[479] und dabei versucht, die damals vorliegenden Urteile des BVerfG und EuGH umzusetzen.[480] Die Speicherfrist wurde in § 113b a.F. TKG (heute § 176 TKG) auf 10 Wochen beschränkt und die Zugangsmöglichkeiten der Sicherheitsbehörden von hohen Anforderungen abhängig gemacht, § 113c a.F. TKG (heute § 177 TKG), vgl. etwa § 100g Abs. 2 StPO. Es handelte sich aber weiterhin um eine universelle Pflicht der TK-Provider, für die Strafverfolgungs- und Gefahrenabwehrbehörden Verkehrsdaten anlasslos zu speichern. Insofern schlug sich in der deutschen Regelung eine Lesart von *Digital Rights Ireland* nieder, die kein absolutes Verbot der Vorratsdatenspeicherung zur Verhütung und Verfolgung schwerer Kriminalität erkennen wollte (s. o.).[481]

Erwartungsgemäß regte sich denn auch gleich großer Widerstand gegen die deutsche Regelung. Zwar wies das BVerfG sämtliche Eilanträge gegen die neuen Regelungen ab.[482] Aufgrund der Ergänzungen des EuGH in der Sache *Tele2 Sverige* kamen jedoch verschiedene Verwaltungsgerichte zu dem Ergebnis, dass auch die aktuelle Version der Vorratsdatenspeicherung in der Bundesrepublik jedenfalls mit europäischen Grundrechten nicht zu vereinbaren sei.[483] Das BVerwG leitete deshalb ein Vorabentscheidungs-

477 EuGH, Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135.

478 *Roßnagel*, NJW 2016, 533 (534); zur Genese auch *Oehmichen/Mickler*, NZWiSt 2017, 298 (298 ff.).

479 Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218).

480 Dazu krit. *Wissenschaftliche Dienste des Bundestags,* WD 3 - 3000 - 108/15, Vorratsdatenspeicherung, 2015; *Roßnagel*, NJW 2016, 533 (538 ff.); *ders.*, NJW 2017, 696 (697 ff.); *Gercke*, ZUM 2016, 825 (826).

481 Vgl. *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.).

482 BVerfG, ZD 2016, 433; auch noch nach Erlass von *Tele2 Sverige*: BVerfG ZD 2017, 300.

483 OVG Münster, NVwZ-RR 2018, 43; VG Köln, ZD 2019, 187; Übersicht bei *Bär* in BeckOK StPO, § 175 TKG Rn. 15 ff.

verfahren ein.[484] Die Bundesnetzagentur setzte die Speicherpflichten der TK-Diensteanbieter nicht mehr aktiv durch.[485]

Der EuGH bestätigte vorhersehbar[486] die von den Verwaltungsgerichten vertretene Ansicht und erkannte in der deutschen Regelung über die Vorratsdatenspeicherung einen Verstoß gegen Art. 15 Abs. 1 e-Privacy-RL, interpretiert im Lichte der Art. 7, 8 EU-GRC.[487]

cc. Ausweitung der Rechtsprechung auf sämtliche Verkehrsdatenübermittlungen durch Private

Sämtliche bisher beschriebenen Urteile befassten sich im Kern mit Regelungen, die den Anbietern von Telekommunikationsdiensten selbst die Speicherung von Verkehrs- und Standortdaten auferlegten. Unterschiede bestanden nur dahingehend, dass Daten für verschiedene Behörden und folglich zu unterschiedlichen Zwecken aufbewahrt wurden.

Die Inpflichtnahme Privater war für den EuGH entscheidend, da sich erst daraus die Eröffnung des Anwendungsbereichs des EU-Rechts ergab.[488] Der Gerichtshof machte sich insofern die typische Struktur von Massenüberwachungsmaßnahmen zu eigen, die ohne eine Inpflichtnahme Privater kaum möglich wären und deshalb einen wirtschaftsrechtlichen Einschlag haben.

Die Mitgliedstaaten sahen und sehen diese Rechtsprechung insofern kritisch, als sich der EuGH über diesen Weg ein intensives Mitspracherecht bei der Zulässigkeit nationalstaatlicher Strafverfolgungs-, Gefahrenabwehr- und nachrichtendienstlicher Maßnahmen einräumt. Ein solches Mitspracherecht wähnten die Mitgliedstaaten durch Regelungen wie Art. 4 Abs. 2

484 BVerwG, NVwZ 2020, 1108.

485 *BNetzA,* Mitteilung zu § 113b TKG, 2017, https://web.archive.org/web/20210307231333/https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html , zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im Juli 2021); *Rückert* in MüKo StPO, § 100g Rn. 15.

486 *Roßnagel*, ZD 2022, 650 (651).

487 EuGH, Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 66 ff. = NJW 2022, 3135.

488 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; krit. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

EUV, Art. 3 Abs. 2 e-Privacy-RL und Art. 2 Abs. 2 lit. d) DSGVO aber gerade ausgeschlossen.[489]

Das stärkste Argument des EuGH dafür, nationale TK-Vorratsdatenspeicherungspflichten dem Anwendungsbereich des EU-Rechts zu unterstellen, war stets, dass Art. 15 Abs. 1 e-Privacy-RL ausdrücklich die Notwendigkeit vorsah, solche Regime verhältnismäßig auszugestalten. Es ist völlig richtig, dass die Norm keinen Sinn mehr hätte, wenn man Art. 3 Abs. 2 e-Privacy-RL weit auslegen und sämtliche sicherheitsrechtlichen Inpflichtnahmen der TK-Provider aus dem Geltungsbereich der Richtlinie herauslösen würde.[490]

Der Gerichtshof beließ es allerdings nicht dabei, allein die Pflichten zur Vorratsdatenspeicherung und sinnvollerweise die damit verwobenen Zugriffsregeln dem Anwendungsbereich des Unionsrechts, insbesondere der Charta nach Art. 51 Abs. 2 EU-GRC, zu unterstellen.

In den beiden bedeutenden Urteilen *Privacy International*[491] und *Prokuratuur*[492] erweiterte er seine Kompetenz dahingehend, dass sämtliche Überwachungsmaßnahmen im Bereich der Telekommunikationsdaten dem Unionsrecht unterfielen, solange die privaten Dienstleister auch nur irgendwie an dem Prozess beteiligt würden.[493] Diese Urteile stehen deshalb beispielhaft für die immer stärkere Europäisierung des Strafverfahrens[494] bzw. des Sicherheitsverfassungsrechts.

dd. Zusammenfassung und Fazit

Der EuGH hat mit seiner Rechtsprechung in den vergangenen knapp zehn Jahren eine bedeutende sicherheitsrechtliche Überwachungsmaßnahme maßgeblich rechtlich geprägt.

---

489 Vgl. EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 65 ff. = NJW 2017, 717; krit. auch *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, 397 f.; *dies.*, NJW 2021, 2079 (2081); *A. Baumgartner*, GSZ 2021, 36.

490 *Classen*, JZ 2019, 1057 (1062).

491 EuGH, Urteil v. 6.10.2020, C-623/17 (Privacy International), Rn. 30 ff. = GSZ 2021, 36.

492 EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 32 ff. = NJW 2021, 2103; s.a. Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 35 ff. = NJW 2019, 655 zu den Bestandsdaten.

493 *M. W. Müller/Schwabenbauer*, NJW 2021, 2079 (2082).

494 Dazu allg. *Safferling/Rückert*, NJW 2021, 287 (288 ff.).

Die Entscheidungsserie hat dem EuGH aufgrund seiner Positionierung als *Grundrechtsgericht* zwar viel Lob eingebracht[495], allerdings auch erheblichen Widerstand der Mitgliedstaaten hervorgerufen. Kritiker werfen dem Gerichtshof vor, mittels weiter Auslegung der e-Privacy-RL letztlich eine vollständige unionsrechtliche Überformung des nationalen Sicherheitsrechts eingeleitet zu haben. Der Gedanke, dass die nationalen Sicherheitsgesetze aufgrund der Inpflichtnahme Privater Teil des von der Union geprägten Wirtschafts- bzw. in diesem Rahmen geltenden Datenschutzrechts sein sollten[496], machten einige Mitgliedstaaten als reinen Vorwand des EuGH aus und sperrten sich gegen dessen Einmischung im Sicherheitsbereich.[497]

Der Gerichtshof hatte selbst zugegeben, dass die Pflicht zur Vorratsdatenspeicherung mitnichten auf eine Harmonisierung im Interesse der Provider abzielte, sondern ganz primär dem staatlichen Sicherheitsinteresse diente.[498] Entsprechend bleibt der Widerstand gegen die Aktivität des EuGH im Bereich der TK-Verkehrsdaten enorm.[499]

---

495 *Kühling*, NVwZ 2014, 681 (684 f.); *Granger/Irion*, Eur. Law Rev. 2014, 834 (844 ff.); *Wendel,* Wider die Mär vom Grundrechtsblinden, 09.04.2014, https://verfassungsblog.de/wider-maer-vom-grundrechtsblinden-eugh-und-vorratsdatenspeicherung/, zuletzt aufgerufen am 12.01.2025; *Prantl* – Ende der Maßlosigkeit, SZ vom 08.04.2014, https://www.sueddeutsche.de/politik/urteil-zur-vorratsdatenspeicherung-ende-der-masslosigkeit-1.1932057, zuletzt aufgerufen am 12.01.2025.

496 Vgl. EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 85 ff. = NJW 2021, 531; dazu *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap G Rn. 397 f.; *dies*., NJW 2021, 2079 (2080 f.); *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.); *A. Baumgartner*, GSZ 2021, 36 (43).

497 Vgl. EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 65 = NJW 2017, 717; *Zalnieriute*, Modern Law Rev. 85 (2022), 198 (207 ff.); *Cameron*, Common Market Law Rev. 58 (2021), 1433 (1458 f.); zu den Konsequenzen der Infpflichtnahme Privater für die grundrechtliche Bewertung vgl. BVerfGE 125, 260 (321) – Vorratsdatenspeicherung; *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff.; zur entsprechenden Diskussion im Geldwäscherecht vgl. *Degen,* Geldwäsche, 2009, S. 130 ff.; *Dahm/Hamacher*, wistra 1995, 206.; *Herzog*, WM 1996, 1753 (1762).

498 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 41 = NJW 2014, 2169; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 84 = NJW 2021, 531.

499 Vgl. *Mitsilegas/Guild/Kuskonmaz ua*., European Law Journal 2022 (online preprint), 1 (23 ff.); *Rojszczak*, Computer Law & Security Review 2021, 105572 (7 ff.).

Wie auch das BVerfG[500] betrachtete der Gerichtshof die Vorratsdatenspeicherung von TK-Verkehrsdaten als zweifachen Eingriff in den unionsgrundrechtlichen Schutz privater Daten, wobei er erstmals eine differenzierte Darstellung der Schutzbereiche von Art. 7 und 8 EU-GRC versuchte.[501] Entscheidend für die grundrechtliche Bewertung waren für den EuGH dann aber nicht die einzelnen Datenverarbeitungsschritte, die jeweils eigens einen Eingriff darstellten, sondern die Nachteile der Betroffenen, die sich gerade aus der finalen Kombination der Verarbeitungsschritte ergäben.[502] Damit prägte der EuGH die Art und Weise, wie sicherheitsrechtliche Maßnahmen der Massenüberwachung grundrechtlich zu fassen sind.

Das ursprünglich rigide Verbot der Vorratsdatenspeicherung ist mittlerweile zwar einem eher unübersichtlichen System verschiedener Ausnahmen und davon abhängender Gestaltungsformen gewichen.[503] In allen Fällen der zulässigen Speicherung sind aber stets strenge Anforderungen an die Verhältnismäßigkeit zu beachten. Dazu gehört insbesondere, dass der Zugang zu den gespeicherten Daten durch materielle und formelle Anforderungen, insbesondere durch eine unabhängige Vorabkontrolle der Zulässigkeit, eng begrenzt wird und datenschutzrechtliche Sicherheits- und Transparenzvorschriften flankierend erlassen werden.[504] Auch eine Unterrichtungspflicht gehört zu den unionsgrundrechtlichen Anforderungen.[505]

500 BVerfGE 125, 260 (309 f.) – Vorratsdatenspeicherung.

501 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 38 ff. = NJW 2014, 2169; dazu *Marsch,* Datenschutzgrundrecht, 2018, S. 202 ff.; *W. Michl*, DuD 2017, 349; *Nettesheim* in Grabenwarter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 52; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 23, 31 f.

502 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 ff. = NJW 2014, 2169; „*Mitsilegas/Guild/Kuskonmaz ua*., European Law Journal 2022 (online preprint), 1 (4): "holistic approach".

503 Vgl. *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143; übersichtlich die Tabelle bei *Mitsilegas/Guild/Kuskonmaz ua*., European Law Journal 2022 (online preprint), 1 (7).

504 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 54 ff. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 113 ff. = NJW 2017, 717; Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 31 ff. = NJW 2021, 2103; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 126 ff. = NJW 2022, 3135.

505 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 121 = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 190 ff. = NJW 2021, 531.

b. Bestandsdaten: Ministerio Fiscal

Die Rechtsprechung des EuGH ist nicht auf TK-Verkehrsdaten begrenzt. Auch zum Zugriff auf bei den Providern gespeicherten Identitäts- bzw. Bestandsdaten hat der Gerichtshof mittlerweile in der Sache *Ministerio Fiscal*[506] entschieden.

Bestandsdaten sind allerdings im europäischen Recht nicht ausdrücklich definiert. Die e-Privacy-RL kennt nur den Begriff der Verkehrsdaten, Art. 2 lit. b), der Vorschlag zur e-Privacy-VO nur die „Metadaten", Art. 4 Abs. 3 Lit a) b) c) e-Privacy-VO.[507] Entsprechend sieht die e-Privacy-RL auch keinen spezifischen Schutz der Bestandsdaten vor.

Der Begriff der Bestandsdaten findet sich hingegen ausdrücklich im deutschen Recht. § 3 Nr. 6 TKG definiert sie etwa als Daten, „die erforderlich sind für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste", also Daten, die die Identität des Vertragspartners und die Umstände des Vertrags betreffen.

Der Sache *Ministerio Fiscal* lag ein Strafverfahren zugrunde, in dem der Täter eines Handydiebstahls ermittelt werden sollte. Von dem Gerät war die IMEI-Nummer (International Mobile Station Equipment Identity)[508] bekannt, weshalb die Ermittler bei verschiedenen TK-Dienstleistern anfragten, ob sich in einer bestimmten Zeit eine SIM-Karte ihres Dienstes mit der bekannten IMEI in ein Netz eingewählt hatte, und wenn ja, welche Personendaten mit dieser SIM-Karte verbunden waren.[509] Es wurde also nicht nach den TK-Verbindungen gesucht, sondern allein nach der Identität einer Person.

Der EuGH nahm mangels gesetzlicher Definition keine dem deutschen Recht entsprechende formalistische Einteilung der angefragten Daten vor, sondern stellte lediglich fest, dass Art. 3 Abs.1 e-Privacy-RL die *Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommu-*

506 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal) = NJW 2019, 655.

507 Vorschlag der EU Kommission, COM(2017) 10 final - 2017/0003 (COD); zu den Begriffen auch *Schramm/Shvets*, MMR 2019, 568 (569 (Fn. 24)).

508 Teil der Bestandsdaten, wenn bei Vertrag überlassen, *Graf* in BeckOK StPO, § 100a Rn. 29.

509 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 19 ff. = NJW 2019, 655.

nikationsnetzen regle.[510] Somit fielen sämtliche Daten, die TK-Provider im Rahmen ihrer Tätigkeit verarbeiten, in den Geltungsbereich der Richtlinie.

Der Anwendungsbereich des Unionsrechts sei deshalb eröffnet, wenn solche Daten verarbeitet würden. Dies schließe den Zugriff staatlicher Behörden auch dann ein, wenn keine korrespondierende Speicherpflicht existiere, da der Zugriff durch Übermittlung der Provider erfolge, was zwangsläufig eine Verarbeitung durch diese mit sich bringe.[511]

Für die dem Fall zugrunde liegenden Daten gelte daher im Grunde nichts anderes als für Verkehrsdaten. Da die Übermittlung eine Verarbeitung darstelle, die die von Art. 5 Abs. 1 e-Privacy-RL geschützte Vertraulichkeit der Kommunikation betreffe, richte sich die Zulässigkeit nach Art. 15 Abs. 1 e-Privacy-RL im Lichte der Art. 7, 8 EU-GRC.[512]

Danach kommt es auf die Verhältnismäßigkeit der Maßnahme an. Diese wiederum ist von der Intensität der Maßnahme abhängig. Aus den Urteilen zur Speicherung und Abfrage von Verkehrsdaten ergibt sich insofern nur, dass schwere Eingriffe nur zur Bekämpfung schwerer Kriminalität gerechtfertigt sein können. Schwache Eingriffe sind schon zur Bekämpfung allgemeiner Kriminalität zulässig.[513]

Um Letztere handelt es sich bei der Abfrage von Daten, aus denen sich nur die Identität eines TK-Nutzers ergibt, da sich aus diesen keine umfangreichen Schlüsse über das Privatleben der betroffenen Person ableiten lassen.[514] Die Abfrage von Bestandsdaten ist danach also auch zur allgemeinen Verbrechensbekämpfung zulässig.

2. Fluggastdaten

Neben den Telekommunikationsdaten war auch schon die sicherheitsrechtliche Überwachung von Fluggastdaten (*Passenger Name Records* - PNR) Gegenstand der Rechtsprechung des EuGH.

Bei den PNR ist eine Einteilung in verschiedene Datenkategorien analog zu der Dreiteilung der Kommunikationsdaten in Bestands-, Verkehrs- und

510 Idem, Rn. 33 ff.
511 Idem, Rn. 35 ff.; bestätigt durch EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 35 = NJW 2021, 2103.
512 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 48 ff. = NJW 2019, 655.
513 Idem, Rn. 56 f.
514 Idem, Rn. 69.

Inhaltsdaten nicht möglich. Die Bezeichnung stellt daher stets auf sämtliche Umstände eines Passagierfluges ab. Die aktuelle europäische PNR-Richtlinie[515] ist umfangreich und erfasst nicht nur die Adress- und Identitätsdaten des Passagiers und der Eigenschaften des jeweiligen Flugs, etwa Start- und Zielflughafen, Abflugdatum, Start- und Landezeit sowie der Flugscheindaten bzw. -Nummer, sondern unter anderem auch Namensangaben der Sitznachbarn oder den Vielfliegereintrag nach Art. 6 Abs. 2 PNR-RL, § 2 Abs. 2 FluGDaG.

a. PNR-Abkommen mit den USA

Seinen Ursprung nahm die sicherheitsrechtliche Verwendung von Fluggastdaten in den entsprechenden Abkommen der EU mit den USA, die als Reaktion auf die Terroranschläge von 2001 abgeschlossen wurden.[516]

Schon nach der EU-Datenschutzrichtlinie (DSRL)[517] war eine Datenübermittlung in Drittländer nur zulässig, wenn die Übermittlung im Rahmen einer Angemessenheitsentscheidung der Kommission nach Art. 25, 31 Abs. 2 EU-Datenschutz-Rl für zulässig erachtet wurde. Da aber stets auch eine rechtliche Grundlage für die Datenübermittlung nötig war, ging die Kommission davon aus, dass ein begleitendes Abkommen abgeschlossen werden musste – auch, um solche Rechtsfragen zu klären, die nicht in der Angemessenheitsentscheidung adressiert werden konnten.[518]

515 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.

516 Ausf. zur Historie *Baumann,* Datenschutzkonflikte, 2016, S. 412 ff.

517 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995, L 281/31; konsolidierte Fassung: Dokument 01995L0046-20031120.

518 *Europäische Kommission*, Commission Staff Working Paper – An EC-U. S. Agreement on Passenger Name Records (PNR) vom 31.01.2004, SEC(2004) 81, S. 3

aa. EuGH-Entscheidung zum PNR-Abkommen USA 2004

Ein erstes solches Abkommen wurde am 17.05.2004 vom Rat beschlossen[519] und trat am 28.05.2004 mit der Unterzeichnung durch die USA und Ratifizierung durch das EU-Parlament in Kraft.[520]

Das Abkommen blieb hinsichtlich seines Inhalts noch ziemlich vage. Auf gerade einmal zwei Seiten wurde vor allem vereinbart, dass das Bureau of Customs and Border Protection (CBP) des United States Department of Homeland Security (DHS) *elektronischen Zugriff auf PNR-Daten aus den von den Fluggesellschaften im Hoheitsgebiet der EG betriebenen Buchungssysteme erhält, solange kein befriedigendes System für die Übermittlung solcher Daten durch die Fluggesellschaften vorhanden ist.*

Die eigentlichen Regelungen des Abkommens ergaben sich erst aus einer Zusammenschau mit der Angemessenheitsentscheidung[521] i. S. d. Art. 25, 31 Abs. 2 EU-Datenschutz-Rl, die die Kommission kurz zuvor erlassen hatte, und die wiederum eine Verpflichtungserklärung des CBP als Anhang enthielt, in dem die US-Behörde über die rechtlichen Umstände der von ihr geplanten Datenverarbeitung aufklärte.

Der Zugriff des CBP sollte danach nur für Flüge in die und aus den USA ermöglicht werden. Der Katalog der PNR-Daten war umfassend und enthielt im Prinzip sämtliche Daten, die die Fluggesellschaften über die Passagiere anlegten: vom Namen des Passagiers über die Flugscheindaten bis hin zum zuständig gewesenen Bearbeiter im Reisebüro.[522]

Gegen das Abkommen und die Angemessenheitserklärung der Kommission erhob das EU-Parlament Klage vor dem EuGH.

Als Kernargument wurde vorgetragen, dass die für die Rechtmäßigkeit der Datenübermittlung in ein Drittland (unbestritten) notwendige Ange-

519 Abkommen zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika uber die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security, ABl. 2004, L 183/83.

520 Vgl. EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA), Rn. 32 = NJW 2006, 2029; *Nitschke* Jahrbuch Terrorismus 2007, 209 (209 Fn 1); zur Historie *Baumann,* Datenschutzkonflikte, 2016, S. 424 ff.; *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (901 ff.);

521 Entscheidung der Kommission vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Passenger Name Records enthalten sind, welche dem United States Bureau of Customs and Border Protection übermittelt werden, Abl. 2004, L 235/11.

522 Anhang A Verpflichtungserklärung CBD, Abl. 2004, L 235/11(21).

messenheitsentscheidung der Kommission i. S. d. Art. 25, 31 Abs. 2 DS-RL nicht ergehen hätte dürfen, da ihr Regelungsziel nicht in den Anwendungsbereich der Richtlinie fiel.[523] Art. 3 Abs. 2 der DSRL nahm Verarbeitungen vom Anwendungsbereich der Richtlinie aus, die *die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich* [betrafen].

Dieser Argumentation folgte der Gerichtshof. Zwar würden die Daten von privaten Wirtschaftsteilnehmern erhoben, die konkrete Übermittlung erfolgt aber allein aufgrund der staatlichen Rahmensetzung und diente der öffentlichen Sicherheit.[524] Insofern legte der EuGH den Anwendungsbereich der DSRL deutlich enger aus als bei der Vorratsdatenspeicherung von Verkehrsdaten im Rahmen der e-Privacy-RL.[525]

Auch dem Beschluss des Rats der EU (und damit dem Abkommen selbst) wurde primär die fehlende Kompetenz entgegengehalten. Als Rechtsgrundlage wurde – wie später abermals bei der TK-Vorratsdatenspeicherung (s. o. II. 1. aa. (1))[526] – Art. 95 Abs. 1 EG[527] (heute Art. 114 Abs. 1 AEUV) herangezogen, der die EU zur Harmonisierung der Wirtschaft ermächtigte.

Der EuGH folgte konsequent dem Vortrag des Parlaments. Er befand, dass die Richtlinie tatsächlich nicht primär der Harmonisierung diente, sondern der öffentlichen Sicherheit. Die Rechtsgrundlage hätte daher in der „dritten Säule“[528] der EU gesucht werden müssen.[529] Von dieser Ansicht rückte der Gerichtshof hinsichtlich der Vorratsdatenspeicherung von

523 EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA), Rn. 51 = NJW 2006, 2029.

524 Idem, Rn. 57 f.

525 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 73 ff. = NJW 2017, 717; so auch *Boehm/Cole* ZD 2014, 553 (555); *Granger/Irion*, Eur. Law Rev. 2014, 834 (848); *Kühling/Heitzer*, Eur. Law Rev. 40 (2015), 263 (267); krit. *Wollenschläger/Krönke*, NJW 2016, 906 (907 f.).

526 EuGH, Urt. v. 10.2.2009, C-301/06 (Irland / Parlament und Rat) = MMR 2009, 244.; krit. *Ambos*, JZ 2009, 466 (470 f.).

527 Vertrag zur Gründung der Europäischen Gemeinschaft, Konsolidierte Fassung 2002, Abl. 2002, C 325/1.

528 Vgl. *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (888 ff.).

529 EuGH, Urteil v. 30.6.2006, C-317/04 (PNR Abkommen USA), Rn. 67 ff. = NJW 2006, 2029.

TK-Verkehrsdaten später ab. Er begründete dies damit, dass dort nur eine Speicherung und keine Übermittlung geregelt worden war.[530]

Unabhängig davon, dass der „Erfolg" von kurzer Dauer war, wurde das Urteil im Nachgang als Pyrrhussieg[531] bezeichnet, da es sich inhaltlich nicht mit der Rechtmäßigkeit der PNR-Sammlung und Übermittlung auseinandersetzte und durch die rein formelle Argumentation die Gesetzgebung allenfalls zu einem neuen Versuch aufforderte.

bb. PNR-Abkommen EU-USA 2007 und 2012

Das Urteil des EuGH brachte die Airlines in die Bredouille. Die amerikanische Rechtslage verpflichtete sie zur Datenübermittlung an das DHS, während das Europäische Datenschutzrecht eine solche mangels gültiger Kommissionsentscheidung untersagte. Es stand bereits der Vorschlag im Raum, keine Flüge zwischen den USA und der EU zuzulassen, da nur so ein (global) rechtmäßiges Verhalten der Airlines gesichert werden könnte.[532] Im Jahr 2007 kam es deshalb zu einem neuen Abkommen[533] zwischen der EU und den USA – diesmal gestützt auf die Art. 24, 38 des EUV[534] (Nizza).[535]

Das Abkommen war wieder vage und kurzgehalten. Substanziell ergänzt wurde es, ähnlich dem Abkommen von 2004, durch eine Erklärung des DHS, das sogenannte „DHS-Schreiben", auf das in Nr. 1 der Erwägungsgründe des Abkommen ausdrücklich Bezug genommen wurde.[536]

---

530 EuGH, Urt. v. 10.2.2009, C-301/06 (Irland / Parlament und Rat) = MMR 2009, 244.; krit. *Ambos*, JZ 2009, 466 (470 f.); s.a. *Flynn* UC Dublin Law Rev. 8 (2008), 1 (11 f.); *Westphal*, EuR 2006, 706 (712 f.); *Gitter/Schnabel*, MMR 2007, 411 (412 f.) *Breyer*, StV 2007, 214 (215 f.).

531 *Maxian Rusche/Kullak* in Grabitz/Hilf/Nettesheim Recht der EU, AEUV Art. 100 Rn. 147.

532 *Nitschke*, Jahrbuch Terrorismus 2007, 209 (210).

533 Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS) (PNR-Abkommen von 2007), ABl. 2007, L 204/18.; zur Historie ausf. *Baumann,* Datenschutzkonflikte, 2016, S. 461 ff.

534 Vgl. Beschluss 2007/551/GASP/JI des Rates vom 23. Juli 2007, ABl. 2007, L 204/16.

535 Konsolidierte Fassung des Vertrags über die Europäische Union, ABl. 2002, C 325/01.

536 Dazu krit. *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (910 ff.).

Obwohl mit dem Abkommen von 2007 eine weitreichende Zugriffsmöglichkeit für die US-Behörden geschaffen worden war, herrschte auf beiden Seiten des Abkommens Unzufriedenheit.[537] Daher wurde das Abkommen revidiert und 2012 durch ein Drittes ersetzt[538], das nunmehr nach dem Verfahren des Art. 218 AEUV und daher mit Zustimmung des EU-Parlaments zustande kommen musste.[539]

Es enthielt erstmals selbstständig eine ausführliche Regelung, ohne auf Zusatzerklärungen wie das „DHS-Schreiben" zu verweisen. Inhaltlich wurden die bestehenden Intensitätsmerkmale allerdings erneut ausgeweitet.

Das PNR-Abkommen mit den USA stand und steht ebenso wie die entsprechenden Abkommen mit Australien[540] und Kanada in der Kritik[541], auch aufgrund der heute strengen Rechtsprechung des EuGH hinsichtlich der Übermittlung persönlicher Daten in Drittstaaten.[542] Diese soll nach Erwägungsgrund 102 der DSGVO zwar bei entsprechenden Abkommen weiterhin möglich sein, ohne dass die Bedingungen der Art. 45 ff. DSGVO erfüllt sein müssen. Der EuGH leitet die Notwendigkeit einer Schutzäquivalenz aber aus den EU-Grundrechten ab und stellt somit auch an die Abkommen hohe Anforderungen, wie sogleich zu zeigen sein wird. Zum heutigen Zeitpunkt haben die PNR-Abkommen mit den USA und Australien jedoch weiterhin Bestand.

537 Vgl. *Baumann,* Datenschutzkonflikte, 2016, S. 476 ff.; *Hert/Papakonstantinou*, Common Market Law Rev. 46 (2009), 885 (917 ff.).

538 Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security, ABl. 2012, L 215/15.

539 *Baumann,* Datenschutzkonflikte, 2016, S. 476 ff.

540 Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records — PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service, ABl. 2012, L 186/3, berichtigt in Abl. 2012, L 302/14.

541 Übersichtlich *Gleß/Wahl* in Schomburg/Lagodny, Int. Rechtshilfe Strafsachen, III B 4ab FlugastAbkEU-USA Rn. 8 ff.

542 Zur USA insbesondere EuGH, Urt. v. 06.10.2015, C-362/14 (Schrems I) = NJW 2015, 3151; Urt. v. 16.07.2020, C-311/18 (Schrems II) = NJW 2020, 2613

b. EuGH-Gutachten zum PNR-Abkommen EU – Kanada

Das geplante PNR-Abkommen mit Kanada[543] ist hingegen nicht zustande gekommen, da es der EuGH in einem Gutachten für rechtswidrig befand.[544] Inhaltlich entsprach das geplante Kanada-Abkommen weitestgehend jenem mit den USA. Die Fluggesellschaften sollten bei Flügen zwischen der EU und Kanada verpflichtet werden, umfangreiche PNR-Daten an eine kanadische Behörde zu übermitteln. Dort hätten die Daten insgesamt für fünf Jahre gespeichert werden sollen, wobei nach dreißig Tagen eine erste und nach zwei Jahren eine weitere Anonymisierung vorgeschrieben war, Art. 16 PNR-Abkommen-Kanada. Die Daten sollten nach Aussage des Generalanwalts hauptsächlich *automatisierten Analysen unterzogen werden, die auf im Voraus festgelegten Modellen und Kriterien und dem Abgleich mit verschiedenen Datenbanken* beruhten und vor Ankunft des Flugzeugs stattfinden sollten.[545] Diese automatisierte Analyse wurde im Abkommen allerdings nicht ausdrücklich geregelt, sondern lediglich in Art. 15 vorausgesetzt, nach dem Kanada *Entscheidungen, die einen Fluggast erheblich beeinträchtigen, nicht allein auf der Grundlage der automatisierten Verarbeitung von PNR-Daten treffen sollte.*

Bei dem PNR-Abkommen mit Kanada sollten also verschiedene Überwachungsformen, namentlich die automatische Datenanalyse und die Vorratsdatenspeicherung, miteinander verknüpft werden.[546] Aufgrund der deshalb absehbaren Grundrechtsrelevanz forderte das Europäische Parlament ein Gutachten des EuGH nach Art. 218 Abs. 11 AEUV an.

Der Gerichtshof erkannte zunächst, dass aufgrund des PNR-Abkommens in Art. 7 *und* 8 EU-GRC eingegriffen werden sollte, und zwar eigen-

543 Empfehlung für einen Beschluss des Rates zur Genehmigung der Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und Kanada über die Übermittlung und Verwendung von Fluggastdatensätzen (Passenger Name Records – PNR) zu Zwecken der Verhütung und Bekämpfung von Terrorismus und sonstiger grenzübergreifender schwerer Kriminalität vom 18.10.2017, COM(2017) 605.

544 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 154 ff. = ZD 2018, 23.

545 Idem, Rn. 130 ff. mit Verweis auf, GA *Mengozzi,* Schlussanträge v. 08.09.2016, Gutachten 1/15 (PNR Canada), Rn. 252; s.a. *Europäische Kommission,* Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer vom 21.09.2010, KOM(2010) 492 e, S. 4 ff.

546 Vgl. zum FlugDaG: *Ruthig* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, FlugDaG Vorb Rn. 3.

ständig jeweils durch die Datenübermittlung der Airlines, die Speicherung bei der kanadischen Behörde und die Möglichkeit der Weitergabe an Behörden in Kanada und weiteren Drittstaaten.[547] Durch das Abkommen würden die PNR-Daten sämtlicher Fluggäste zwischen der EU und Kanada überwacht.[548]

Sodann widmete sich der Gerichtshof der Frage, ob diese Eingriffe gerechtfertigt wären. Dabei bemühte er die aus *Digital Rights Ireland* bekannte Vermischung aus Bestimmtheit und Erforderlichkeit (s. o. II. 1. a. aa. (2) (b)).[549]

Erste Mängel identifizierte der EuGH bei der Bestimmtheit einzelner PNR-Datenrubriken, da diese durch offene Aufzählungen wie etwa „sämtliche verfügbaren Kontaktangaben" oder der Verwendung von „etc." nicht hinreichend klar zu erkennen geben, welche Daten gemeint sind.[550] Die Umschreibungen waren insofern nicht auf das Notwendigste beschränkt

Einen weiteren Grundrechtsverstoß hinsichtlich der zu verarbeitenden Daten erkannte der EuGH in dem fehlenden Ausschluss besonders sensibler Daten. Deren Verarbeitung lässt sich nicht mit der Bekämpfung von Terrorismus und schwerer Kriminalität rechtfertigen, denn dies müsste konsequenterweise bedeuten, dass Kenntnisse über sensible Merkmale (Herkunft, Rasse, Religion etc.) bei der Bekämpfung hilfreich bzw. notwendig sein könnten. Darin läge eine immanente Diskriminierung.[551]

Zu den Datenverarbeitungen selbst äußerte sich der EuGH weniger absolut. Hinsichtlich der automatischen Datenanalyse etwa folgte er den Ausführungen des Generalanwalts dahingehend, dass das Eingriffsgewicht insbesondere von der Fehlerquote und dem Diskriminierungspotential abhängen würde, was wiederum von den verwendeten Modellen, Kriterien und Datenbanken abhängig sei, anhand derer der Abgleich durchgeführt wurde. Um die Verhältnismäßigkeitsbedingungen zu erfüllen, *müsse deren Zuverlässigkeit und Aktualität unter Berücksichtigung statistischer Daten*

547 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 125 = ZD 2018, 23

548 Idem, Rn. 127.

549 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 54 = NJW 2014, 2169; vgl. dazu *Schwerdtfeger* in Meyer/Hölscheidt EU-GRC, Art. 52 Rn. 31.

550 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 155 ff. = ZD 2018, 23

551 Idem, Rn. 165.

und der Ergebnisse der internationalen Forschung, Gegenstand einer gemeinsamen Überprüfung seiner Durchführung sein.[552]

Wie auch in den Urteilen zur Vorratsdatenspeicherung kritisierte der Gerichtshof aber, dass auch solche Daten übermittelt und analysiert wurden, bei denen im (Moment der Verarbeitung) keine Hinweise darauf bestehen, dass die Verarbeitung für den sicherheitsrechtlichen Zweck des Abkommens förderlich ist. Anders als noch hinsichtlich der universellen Speicherung von Verkehrsdaten bemerkte der EuGH aber ausdrücklich, dass gerade in der Universalität der Sinn der Analyse liege, da erst aus dem Abgleich aller verfügbaren Daten eine automatische Identifizierung verdächtiger Muster möglich würde.[553] Außerdem erfolgten auch die bei der Ankunft stets notwendigen Grenzkontrollen im Ergebnis anlasslos, weshalb Flugpassagiere universell mit einer Verarbeitung ihrer Daten im Rahmen von Flugreisen rechnen müssten.[554] Dass die Datenanalyse sämtliche Fluggäste betraf, stellte für den EuGH deshalb keine Verletzung der Art. 7, 8 EU-GRC dar.

Anders begegnete er der Speicherung der PNR-Daten. Bei diesem Verarbeitungsschritt differenzierte der EuGH zwischen der Ankunft der Fluggäste, der Zeit des Aufenthalts in Kanada und der Ausreise.

Die Speicherung und Verwendung bei der Anreise sah der Gerichtshof grundsätzlich als unproblematisch an, da in dieser Zeit die Daten schon zur Abwicklung der Grenzkontrollen sinnvoll sein könnten und außerdem das Ergebnis der automatischen Analyse gerade dann zur Terrorismus- und Kriminalitätsbekämpfung sinnvoll zu weiteren Maßnahmen führen könnte. [555] Allerdings sei zu beachten, dass mit der Gestattung der Einreise trotz durchgeführter Analyse letztlich zum Ausdruck gebracht wird, dass in diesem Moment keine entsprechende Gefährdung durch die jeweilige Person vorliegen kann. Daher müsse für die Zeit des Aufenthalts in Kanada ein eigenständiger Grund für die Speicherung vorliegen.[556] Mangels einer solchen Bedingung im Abkommen sei dieses schon deshalb unverhältnismäßig.

552 Idem, Rn. 174.
553 Iden, Rn. 187.
554 Idem, Rn. 188; ähnlich der Vergleich anlassloser Kennzeichenüberwachung mit Grenzkontrollen bei *Möstl*, GSZ 2019, 101 (105 ff.).
555 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 197 ff. = ZD 2018, 23.
556 Idem, Rn. 200.

Noch strenger aber behandelte der EuGH die Speicherung von PNR-Daten nach der Ausreise der betroffenen Personen. Da diese im Zeitpunkt der Ausreise mindestens zweimal kontrolliert würden, sei in diesem Moment sichergestellt, dass die Verarbeitung ihrer Daten den Zweck des Abkommens nicht mehr fördern könnte. Insofern handelt es sich um eine anlasslose Speicherung, die entsprechend den Erkenntnissen aus *Tele2Sverige/Watson* (s.o.)[557] nicht mit der Bekämpfung von Terrorismus und schwerer Kriminalität gerechtfertigt werden kann.[558]

Aufgrund all dieser Mängel erklärte der EuGH das geplante Abkommen der EU mit Kanada für unvereinbar mit Art. 7, 8 EU-GRC. Von einem Beschluss des Abkommens wurde entsprechend abgesehen. Stattdessen empfahl die Kommission, neue Verhandlungen mit Kanada anzutreten.[559] Ein Ergebnis solcher Verhandlungen liegt aktuell noch nicht vor.

c. Das EuGH-Urteil zur PNR-Richtlinie

Parallel zu den Abkommen mit Drittstaaten etablierte die EU ein für die Mitgliedstaaten verpflichtendes PNR-System für Flüge zwischen Drittstaaten und der EU in Form der PNR-RL,[560] die in Deutschland durch das FluGDaG umgesetzt wurde.[561]

Die Airlines sollen vor dem Start von Flügen in und aus der EU, von oder in Drittstatten die Fluggastdaten per Push-Verfahren an eine zentrale Meldestelle des Mitgliedstaates übermitteln, aus dem der Flug startet bzw.

557 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717.

558 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 207 = ZD 2018, 23.

559 *Europäische Kommission,* Empfehlung für einen Beschluss des Rates zur Genehmigung der Aufnahme von Verhandlungen über ein Abkommen zwischen der Europäischen Union und Kanada über die Übermittlung und Verwendung von Fluggastdatensätzen (Passenger Name Records – PNR) zu Zwecken der Verhütung und Bekämpfung von Terrorismus und sonstiger grenzübergreifender schwerer Kriminalität vom 18.10.2017, COM(2017) 605 final.

560 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).

561 Zur Historie *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 248 ff.; *Kostov*, GSZ 2022, 267 (267 ff.); *Orrù*, Information Polity 27 (2022), 131 (132 ff.); *Lowe*, ICLR 17 (2017), 78 (85 ff.).

in dem er landet, Art. 8 Abs. 1 PNR-RL. Dabei ist zu beachten, dass die Mitgliedstaaten ermächtigt wurden, die Richtlinie auf Flüge innerhalb der EU auszuweiten, Art. 2 PNR-RL.

Bei der zentralen Meldestelle können die PNR-Daten nach Art. 6 Abs. 3 PNR-RL abgeglichen werden mit *Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, einschließlich Datenbanken, betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind, unter Einhaltung der für solche Datenbanken einschlägigen nationalen, internationalen und* Unionsvorschriften (lit. a), oder *anhand im Voraus festgelegter Kriterien*. Im letzten Fall ist sicherzustellen, dass die Kriterien nicht auf sensiblen bzw. diskriminierenden Faktoren beruhen (Art. 6 Abs. 4 PNR-RL.

Die Daten werden bei der zentralen Meldestelle für fünf Jahre gespeichert, wobei nach sechs Monaten eine Anonymisierung stattfindet, die nur unter strengen Auflagen rückgängig gemacht werden kann, Art. 12 PNR-RL. Die zentrale Meldestelle soll bei begründeten Anfragen zuständiger Behörden PNR-Daten zur Verfügung stellen und verarbeiten bzw. die Ergebnisse der Verarbeitung zur Verfügung stellen und zwar in *besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität*, Art. 6 Abs. 2 lit. b) PNR-RL.

Dieses PNR-Überwachungsregime wurde jüngst vom EuGH in der Entscheidung *Ligue des droits humains* auf seine Vereinbarkeit mit europäischen Grundrechten, insbesondere Art. 7, 8 EU-GRC, überprüft.[562]

Dabei wählte der EuGH eine fragwürdige Vorgehensweise.[563] Er beanstandete zwar viele Inhalte der Richtlinie, anstatt sie aber deshalb aufzuheben, gab er lediglich vor, wie die Richtlinie an den entsprechenden Stellen ausgelegt werden muss, um nicht gegen Art. 7, 8 EU-GRC zu verstoßen. In manchen Fällen handelt es sich dabei um eine Auslegung *contra legem*.

Die Ausweitung auf EU-interne Flüge etwa hielt der EuGH nur für gerechtfertigt, wenn der Mitgliedsstaat sich in einer spezifischen Bedrohungs-

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

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

situation befände.[564] Insofern übertrug er die aus *La Quadrature du net* bekannte Ausnahmeregel[565] auf die Ausweitung der PNR-Überwachung. Obwohl aber in Art. 2 PNR-RL nichts von einer solchen Begrenzung steht, durfte die Vorschrift in Kraft bleiben. Hier handelt es sich um eine teleologische Reduktion. Auch bei der Bestimmtheit der im Katalog des Anhang 1 aufgeführten PNR-Daten monierte der Gerichtshof mehrere Rubriken, stellte dann aber fest, dass diese klar und präzise formuliert sind, wenn man sie nur anhand der Urteilserwägungen auslegt.[566]

Der Effekt dieser Methode ist, dass der EuGH faktisch eine neue Richtlinie geschaffen hat, deren Inhalt sich nur aus dem Gesetzestext in gemeinsamer Lesung mit dem hierzu ergangenen Urteil erschließt.[567]

Inhaltlich entsprechen diese verhältnismäßigkeitswahrenden Auslegungsanforderungen weitestgehend dem Gutachten des EuGH zum PNR-Abkommen mit Kanada. Der Gerichtshof ging allerdings noch spezifischer auf die Zweckbindung der PNR-Datenverarbeitung ein.

Da das PNR-System zu einer anlasslosen, kontinuierlichen Überwachung der Fluggäste führt, handelt es sich um einen schwerwiegenden Eingriff, der nur dann gerechtfertigt sein kann, wenn er unmittelbar zu den mit der Richtlinie verfolgten Zwecken in Zusammenhang steht. Die einzelnen Datenverarbeitungsschritte der Fluggastüberwachung kommen daher nur infrage, wenn die verfolgten Zwecke derart mit Flugreisen in Zusammenhang stehen, sodass die Überwachung des Flugverkehrs insofern sinnvoll erscheint. Dies sei bei Terrorismus grundsätzlich anzunehmen, bei schwerer Kriminalität allerdings nicht. Die Richtlinie muss daher so interpretiert werden, dass das Überwachungssystem nur zur Bekämpfung solch schwerer Kriminalität verwendet werden darf, die *wenigstens mittelbar in objektivem Zusammenhang mit der Beförderung von Fluggästen* steht.[568] Hierbei ist etwa an den Menschenhandel, Handel mit Drogen und

564 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 166 ff. = EuZW 2022, 706.

565 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 137 ff. = NJW 2021, 531.

566 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 155 ff. = EuZW 2022, 706.

567 Dazu krit. *Thönnes*, Die Verwaltung 2022, 527 (531 ff., 539); ders., Die Verwaltung 2022, 527 *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

568 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 140 = EuZW 2022, 706.

Waffen, Beihilfe zur illegalen Einreise und zum illegalen Aufenthalt oder auch an Flugzeugentführungen zu denken.[569] Anhand dieser engeren[570] Zweckbestimmung als Auslegungsgrundsatz untersuchte der EuGH dann die einzelnen Datenverarbeitungsschritte.

Wie schon im Kanada-Gutachten kam er zu dem Ergebnis, dass eine automatisierte Datenanalyse vor der Landung grundsätzlich mit Art. 7, 8 EU-GRC vereinbar ist, wenn ausreichende Kontrollmechanismen eingeführt würden. Um die enge Bindung an den Richtlinienzweck zu gewährleisten, dürfen zum Abgleich nur Datenbanken verwendet werden, in denen Daten von Personen gespeichert sind, bei denen ein objektiver Verdacht auf einen Zusammenhang mit Terrorismus oder (grenzübergreifender) schwerer Kriminalität besteht, und nach denen deshalb gefahndet wird.[571] Der Datenbankabgleich muss also auf einen speziellen Fahndungsabgleich hinauslaufen.

Weiter muss gesichert sein, dass keinerlei weitere nachteilige Grundrechtseingriffe allein auf Grundlage des automatisierten Abgleichs erfolgen.[572] Stets muss der „Treffer" menschlich nachgeprüft werden. Insofern erkannte der EuGH ein Recht auf menschliche Entscheidung und brachte den persönlichen Datenschutz gegen die aufkommende Tendenz zum Einsatz künstlicher Intelligenz in Stellung.[573] Diesen Ansatz verfolgte er weiter, indem er den alleinigen Einsatz künstlicher Intelligenz bei der Bestimmung der *im Voraus festgelegter Kriterien* zum Datenabgleich i. S. d. Art. 6 Abs. 3 lit. b) PNR-RL ausschloss. Stets müssten die Kriterien durch den Menschen – insbesondere auf deren Diskriminierungsfreiheit – kontrolliert werden.[574]

Auch bei der Weiterübermittlung von Daten durch die Zentralstelle auf Anfrage muss die enge Zweckbindung beachtet werden, damit die Voraussetzungen an die automatisierte Datenverarbeitung nicht unterlaufen werden. Die Ergebnisse der automatisierten Verarbeitung sind daher nur zu

569 Vgl. insofern zum Anhang 2 der PNR-RL: *Wissenschaftliche Dienste des Bundestags,* PNR-Urteil, 2022, S. 8.
570 *Kostov*, GSZ 2022, 267 (271).
571 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 182 ff. = EuZW 2022, 706.
572 Idem, Rn. 179.
573 Dazu *Orrù, Information Polity* 27 (2022), 131 (135 ff.).
574 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 193 ff. = EuZW 2022, 706.

übermitteln, wenn sich aus ihnen ein objektiver Verdacht auf Terrorismus oder schwerer Kriminalität ergibt.[575]

Überhaupt ist die Weiterleitung der Daten im Hinblick auf die strenge Rechtsprechung zur Vorratsdatenspeicherung nur unter engen Voraussetzungen möglich. Soweit die Anfrage nach der Ankunft im Zielland stattfindet, muss beachtet werden, dass die automatisierte Überprüfung offensichtlich ergeben hat, dass die betroffene Person keine Anhaltspunkte für ihre *mögliche Beteiligung an terroristischen Straftaten oder an schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen* geliefert hat. Die Gründe der Abfrage müssen daher im Nachhinein entstanden sein.[576]

Dabei ist eine Abfrage grundsätzlich nur bei entsprechendem Anlass möglich, es sei denn, dass der jeweilige Mitgliedstaat sich in einer außergewöhnlichen Bedrohungssituation für seine nationale Sicherheit befindet.[577] Außer in besonderen Eilfällen ist dabei stets ein Richtervorbehalt zu implementieren, und zwar entgegen Art. 12 Abs. 3 lit. b) PNR-Richtlinie auch innerhalb der ersten sechs Monate, d. h. bevor die Daten anonymisiert wurden.[578]

Die anlasslose Speicherung der PNR-Daten bei der zentralen Stelle (und mithin die massenhafte Übermittlung durch Private) für sechs Monate hielt der Gerichtshof überraschenderweise für zulässig.[579] Art. 12 Abs. 1 PNR-RL steht nur nationalen Vorschriften entgegen, die eine anlasslose Speicherung über sechs Monate vorsehen. Allein solche Daten, die im Rahmen der Vorabprüfung auffällig wurden und daher im Verdacht stehen, eventuell für die Bekämpfung schwerer Kriminalität oder Terrorismus im Zusammenhang mit der Fluggastbeförderung relevant zu werden, könnten länger gespeichert werden, wobei auch für solche Daten die Pflicht zur Depersonalisierung nach sechs Monaten gilt, Art. 12 Abs. 2 PNR-RL.

In diesen beiden Aspekten dürfte der bedeutsamste Teil der Entscheidung liegen. Das allgemeine Verbot anlassloser Speicherung im Sicherheitsrecht kann nach dieser Entscheidung nicht mehr als universelles Prinzip betrachtet werden, sondern gilt (mit vielen Ausnahmen) nur bei TK-Ver-

575 Idem, Rn. 204.
576 Idem, Rn. 218 mit Verweis auf EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 (PNR Canada) Rn. 200 = ZD 2018, 23.
577 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 218 ff. = EuZW 2022, 706.
578 Idem, 220 ff.
579 Idem, 248 ff.

kehrsdaten. Weiter ist die Entscheidung aufgrund der kuriosen Methodik, eine Richtlinie durch Auslegung völlig zu entstellen, als Schritt hin zu einer stärker balancierten Rechtsprechung gegenüber staatlicher Massenüberwachung zu bewerten.[580] Aus grundrechtlicher Sicht stellt die Entscheidung gegenüber den Entscheidungen zur Verkehrsdatenspeicherung insofern einen Rückschritt dar.

3. Zusammenfassung

Der EuGH kann mittlerweile also ebenfalls auf eine umfassende Rechtsprechungshistorie zu staatlichen Massenüberwachungsmaßnahmen zurückschauen. Durch eine weitgehende Kompetenzwahrnehmung hat er sich als bedeutende Institution im Sicherheitsrecht etabliert und als *Grundrechtsgericht* eigene Maßstäbe – auch für die nationalen Gesetzgeber – gesetzt.

Das Vorgehen entspricht dabei grob demjenigen des BVerfG.[581] Im Grunde entwickelt der Gerichtshof durch Anwendung des Verhältnismäßigkeitsgrundsatzes spezifische Voraussetzungen für staatliche Überwachungsmaßnahmen in Abhängigkeit von deren Intensität.[582] Überwachungsmaßnahmen werden nicht mehr prinzipiell verboten, sondern *prozeduralisiert*.[583]

Dogmatisch zeichnet sich die Rechtsprechung des EuGH aber durch eine geringere Komplexität gegenüber dem BVerfG aus. Zwar ordnet der Gerichtshof ebenfalls Maßnahmen schematisch in Schwerekategorien, er unterscheidet bislang aber nur zwischen *schweren* und *nicht schweren* Ein-

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

581 Beispielhaft BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; dazu *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84: "Operationalisierung der Verhältnismäßigkeit"; *M. Hong* in Scharrer/Dalibor/Fröhlich ua. (Hrsg.), Assistententagung Öffentliches Recht, Risiko im Recht, 2011, S. 111 (123 ff.); *Volkmann*, NVwZ 2022, 1408 (1411): „Steuerungsmodell"; *Trute*, Die Verwaltung 2009, 85 (85 ff; 96 ff.); *Groß* KJ 2002, 1 (9 ff.); krit. *Schluckebier* abw. Meinung BVerfGE 125, 260 (364 ff., insbesondere 373); *Schoch* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 63 (67 ff.).

582 Jüngst EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 112 ff. = EuZW 2022, 706. mwN.

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

griffen, die dann entsprechend nur zur Bekämpfung und Verhütung von schwerer oder allgemeiner Kriminalität zulässig sind[584].

Unterschiede bei den Merkmalen, anhand derer die Intensität bestimmt wird, bestehen dabei kaum. Die Heimlichkeit, Streubreite und Datenqualität stehen auch beim Gerichtshof im Vordergrund, wenngleich Letztere gegenüber der Rechtsprechung des BVerfG zuletzt eine besonders prominente Stellung eingenommen hat.[585] Auf theoretische Erklärungen der Intensitätsmerkmale verzichtet der EuGH allerdings völlig und begnügt sich stets mit der pauschalen Feststellung, dass heimliche Massenüberwachungsmaßnahmen aufgrund möglicher Einschüchterungen das Gefühl totaler Überwachung herbeiführen könnten.

Die anlasslose Vorratsdatenspeicherung von TK-Verkehrsdaten lehnte der EuGH zunächst prinzipiell ab,[586] schuf aber im Laufe der Zeit doch eine Reihe von Ausnahmen.[587] Eine anlasslose, vorratsmäßige Speicherung ist danach nur noch zulässig zum Schutz der *nationalen Sicherheit* und auch dann nur, wenn für diese eine besondere Bedrohungslage besteht.[588] Ansonsten ist der Sicherheitsgesetzgeber auf die *targeted retention*[589] und das *quick freezing*[590] verwiesen.[591]

Der EuGH hat sich nicht auf eine schematische Gleichbehandlung sämtlicher Daten festgelegt, sondern behält sich offenbar vor, je nach Daten-Art unterschiedliche Anforderungen und Grundsätze zu entwickeln. Eine anlasslose Speicherung von Fluggastdaten hält der Gerichtshof auch

584 Vgl. EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 54 ff. = NJW 2019, 655.

585 Vgl. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), 100 = EuZW 2022, 706; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 71 = NJW 2022, 3135.

586 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

587 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), 137 ff. = NJW 2021, 531; übersichtlich *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (148 ff.).

588 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 137 ff. = NJW 2021, 531.

589 Dazu Vgl. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (101); *Cameron*, Common Market Law Rev. 58 (2021), 1433 (1449); *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (149).

590 Dazu *Juszczak/Sason*, eucrim 2021, 238 (247); zur Rechtslage in der StPO: *Rückert* in MüKo StPO, § 100g Rn. 116.

591 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), 140 ff., 160 ff. = NJW 2021, 531.

zur Kriminalitätsbekämpfung für eine Dauer von sechs Monaten nicht für grundsätzlich unverhältnismäßig.[592] Dasselbe gilt in diesem Zeitraum für die Analyse der PNR-Daten, solange die zur Analyse herangezogenen Daten bestimmten Kriterien unterliegen, kein Maschinenlernen eingesetzt und jeder Treffer vor der Weiterverarbeitung einer menschlichen Kontrolle unterzogen wird.[593]

Jedenfalls seit dem PNR-Urteil ist also offen, inwiefern der EuGH seine Rechtsprechung zu sicherheitsrechtlichen Überwachungsmaßnahmen auf Regelungen zur Finanzdatenüberwachung übertragen würde. Soweit bei Speicherung, Zugriff und Analyse dieser Daten-Art besondere Umstände hinzukommen, werden diese bei der Verhältnismäßigkeit Beachtung finden müssen.

Das PNR-Urteil ist jedoch auch insoweit richtungsweisend, als der EuGH eine neue, äußerst fragwürdige Methode zum Einsatz bringt. Anstatt die mit den Art. 7, 8 EU-GRC nicht vereinbarten Bestimmungen der Richtlinie aufzuheben, gab der EuGH vor, wie diese Normen vor dem grundrechtlichen Hintergrund auszulegen sind. Dabei reizte er den Wortlaut nicht nur aus, sondern änderte die Richtlinie letztlich so stark ab, dass von ihrem eigentlichen Wortlaut kaum mehr etwas übrigblieb.[594]. Die Rechtsanwendung wird für somit jeden, der mit dem PNR-Urteil nicht vertraut ist, unmöglich.

III. Rechtsprechung des EGMR

Auch der EGMR hat sich zu sicherheitsrechtlichen Überwachungsmaßnahmen, insbesondere im Hinblick auf Art. 8 EMRK, bereits geäußert. Da sich die Rechtsprechung des EGMR nach Art. 53 EU-GRC auf die Auslegung der Unionsgrundrechte auswirkt und dementsprechend bei der Bewertung der Geldwäschemaßnahmen eine Rolle spielen könnte, soll auch die EGMR-Rechtsprechung hier kurz vorgestellt werden.

592 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 255 = EuZW 2022, 706.

593 Idem, Rn. 176 ff.

594 *Thönnes*, Die Verwaltung 2022, 527 (531 ff., 539); *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

1. Frühe Rspr. des EGMR zu sicherheitsrechtlichen Überwachungsmaßnahmen, insbesondere Verkehrsdatenabfrage

Urteile des EGMR zu staatlichen Überwachungsmaßnahmen gibt es nunmehr schon seit fast fünfzig Jahren.[595] Als erster *landmark case*[596] gilt das Urteil *Klass/Bundesrepublik Deutschland*[597], in dem über die Legalität heimlicher nachrichtendienstlicher Maßnahmen nach dem G-10 gestritten wurde.

Die Kläger zweifelten zwar nicht an der grundsätzlichen Zulässigkeit, nachrichtendienstlicher Kommunikationsüberwachung, waren aber überzeugt, dass solche stets mit Benachrichtigungspflichten versehen werden müssen, damit (nachträglicher) Rechtsschutz möglich bleibt. Der EGMR gab ihnen insofern auch recht, entscheidend war aber schon, dass der Gerichtshof die Klage überhaupt für zulässig hielt, da nicht belegt werden konnte, ob die Kläger selbst von den fraglichen Maßnahmen *betroffene Opfer* i. S. d. Art. 25 EMRK waren. Der EGMR stellte im Sinne eines effektiven Rechtsschutzes fest, dass die jeweiligen Antragsteller bereits dann gegen heimliche Überwachungsmaßnahmen bzw. deren gesetzliche Grundlagen vorgehen können, wenn es nicht ausgeschlossen scheint, dass sie von den Maßnahmen betroffen sein könnten.[598] Der Gerichtshof eröffnete damit die Möglichkeit einer objektiven Kontrolle sicherheitsrechtlicher Überwachungsgesetze am Maßstab der EMRK und schuf so die Grundlage für seine künftige Rechtsprechungslinie.

Schon 1984 urteilte der EGMR daraufhin, dass der sicherheitsrechtliche Zugriff auf TK-Verkehrsdaten einen Eingriff in Art. 8 Abs. 1 EMRK darstellt.[599] Er hatte sich hier aber noch nicht zu der Frage zu äußern, ob schon die Speicherung bzw. die Pflicht zur Speicherung einen Grundrechtseingriff in Art. 8 Abs. 1 EMRK konstituiert, sondern lediglich, ob für die polizeiliche Abfrage von TK-Verkehrsdaten eine ausreichend bestimmte Rechtsgrundlage in England und Wales bestand. Dies wurde schließlich verneint, wobei der EGMR schon früh forderte, Ermächtigungen zu staatlichen Überwachungsmaßnahmen mit bestimmten Voraussetzungen zu versehen , die auf

595 Ausf. *Marsch,* Datenschutzgrundrecht, 2018, S. 8 ff.; *Schiedermair,* Schutz des Privaten, 2012, 167 ff.
596 *Górski* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 19 (20).
597 EGMR, Urt. v. 06.09. 1978, Nr. 5029/71 (Klass u.a./Deutschland) = NJW 1979, 1755.
598 Idem, Rn. 34 ff.
599 EGMR, Urt. v. 02.08.1984, Nr. 8691/79 (Malone/Vereinigtes Königreich), Rn. 83 f.

legislativer Ebene eine Verhältnismäßigkeitsgewähr darstellten, ohne aber näher zu spezifizieren, welche dies sein könnten.[600]

2. (Vorrats-)Datenspeicherungen als Beeinträchtigung von Art. 8 Abs. 1 EMRK

Inwiefern Datenspeicherungen Art. 8 Abs. 1 EMRK beeinträchtigen, sprach der EGMR allgemein erstmals in der Entscheidung *Leander/Schweden*[601] an. Dieser lag ein Streit um die Beschäftigungsmöglichkeit des Betroffenen in einem Militärmuseum zugrunde, im Zuge dessen persönliche Informationen über ihn in einem Polizeiregister angelegt wurden, ohne dass dessen Inhalt je offenbart wurde. Der EGMR stellte hier pauschal fest, dass schon das Anlegen solcher Informationen in einem Register einen Eingriff in Art. 8 Abs. 1 EMRK darstellt.[602]

Über die anlasslose Vorratsdatenspeicherung war damit aber noch nichts gesagt, da spezifische Registereinträge gerade nicht anlasslos (und somit auch nicht universell) erfolgen. Diese Problematik wurde erstmals in *Marper/Vereinigtes Königreich*[603] angesprochen.

In dieser Entscheidung ging es um die Speicherung von Fingerabdrücken und DNA-Proben von Straftatverdächtigten, die im Rahmen des Ermittlungsverfahrens angelegt wurden. Nach der britischen Rechtslage sollten diese auch dann noch weiterhin gespeichert werden, wenn das Verfahren eingestellt wurde oder es nach einer Verhandlung zu einem Freispruch gekommen war. Der Fall betraf also eine sicherheitsrechtliche Speicherung von Daten, die im ersten Moment zwar anlassbezogen erfolgte, deren Anlasszweck aber nachträglich entfiel.

Zuvor hatte der EGMR bereits entschieden, dass eine systematische Vorratsdatenspeicherung von DNA-Material strafrechtlich Verurteilter keine Verletzung von Art. 8 Abs. 1 EMRK darstellt.[604] Die vorratsmäßige Speicherung der Fingerabdrücke von nur Tatverdächtigen, bei denen es zu einer

600 Idem, Rn. 69 ff, zum „Metering" Rn. 83 ff.
601 EGMR, Urt. v. 26.03.1987, Nr. 9248/81 (Leander/Schweden).; ähnlich EGMR, Urt. v. 04.05.2000, Nr. 28341/95 (Rotaru/Rumänien).
602 Idem, Rn. 84; s.a. EGMR, Urt. v. 16.2.2000, Nr. 27798/95 (Amann/Schweiz), Rn. 69.
603 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich) = EuGRZ 2009, 299.
604 EGMR, Urt. 07.12.2006, Nr. 29514/05 (van der Welden/Niederlande); bestätigt in Entsch. V. 04.06.2013, Nr. 7841/08, 57900/12 (Peruzzo/Deutschland); kritischer

Einstellung oder einem Freispruch kam, behandelt der EGMR nun aber strenger.

Für die Bewertung kommt es dabei nach Art. 8 Abs. 2 EMRK darauf an, ob der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft *für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer* notwendig ist.

Auch der EGMR nimmt bei staatlichen Datenverarbeitungen also primär eine Verhältnismäßigkeitsprüfung vor.[605] Dabei räumt der Gerichtshof den nationalen staatlichen Stellen aber einen Ermessenspielraum ein, dessen Ausmaß von der Intensität des Eingriffs und der Bedeutung des jeweiligen Konventionsrechts abhängt, wobei sich letzterer aus dem Konsens der Mitgliedstaaten ergeben soll.[606]

In England und Wales wurde seinerzeit auch bei der Speicherung der Daten von Strafverdächtigen nicht zwischen unterschiedlichen Delikten unterschieden, sondern eine Speicherung bei Straftaten jeder Schwere vorgenommen. Außerdem war keine zeitliche Begrenzung der Speicherung vorgesehen. Diese unterschiedslose Sammlung von Fingerabdrücken und DNA-Daten hielt der EGMR im Ergebnis für unverhältnismäßig.[607]

Nun unterscheidet sich die Speicherung solcher Daten aber maßgeblich von der Speicherung von TK-Verkehrsdaten. Anders als die alltägliche Telekommunikation fällt die Speicherung einzelner persönlicher Daten bei der Bevorratung von Fingerabrücken u. ä. einmalig an und dient dann mehr als Register, denn als laufende Überwachung.

Dennoch lassen sich aus der Entscheidung wichtige Erkenntnisse für die Bewertung staatlicher Überwachungsmaßnahmen durch den EGMR ziehen. So wies der Gerichtshof das Argument der Regierung des Vereinigten Königreichs zurück, dass sich aus der Datenverarbeitung unmittelbar keine Nachteile für die Betroffenen ergäben.

---

jüngst zu DNA, Fingerabdrücken und Fotografien: Urt. v. 13.2.2020, Nr. 45245/15 (Gaughran/Vereinigtes Königreich) = NJOZ 2022, 476

605 Vgl. *Górski* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 19 (35).

606 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 102 = EuGRZ 2009, 299; Urt. v. 18.4.2013, Nr. 19522/09 (M.K./. Frankreich), Rn. 34 = NJOZ 2014, 1278; s.a. *Meyer-Ladewig/Nettesheim* in Meyer-Ladewig/Nettesheim/von Raumer EMRK, Art. 8 Rn. 111 ff.; allg. *Frowein* in Frowein/Peukert EMRK, 3. Aufl. 2009, Vorb. Art. 8-11, Rn. 13 ff.

607 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 125 = EuGRZ 2009, 299.

Die Speicherung selbst führe tatsächlich zu einer *Stigmatisierung* Nicht-Verurteilter, die mit der konventionsrechtlichen Unschuldsvermutung i. S. d. Art. 6 Abs. 2 EMRK nicht vereinbar sei.[608] Würde man dem Argument der Regierung folgen, wäre eine universelle Speicherung der Fingerabdrücke u. ä. sämtlicher Bürger ebenfalls verhältnismäßig, was laut späterer Entscheidungen des EGMR *zweifellos übermäßig und nicht angemessen wäre*.[609] Auch der EGMR hält universelle Überwachungsmaßnahmen also für grundsätzlich unzulässig und fordert stets eine angemessene Ausgestaltung der Datenverarbeitungsmaßnahmen, die wiederum von der Intensität abhängt. Diese bestimmt er zunächst nach den Eigenschaften der jeweiligen Datenkategorie, nimmt aber zur abstrakten Bewertung des Eingriffs auch rechtsstaatliche Gesichtspunkte, wie den Stigmatisierungseffekt, in den Blick.

Ausgehend von der danach festgestellten Eingriffsintensität soll sich die Verhältnismäßigkeit danach bestimmen, ob das staatliche Recht *angemessene Sicherungen vorsieht, um eine Verwendung solcher Daten zu verhindern, die mit den Garantien jener Vorschrift nicht vereinbar wäre*.[610]

3. Verhältnismäßigkeit durch *Sicherungsvorkehrungen* am Beispiel der TKÜ: *Zakharov/Russland*

Marper/Vereinigtes Königreich legte somit den Grundstein für eine Rechtsprechungslinie des EGMR, die sich letztlich stark am Vorgehen des BVerfG und EuGH orientiert.

Anstatt einer reinen Rationalitätskontrolle leiten diese Gerichte aus den verfassungs- bzw. primärrechtlichen Bestimmungen spezifische Anforderungen an die gesetzlichen Grundlagen im Sicherheitsrecht ab, die schon auf dieser Ebene einen Ausgleich von sicherheits- und grundrechtlichen Interessen gewährleisten sollen.[611]

---

608 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 122 = EuGRZ 2009, 299

609 EGMR, Urt. v. 18.4.2013, Nr. 19522/09 (M.K./. Frankreich), Rn. 40 = NJOZ 2014, 1278; Urt. v. 13.2.2020, Nr. 45245/15 (Gaughran/Vereinigtes Königreich), Rn. 89 = NJOZ 2022, 476

610 EGMR, Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 103 = EuGRZ 2009, 299

611 Vgl. BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 353 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245

Ein solches Vorgehen lässt sich mittlerweile auch beim EGMR beobachten, wenngleich dessen Rechtsprechung insgesamt noch kasuistisch geprägt ist[612] und kein ganz so nuanciertes Schema etabliert hat wie das BVerfG (das aber auch entsprechend kritisiert wird).[613]

Dies lässt sich an einer Überprüfung der Vorschriften zur Telekommunikationsüberwachung im Fall *Zakharov/Russland*[614] darstellen.

Mit den einzelnen Anforderungen der russischen TKÜ setzte sich der Gerichtshof intensiv auseinander. Anders als das BVerfG war seine Betrachtungsweise allerdings negativ in dem Sinne, dass er nicht selbstständig spezifische Anforderungen aufstellte und dann prüfte, ob die vorhandenen damit übereinstimmten, sondern er zeigte nur die Mängel bzw. das *Missbrauchspotential* der bestehenden gesetzlichen Grundlagen konkret auf. Dies tat er allerdings so ausführlich, dass sich im Wege eines Umkehrschlusses positive Anforderungen an die gesetzlichen Tatbestände ableiten lassen.

Konkret kritisierte der EGMR vor allem die Ausgestaltung der formellen Sicherungsvorkehrungen. Der vorgesehene Richtervorbehalt würde in der Praxis wenig nutzen, da das russische Gesetz keine Verhältnismäßigkeitsprüfung der Maßnahme durch die Gerichte vorsah und in Eilfällen vom Vorbehalt abgesehen werden durfte. Der Richtervorbehalt würde praktisch nur eine Formalie darstellen, die keinen effektiven Schutz der Betroffenen gewährleiste.[615]

Weiter kritisierte der EGMR die Anordnungspraxis in Bezug auf die materiellen Anforderungen. Die Ermächtigungsgrundlage der Nachrichtendienste war nicht auf konkretisierte Personen begrenzt, sondern erlaubte auch Anordnungen, die sich auf nur umrissene Personenkreise oder örtliche Begrenzungen bezogen, bzw. sie wurden für solche verwandt.[616]

Letztlich beanstandete der Gerichtshof auch die Kontrollmechanismen in der russischen Föderation. Die einzige Aufsichtsmaßnahme bestand in der (mangelhaften) Vorabprüfung im Rahmen des Richtervorbehalts. Ab dieser Zulassung wurden die Rechtmäßigkeit der Maßnahme bzw. deren

(253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84.

612 Vgl. *Schiedermair,* Schutz des Privaten, 2012, S. 238 ff.

613 *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.).

614 EGMR, Urt. v. 4.12.2015, 47143/06 (Zhakarov/Russland) = NMLR 2015, 509.

615 Idem, Rn. 259 ff.

616 Idem, Rn. 265.

Ausgestaltung und Durchführung nur noch von den Staatsanwälten kontrolliert, deren Unabhängigkeit allerdings zweifelhaft sei und, für die eine öffentliche Kontrollaufsicht nicht etabliert war.[617] Insofern war eine rechtliche Überprüfung kaum effektiv möglich. Dies galt erst recht, wenn die Informationen nicht zu einem Verfahren führten, da Benachrichtigungspflichten nicht existierten und die technischen Vorrichtungen zum Abhören in den Endgeräten keine Protokolle anlegten.[618]

4. Strategische Fernmeldeüberwachung: *Big Brother* und *Rättvisa*

Zu klassischen Vorratsdatenspeicherungen im Rahmen der Strafverfolgung und Gefahrenabwehr durch Inpflichtnahme Privater hat sich der EGMR bislang nur bzgl. TK-Bestandsdaten geäußert und diese, wie auch das BVerfG und der EuGH, prinzipiell für verhältnismäßig befunden.[619] Dabei ist zu sehen, dass die Bestandsdaten, insbesondere die Vertragsdaten, bei den jeweiligen Unternehmen ohnehin vorliegen werden. Die Bestandsdatenspeicherungskomplexe sind grundrechtlich nur insofern problematisch, wie sie auch die Speicherung eigentlich nicht notwendiger Daten vorsehen und weil sie den Zugang für staatlicher Sicherheitsbehörden zentralisieren und automatisieren (zur Kontostammdatenspeicherung s. Kap D. I. und zur Diskussion Kap. F. I.).

Über diese Kategorie der Telekommunikationsdaten hinaus liegen nur Urteile[620] vor, die sich mit der strategischen Kommunikationsüberwachung durch die Nachrichtendienste beschäftigen, wobei diese auch die Sammlung von Verkehrsdaten ermöglicht.[621]

Die entscheidenden Urteile zur strategischen Fernmeldeüberwachung ergingen parallel im Jahr 2021 und betrafen die Nachrichtendienste des Vereinigten Königreichs und den Militärgeheimdienst von Schweden.[622] In

617 Idem, Rn. 272 ff.
618 Idem, Rn. 289 ff.
619 EGMR, Urt. v. 30.1.2020, Nr. 50001/12 (Breyer/Deutschland) = NJW 2021, 999.
620 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich) = NVwZ-Beil. 2021, 11; Urt. v. 25.5.2021, Nr. 35252/08 (Centrum för Rättvisa / Schweden) = NVwZ-Beil. 2021, 30.; zuvor schon Entsch. vom 29.06.2006, Nr.54934/00 (Weber u. Saravia/Deutschland) = NJW 2007, 1433.
621 Vgl. Zur Übersicht *B. Huber*, NVwZ-Beilage 2021, 3; *Ibel* ZD-Aktuell 2021, 5246.
622 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich) = NVwZ-Beil. 2021, 11; Urt. v. 25.5.2021, Nr. 35252/08 (Centrum för Rättvisa / Schweden) = NVwZ-Beil. 2021, 30

älteren Verfahren, insbesondere zum G-10,[623] hatte der EGMR schon entschieden, dass Massenüberwachung nicht grundsätzlich unzulässig sei.[624] Da sich die Telekommunikation und deren Stellenwert in der Gesellschaft seither aber enorm verändert habe und in den früheren Entscheidungen weder die speziellen Eigenschaften der Verkehrsdaten noch der Unterschied von Massenüberwachung zu individueller Überwachung ausreichend berücksichtigt wurde, sah sich der EGMR zu einer ausführlichen Neubearbeitung veranlasst,[625] die hier allein thematisiert werden soll.

Bemerkenswert ist dabei zunächst, wie intensiv der EGMR sich mit den einzelnen Datenverarbeitungsschritten der Überwachung auseinandersetzt, und auf deren Verknüpfung eingeht.[626] Dabei stellt der Gerichtshof zunächst fest, welche einzelnen grundrechtsrelevanten Schritte sich bei der strategischen Überwachung identifizieren lassen (dazu auch oben Kap. B. I.2).[627]

Zunächst werden Kommunikationsinhalts- und Verkehrsdaten durch die Nachrichtendienste massenweise durch „Pakete" erhoben. In einem nächsten Schritt werden all diese Daten dann automatisiert auf bestimmte Suchbegriffe hin bzw. mit *umfassenden Abfragemechanismen* durchsucht. Im dritten Schritt werden die so erhobenen Daten von Analysten untersucht. Daran schließt sich eventuell ein vierter Schritt an: die tatsächliche Nutzung der Daten durch den Geheimdienst in Form von Berichten oder durch eine Weitergabe an andere Sicherheitsbehörden bzw. ausländische Dienste.

In diesem graduellen Prozess erkennt der EGMR eine fortschreitende Eingriffsintensivierung.[628] Während also die Datenerhebung und das erstmalige Aussortieren noch keine intensive Belastung herbeiführen, steigt

623 In der Fassung des Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) vom 28.10.1994, BGBl. I 1994, S. 3186; dazu auch BVerfGE 100, 313 – Strategische Fernmeldeaufklärung.

624 EGMR, Entsch. vom 29.06.2006, Nr.54934/00 (Weber u. Saravia/Deutschland) = NJW 2007, 1433; Urt. v. 01.07.2008 , Nr. 58243/00 (Linerty/Vereinigtes Königreich).

625 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 340 ff. = NVwZ-Beil. 2021, 11.

626 Idem, Rn. 324 ff.

627 Vgl. zum deutschen G-10 *Marxsen*, DÖV 2018, 218 (219 f.); *Papier*, NVwZ-Extra 15/2016, 1; *Schantz*, NVwZ 2015, 873 (874); *Bäcker*, K&R 2014, 556 (557).

628 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 325. = NVwZ-Beil. 2021, 11.

die Intensität mit jedem weiteren Schritt. Entsprechend müssen die Sicherheitsvorkehrungen graduell angepasst werden. [629]

Bei der darauf aufbauenden Bewertung der Verhältnismäßigkeit trifft der EGMR zu Beginn eine prägnante Feststellung: Heimliche Massenüberwachung könnten zwar durchaus zum Schutz der nationalen Sicherheit geeignet und somit auch gerechtfertigt sein, gleichzeitig hätten sie aber das Potential, das ordnungsgemäße *Funktionieren demokratischer Prozesse unter dem Vorwand, sie zu verteidigen, zu unterminieren und sogar zu zerstören*.[630] Der EGMR betrachtet die Überwachung also nicht nur aus einer individuellgrundrechtlichen Perspektive, sondern aus einer abstrakten Perspektiven mit Bezügen zu demokratietheoretischen und rechtsstaatlichen Aspekten. Diese Perspektive drängt sich stärker als im Rahmen des GG oder der EU-GRC auch auf, denn Art. 8 Abs. 2 EMRK verlangt nicht nur allgemein eine Verhältnismäßigkeit von Eingriffen in die Privatheit, sondern deren Notwendigkeit *in einer demokratischen Gesellschaft*. Die eigentlich rechtsstaatlichen Elemente, die auch das BVerfG in seiner Perspektive berücksichtigt (siehe oben Kap. B. III. 2. c.), werden hier also vom Grundrechtstext unmittelbar eingefordert.

Dogmatisch sortiert der Gerichtshof die einzelnen Datenverarbeitungsschritte in unterschiedliche Problemkategorien ein. Die späteren Schritte, bei denen es tatsächlich zu einer relevanten Verarbeitung durch die Sicherheitsbehörden kommt, lassen sich wie die individuellen Überwachungsmaßnahmen ganz klassisch als intensive Eingriffe verstehen, da sie die Privatheit tatsächlich einschränken. Die frühen Stadien von Massenüberwachungsmaßnahmen sind aus anderen Gründen problematisch, weil sie demokratische bzw. rechtsstaatliche Prinzipien gefährden.

Dass die Schritte nicht losgelöst voneinander betrachtet werden können, stellt der EGMR anhand der Missbrauchsmöglichkeiten fest. Da in der graduellen Betrachtung mit der steigenden Intensität höhere Vorkehrungen einhergehen, darf nicht schon auf Ebene der Massenüberwachung eine individuelle Überwachung stattfinden, um diese Vorkehrungen zu umgehen. Suchkriterien, die eine individuelle Überwachung ermöglichen würden (etwa spezifische Emailadressen), sind daher nicht zulässig.[631] Es bedarf insofern auf dieser Ebene vor allem einer typisierten Kontrolle der Selektoren durch eine unabhängige Stelle.[632] Überhaupt ist die Kontrolle durch

629 Idem, Rn. 330, 347.
630 Idem, Rn. 339.
631 Idem, Rn. 348 ff.
632 Idem, Rn. 350 ff.

eine unabhängige Stelle in formeller Hinsicht für sämtliche Schritte der Massenüberwachung notwendig.

Darüber hinaus muss die gesetzliche Ermächtigung auch in materieller Hinsicht regeln: *„1.) die Gründe, aus denen die Massenüberwachung genehmigt werden kann, 2.) die Umstände, unter denen die Kommunikationen eines Einzelnen überwacht werden können, 3.) das Verfahren, das bei der Genehmigung einzuhalten ist, 4.) das Verfahren bei der Auswahl, Auswertung, und Verwendung des abgefangenen Materials, 5.) die Vorsichtsmaßnahmen, die bei Weitergabe des Materials an andere zu treffen sind, 6.) die zeitliche Begrenzung der Überwachung und Speicherung des erhobenen Materials sowie die Umstände, unter denen dieses Material gelöscht und vernichtet werden muss, 7.) das Verfahren und die Einzelheiten der Überwachung durch eine unabhängige Stelle, ob die genannten Garantien beachtetet wurden, und die Befugnis dieser Stelle, bei Verstößen zu entscheiden und 8.) das Verfahren für eine unabhängige, nachträgliche Kontrolle der Einhaltung dieser Garantien und die Befugnis der zuständigen Stelle zu entscheiden, wenn das nicht der Fall war.“*[633]

Diese Regeln gelten für die nachrichtendienstliche Verarbeitung von sowohl Inhalts- als auch Verkehrsdaten[634], wobei der EGMR sich nicht dazu verhält, wie eine Speicherung von Verkehrsdaten (nur) bei den Privatunternehmen zu bewerten wäre.

Die Einhaltung der vage umschriebenen Anforderungen prüfte der EGMR anhand der britischen und schwedischen Regelungen negativ und kasuistisch, machte also nur auf einzelne Mängel aufmerksam, anstatt konkrete Regeln positiv zu formulieren.[635]

5. Zusammenfassung

Resümierend lässt sich also feststellen, dass der EGMR gegenüber staatlicher Überwachung eine ähnliche „Ja-Aber-Haltung“[636] eingenommen hat wie das BVerfG. Soweit die Ermächtigungsgrundlagen hinreichend bestimmt sind und Regeln enthalten, die ausreichend von einer missbräuchlichen Verwendung der Überwachungsmaßnahmen schützen, steht Art. 8

633 Idem, Rn. 361.
634 Idem, Rn. 363 f.
635 Übersichtlich *B. Huber*, NVwZ-Beilage 2021, 3.
636 *Ibel* ZD-Aktuell 2021, 5246.

Abs. 2 EMRK selbst einer universellen Überwachung der (Auslands-)Kommunikation nicht entgegen.[637]

Die Herangehensweise des Gerichtshofs fällt jedoch kasuistischer aus. Konkrete Anforderungen in Form von „Handlungsanweisungen" ergeben sich nur dann, wenn der Gerichtshof Mängel der geprüften Normen konkret feststellt. Eine immer weiter ausdifferenzierte Je-Desto-Formel wie jene des BVerfG, die sich letztlich zu einer nuancierten *Handlungsanweisung*[638] entwickelt hat, findet sich in der Rechtsprechung des EGMR nicht.

Auch in dogmatischer Hinsicht zeigt sich dessen Rechtsprechung als wenig komplex. Anstatt über einen Katalog theoretisch fragwürdiger Intensitätsmerkmale die Eingriffsschwere von Überwachungsmaßnahmen zu bestimmen, stellt der Gerichtshof primär auf die tatsächliche Beschränkung der Privatheit ab und sieht diese bei Massenüberwachungen erst in den Stadien, die eine relevante Verwendung der individuellen Daten vorsehen, als verletzt an,[639] wenngleich er konsequent in jedem Datenverarbeitungsschritt einen Grundrechtseingriff erkennt[640]. Die graduelle Bewertung dieser Schritte erfolgt dann, ausgehend von Art. 8 Abs. 2 EMRK, dergestalt, dass bei den frühen Stadien rechtsstaatliche Erwägungen in den Vordergrund gerückt und entsprechende Verfahrensgarantien gefordert werden, die eine Umgehung der strengen Voraussetzungen individueller Überwachung verhindern.[641]

Aus der Rechtsprechung des EGMR ergeben sich für die Bewertung von Überwachungsmaßnahmen in Hinsicht auf Finanzdaten also nicht unbedingt konkrete Anforderungen an Speicherpflichten und Zugangsrechte, jedoch folgt aus ihr, dass Überwachungsmaßnahmen strukturell betrachtet werden müssen. Die Speicherung, Analyse und Weiterleitung von Daten

637 Vgl. Jüngst EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 334 ff. = NVwZ-Beil. 2021, 11; Urt. v. 25.5.2021, Nr. 35252/08 (Centrum för Rättvisa / Schweden), Rn. 248 ff. = NVwZ-Beil. 2021, 30

638 Insofern krit. *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.).

639 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 325 ff. ff. = NVwZ-Beil. 2021, 11

640 EGMR, Urt. v. 26.03.1987, Nr. 9248/81 (Leander/Schweden), Rn. 84; Urt. v. 16.2.2000, Nr. 27798/95 (Amann/Schweiz), Rn. 69.

641 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 348 ff. = NVwZ-Beil. 2021, 11

sind nicht nur individuell, sondern mit Rücksicht auf deren Synergieeffekte zu bewerten.

Kapitel D: Speicherung und Überwachung von Finanzdaten

Die bislang dargestellte Rechtsprechung hat sich noch nicht tiefergehend mit der Rolle von Finanzdaten im Sicherheitsverfassungsrecht auseinandergesetzt. Dabei besteht eine ganze Reihe von Vorschriften, die auch bzgl. der Finanzdaten bestimmte Speicher- und Analysekonzepte etabliert haben, insbesondere § 8 Abs. 1 GwG. Anders als im Rahmen der Telekommunikations- und PNR-Daten handelt es sich aber nicht nur um Normen aus dem Sicherheitsrecht.

Diese Vorschriften sollen im Folgenden beschrieben werden, bevor untersucht werden soll, wie sich die Rechtsprechung zu staatlichen Überwachungsmaßnahmen auf ihre Bewertung auswirkt.

I. Bestandsdatenspeicherung nach § 24c KWG

Eine Anordnung zur Vorhaltung bestimmter Informationen findet sich zunächst in § 24c KWG[642] hinsichtlich der Bestandsdaten von Kontoinhabern bei Kreditinstituten. Auf § 24c KWG verweisen die §§ 93 b, § 93 Abs. 7, 8 AO und § 27 Abs. 2 ZAG, § 28 Abs. 2 KAGB, die den Umfang der Speicherpflicht erweitern und den Anwendungsbereich auf Zahlungsinstitute und Kapitalanlagegesellschaften ausdehnen. Die angeführten Normen können als gemeinschaftliches Speicherregime verstanden werden.

Nach § 24c Abs. 1 KWG haben Kreditinstitute ein Dateisystem zu führen, in dem für jedes Konto, Depot oder Schließfach die Kontonummern, Namen der Inhaber, Verfügungsberechtigten und, soweit vorhanden, wirtschaftlich Berechtigten i. S. d. § 3 GwG[643], außerdem das Geburtsdatum der Inhaber sowie Eröffnungs- und Schließungsdatum gespeichert werden. Es handelt sich somit um eine Speicherpflicht für Bestandsdaten. Allerdings werden die Daten in diesem Kontext oft nicht so bezeichnet, sondern als

642 Kreditwesengesetz (KWG) in der Fassung der Bekanntmachung vom 09.09.1998 (BGBl. I S. 2776), zuletzt geändert durch Gesetz vom 22.02.2023 (BGBl. I S. 51).

643 Geldwäschegesetz (GwG) vom 23. Juni 2017 (BGBl. I S. 1822), zuletzt geändert durch durch Artikel 8 des Gesetzes vom 31. Mai 2023 (BGBl. 2023 I Nr. 140).

„Kontostammdaten".[644] Da dieser Arbeit aber u. a. ein Vergleich mit den TK-Vorschriften zugrunde liegt, soll hier die aus § 3 Nr. 6 TKG bekannte Bezeichnung „Bestandsdaten" verwendet werden. [645]

I. Historische Entwicklung

§ 24c KWG wurde durch das Vierte Finanzmarktförderungsgesetz vom 21. Juni 2002[646] mit Wirkung zum 1. April 2003 als Teil der gesetzgeberischen Reaktion auf die Terroranschläge vom 11. September 2011[647] eingeführt[648].

Die Bankenaufsicht sollte in die Lage versetzt werden, auf einen Schlag herauszufinden, bei welchen Instituten eine oder mehrere bestimmte Personen ein Konto unterhält bzw. unterhalten, um somit die Recherche von Finanzströmen durch die Strafverfolgungsbehörden erheblich zu erleichtern.[649] Insbesondere, wenn lediglich die Namen von verdächtigen Personen bekannt wurden, ging der Gesetzgeber von der Notwendigkeit aus, herauszufinden, wo die Verdächtigen über Konten verfügten, um sodann darüber hinausgehende Ermittlungen bei den entsprechenden Instituten einleiten zu können.[650] Vor der Einführung des § 24c KWG war dies nur durch massenhafte Einzelanfragen, gestützt auf § 44 KWG , bei den (im Jahr 2002 etwa 2900) in der Bundesrepublik lizensierten Instituten möglich.[651] Dieses Verfahren hielt der Gesetzgeber für zu zeitaufwendig.[652]

644 Vgl. BVerfGE 118, 168 – Kontostammdaten; *Achtelik* in Herzog GwG, KWG § 24c Rn. 2; *Tolani*, BKR 2007, 275 (276 ff.).

645 So auch *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 38; *Gnüchtel*, NVwZ 2016, 13 (16); zum Inhalt des § 3 TKG siehe nur *Ricke* in Spindler/Schuster/Anton (Hrsg.), Elektronische Medien, 4. Auflage 2019, TKG § 3 Rn. 6.

646 Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) vom 21 Juni 2002 (BGBl. I, S. 2010).

647 BT-Drs. 14/8017, S. 122 f.; *Deutsche Bundesbank*, (Deutsche Bundesbank), Monatsbericht, Oktober 2002, S. 28; *Schily*, WM 2003, 1249 (1252); *Kokemoor*, BKR 2004, 135 (136); *Jahn*, ZRP 2002, 109 (110); *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (118 ff.).

648 Zum Gesetzgebungsprozess ausf. *Zubrod*, WM 2003, 1210 (1210 f.).

649 *Schily*, WM 2003, 1249 (1252).

650 BT-Drs. 14/8017, S. 122 f.

651 Idem, S. 123; *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (120); *Schily*, WM 2003, 1249 (1252).

652 BT-Drs. 14/8017, S. 123.

Die Norm ging nicht auf eine europarechtliche Verpflichtung zurück, sondern wurde vom deutschen Gesetzgeber eigenständig initiiert. Im Gegensatz dazu orientierte sich die europäische Union bei den künftigen Änderungen des Anti-Geldwäscherechts an der deutschen Vorlage. So wurde zunächst durch Art. 32 der 3. EU-Geldwäscherichtlinie (GWRL)[653], begleitet von dem Verbot anonymer Konten nach Art. 6, eine Auskunftsverpflichtung der Banken und anderer Verpflichteter entsprechend § 44 KWG eingeführt. Eine europarechtliche Pflicht zur automatisierten Bestandsdatenabfrage, die sich an § 24c KWG orientierte[654], wurde erst mit Art. 32a der 5. GWRL[655] im Jahr 2018 obligatorisch.

Ursprünglich war nicht nur die automatisierte Abfrage bei speziellen Dateien der einzelnen Institute, sondern eine Kontenevidenzzentrale beim Bundesaufsichtsamt für das Kreditwesen (heute BaFin) angedacht, wo sämtliche Kontobestandsdaten zentral geführt werden sollten.[656] Eine solche zentrale Datei hätte aber einen deutlich höheren Arbeitsaufwand sowohl der Kreditwirtschaft als auch der führenden staatlichen Stelle bedeutet, weshalb man sich dafür entschied, dezentrale, von den Banken selbst geführte Dateien einzuführen.[657] Eine ähnliche Regelung, die insofern für § 24c KWG als Vorbild diente[658], fand sich in § 90 TKG aF,[659] der die Anbieter von Telekommunikationsdiensten zur Vorhaltung von Bestandsdaten für Sicherheitsbehörden im Rahmen eines automatisierten Verfahrens verpflichtete (heute §§ 172 ff. TKG).

---

653 Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, ABl. 2005, L 309/15.

654 *BaFin,* Journal, Mai 2018, S. 23; *Engels*, WM 2018, 2071 (2077 f.).

655 Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. 2018, L 156/43.

656 *Deutsche Bundesbank,* (Deutsche Bundesbank), Monatsbericht, Oktober 2002, S. 28; *Escher*, BKR 2002, 652 (658); *Teichmann/Achsnich* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 33 Rn. 8; *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (120); *Jahn*, ZRP 2002, 109 (110); *Internetredaktion beck-aktuell*, (Beck Online, Verlag C.H. Beck), Bundesfinanzministerium Maßnahmenpaket, becklink 34689, 08.10.2001.

657 *Teichmann/Achsnich* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 33 Rn. 8; *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (120).

658 BT-Drs. 14/8017, S. 123.

659 Telekommunikationsgesetz (TKG) vom 25. Juli 1996, BGBl. I, S. 1120.

Im Übrigen hat die Bestandsdatenauskunft nach § 24c KWG, § 93b, § 93 Abs. 7, 8 AO seit ihrer Einführung nur eine überschaubare Anzahl an Änderungen erfahren.[660] Erwähnenswert sind etwa die Erweiterung der Vorhaltefrist nach Ende der jeweiligen Geschäfts- bzw. Kontobeziehung von ursprünglich drei auf zehn Jahre[661] im Jahr und die Erweiterung des Anwendungsbereichs auf Schließfächer durch das Gesetz zur Umsetzung der 4. GWRL.

2. Übersicht

Unmittelbar nach § 24c Abs. 1 Nr. 2 KWG sind als persönliche Daten eigentlich nur Name und Geburtsdatum des Kontoinhabers im Dateisystem aufzuführen. Die Angabe der Anschrift ist nur für die vom Inhaber abweichenden wirtschaftlich Berechtigten vorgesehen, § 24c Abs. 1 Nr. 2 GWG.

Eine Erweiterung der notwendigen Daten des Inhabers finden sich aber im Steuerrecht. Nach § 93 b Abs. 1a AO müssen zusätzlich zu den nach § 24c Abs. 1 KWG zu erhebenden Daten auch die Adressen und die in § 154 Abs. 2a AO genannten steuerrechtlichen Ordnungsmerkmale[662] aller Verfügungsberechtigten in das Dateisystem übernommen werden. Bei Letzteren handelt es sich um die Steuer-Identifikationsnummer i. S. d. § 139b AO und die Wirtschafts-Identifikationsnummer nach § 139c AO sowie bei natürlichen Personen um die Steuernummer.

Diese steuerrechtlichen Erweiterungen gelten jedoch nur für die Abfrage nach § 93b Abs. 1, 93 Abs. 7, 8 AO, also für die Abfrage durch das BZSt. Die BaFin darf nur die in § 24c KWG aufgeführten Daten abfragen.[663] Dies stellt die Rechenzentren vor ein Problem, da sie abhängig vom Anfrageersuchen unterschiedliche Daten bereitstellen müssen, gleichzeitig aber nicht erkennen dürfen, zu welchem Zweck die Abfrage stattfindet.[664] Ab dem 01. Januar 2020 sollen nach Art. 97 § 26 Abs. 3 EGAO deshalb alle nach den steuerrechtlichen Vorschriften und § 24c Abs. 1 KWG zu erhebenden

660 *Achtelik* in Herzog GwG, § 24c KWG Rn. 1.
661 Gesetz zur Bekämpfung der Steuerumgehung und zur Änderung weiterer steuerlicher Vorschriften (StUmgBG) vom 23. Juni 2017, BGBl. I S. 1682.
662 *C. Pohle* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap 11 Rn. 77 ff; 204.
663 BT-Drs. 18/12127, S. 51; *Achtelik* in Herzog GwG, § 24c KWG Rn. 5.
664 BT-Drs. 18/12127, S. 51.

Daten einheitlich im selben Datensatz gespeichert werden.[665] Da § 24c Abs. 1 KWG noch nicht an § 93b Abs. 1a AO angepasst wurde, muss die Differenzierung durch das Informationstechnikzentrum Bund (ITZBund) als gemeinsames Rechenzentrum des BZSt und der BaFin im Rahmen der Zuordnung der Ausgabe-Datensätze erfolgen.[666]

§ 24c KWG ist begrenzt auf Konten, die der Legitimationsprüfung des § 152 Abs. 2 AO unterfallen. Unter den Begriff fallen nach der noch heute gültigen[667] Definition des Reichsfinanzhofes alle *„im Rahmen einer laufenden Geschäftsbeziehung für Kunden geführte Rechnung, in der Zu- und Abgänge von Vermögensgegenständen erfasst werden/buch- und rechnungsgemäße Darstellung einer Geschäftsbeziehung zwischen Kontoinhaber und kontoführendem Institut"*.[668] Hierzu zählen nur externe, keine internen Verrechnungskonten.[669] Außerdem gilt § 24c KWG nicht für klassische Kreditkartenkonten, bei denen keine Einlagen eingezahlt werden, sondern eine turnusmäßige Umsatzabrechnung im Wege des Lastschrifteinzugs erfolgt.[670] Noch recht neu ist die Einbeziehung virtueller IBAN von Zahlungsdienstleistern, die mit einem Konto bei einem Kreditinstitut verknüpft sind,[671] aufgrund Allgemeinverfügung[672] der BaFin. Diese virtuellen IBAN werden von Kreditinstituten an Zahlungsdienstleister, z. B. Prepaid-Kreditkarten, ausgegeben und fungieren als Konto des Endkunden.[673] Zwar gelangen Zahlungen zunächst auf das Konto des Zahlungsdienstleisters, diese werden aber umgehend dem Zahlungskonto des Endkunden zugeschrieben. Insofern ist dieser wirtschaftlich Berechtigter.[674]

Die Dateien müssen bei den Verpflichteten gesondert geführt und technisch so eingerichtet werden, dass die befugten Behörden unmittelbar und ohne, dass dies zur Kenntnis des dateiführenden Instituts gelangt, darauf

665 Ibid.
666 Vgl. Ibid.
667 Vgl. *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 24c KWG Rn. 4.
668 RFHE 24, 203 (205).
669 *Achtelik* in Herzog GwG, § 24c KWG Rn. 6; *Kokemoor*, BKR 2004, 135 (138).
670 *Bundesministerium der Finanzen*, (Bundesministerium der Finanzen), Schreiben KWG 11.80c (VII B 7 – WK 5023 – 26/03), 15. Januar 2003; *Escher*, BKR 2002, 652 (659).
671 *BaFin,* Allgemeinverfügung zu § 24c KWG, 08.12.2020.
672 Gestützt auf § 6 Abs. 3 i. V. m. § 24c Abs. 1 KWG.
673 Ibid.
674 Ibid.

zugreifen können. Die technischen Einzelheiten dieser Schnittstelle werden von der BaFin vorgeschrieben.[675]

Die Schnittstelle muss jederzeit erreichbar sein, unabhängig von den Geschäftszeiten.[676] Die Dateien müssen allerdings nicht zwingend von den Kreditinstituten selbst vorgehalten werden. Nach § 25b KWG dürfen Kreditinstitute bestimmte Aktivitäten und Prozesse unter gewissen Umständen an andere Unternehmen auslagern. Von dieser Möglichkeit haben die Institute im Rahmen des § 24c KWG mehrheitlich Gebrauch gemacht.[677] Abhängig ist dies stets von der Art, Umfang, Komplexität und dem Risikogehalt des jeweiligen Prozesses. Die Verantwortung für die Durchführung des Auskunftsverfahren bleibt aber stets bei den jeweiligen Kreditinstituten.[678]

Nach § 24c Abs. 1 KWG sind die Daten *unverzüglich* zu speichern, wobei der Begriff der Unverzüglichkeit dem BGB entnommen ist, also *ohne schuldhaftes Zögern* bedeutet.[679] Dasselbe gilt nach § 24 Abs. 1 S. 2 KWG, wenn sich an bestehenden Daten Änderungen ergeben. In diesem Fall werden die Daten auch nicht überschrieben, etwa bei einer Namensänderung, sondern ein neuer Datensatz angelegt. Der alte Datensatz muss nach Ablauf von drei Jahren nach Anlage des neuen gelöscht werden, § 24 Abs. 1 S. 3 Alt. 2 KWG. In der Praxis wird dem Unverzüglichkeitserfordernis durch eine tägliche Aktualisierung des Datenbestandes nachgekommen.[680] Zehn Jahre nach Auflösung eines Kontos sind die Daten nach § 24c Abs. 1 S. 3 KWG endgültig zu löschen.

Auf die nach § 24c KWG zu führenden Dateien der Kreditinstitute und anderen Verpflichteten hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) nach § 24c Abs. 2, 5, 6 KWG automatisierten Zugriff. Diesen darf sie nicht nur zur Erfüllung ihrer bankenaufsichtsrechtlichen Pflichten nach dem KWG nutzen, sondern nach § 24c Abs. 2, 3 KWG auch für

675 Vgl. *Achtelik* in Herzog GwG, KWG § 24c Rn. 17; danach zuletzt wohl *BaFin*, Rundschreiben 01/2018 (GW), das aber nicht öffentlich zugänglich ist.

676 *C. Pohle* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 11 Rn. 21; *Kokemoor*, BKR 2004, 135 (140).

677 *Zubrod*, WM 2003, 1210 (1212) verweist etwa auf die FIDUCIA AG (seit 01.09.2021: Atruvia AG), welche als Zentralstelle für die Mitglieder der Genossenschaftlichen FinanzGruppe VolkbankenRaiffeisenbanken tätig wird; *Achtelik* in Herzog GwG, § 24c KWG Rn. 4; *ders.* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 24c KWG Rn. 3.

678 *Schatz* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 549 (566).

679 *Kokemoor*, BKR 2004, 135 (139).

680 *Zubrod*, WM 2003, 1210 (1212); *Kokemoor*, BKR 2004, 135 (139).

dezidiert sicherheitsrechtliche Pflichten.[681] So kann sie einmal eigenständig Daten abrufen, um ihre Pflichten aus dem GWG zu erfüllen oder sonstige strafbare Handlungen zuungunsten der Institute zu verhindern, und andererseits auf Anfragen der Strafverfolgungsbehörden reagieren, soweit dies zur Erfüllung derer Pflichten notwendig ist. Ob diese Auskunftsersuchen legitim sind, hat die BaFin gem. § 24c Abs 3 S. 3 KWG nur zu prüfen, wenn ein *besonderer Anlass* dazu besteht.

Neben der BaFin haben auch das Bundeszentralamt für Steuern (BZSt) nach § 93, Abs. 7, 8, § 93b AO und die Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit – FIU) nach § 31 Abs. 6 GWG automatisierten Zugriff auf das Dateisystem. Sie sind ebenfalls berechtigt, diese Daten auf deren Ersuchen an bestimmte Sicherheitsbehörden, insbesondere die Gefahrenabwehrbehörden, weiterzuleiten.

Die Umstände des Zugriffs staatlicher Stellen auf das Dateisystem sollen im Einzelnen an späterer Stelle noch detailliert erörtert werden (Kap. E. II. 1.). Außerdem soll die Diskussion rund um die Kontobestandsdatenauskunft samt dem hierzu ergangenen Urteil des Bundesverfassungsgerichts umfänglich beschrieben und kommentiert werden (Kap. F. I.).

II. Speicherpflichten für Inhaltsdaten außerhalb des Sicherheitsrechts

Neben den viel besprochenen Kontobestandsdaten[682] fristen diese Kontoinhaltsdaten überraschenderweise noch ein Schattendasein, was sich vielleicht mit der deutlich komplexeren Gesetzeslage erklären lässt. Anders als bei den Bestandsdaten fehlt es hier an einem einheitlichen Dateisystem bzw. einer konkreten Norm, die sowohl Speicherpflicht als auch Zugriffsrechte einheitlich normiert und somit dem § 24c KWG oder §§ 173, 174 TKG entsprechen würde. Die Speicherung von Kontoinhaltsdaten, also die Details von Kontoständen, Transaktionen und anderen Kontobewegungen, wird jedoch ebenso im Rahmen einer ganzen Reihe von Vorschriften vorgeschrieben.

In den bisherigen Untersuchungen der sicherheitsrechtlichen Zugriffe auf Kontoinhaltsdaten wurde bislang zumeist nur unzureichend dargestellt, welche Kontoinhaltsdaten von den Finanzinstituten über ihre Privatkunden

681 Vgl. *Kokemoor*, BKR 2004, 135 (136).
682 Übersicht bei *Pfisterer*, JöR 2017, 393.

gespeichert werden und auf welcher Grundlage dies geschieht.[683] Zwar finden sich in der Literatur zum GwG durchaus entsprechende Ansätze, eine umfassende Betrachtung auch der Normen außerhalb des Sicherheitsrecht wird aber nicht vorgenommen.[684]

Für die sicherheitsrechtliche Debatte lässt sich dieser Umstand damit erklären, dass die allermeisten Speicherpflichten für Kontodaten nicht mit entsprechenden (sicherheitsrechtlichen) Zugriffsnormen verknüpft sind. Im Rahmen einer sicherheitsrechtlichen Betrachtung können nur solche Datenpools als unmittelbar grundrechtsrelevante Vorratsdatenspeicherung angesehen werden, die es gerade bezwecken, dass der Staat im Rahmen der Sicherheitsgewährleistung (zum Begriff des Sicherheitsrechts, oben Kap. B. I. 2. c.) unmittelbar und verdeckt auf sie zugreifen kann. Die schiere Tatsache, dass Daten gesammelt werden, auf die sich Sicherheitsbehörden nach ihren allgemeinen Ermittlungsbefugnissen Zugriff verschaffen können, ist ein gewöhnlicher Umstand der Kommunikationsgesellschaft (s. o. Kap B. III. 2. b. aa.).

Dokumentations- und Aufbewahrungspflichten der kontoführenden Institutionen finden sich im Privat- und Steuerrecht und zielen – soweit man diesen Bereich der Finanzverwaltung insbesondere das Steuerstrafrecht einmal außen vorlässt – nicht unmittelbar darauf ab, den Staat zur Aufklärung und Abwehr von Gefahren bzw. zur Sanktionierung von Kriminalität mit Daten zu versorgen. Sie dienen vielmehr dem Rechtsverkehr und der ordnungsmäßigen Abwicklung der Finanzverwaltung.

683 Von „vast/large amount of stored data" in Bezug auf die Geldwäscherechtlichen Speicherpflichten sprechen etwa *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (243) und *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 103. Bei *Kahler,* Kundendaten, 2017, S. 16 Ist von „riesigen Kundendaten" die Rede. Auf die zivil- und steuerrechtlichen Vorschriften wird jeweils nicht eingegangen.

684 *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438 stellt immerhin fest, dass die Geldwäscherechtlichen Fristen neben § 257 Abs. 1 HGB und § 147 Abs. 1 Nr. 4, Abs. 3 AO leerlaufen

1. Allgemeine Rechnungslegungspflicht nach §§ 666, 675 BGB, 355 HGB – Kontoauszüge

Bei den Kontokorrentverträgen i. S. d. § 355 HGB – zu diesen gehört insbesondere auch das Girokonto eines Bankkunden[685] – handelt es sich um Geschäftsversorgungsverträge i. S. d. § 675 BGB. Im Rahmen dieser hat der Kunde einen Anspruch gegenüber dem Geschäftsbesorger auf Auskunft und Rechnungslegung gem. §§ 675, 666 BGB.[686]

Sowohl im Rahmen von Giro- als auch Kreditkartenverträgen schulden die jeweiligen Institute danach die fortlaufende Dokumentation von Kontobewegungen in Form von Kontoauszügen.[687] Diese können auch digital ausgestellt werden, wovon die Kunden heutzutage in großem Umfang Gebrauch machen.[688]

Dabei dienen die Auszüge nicht als Rechnungsabschluss i. S. d. § 355 Abs. 1 HGB, sondern lediglich der Information des Kunden über den Stand und Verlauf seines Kontos.[689] Damit der Kunde diesen Verlauf nachvollziehen kann, sind die Kreditinstitute im Rahmen von Treu und Glauben zu einer umfassenden Darstellung aller Änderungen[690], also sämtlicher Einzahlungen, Auszahlungen und anderer Buchungen verpflichtet.

Die Kontoauszüge beinhalten regelmäßig die Höhe der Buchung, den Namen des Empfängers sowie einen Verwendungszweck.[691] Schon die Verpflichtung zur Ausstellung von „klassischen Kontoauszügen" verpflichtet die Kreditinstitute also dazu, die Kontobewegungen ihrer Kunden in vollem Umfang aufzuzeichnen.

Der Informationsanspruch des Kunden wird durch die einmalige Aushändigung der Kontoauszüge grundsätzlich erfüllt, eine erneute Auskunft kann nur ausnahmsweise auf §§ 666, 675 BGB gestützt werden. [692]

685 *Fest* in MüKo HGB Bd. VI BankvertragsR, Teil 2 N Rn. 263.
686 *Bitter* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 33 Rn. 56; BGH, NJW-RR 2003, 1555 (1556).
687 *Löhnig*, JR 2007, 73 (75); BGHZ 165, 53; BGH, NJW 1985, 2699.
688 siehe etwa *Deutsche Bundesbank,* Zahlungsverhalten in Deutschland, 2017, S. 21; *BayLfSt* DB 2017, 280.
689 *Canaris,* Handelsrecht, 24. Aufl. 2020, § 25 Rn. 19.
690 BGH, NJW 1985, 2699 (2699).
691 Vgl. *Bankenverband,* Elektronische Kontoauszüge, 2009, https://bankenverband.de/media/publikationen/elektronische-k.pdf.
692 BGH, NJW 2001, 1486 (1486); OLG Schleswig, NJW-RR 2000, 780 (781).

Bankgeschäfte fallen als „Standardgeschäfte" grundsätzlich auch in den Anwendungsbereich des § 675a BGB, der eine Pflicht zur Information über Entgelte und Auslagen der Geschäftsbesorgung (etwa einer Überweisung) vorsieht. Durch die Einführung der §§ 675c ff. BGB (s. u.) wurden jedoch die Informationspflichten hinsichtlich sämtlicher Zahlungen abschließend geregelt. Für Informationen über Kontobewegungen spielt der § 675a BGB daher keine Rolle mehr.[693]

2. Unterrichtungspflicht für Zahlungen nach § 675d BGB, Art. 248 EGBGB, Art. 5 SEPA-VO

Aufgrund der 1. EU-Zahlungsdiensterichtlinie (PSD 1)[694] wurde das bargeldlose Zahlungsrecht im deutschen Privatrecht mit Einführung der §§ 675c ff. BGB modifiziert.[695] Die zahlungsrechtlichen Vorschriften betreffen gem. § 675c Abs. 3 BGB nicht nur Banken bzw. Kreditinstitute, sondern den umfangreichen Katalog an verpflichteten Dienstleistern aus § 1 ZAG. Aus sicherheitsrechtlicher Perspektive sind vor allem die Zahlungsdienstleister relevant, die von Privatpersonen regelmäßig in Anspruch genommen werden, also Banken, Sparkassen, Kreditkartenunternehmen und Online-Zahlungsdienste wie PayPal.[696]

Soweit Kreditinstitute als Zahlungsdienstleister i. S. d. § 675 f. BGB in Erscheinung treten, etwa Banken und Sparkassen im Rahmen der gängigen Giro-Konten,[697] ergeben sich hieraus spezielle Informations- bzw. Un-

693 BT-Drs. 16/11643, S. 98; *Heermann* in MüKo BGB, § 675a Rn. 15.

694 Richtlinie 2007/64/EG des Europäischen Parlaments und des Rates vom 13. November 2007 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 97/7/EG, 2002/65/EG, 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 97/5/EG, ABl. 2007 L 319/1; neu gefasst durch Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/E, ABl. 2015, L337/35.

695 Gesetz zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsdiensterichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 28. Juli 2009, BGBl. I S. 2355.

696 PayPal (Europe) S.à r.l. et Cie, S.C.A. ist allerdings als Kreditinstitut geführt und wird in Luxemburg gelistet, vgl. https://www.paypal.com/de/webapps/mpp/imprint, zuletzt aufgerufen am 12.01.2025.

697 Vgl. *Herresthal* in MüKo HGB Bd. VI BankvertragsR, Teil 1 A Rn. 38, 169; *Wahlers,* Zahlungssysteme, 2013, S. 30 ff.

terrichtungspflichten gegenüber den Kunden nach § 675d Abs. 1, 3 BGB i. V. m. Art. 248 §§ 7,8, 14, 15 EGBGB.[698] Danach müssen die jeweiligen Zahlungsdienstleister sowohl des Zahlenden als auch des Empfängers der Zahlung ihre Kunden über die Umstände der Zahlung unterrichten. Dazu gehören eine Kennung der Zahlung, der Zahlungsbetrag, die Höhe der Entgelte, das Wertstellungsdatum und Angaben zum Zahlungsempfänger, § 248 §§ 7, 8, 14, 15 EGBGB. Soweit Kontobewegungen bargeldlos abgewickelt werden, tritt diese Unterrichtungspflicht neben die allgemeine vertragliche Informationspflicht aus §§ 666, 675 BGB.[699]

Die Unterrichtung hat grundsätzlich durch „Mitteilung" in der besonderen Form des Art. 248 § 3 EGBGB zu erfolgen, was grundsätzlich die Übergabe der gespeicherten Informationen auf einem dauerhaften Datenträger i. S. d. § 126b BGB voraussetzt.[700] Allerdings erlaubt Art. 248 § 10 EGBGB abweichende Vereinbarungen. Von diesen haben die meisten Banken Gebrauch gemacht und teilen die Informationen als Online-Kontoauszüge mit.[701] Durch die Kontoauszüge werden die zahlungsdienstrechtlichen Informationspflichten also abgedeckt.[702]

Bei Überweisungen und Buchungen im Wege des SEPA-Lastschriftverfahrens gilt im Ergebnis dasselbe. Die Zahlstelle, also die Bank des zahlenden Giro-Kunden, muss die Daten aus dem Lastschriftdatensatz auf dem Kontoauszug mitteilen, Art. 5 Abs. 1, 3 SEPA-VO[703] i. V. m. Nr. 1, 2 Anhang SEPA-VO. Hierzu gehören u. a. der Betrag, das Fälligkeitsdatum, die IBAN der einzahlenden Stelle, der Verwendungszweck und eine Angabe, ob die Zahlung wiederkehrend oder einmalig ist, Nr. 1,2 Anhang SEPA-VO. [704]

698 Umsetzung von Art. 30 ff. der ZahlungsdiensteRL 2007/64/EG (a.F.); dazu BT-Drs. 16/11643, S. 100; nunmehr geregelt in Art. 43 ff. (Einzelzahlungen) und Art. 50 ff. (Zahlungen innerhalb von Rahmenverträgen) EU-ZahlungsdiensteRL (EU) 2015/2366.

699 vgl. *Schmieder* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 47 Rn. 24c f.

700 BT-Drs. 16/11643, S. 98; *Casper* in MüKo BGB, Art 248 § 3 EGBGB Rn. 2.

701 *Casper* in MüKo BGB, Art 248 § 10 EGBGB Rn. 1; *Henn/Kuballa*, DB 2016, 1900.

702 BT-Drs. 16/11643, S. 136; BGH, NJW 2014, 922 (922); *Casper* in MüKo BGB, Art. 248 § 7 EGBGB Rn. 4.

703 Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro und zur Änderung der Verordnung (EG) Nr. 924/2009, ABl. 2012 L 94/22.

704 Siehe auch *Zahrte* in Bunte/Zahrte Banken/Sparkassen-AGB, Teil 4, VII Rn. 31.

Aus den zahlungsrechtlichen Vorschriften § 675d BGB, Art. 248 EGBGB und Art. 5 SEPA-VO folgen also spezifische Dokumentationspflichten für Zahlungen und Lastschriften, die einen Großteil der Kontobewegungen im alltäglichen Geschäftsverkehr ausmachen dürften. In der Praxis werden diese Dokumentationspflichten zumindest im Rahmen der Giro-Konten über die Ausstellung von Kontoauszügen abgedeckt.[705]

3. Aufbewahrungspflicht nach §§ 25a KWG, 257 HGB, 22 UStG, 147 AO

Die umfangreiche Dokumentation der Transaktionen geht Hand in Hand mit der bankenaufsichts-, steuer- und handelsrechtlichen Aufbewahrungspflicht. Diese ist in den insoweit aufeinander abgestimmten[706] §§ 25a KWG, 257 HGB und 147 AO normiert.

Nach § 257 HGB ist jeder Kaufmann i. S. d. § 1 HGB – das werden aufgrund der Eigenart des Gewerbes alle aus sicherheitsrechtlicher Perspektive interessanten Institute sein – verpflichtet, die im Katalog des § 257 HGB aufgeführten Unterlagen für teilweise sechs, teils für zehn Jahre aufzubewahren. Eine fast identische Regelung findet sich im Steuerecht in den §§ 22 UstG und § 145 ff. AO, wonach zur Erhebung der Steuer Aufzeichnungen zu machen, §§ 22 UstG, 146 AO, und aufzubewahren sind, § 147 AO. Die hier geregelte Pflicht dient freilich der Steuerhebung, also nicht dem (Privat-) Rechtsverkehr, sondern der Finanzverwaltung. Die Aufzeichnungspflicht des §§ 22 UstG regelt den materiellen Inhalt, der sich aus den Aufzeichnungen für die Steuerbehörden erschließen lassen muss.[707] Die §§ 146, 147 AO hingegen stellen auf die Form der aufzuzeichnenden Dokumente ab. Eine Pflicht zur Aufbewahrung der Aufzeichnungen folgt aber nur aus § 147 AO[708]. Das UStG enthält diesbezüglich keine eigene Regelung.

Die steuerrechtliche Aufbewahrungspflicht bestimmter Dokumente aus § 147 AO unterscheidet sich von § 257 HGB wiederum nur darin, dass sie in Nr. 5 mit den „sonstigen Unterlagen von steuerlicher Bedeutung" einen Auffangtatbestand enthält und die Aufbewahrungsfrist in Einzelfällen auch

705 *Schmieder* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 47 Rn. 24b, § 49 Rn. 112.
706 *Shin,* Organisationspflichten, 2013, S. 169; *Rätke* in Klein AO, § 147 Rn. 147.
707 Siehe § 63 Abs.1 UStDV; *Heidner* in Bunjes UStG, § 22 Rn. 5.
708 Vgl. *Heuermann* in Sölch/Ringleb UStG, § 22 Rn. 68.

über zehn Jahre anordnet, wenn die Unterlagen für laufende Steuerverfahren von Bedeutung sind.[709]

Die Aufbewahrungspflicht aus § 147 AO betrifft sämtliche buchführenden Steuerpflichtigen, wozu nach § 238 Abs. 1 HGB wiederum alle Kaufleute gehören. Für Banken und Zahlungsdienstleister wird schon deshalb in allen relevanten Fällen eine Aufzeichnungs- und Aufbewahrungspflicht bestehen.

Zu den Buchungsbelegen i. S. d.. § 237 Abs.1 Nr. 4 HGB, § 147 Nr. 4 AO gehören alle Unterlagen, die sich auf die in den Büchern und Aufzeichnungen enthaltenen Geschäftsvorfälle beziehen[710], also auch Kontoauszüge.[711] Dabei ist zu berücksichtigen, dass die Kontoauszüge aus Sicht der Bank immer einen Geschäftsvorfall betreffen. Rein privat geführte Kontoauszüge müssen deshalb zwar nicht von den Kunden[712], wohl aber stets von den Banken bzw. Kredit- und Zahlungsinstituten aufbewahrt werden[713]. Davon gehen auch die Banken selbst aus.[714] Aufgrund der Fülle an Dokumenten ist die Aufbewahrung heute nur noch digital möglich.[715] Die §§ 257 Abs. 3 HGB, 147 Abs. 2 AO und 25a Abs. 1 S. 6 Nr. 2 KWG erlauben dies ausdrücklich, soweit die *Grundsätze ordnungsmäßiger Buchführung* beachtet werden. Hierzu hat das Bundesfinanzministerium ein interpretierendes Schreiben herausgebracht (GoBD),[716] das den aktuellen Stand der rechtlichen Anforderungen an die digitale Aufbewahrung aus Sicht der Steuerverwaltung zusammenfasst.[717]

709 Zum Verhältnis der Normen *Schober*, BC 2013, 528; *Treppmann* DB 1989, 1482 (1483).

710 *Cöster* in Koenig AO, § 147 Rn. 12.

711 *Ders.* in Koenig AO, § 147 Rn. 12; *Rätke* in Klein AO, § 147 Rn. 35.

712 *BayLfSt* DB 2017, 280, 50; FG Rheinland-Pfalz, Urteil vom 25.04.1988 – 5 K 351/87; *Cöster* in Koenig AO, § 157 Rn. 12.

713 *T. Knierim* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 10 Rn. 25.

714 *Comdirect,* Aufbewahrung Kontoauszüge, https://magazin.comdirect.de/finanzwissen/wie-lange-kontoauszug-aufbewahren#muss-ich-kontoauszuege-aufbewahren, zuletzt aufgerufen am 12.01.2025.

715 *T. Knierim* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap 10 Rn. 25; *Commerzbank,* Kontoauszüge, https://www.commerzbank.de/portal/de/ratgeber/finanzen/aufbewahrungsfrist-Ihrer-kontoauszuege-das-muessen-sie-wissen.html, zuletzt aufgerufen am 12.01.2025.

716 *Bundesministerium der Finanzen,* GoBD, 2019, BMF-Schreiben vom 28.11.2019 - IV A 4 - 0316/19/10003:001 -, BStBl I S.1269, Anhang 64).

717 *U. Braun* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25a KWG Rn. 679.

Die aufsichtsrechtlichen Aufbewahrungspflichten gem. § 25a S. 6 Nr. 2 KWG verlangen von den in §§ 1, 53, 53b KWG genannten Instituten, dazu gehören insbesondere sämtliche im deutschen Inland tätigen Banken, eine „vollständige Dokumentation der Geschäftstätigkeit, die eine lückenlose Überwachung durch die Bundesanstalt für ihren Zuständigkeitsbereich gewährleistet." Die aufsichtsrechtliche Aufbewahrungspflicht ist folglich offen formuliert und nur auf den Aufsichtsbereich der BaFin beschränkt.[718] Nach der einschlägigen Literatur geht sie dem Umfang nach über die steuer- und handelsrechtlichen Pflichten hinaus.[719]

Für die im Bereich dieser Arbeit interessanten Kontodaten der Privatkunden dürfte dieser erweiterte Umfang aber keine besondere Rolle spielen, da durch die Aufzeichnung der Einlagen, Auszahlungen und Transaktionen auf den Kontoauszügen bereits das Gros der sensiblen Privatdaten abgedeckt wird.

Festzuhalten ist damit zunächst, dass zumindest für einen Zeitraum von zehn Jahren[720] aufgrund verschiedener Regelungen außerhalb des Sicherheitsrechts eine Pflicht zur Aufzeichnung und Aufbewahrung von sämtlichen Geschäftsvorfällen im Rahmen von Giro- und anderen Zahlungskonten besteht, die von den Finanzdienstleistern durch die (digitale) Speicherung der Kontoauszüge erfüllt wird.

III. Sicherheitsrechtliche Speicherpflicht und Überwachung von Kontoinhaltsdaten

Die dargestellten Speicherpflichten verfolgen, abgesehen von der Ahnung von Steuerdelikten, keine unmittelbaren sicherheitsrechtlichen Zwecke. Sie unterscheiden sich damit grundlegend von Normen wie §§ 112b, c TKG, § 2 FlugDaG oder § 24c KWG. Diese zielen darauf ab, private Akteure als Gehilfen der Sicherheitsbehörden einzubinden, indem sie zur Einrichtung und anlasslosen Speisung gesonderter Datenpools verpflichtet werden, die wiederum primär von den Sicherheitsbehörden zur Erfüllung derer Zwecke genutzt werden.

Eine diesem System vergleichbare Speicherung findet sich bei genauerem Hinsehen aber auch im Geldwäschegesetz (GwG) und der Geldtransfer-

718 Idem, Rn. 658

719 *Shin,* Organisationspflichten, 2013, S. 169; *U. Braun* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25a KWG Rn. 668.

720 Vgl. auch die Tabelle bei *Schober*, BC 2013, 528 (532).

verordnung. Dieses Anti-Geldwäscherecht soll im Folgenden beschrieben werden, wobei der Fokus auf den Überwachungsaspekten dieses Systems liegen soll.

1. Geldtransferverordnung

Zunächst ist dabei die GeldtransferVO[721] zu untersuchen. Diese wurde ursprünglich im Jahr 2006[722] erlassen und neun Jahre später, im Zuge der Überarbeitung der GWRL (dazu unten II. 2. a. gg.), überarbeitet.

Die GeldtransferVO und die GWRL stehen in einem engen inhaltlichen Zusammenhang und dienen der Verhinderung von Geldwäsche und Terrorismusfinanzierung.[723] Dabei kommt der GeldtransferVO die Aufgabe zu, die „Papierspur" bzw. den elektronischen Geldverkehr lückenlos rückverfolgbar zu machen.[724] Sie setzt damit Punkt VII der *Special Recommendations* der Financial Action Task Force (FATF) aus dem Jahr 2001[725] um, die heute in Nr. 16 der FATF-Empfehlungen enthalten sind.[726] Anders als etwa die PSD[727] verfolgt sie also primär einen sicherheitsrechtlichen, keinen wirtschaftsrechtlichen Zweck.

Zur Auslegung und Anwendung der Verordnung werden von den Europäischen Aufsichtsbehörden gem. Art. 25 GeldtransferVO Leitlinien verfasst[728], die von der BaFin grundsätzlich übernommen werden.[729]

721 Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006, Abl. 2015, L 141/1.

722 Verordnung (EG) Nr. 1781/2006 des Europäischen Parlaments und des Rates vom 15. November 2006 über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers, Abl. 2006, L 345/1.

723 Erwägungsgründe 8,9 , EU-GeldtransferVO, (EU) 2015/847.

724 Ibid.

725 *FATF,* IX Special Recommendations, 2001, konsolidierte Fassung Feb. 2008.

726 *Dies.,* IX Special Recommendations, 2001, konsolidierte Fassung Feb. 2008, VII; *dies.,* Recommendations 2012, konsolidierte Fassung März 2022, Nr. 16; zur Historie der FATF unten; s.a. *B. Michael Lindner/Lienke/Aydur*, CCZ 2016, 90; *Kunz* CB 2016, 54.

727 Vgl. Erwägungsgründe 4, 5, 7, PSD2, (EU) 2015/2366.

728 Zuletzt *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung.

729 Vgl. *BaFin,* Leitlinien und Q&As der ESA, https://www.bafin.de/DE/RechtRegelungen/Leitlinien_und_Q_and_A_der_ESAs/Leitlinien_und_Q_and_A_der_ESAs_node.html, zuletzt aufgerufen am 12.01.2025.

a. Geltungsbereich

Die Verordnung enthält Vorschriften über Angaben, die von Zahlungsdienstleistern i. S. d. Art. 1 PSD2[730] bzw. § 1 ZAG bei der Ausführung von Geldtransfers übermittelt werden müssen. Der Begriff des Geldtransfers aus Art. 3 Nr. 9 EU-Geldtransferverordnung ist denkbar weit. Er umfasst sämtliche, zumindest teilweise elektronisch ausgeführten Transaktionen von Geld durch einen Zahlungsdienstleister, insbesondere Überweisungen und Lastschriftzahlungen – nach der BaFin aber auch Bareinzahlungen auf ein Fremdkonto.[731]

Allerdings wird eine ganze Reihe an Geldtransfers von der Verordnung ausgenommen, etwa nach Art. 2 Abs. 2 GeldtransferVO alle in Artikel 3 lit. a) – m) und o) PSD2 aufgeführten Zahlungen.[732]

Hierzu gehören insbesondere Bargeldeinzahlungen von Bankkunden auf deren Konto. Außerdem, nach Art. 2 Abs. 4 UAbs. 2 lit. a) – d) GeldtransferVO, Bargeldabbuchungen des Kontoinhabers, Zahlungen an Verwaltungsbehörden, Überweisungen von Zahlungsdienstleistern untereinander in eigenem Namen und Transfers mittels des Austausches von eingelesenen Schecks, einschließlich beleglosem Scheckeinzug

Ebenfalls ausgenommen sind nach Art. 2 Abs. 3 „Geldtransfers, die mit einer Zahlungskarte, einem E-Geld-Instrument oder einem Mobiltelefon oder anderen im Voraus oder im Nachhinein bezahlten digitalen oder IT-Geräten mit ähnlichen Merkmalen durchgeführt werden", wenn die Zahlung ausschließlich für Waren oder Dienstleistungen ergeht und die Nummer des Zahlinstruments übermittelt wird. Dies aber nur, wenn der Geldtransfer an einen Unternehmer geleistet wird, Art. 2 Abs. 3 S. 2, Art. 3 Nr. 12 GeldtransferVO.

Art. 2 Abs. 5 GeldtransferVO erlaubt den Mitgliedstaaten eine weitere Ausnahme einzuführen. Danach können Inlandtransfers bis zu einem Wert von 1.000,00 € auf ein Konto ausgenommen werden. Voraussetzung ist, dass auf das Konto ausschließlich Zahlungen für die Lieferung von Gütern

730 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (Text von Bedeutung für den EWR), ABl. 2015, L 337/35.

731 *BaFin.*, Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 28.

732 Art. 2 Abs. 2 EU-GeldtransferVO verweist (auch in der konsolidierten Fassung, Document 02015R0847-20200101) auf die PSD1., 2007/64/EG.

oder Dienstleistungen vorgenommen werden können. Außerdem muss der Zahlungsdienstleister des Begünstigten den Verpflichtungen der GeldtransferVO unterliegen und in der Lage sein, anhand einer individuellen Transaktionskennziffer über den Begünstigten den Geldtransfer bis zu der Person zurückzuverfolgen, die mit dem Begünstigten eine Vereinbarung über die Lieferung von Gütern und Dienstleistungen getroffen hat. Die Bundesrepublik Deutschland hat von dieser Möglichkeit in § 14 Abs. 5 GwG Gebrauch gemacht.

b. Übermittlung von Angaben

Kernvorschriften der Verordnung sind deren Art. 4 – 6. Diese enthalten Pflichten der Zahlungsdienstleister bei Ausführung von Geldtransfers. Art. 4 nimmt dabei den Zahlungsdienstleister des Auftraggebers in den Blick, also etwa eine Bank, die im Rahmen eines Girovertrags eine Überweisung im Online-Banking durchführt.[733]

Der Zahlungsdienstleister des Auftraggebers muss nach Art. 4 Abs. 1 lit. a) – c) GeldtransferVO sicherstellen, dass Name (lit. a)) und Kontonummer (lit. b)) sowie Kundennummer, Anschrift, Geburtsort- und Datum oder die Nummer eines amtlichen persönlichen Dokuments (lit. c)) des Auftraggebers übermittelt werden.

Auch bzgl. des vom Transfer Begünstigten muss der Zahlungsdienstleister Angaben übermitteln: nach Art. 4 Abs. 2 lit. a) und b) GeldtransferVO Name und Kontonummer des Begünstigten. Erfolgt der Transfer nicht von oder auf ein Konto, muss nach Art. 4 Abs. 3 anstelle der Nummer(n) des Zahlungskontos bzw. der Zahlungskonten eine individuelle Transaktionskennziffer übermittelt werden.

Die Richtigkeit aller Angaben sind von dem Zahlungsdienstleister zu überprüfen, Art. 4 Abs. 4 GeldtransferVO. Diese Überprüfung gilt aber in den Fällen des Art. 4 Abs. 5 GeldtransferVO als automatisch ausgeführt, insbesondere wenn die geldwäscherechtliche Identifikation i. S. d. § 10 Abs. 1 Nr. 1 GwG i. V. m. §§ 11 ff. GwG stattgefunden hat.

Von diesen Übermittlungserfordernissen bestehen bedeutende Ausnahmen nach Art. 5, 6 GeldtransferVO. So reicht nach Art. 5 Abs. 1 GeldtransferVO bei Transfers innerhalb der Union die Übermittlung der Kontonum-

733 *Lienke/Gittfried* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 10 Rn. 20.

mern oder der individuellen Transaktionsnummern aus. Die Regelungen der SEPA-VO bleiben hiervon gem. Art. 5 Abs. 1 S. 2 GeldtransferVO unberührt.

Der Zahlungsdienstleister der Begünstigten darf allerdings innerhalb von drei Tagen die Übermittlung der Informationen verlangen, Art. 5 Abs. 2 GeldtransferVO – bei Transfers unterhalb von 1.000,00 € jedoch nur die Namen von Begünstigtem und Auftraggeber sowie die Kontonummern bzw. Transaktionsnummern. Bei den Transfers unterhalb dieser Schwelle entfällt gem. § 5 Abs. 3 lit. a) und b) GeldtransferVO auch generell die Überprüfungspflicht nach Art. 4 Abs. 4 – es sei denn, es besteht der Verdacht auf Geldwäsche oder Terrorismusfinanzierung oder die zu transferierenden Gelder wurden in Form von Bargeld oder anonymem E-Geld entgegengenommen. Für Geschäfte und Überweisungen des alltäglichen Lebens, die zumeist unter 1.000,00 € liegen und sich innerhalb der EU abspielen, hat die Verordnung somit nur eine untergeordnete Bedeutung.

Die Zahlungsdienstleister müssen stets über Systeme verfügen, mit denen sie jeweils feststellen können, ob und welche Voraussetzungen der Ausnahmetatbestände erfüllt sind.[734]

c. Überprüfungspflichten beim Zahlungsdienstleister des Begünstigten

Die Pflichten des Zahlungsdienstleisters des Begünstigten enthalten die Art. 7 GeldtransferVO. Nach Art. 7 Abs. 1 hat der Zahlungsdienstleister des Begünstigten wirksame Verfahren einzurichten, mit denen er zunächst prüfen kann, ob die Felder für alle notwendig zu übermittelnden Daten eines Transfers in dem verwendeten System überhaupt ausgefüllt wurden.

Mit den eingerichteten Systemen muss er nach Art. 7 Abs. 2, 4 – 6 GeldtransferVO aber auch erkennen können, ob die jeweils notwendigen Angaben nach Art. 4, 5 vorhanden sind. Diese Überprüfungen sollen jedenfalls beim Zahlungsdienstleister des Begünstigten in Echtzeit erfolgen.[735] Ob dies auch für den Zahlungsdienstleister des Auftraggebers gilt, lässt sich den Leitlinien, geschweige denn der Verordnung, nicht entnehmen.

Bei Transfers über 1.000,00 € müssen die Angaben nach Art. 7 Abs. 3 darüber hinaus auf ihre Richtigkeit überprüft werden. Unter diesem Betrag ist keine Prüfung notwendig – es sei denn die Auszahlung erfolgt bar oder

734 *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung, lfd. Nr. 11.
735 Dazu Ibid. lfd. Nr. 22.

in anonymen E-Geld oder es besteht ein hinreichender Verdacht auf Geldwäsche oder Terrorismusfinanzierung. Die Überprüfung gilt aber auch hier als ausgeführt, wenn die geldwäscherechtliche Identifikation stattgefunden hat und die entsprechenden Daten gespeichert wurden, Art. 7 Abs. 5 GeldtransferVO. Außerdem dürfen die Zahlungsdienstleister der Begünstigten nach den ESA-Leitlinien davon ausgehen, dass sie die Vorschriften nach Artikel 7 Absatz 1 und Artikel 11 der Verordnung (EU) 2015/847 einhalten, *wenn sie sich davon überzeugt haben und gegenüber ihrer zuständigen Behörde nachweisen können, dass sie mit den Validierungsregeln des Nachrichten- oder Zahlungs- und Abwicklungssystems vertraut sind und dieses System die Voraussetzungen der Verordnung erfüllt.*[736] Das ist etwa bei der SEPA-Überweisung der Fall.[737]

Nach Art. 8 Abs. 1 GeldtransferVO sind überdies Verfahren einzurichten, „mit deren Hilfe festgestellt werden kann, ob ein Geldtransfer, bei dem die vorgeschriebenen vollständigen Angaben zum Auftraggeber und zum Begünstigten fehlen, auszuführen, zurückzuweisen oder auszusetzen ist, und welche angemessenen Folgemaßnahmen zu treffen sind."

Wird festgestellt, dass Angaben fehlen oder unvollständig sind, so muss der Zahlungsdienstleister des Begünstigten den Transfer zurückweisen oder die Angaben anfordern, bevor er den transferierten Betrag gutschreibt oder sonst zur Verfügung stellt, Art. 8 Abs. 2 GeldtransferVO.

d. Informationserteilung und Speicherung von Daten

Die Art. 14 ff. GeldtransferVO regeln den Umgang der Zahlungsdienstleister mit den aufgrund der Verordnung entstandenen Informationen. Art. 14 bestimmt, dass die Zahlungsdienstleister den für die Terrorismusfinanzierung und Geldwäschebekämpfung zuständigen Behörden unter Einhaltung der Verfahrensvorschriften des Rechts ihrer Sitzmitgliedstaaten auf deren Anfragen hin die nach der Verordnung erhobenen Daten übermitteln müssen.

Die nach Art. 4–7 genannten Angaben sind von den Zahlungsdienstleistern nach Art. 16 Abs. 1 S. 2 GeldtransferVO fünf Jahre lang aufzubewahren. Art. 16 der GeldtransferVO legt allerdings nicht fest, wann die Frist beginnt. Art. 40 Abs. 1 lit. b) der GWRL stellt für den Fristbeginn bzgl. Transaktions-

736 *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung, lfd. Nr. 22.

737 *Lienke/Gittfried* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap 10 Rn. 57.

belegen aus Geschäftsbeziehungen nicht auf das Entstehen des Beleges ab, sondern auf das Ende des Kalenderjahres, in dem der Beleg entstand (siehe unten III. 2. d. bb. (3)). Eine analoge Anwendung drängt sich auf, damit ein Gleichlaufen der Fristen erzielt werden kann.

Es ist somit festzustellen, dass auch nach der GeldtransferVO eine Speicherpflicht für Kontotransaktionsdaten besteht. Aufgrund der umfassenden Ausnahmen, insbesondere Art. 5 Abs. 1 GeldtransferVO und § 14 Abs. 5 GwG, umfasst die Pflicht aber etliche persönlichkeitsrelevante Alltagsgeschäfte nicht. Sie bleibt insofern hinter umfangreicheren Aufbewahrungspflichten zurück und soll daher nicht im Fokus dieser Abhandlung stehen.

2. Geldwäschegesetz – GwG

Eine weitergehende Pflicht zur Speicherung von Kontoinhaltsdaten findet sich auch im Geldwäschegesetz - GwG,[738] das im Zentrum des deutschen Geldwäscherechts steht.

a. Historische Entwicklung des GwG

Das System des GwG kann auf eine recht stringente, nunmehr schon dreißig Jahre dauernde Entwicklung zurückgeführt werden. Da das Untersuchungsobjekt dieser Arbeit das GwG in seiner aktuellen Fassung darstellt, soll die Entwicklung der Gesetzesnormen in angemessener Kürze geschildert werden. Auf eine umfassende Schilderung der einzelnen Regeln und deren Zusammenhänge in den jeweils geltenden Fassungen kann daher verzichtet werden. Stattdessen sollen nur die bedeutsamen Neuerungen der jeweiligen Gesetzesnovellen vorgestellt werden. Um die Systematik des aktuellen Normenkomplex des GwG und der verbundenen Gesetze zu verstehen, ist solch eine überschaubare Übersicht der historischen Fassungen ausreichend.[739]

738 Dass die Aufbewahrungspflichten weitergehend sind, deutet schon *ESA,* Leitlinien Geldtransfer, JC/GL/2017/16, 16.01.2018, dt. Fassung, lfd. Nr. 64 an.

739 Umfassend mit der Entwicklung des GwG beschäftigen sich *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010; *Gürkan,* Geldwäscheprävention, 2019; Übersicht zur europäischen Entwicklung bei *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 80 ff.

aa. FATF-Empfehlungen, erste Geldwäscherichtlinie und GwG

Das GwG wurde ursprünglich mit Gesetz vom 25.10.1993 eingeführt[740] und setzte die 1991 erlassene Richtlinie der EG zur Bekämpfung der Geldwäsche um (1. EG-GeldwäscheRL – GWRL)[741] auf deren Grundlage ein Jahr zuvor schon der Tatbestand der Geldwäsche nach § 261 StGB neu eingeführt wurde.[742]

Die Richtlinie ging inhaltlich auf den ersten Bericht[743] und die „40 Empfehlungen"[744] der von den G-7 Staaten zwei Jahre zuvor geschaffenen „Financial Action Task Force on Money Laundering" (FATF) zurück.[745] In der Erkenntnis, dass es sich bei der Geldwäsche um ein originär internationales Problem handelt[746], war die FATF als Arbeitsgruppe mit dem Ziel gegründet worden, die Ausnutzung der weltweit vernetzten Finanzsysteme zur Verschleierung illegal erwirtschafteter Gelder (und später insbesondere die Terrorismusfinanzierung) zu bekämpfen.[747] Hierzu bedurfte es nach Auffassung der FATF-Staaten eines länderübergreifenden Systems zur Erkennung und Verhinderung illegaler Geldströme.[748]

In seiner Ursprungsform aus dem Jahr 1993 wirkte das GwG aF im Vergleich zum heute gültigen Pflichtenkatalog der §§ 10 ff. GwG noch vergleichsweise überschaubar. Es beschränkte sich zunächst auf eine Identifizierungspflicht bei bestimmten Einzahlungsgeschäften, § 2 GwG aF 1993 und bei „verdächtigen" Transaktionen gem. § 6 GwG aF 1993. Auch der

740 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) vom 25.Oktober 1993 (BGBl. I S. 1770).

741 Richtlinie 91/308/EWG des Rates der Europäischen Gemeinschaften vom 10. Juni 1991 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche (ABl. 1991, L 166/77)

742 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität" (OrgKG) vom 15. Juli 1992 (BGBl. I S. 1302).

743 *FATF,* Report 1990-1991, 1991.

744 *Dies.,* 40 Recommendations, 1990.

745 *Schnabl* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 6 Rn. 1; zur Entstehung der FATF *Pieth* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 4 Rn. 8 f.; *Jekewitz* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 9 Rn. 27; *Krämer,* Geldwäsche und Terrorismusbekämpfung, 2008, S. 46 ff.

746 *Jekewitz* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 9 Rn. 27.

747 *Maillart* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 11 (11 f.).

748 *FATF,* 40 Recommendations, 1990, S. 4 f.; hierzu *Krämer,* Geldwäsche und Terrorismusbekämpfung, 2008, S. 81 ff.

Kreis der allgemein Verpflichteten gem. § 1 GwG aF 1993 war deutlich eingeschränkter als jener des aktuellen § 2 GwG.

Neben der Identifizierungspflicht sah das Ursprungs-GwG bereits eine Meldepflicht der Verpflichteten vor – und zwar dann, wenn eine Transaktion in dem Verdacht stand, den Tatbestand der Geldwäsche i. S. d. § 261 StGB aF 1992 zu erfüllen, § 11 GwG aF 1993. Die Meldung musste sich direkt an die zuständige Strafverfolgungsbehörde richten. Eine zwischengeschaltete Behörde, wie heute die FIU, gab es 1993 noch nicht.

Vor allem beinhaltete das GwG in seiner ersten Fassung schon die für diese Untersuchung bedeutsame Aufzeichnungs- und Aufbewahrungspflicht für alle im Rahmen der Identifizierungspflichten getroffenen Feststellungen, § 9 GwG aF 1993. Anders als Art. 4 der 1. GWRL wurde die Pflicht aber ausdrücklich auf solche Informationen beschränkt, die den Verpflichteten im Rahmen ihrer geldwäscherechtlichen Pflichten entstanden waren. Die Bundesregierung machte sich über die oben angesprochene Frage, ob die 1. GWRL eine Pflicht zur Aufbewahrung sämtlicher Transaktionsdokumente vorsieht, bei der Umsetzung der Richtlinie offenbar ebenfalls Gedanken. In der Gesetzesbegründung führte sie aus, dass sich eine gesondert geregelte Pflicht zur Aufbewahrung der einschlägigen Geschäftsunterlagen im GwG erübrigt, da sich eine solche ohnehin aus § 257 HGB ergäbe.[749]

Dass durch die Aufbewahrungspflicht eine Information „auf Vorrat" für die Ermittlungsbehörden bereitgestellt wird, wurde selbst vom zuständigen Referenten des Bundesaufsichtsamt für das Kreditwesen (BAKred) festgestellt.[750] Dementsprechend wurden die Aufzeichnungspflichten und § 10 GwG aF 1993 auch aus der Perspektive des Rechts auf informationelle Selbstbestimmung diskutiert.[751]

Da nach der GWRL nur die Informationsweitergabe zur Verfolgung der Geldwäsche vorgesehen war, musste sich jedenfalls eine Verwendung der Aufzeichnungen zu anderen Strafverfolgungszwecken oder aus steuerlichen Zwecken an den Grundrechten des Grundgesetzes messen lassen, da insofern keine europarechtlich Überlagerung vorlag.[752] Die überwiegende

749 BT-Drs. 12/2704, S. 16.

750 *Findeisen*, wistra 1997, 121 (123).

751 *Fülbier* in Fülbier/Aepfelbach GWG, 2. Aufl. 1994, § 10 S. 127; ausführlich *Werner,* Geldwäsche, 1996, S. 91 ff; 102 f.

752 *Fülbier* in Fülbier/Aepfelbach GWG, 2. Aufl. 1994, § 10 S. 129; grundlegend BVerfGE 73, 339 [1986] – Solange II;, NJW 1990, 974 – Tabaketikettierungsrichtlinie.

Ansicht kam hier zu dem Ergebnis, dass aufgrund der engen Einschränkung der Weitergabe im Bereich der Geldwäsche und dem geringen legitimen Interesse der Bankkunden an Anonymität im Bereich der betroffenen Transaktionen kein unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung gegeben war.[753] Auch in der späteren Betrachtung wurde § 10 GwG aF 1993 als Ergebnis einer (gelungenen) Abwägung der durch die Aufzeichnungspflichten betroffenen informationellen Selbstbestimmung und dem Strafverfolgungsinteresse gedeutet[754] (zur Diskussion s. Kap F. II. 1.).

Eine konkrete Pflicht im Vorfeld der geldwäscherechtlichen Aufgaben, nach Auffälligkeiten in den Kontodaten ihrer Kunden zu suchen, enthielt das ursprüngliche GwG nicht. Nach § 14 Abs. 2 Nr. 2 GwG 1993 waren aber die in § 14 Abs. 1 GwG 1993 bezeichneten Verpflichteten, insbesondere Kreditinstitute und Versicherungsunternehmen gehalten, *„interne Grundsätze, Verfahren und Kontrollen zur Verhinderung der Geldwäsche“* einzuführen. Diese Norm wurde vom BAKred als geldwäscherechtliche Generalklausel[755] verstanden. Ausgehend von dieser Vorschrift wollte das BAKred ab der zweiten Hälfte der 1990er Jahre eine Verpflichtung zur Etablierung von EDV-Systemen ableiten, mit denen sich im Wege aktiver Nachforschung Auffälligkeiten, die auf einen Geldwäscheverdacht hindeuten konnten, finden ließen.[756] Dieser Prozess[757] wurde als „Research“ oder „Monitoring“ bezeichnet, wobei die genauen Definitionen dieser Begriffe zu Beginn noch schwammig waren.[758] Auch die Einführung dieser EDV-Prozesse wurde heftig diskutiert (zur Diskussion s. Kap. F. II. 3.).

753 *Werner,* Geldwäsche, 1996, S. 91 ff., 102 f.; *Fülbier* in Fülbier/Aepfelbach GWG, 2. Aufl. 1994, § 10 S. 127, 131.

754 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 285.

755 *Findeisen*, wistra 1997, 121 (127).

756 *Artopeus/Findeisen*, (BAKred), Entwurfspapier Anhörung CDU/CSU im Bundestag, 21.08.1995; *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, Ziff. 30, 34d; *BAKred*, Rundschreiben 5/1998, 24.04.1998; *BAKred.,* Jahresbericht, 1998, S. 92.

757 Ein erster Vorschlag zur Funktionsweise solcher Systeme bei *Bergles/Schirnding*, ZBB 1999, 58.

758 Klarheit brachten *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff., Rn. 8.77.

cc. Die zweite Geldwäscherichtlinie

Zu einer ersten Änderung der geldwäscherechtlichen Vorschriften im europäischen Raum kam es im November 2001 durch den Erlass der zweiten EG-Geldwäscherichtlinie.[759] Die 2. GWRL sah nur Änderungen am bestehenden Text vor, keine völlige Neuformulierung. Die Grundstruktur der Richtlinie wurde nicht wesentlich modifiziert. Intensiviert wurde in dieser Hinsicht allenfalls das Kooperationsverhältnis der privaten und staatlichen Akteure.[760]

Die zweite Geldwäscherichtlinie erweiterte vor allem den Anwendungsbereich und den Kreis der Verpflichteten erheblich. Ausgangspunkt dieser Entwicklung war der 1997 durch den Europäischen Rat adoptierte „Aktionsplan zur Bekämpfung der organisierten Kriminalität"[761], den eine von der EG ein Jahr zuvor eingesetzte hochrangige Gruppe ausgearbeitet hatte.[762] Die EG ging davon aus, dass die verschärften Kontrollen der Kreditinstitute dazu geführt hätten, dass sich Geldwäscher andere Wege gesucht hätten.[763] Schon im Aktionsplan war – wohl deshalb – vorgeschlagen worden, die geldwäscherechtlichen Verpflichtungen auf Berufsträger zu erweitern, die ihrer Natur nach gewöhnlich mit Geldwäschern in Berührung kommen.[764] Das sei insbesondere bei Notaren und manchen Angehörigen der Rechtsberufe der Fall.[765]

Insbesondere die Einbeziehung von Anwälten wurde dabei heftig kritisiert, vorwiegend aus den Reihen der Anwaltschaft selbst, die die Vertrau-

759 Richtlinie 2001/97/EG des Europäischen Parlaments und des Rates vom 4. Dezember 2001 zur Änderung der Richtlinie 91/308/EWG des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche - Erklärung der Kommission (ABl. 2001, L 344/76).

760 Darauf weißen auch *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 82 hin.

761 ABl. 1997 C 251/01.

762 Zur Entwicklung *Stefanou/Xanthaki*, J. of Money Laundering Control 3 (2000), 325.

763 Richtlinie 2001/97/EG, Erwägungsgrund 13, ABl. 2001 L 344/76 (77).

764 Aktionsplan zur Bekämpfung der organisierten Kriminalität, Teil III Nr. 10, ABl. 1997 C 251/1 (9).

765 Richtlinie 2001/97/EG, Erwägungsgrund 16, ABl. 2001 L 344/76 (77); empirisch konnte eine solches Gefährdungspotential von Rechtsanwälten, Steuerberatern, Notaren und Wirtschaftsprüfern nicht nachgewiesen werden, *Kilchling/Lukas*, (Max-Planck-Institut für Ausländisches und Internationales Strafrecht), Endbericht Gefährdung, 2004, S. 91 ff.

lichkeit ihrer Mandantenverhältnisse angegriffen sah.[766] Zum Schutz dieser Vertrauensverhältnisse waren in der Richtlinie allerdings Schutzmechanismen implementiert worden.

Neben der Erweiterung des betroffenen Personenkreises war insbesondere die Neukonzeption des Begriffs der „kriminellen Tätigkeit" von Bedeutung, die unter dem Eindruck des Terrorismus als neuer Hauptgefahr entstand.[767] Der Begriff war zuvor auf den Rauschgifthandel gemünzt. Die Richtlinie ließ den Mitgliedstaaten aber die Möglichkeit, weitergehende Definitionen zu implementieren. Neben Deutschland hatten davon auch Frankreich und Griechenland Gebrauch gemacht.[768] Die neue Definition des Art. 1 lit. e) der 2. GWRL folgte diesem Trend und sah nun jede Form der kriminellen Beteiligung an der Begehung einer schweren Straftat als kriminelle Aktivität an. Er enthielt außerdem einen Katalog an Straftatbeständen, die *mindestens* als schwere Straftat in diesem Sinne gelten müssten.

dd. Die Umsetzung der 2. EG-Geldwäscherichtlinie vor dem Hintergrund des 11. Septembers 2001

Die Umsetzung der 2. GWRL in Deutschland wurde flankiert von acht Sonderempfehlungen der FATF, die in einer Sondersitzung zu den Ereignissen des 11. Septembers beschlossen wurden.[769] Für die Einarbeitung in den Text der EU-Richtlinie kamen die Empfehlungen noch zu spät.[770] Es wurde jedoch eine gemeinsame Erklärung des EU-Rats und des EU-Parlaments abgegeben,[771] in der die Wichtigkeit der 2. GWRL zur Bekämpfung der Terrorismusfinanzierung betont wurde.

Der deutsche Gesetzgeber konnte die FATF-Sonderempfehlungen hingegen in der Umsetzungszeit berücksichtigen. Die Implementierung der

766 *Wägenbaur*, EuZW 2002, 293 (296); *Hellwig* AnwBl 2002, 144 (146); *Wegner*, NJW 2002, 794 (795 f.); *Zuck*, NJW 2002, 1397; *Shaugnessy*, Law & Policy in Int. Business 34 (2002), 25 (29, 36 f.) mwN.

767 *Shaugnessy*, Law & Policy in Int. Business 34 (2002), 25 (30 f.); *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 404.

768 *Stefanou/Xanthaki*, J. of Money Laundering Control 3 (2000), 325 (329).

769 Abgedruckt als Annex A in *FATF,* Annual Report 2001-2002.

770 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 404.

771 *Europäische Kommission,* Erklärung vom 19. November 2001, EU-Doc 14237/01, ADD 1, PV/CONS 69; dt. Übersetzung bei *Busch/Teichmann,* Geldwäscherecht, 2003, S. 124.

Richtlinie war dann auch geprägt von den Anschlägen des 11. Septembers 2001 und erfolgte in engem zeitlichem und inhaltlichem Zusammenhang mit dem Erlass weiterer Novellen im Sicherheitsrecht.[772] So wurden im Jahr 2002 nicht nur das die Richtlinie umsetzende Geldwäschebekämpfungsgesetz[773] erlassen, sondern zuvor auch schon das Terrorismusbekämpfungsgesetz[774] und das Vierte Finanzmarktförderungsgesetz,[775] das besonders aufgrund der Einführung des automatischen Abrufsystems von Kontostammdaten (s. o. I. 1.) für Aufsehen sorgte.[776]

Aufgrund der FATF-Sonderempfehlungen wurden als pflichtenaktivierende Verdachtsfälle neben geldwäscheverdächtigen Handlungen i. S. d. § 261 StGB auch solche Transaktionen miteinbezogen, die im Verdacht standen, der Terrorismusfinanzierung i. S. d. § § 129a, 129b StGB[777] zu dienen, § 6 GwG aF 2003.[778] Entsprechend wurde die Anzeigepflicht von Verdachtsfällen angepasst und nun ebenfalls auf die Fälle der Terrorismusfinanzierung erweitert, § 11 GwG aF 2003. Weitere Änderungen betrafen die Identifizierungspflicht, die nunmehr, ganz dem „Know-Your-Customer"[779]-Prinzip folgend[780], nicht erst bei bestimmten Einzahlungen entstand, sondern bei jeder Eröffnung einer Geschäftsbeziehung, § 2 GwG aF 2003.

Von ganz besonderer Bedeutung war weiter die Einführung einer zentralen Stelle für die Sammlung der Verdachtsanzeigen in § 5 GwG aF 2003. Hiermit wurde Empfehlung Nr. 23 der 40 FATF-Empfehlungen aus dem Jahr 1989 umgesetzt, die zwar nicht unmittelbar Einzug in die Geldwäsche-

772 hierzu *Schily*, WM 2003, 1249 (1250 f.); *Jahn*, ZRP 2002, 109 (109 f.); *Herzog/Christmann*, WM 2003, 6; *Hetzer*, ZRP 2002, 407 (408).

773 Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz) vom 08. August 2002 (BGBl. I S. 3105).

774 Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 9. Januar 2002 (BGBl. I, S. 361).

775 Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) vom 21 Juni 2002 (BGBl. I, S. 2010).

776 Nachweise bei *Kokemoor*, BKR 2004, 135.

777 §129b StGB wurde neu eingeführt durch das 34. Strafrechtsänderungsgesetzes vom 22. August 2002 (BGBl. I 3390); zum Zusammenhang mit den übrigen Sicherheitsgesetzen aus dem Jahr 2002: *Schily*, WM 2003, 1249 (1250 f.).

778 *Busch/Teichmann,* Geldwäscherecht, 2003, S. 43 Rn. 87.

779 Siehe *Spoerr* in BeckOK Datenschutzrecht, Grundlagen Syst. J Rn. 150; *Ruce*, Banking Law Journal 128 (2011), 548 (554); *Nave* CB 2018, 166 (167); *Kerber/Quintus* in Hauschka/Moosmayer/Lösler (Hrsg.), Hdb. Haftungsvermeidung, 3. Aufl. 2016, § 55 Rn. 19.

780 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 408.

richtlinie der EG/EU gefunden hatte, aber nach Ansicht der Bunderegierung auch auf europäischer Ebene „konsentiert" war.[781] Die zentrale Meldestelle, schon damals Financial Intelligence Unit (FIU) genannt[782], wurde beim BKA eingerichtet. Hier wurde schon seit dem September 2000 eine Verbunddatei von GwG-Verdachtsmeldungen geführt, die bis dahin von den Landeskriminalämtern übermittelt wurden.[783]

Aus grundrechtlicher Perspektive zentral war die Änderung des § 14 Abs. 2 Nr. 2 GwG aF 2003, die Hand in Hand ging[784] mit dem zuvor durch das vierte Finanzmarktförderungsgesetz eingeführten § 25a Abs. 1 Nr. 4 KWG 2002. Die Normen sahen jeweils fast gleichlautend vor, dass die Verpflichteten „interne Grundsätze, angemessene und geschäfts- wie kundenbezogene Sicherungssysteme sowie Kontrollen zur Verhinderung von Geldwäsche und Terrorismusfinanzierung" entwickeln. Die Bundesregierung beschrieb die Änderung des § 14 Abs. 2 GwG in der Begründung zum Entwurf als bloße Konkretisierung der Norm in ihrer ursprünglichen Fassung.[785] In der Begründung zu § 25a KWG hatte sie jedoch schon selbst festgestellt, dass zu den internen Sicherungsmaßnahmen auch EDV-gestützte Systeme gehören, die eine umfassende Risikoanalyse der Kundenumsätze vornahmen.[786]

Die Begriffe *Monitoring* und *Screening* wurden zunächst weiterhin noch undifferenziert verwendet[787] und bezogen sich zumeist einheitlich und allgemein auf die Überwachung von Transaktionen mittels EDV-Systemen und manueller Prüfungen. Heutzutage definiert die BaFin das Screening als die Echtzeitkontrolle von Überweisungen, die meist dem automatischen Verweigern von verbotenen Transaktionen, etwa aufgrund eines Embargos, dient.[788] Unter Monitoring hingegen fasst sie den Vorgang der nachträglichen Kontrolle getätigter Zahlungen zusammen, unabhängig davon, ob dies automatisch bzw. digital oder manuell geschieht.[789]

781 BT-Drs. 14/8739, S. 13.
782 Idem, S. 2, 10, 13.
783 Idem, S. 13.
784 *Degen,* Geldwäsche, 2009, S. 190 ff.; *Herzog/Christmann*, WM 2003, 6 (11).
785 BT-Drs. 14/8739, S. 17; BT-Drs. 14/9043, S. 11.
786 BT-Drs. 14/8017, S. 125.
787 Hierzu schon *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff. Rn. 8.77.
788 *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.
789 Ibid.

Die Auswirkungen der Monitoringpflicht wurden kontrovers diskutiert. Die Kritiker – etwa der Bundesrat[790] – befürchteten in den neuen Gesetzen eine Verpflichtung zur Rasterfahndung privater Bankkonten durch die Verpflichteten.[791] In der Literatur war gar von einer „Entfesselung des Rechtsstaats" die Rede.[792] (Ausführlich zur Entwicklung der Diskussion siehe Kap. F. II. 4).

ee. Die dritte Geldwäscherichtlinie

Im Jahr 2005 wurde dann die Harmonisierung der Bekämpfung von Geldwäsche und Terrorismusfinanzierung auf europäischer Ebene durch die Einführung der dritten[793], nunmehr, *EU*-Geldwäscherichtlinie weiterentwickelt. Da die 2. GWRL vor dem 11. September 2001 formuliert wurde, kam es erst mit der 3. GWRL zu einer Priorisierung der Terrorismusbekämpfung.[794] Mit der neuen Richtlinie sollten tiefgreifende Änderungen der Geldwäschebekämpfung eingeführt werden, weshalb die ersten beiden Richtlinien aufgehoben und durch einen ganz neuen Text ersetzt wurden.[795]

Die bedeutsamsten Änderungen brachte die Richtlinie für die Sorgfaltspflichten, deren Struktur grundlegend erneuert wurde. Die starren Pflichtenregelungen der ersten beiden Richtlinien wurden durch einen neuen, an verschiedenen Risiken orientierten, Ansatz ersetzt, der für verschiedenen Arten von Transaktionen und in Abhängigkeit von den jeweiligen Kunden differenzierte Pflichten vorsah. Der „Rule-Based-Approach" wurde durch den „Risk-Based-Approach" ergänzt bzw. ersetzt.[796]

790 BT-Drs. 14/9043; S. 5 f. zu §14 Abs. 2 Nr. 2 GwG 2002; BT-Drs. 14/8958, S. 2 zu § 25a KWG 2002;

791 *Bergles/Eul*, BKR 2002, 556; *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (72, 77).

792 *Herzog/Christmann*, WM 2003, 6 (6).

793 Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (ABl. 2005, L 309/15).

794 *Culley*, Irish J. of EU Law 13 (2006), 161 (162); *Mitsilegas/Gilmore*, Int. & Comp. Law Quarterly 56 (2007), 119 (125 ff.).

795 *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 85.

796 *Sotiriadis/Heimerdinger*, BKR 2009, 234 (234); *Costanzo* in Unger (Hrsg.), HdB Money Laundering, 2013, S. 349; *Gürkan,* Geldwäscheprävention, 2019, 95 ff.; Her-

Diesem Prinzip lag nunmehr die Annahme zugrunde, dass nicht alle Kunden und nicht jede Transaktion ab einem bestimmten Wert dasselbe Risiko einer Geldwäsche tragen.[797] Anstatt einheitlicher Regeln sah die Richtlinie deshalb allgemeine (Art. 6-10), vereinfachte (Art. 11-12) und verstärkte Sorgfaltspflichten (Art. 13) vor. Diese verschiedenen Pflichten wiederum waren nicht ausschließlich an starre Kundenkataloge oder Situationen geknüpft, sondern auch an offene Tatbestände.

Eine weitere heikle Neuerung lag in der Einführung einer neuen Kategorie für die Anwendung der Sorgfaltspflichten, nämlich der Geschäftsbeziehungen zu „politisch exponierten Personen."[798] Diese „PEP" wurden durch Art. 3 Nr. 8 der 3. GWRL als *„diejenigen natürlichen Personen, die wichtige öffentliche Ämter ausüben oder ausgeübt haben, und deren unmittelbare Familienmitglieder oder ihnen bekanntermaßen nahestehende Personen"* definiert.

In Anlehnung an die revidierten FATF-Empfehlungen sah die Richtlinie nunmehr auch die Aufstellung von FIUs für die Mitgliedstaaten verbindlich vor, Art. 21 der 3. GWRL. Deren Stellung im System der Geldwäschebekämpfung wurde im Vergleich zum damals geltenden GwG deutlich herausgehoben. Dass diese erheblichen Berechtigungen der FIU nicht von entsprechenden Datenschutzklauseln tangiert wurden, erregte dabei schon früh entsprechende Kritik.[799]

ff. Das Geldwäschegesetz 2008

Die 3. GWRL wurde durch das Geldwäschebekämpfungsergänzungsgesetz (GwBekErgG) vom 13. August 2008[800] in deutsches Recht implementiert. Der Gesetzgeber beabsichtigte dabei eine „Eins-zu-Eins-Umsetzung" der Richtlinie.[801]

---

zog/*Achtelik* in Herzog GwG, Einl. Rn. 86, 157 zu den Begriffen *Ross/Hannan*, J. of Money Laundering Control 10 (2007), 106 (107 ff.).

797 *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 86.

798 Hierzu kritisch *Herzog/Hoch*, WM 2007, 1997 (1999); *Höche*, WM 2005, 8 (12).

799 *Mitsilegas/Gilmore*, Int. & Comp. Law Quarterly 56 (2007), 119 (127).

800 Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz - GwBekErgG) vom 13. August 2008 (BGBl. I S. 1690).

801 Krit. BT-Drs. 16/9631, S. 6; dazu im Einzelnen *Hetzer*, EuZW 2008, 560 (561).

(1) Umsetzung des risikoorientierten Ansatzes

Die Umsetzung sollte demgemäß vor allem dem risikoorientierten Ansatz Rechnung tragen. Zunächst werden die Sorgfaltspflichten untergliedert in allgemeine Sorgfaltspflichten (§ 3 GwG 2008), vereinfachte Sorgfaltspflichten (§ 5 GwG 2008) und verstärkte Sorgfaltspflichten (§ 6 GwG 2008). Die allgemeinen Sorgfaltspflichten treffen grundsätzlich alle Verpflichteten, aber nur in einer begrenzten Anzahl an Situationen, die in § 3 Abs. 2 GwG 2008 aufgezählt wurden.

Diese Eins-zu-Eins aus der 3. GWRL (dort Art. 7) übernommenen Situationen wiederum lassen sowohl einen regel- als auch risikobasierten Ansatz erkennen.[802] So waren die Sorgfaltspflichten regelmäßig bei allen Transaktionen über 15.000 € und bei jeder Begründung einer Geschäftsbeziehung zu erfüllen. Im Übrigen müssen sie erfüllt werden, wenn der Verdacht von Geldwäsche oder Terrorismusfinanzierung aufgrund (sonstiger) Tatsachen besteht, oder wenn Zweifel an der Identität des Vertragspartners bzw. des wirtschaftlich Berechtigten bestehen. Darüber hinaus sah § 3 Abs. 4 GwG 2008 vor, dass die konkrete Anwendung der Sorgfaltspflichten an dem jeweils entsprechenden Risiko des Einzelfalls auszulegen hat.

(2) Die allgemeinen Sorgfaltspflichten: *Kontinuierliche Überwachung*

Die allgemeinen Sorgfaltspflichten wurden in § 3 i. V. m. § 4 GwG 2008 festgelegt und setzten Art. 8 der 3. EU-Geldwäscherichtlinie mit nahezu identischem Wortlaut um. Die allgemeinen Sorgfaltspflichten umfassten danach *die Identifizierung des Vertragspartners* bzw. des wirtschaftlich Berechtigten (nach Maßgabe des § 4 GwG 2008), die *Einholung von Informationen über den Zweck und die angestrebte Art der Geschäftsbeziehung*, die *Abklärung, ob der Vertragspartner für einen wirtschaftlich Berechtigten* handelt, sowie die *kontinuierliche Überwachung der Geschäftsbeziehung, einschließlich der in ihrem Verlauf durchgeführten Transaktionen*.

Die Identifizierungspflicht lag trotz einer Erweiterung bei der Betrachtung des wirtschaftlich Berechtigten. Es wurde nunmehr nicht nur noch

802 *Gürkan,* Geldwäscheprävention, 2019, S. 228; *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 461; *Ackermann/Reder*, WM 2009, 158 (166 f.).

zwischen der auftretenden Person und dem eigentlichen Vertragspartner unterschieden[803] – nichts grundsätzlich Neues.[804]

Dasselbe lässt sich über die, kontinuierliche Überwachungspflicht nach 3 Abs. 1 Nr. 4 GwG 2008 sagen,[805] die im Fokus dieser Arbeit steht. Schließlich war das sogenannte *Kontenscreening* und -*Monitoring*[806] ja zuvor schon in § 14 Abs. 2 Nr. 2 GwG 2002, § 25a Abs. 1 S. 1Nr. 4 KWG 2002[807] vorgesehen[808], und bereits seit Ende der 1990er Jahre vom BAKred etabliert.[809] Die Überwachungspflicht wurde aber durch die Einführung gleich mehrerer neuer Vorschriften deutlich ausdifferenzierter.[810]

Hierbei wurde abermals versäumt, das Verhältnis des Monitorings als interne Sicherungsmaßnahme zu der neu eingeführten Überwachungspflicht (als allgemeine Sorgfaltspflicht) verständlich im Gesetz zu regeln. Über die Definitionen dieser Begrifflichkeiten herrschte daher noch immer keine Klarheit.[811]

(3) Aufzeichnungs- und Aufbewahrungspflicht

In § 8 Abs. 3 GwG 2008 wurde weiter eine umfangreiche fünfjährige Aufzeichnungs- und Aufbewahrungspflicht bezüglich aller „sonstigen" im Rahmen der Sorgfaltspflichten erhobenen Angaben und eingeholten Informationen über Vertragspartner, wirtschaftlich Berechtigte, Geschäftsbeziehungen und Transaktionen eingeführt. Durch die Einbeziehung von sonstigen Belegen und Aufzeichnungen über Geschäftsbeziehungen und Transaktio-

803 BT-Drs. 16/9038, S. 38.
804 *Sotiriadis/Heimerdinger*, BKR 2009, 234 (236).
805 *Ackermann/Reder*, WM 2009, 158 (164); *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 2.
806 nach *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 2 werden diese Begriffe undifferenziert konvergent verwendet; heutige Definition bei *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.
807 Später § 25a Abs. 1 Satz 3 Nr. 6 KWG (2005) bzw. § 25a Abs. 1 Satz 6 Nr. 3 KWG (2007). Zur Änderungsgeschichte *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 15; *ders.* in Herzog GwG, 3. Aufl. 2018, KWG § 25h Rn. 1 f.
808 Hierzu *Jahn*, ZRP 2002, 109 (110); *Herzog/Christmann*, WM 2003, 6 (11).
809 Dazu nur *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 611 ff.; *Herzog*, WM 1996, 1753; *ders.*, WM 1999, 1905.
810 *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 14.
811 Schon *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff. Rn. 8.77.

nen wurde die bisher in § 9 GwG 2002 geregelte Aufzeichnungs- und Aufbewahrungspflicht erweitert.[812]

Der Wortlaut wurde somit in Bezug auf Transaktionsbelege der Richtlinie angepasst. Die Aufzeichnung und Aufbewahrung waren aber – anders als bei Art. 30 lit. b) der 3. EU-Geldwäscherichtlinie – weiterhin an die Ausführung einer Sorgfaltspflicht geknüpft. Dennoch wollte die Bundesregierung mit der Neuschaffung des § 8 Abs. 3 GwG 2008 auf Art. 30 lit. b) der 3. EU-Geldwäscherichtlinie reagiert haben.[813]

Offenbar hatte die Bundesregierung die zuvor vertretene Auffassung aufgegeben, dass eine umfassende Speicherpflicht im GwG neben § 257 HGB gänzlich entbehrlich wäre.[814] Die Einführung einer eingeschränkten Speicherpflicht in Abhängigkeit von den Sorgfaltspflichten erscheint vor diesem Hintergrund als Kompromiss.

Der genaue Umfang der geldwäscherechtlichen Aufzeichnungs- und Aufbewahrungspflicht, insbesondere die inhaltliche Abgrenzung zu den umfassenden Aufbewahrungspflichten, etwa aus § 257 HGB, blieb damit weiterhin schwammig. Weder aus den Gesetzesmaterialien noch aus der zeitgenössischen Literatur lässt sich einheitlich erkennen, ob sich eine Auszeichnungspflicht für sämtliche Transaktionen aus dem GwG ergab, oder diese (wie bislang) nur auf solche Informationen beschränkt war, die im Rahmen der Erfüllung von Sorgfaltspflichten anfielen.

Die Opposition in Gestalt der FDP-Fraktion äußerte sich zu der Erweiterung des § 8 GwG entsprechend kritisch und befürchtete, dass die neue Regelung als „unbegrenzte Verpflichtung zur Datensammlung und -aufbewahrung" verstanden werden könnte.[815] Sie beantragte deshalb eine Änderung des Entwurfs zu § 8 GwG 2008 dahingehend, dass die Aufzeichnungspflicht nicht für die Überwachungspflicht nach § 3 Abs. 1 Nr. 4 GwG 2008 gelten sollte, sondern nur für die übrigen Sorgfaltspflichten.[816]

812 *Warius* in Herzog GWG, 1. Aufl. 2010, § 8 GWG Rn. 1.
813 BT-Drs. 16/9038, S. 42.; *Ackermann/Reder*, WM 2009, 200 (208) *Warius* in Herzog GWG, 1. Aufl. 2010, § 8 GWG Rn. 19.
814 So noch BT-Drs. 12/2704, S. 16.
815 BT-Drs. 16/9647, S. 3.
816 Idem, S. 4.

gg. Die vierte EU-Geldwäscherichtlinie

Als Reaktion auf die „FATF-Empfehlungen 2012“[817] beschloss die EU-Kommission, das europäische Regelwerk zur Geldwäschebekämpfung zu evaluieren und beauftragte eine große Beratungsfirma mit der Erstellung eines entsprechenden Gutachtens[818]. Obwohl dieses feststellte, dass die 3. GWRL eine effektive Geldwäschebekämpfung gewährleistete, war man sich bei der Kommission sicher, dass die Effektivität und Einheitlichkeit innerhalb der Union noch gesteigert werden müssten, um dem neuen internationalen Standard zu entsprechen.[819] Die EU-Kommission beschloss daher eine Neuauflage der Geldwäscherichtlinie.[820] In der Folge wurde die 3. GWRL im Mai 2015 aufgehoben und wiederum durch einen gänzlich neuen Gesetzestext in der 4. EU-Geldwäscherichtlinie[821] ersetzt.

Diese (in großen Teilen noch heute aktuelle) 4. GWRL basiert weiterhin auf dem risikoorientierten Ansatz bzw. versucht, diesen gegenüber ihrer Vorgängerrichtlinie sogar noch verstärkt zum Ausdruck kommen zu lassen.[822] Die Unterscheidung zwischen allgemeinen, vereinfachten und verstärkten Sorgfaltspflichten, abhängig vom jeweiligen Risiko der Geschäftsbeziehung bzw. Transaktion wird entsprechend beibehalten. Erstmals aber enthielt die Richtlinie im Anhang Faktoren bzw. Variablen, mit denen sich die Risiken von Geldwäsche und Terrorismusfinanzierung bewerten lassen. Anstatt einer weithin regelbasierten Einteilung in die einzelnen Risikogrup-

817 *FATF,* Recommendations 2012, orig. Fassung Feb. 2012; überarbeitet *dies.,* Recommendations 2012, konsolidierte Fassung März 2022.

818 *Deloitte*, AML Study, 2011.

819 *Steenwijk* in Zwaan/Lak/Makinwa ua. (Hrsg.), Governance and Security, 2016, S. 209 (219); *Europäische Kommisison*, COM(2013) 45 final, 2013/0025 (COD), S. 2.

820 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, COM(2013) 45 final, 2013/0025 (COD).

821 Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl. 2015, L 141/73

822 *Ruppert*, DStR 2015, 1708 (1709); *Frantangelo* in Siclari (Hrsg.), Anti-Money-Laundering, 2016, S. 11 (11 f.); *Rößler*, WM 2015, 1405 (1407); kritisch ob dies gelingt: *Steenwijk* in Zwaan/Lak/Makinwa ua. (Hrsg.), Governance and Security, 2016, S. 209 (222).

pen sollte die Bewertung künftig noch dichter am Einzelfall ausgerichtet sein.

Die Stellung der zentralen Meldestellen wurde weiter gestärkt. Diese waren nunmehr als unabhängige, eigenständig arbeitende Behörden zu organisieren, Art. 32 Abs. 3 der 4. GWRL. Ihnen wurde nach Art. 32 Abs. 3 a. E. der 4. GWRL das Recht eingeräumt, von den Verpflichteten zusätzliche Informationen einzuholen und im *„Falle des Verdachts, dass eine Transaktion mit Geldwäsche oder Terrorismusfinanzierung zusammenhängt, unmittelbar oder mittelbar Sofortmaßnahmen zu ergreifen, um die Zustimmung zu einer laufenden Transaktion zu versagen oder auszusetzen, damit sie die Transaktion analysieren, dem Verdacht nachgehen und die Ergebnisse der Analyse an die zuständigen Behörden weitergeben kann",* Art. 32 Abs. 7 der 4. GWRL.

Relevante Änderungen gab es weiter hinsichtlich der organisatorischen Pflichten im Vorfeld und im Nachhinein der Anwendung von Sorgfaltspflichten und zwar sowohl für die Staaten selbst als auch für die Verpflichteten. Diese Änderungen sind im Kontext des verstärkten risikoorientierten Ansatzes zu lesen. Da die Anwendung der verschieden intensiven Sorgfaltspflichten stärker am individuellen Risiko auszurichten ist, mussten die Pflichten zur Risikoerkennung entsprechend verschärft werden.[823]

Das Verhältnis des Geldwäscherechts zum Datenschutz wurde im Vorfeld der vierten Richtlinie schwerpunktmäßig diskutiert.[824] Dass sich der europäische Gesetzgeber der Datenproblematik bewusst war, ergibt sich allein daraus, dass er das Richtlinienkapitel V in „Datenschutz, Aufbewahrung von Aufzeichnungen und statistische Daten", Art. 40-44 der 4. GWRL, umbenannt hatte. Am Umfang der Aufbewahrungspflicht, Art. 40 Abs. 1 der 4. GWRL, hatte sich aber faktisch nicht geändert. Lediglich die Weitergabe der Informationen war auf die Zwecke der „Verhinderung, Aufdeckung und Ermittlung möglicher Geldwäsche oder Terrorismusfinanzierung durch die zentrale Meldestelle oder andere zuständige Behörden" beschränkt.

823 Vgl. *Tonnara* in Siclari (Hrsg.), Anti-Money-Laundering, 2016, S. 57 (61 f.); *Mitsilegas/Vavoula* Maastricht J. of EU and Comp. Law 23 (2016), 261 (267 f.).

824 *Rößler*, WM 2015, 1405 (1411 f.).

hh. Das Geldwäschegesetz 2017

Das vierte Geldwäschegesetz wurde im Juni 2017 durch eine Neufassung des GwG in deutsches Recht umgesetzt.[825] Da die Grundstruktur des GwG – insbesondere der Inhalt und die Systematik der für diese Arbeit relevanten Regelungen – seitdem kaum geändert wurden, soll hier in überschaubarem Umfang über die wesentlichen Änderungen referiert werden. Eine umfangreiche Darstellung des aktuellen GwG erfolgt an späterer Stelle (s. III. 2. b.).

Die Änderungen betrafen zunächst die FIU, die nun nicht mehr Zentralstelle *für Verdachtsmeldungen,* sondern *für Finanztransaktionsuntersuchungen* hieß. Sie wurde vom BKA ausgelöst und beim Zollkriminalamt angesiedelt, § 5a FVG, arbeitete jedoch ausdrücklich als eigenständige, unabhängige Organisationseinheit, als „Behörde in der Behörde"[826], im Geschäftsbereich des Bundesministeriums und war von der Fachaufsicht zumindest partiell befreit, §§ 27 Abs 2, 28 Abs. 2 GwG 2017. [827]

Neben dieser strukturellen Änderung wurden auch die Aufgaben und Aktivitäten der FIU in Umsetzung der Richtlinie neu organisiert. Nach § 28 GwG 2017 hatte die FIU die *„Aufgabe der Erhebung und Analyse von Informationen im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung und der Weitergabe dieser Informationen an die zuständigen inländischen öffentlichen Stellen zum Zwecke der Aufklärung, Verhinderung oder Verfolgung solcher Taten.*" Die Maßnahmen, mit denen die FIU dieser Aufgabe nachzukommen hat, wurden in § 28 Abs. 1 S. 2 GwG 2017 katalogisiert und in den §§ 29 ff. GwG 2017 ausgebreitet. Ihre neuen Kompetenzen gingen deutlich über jene des BKAs und der Strafverfolgungsbehörden hinaus.[828]

Insbesondere wird die Arbeit der FIU nicht auf die Aufklärung und Verhinderung von Geldwäsche beschränkt. Sie hat nach § 28 Abs. 3 GwG 2017 auch hinsichtlich der allgemeinen Gefahrenabwehr und Strafverfolgung

825 Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017 (BGBl. I, S. 1822).

826 BT-Drs. 18/11555, S. 90.

827 Hierzu *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (224); *Spoerr/Roberts*, WM 2017, 1142 (1143); zur Kritik *Da Barreto Rosa* in Herzog GwG, § 27 GWG Rn. 7.

828 *Spoerr/Roberts*, WM 2017, 1142 (1148).

mit den hierfür zuständigen Behörden zusammenzuarbeiten.[829] Das zeigt sich insbesondere in § 32 Abs. 3 Nr. 2 GwG, nach dem die FIU auch zur *Aufklärung sonstiger Gefahren und die Durchführung von anderen Strafverfahren* (die nicht im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung stehen) Daten auf Ersuchen bestimmter Sicherheitsbehörden übermitteln soll.

Aufgrund dieser Regelungen war nun zweifelhaft, ob der FIU weiterhin lediglich eine *Filterfunktion* zukam,[830] oder ob sie nicht eher als eine Art *Finanzgeheimdienst* eingestuft werden müsste (dazu ausf. Kap. G. III. 3. b. bb.).[831]

Neu war auch das aufgrund des Art. 30 der 4. GeldwäscheRL einzuführende Transparenzregister in den §§ 18 ff. GwG 2017. In dieses waren nunmehr Informationen über den wirtschaftlichen Berechtigten einzutragen, und zwar nicht nur von den Verpflichteten nach § 2 GwG 2017, sondern von allen juristischen Personen des Privatrechts, § 20 Abs.1 GwG 2017.[832] Das Transparenzregister schuf somit eine zentrale Schnellübersicht über sämtliche juristische Personen des Privatrechts, in der die wichtigsten Basisinformationen sowie alle geldwäscherelevanten Daten gebündelt hinterlegt wurden. Zur Einsichtnahme, soweit dies zu deren Aufgabenerfüllung erforderlich war, wurden insbesondere die FIU, die Strafverfolgungsbehörden und die Gefahrenabwehrbehörden ermächtigt, § 23 GwG 2017.

Auf das Transparenzregister wurde in der deutschsprachigen Literatur besonders kritisch reagiert.[833] Dabei wurde insbesondere auch ein konkreter Zusammenhang mit der Rechtsprechung des EuGH zur Vorratsdatenspeicherung (von TK-Verkehrsdaten) hergestellt. Da das Register keinerlei Differenzierungen enthalte, stelle es anlasslos private Daten für sämtliche staatliche Behörden inklusive Sicherheitsbehörden zur Verfügung.[834] Es greife daher in unverhältnismäßiger Weise in Art. 7, 8 EU-GRC ein.[835] Die-

829 s.a. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (224 f.).
830 So BT-Drs. 18/11555, S. 90
831 Vgl. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (249 f.); *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21.
832 Hierzu *Diller/Brauneisen/Hütten* NZA 2017, 1512 (1513).
833 *N. Müller*, NZWiSt 2017, 87 (91 ff.) *dies*., NZWiSt 2017, 121; *Escher-Weingart/M. Stief*, WM 2018, 693 (697 ff.); *Spoerr/Roberts*, WM 2017, 1142 (1148).
834 *N. Müller*, NZWiSt 2017, 121 (122).
835 Idem, (122).

ser Auffassung hat sich der EuGH jüngst angeschlossen und die Regelungen als grundrechtswidrig und nichtig erklärt.[836]

ii. Die fünfte Geldwäscherichtlinie, EU-FinanzinformationsRL und das aktuelle GwG

Die GWRL wurde im Juli 2018 zuletzt geändert. Aktuell liegt sie somit in der fünften Fassung vor,[837] wobei kein völlig neuer Gesetzestext geschaffen, sondern nur die 4. GWRL in Teilen geändert bzw. ergänzt wurde.

Die aus sicherheitsrechtlicher Perspektive bedeutsamste Änderung lag in der Einführung des Art. 32 Abs. 9 GWRL. Nach dieser Vorschrift kann *jede zentrale Meldestelle im Rahmen ihrer Aufgaben unbeschadet des Artikels 34 Absatz 2 von jedem Verpflichteten Informationen für (sic) den in Absatz 1 genannten Zweck anfordern, einholen und nutzen, selbst wenn keine vorherige Meldung gemäß Artikel 33 Absatz 1 Buchstabe a oder Artikel 34 Absatz 1 erstattet wurde*. Damit sah die GWRL erstmals ausdrücklich eine umfangreiche Zugriffsmöglichkeit der FIUs auf Informationen der Verpflichteten vor, die konkrete Anforderungen sowohl in materieller als auch formeller Hinsicht vermissen ließ.

Aufgrund der Richtlinie wurde das GwG im Dezember 2019 novelliert.[838] Eine Umsetzung des 32 Abs. 9 GWRL war nicht notwendig, da in § 30 Abs. 3 GwG bereits eine entsprechende Zugriffsnorm enthalten war.

Zu einer wichtigen Änderung kam es aber im Rahmen des Erlasses der EU-Finanzinformationsrichtlinie (FinanzinformationsRL). [839] In dieser

836 EuGH, Urt. v. 22.11.2022 – C-37/20, C-601/20 (WM ua/Luxembourg Business Registers) = NJW 2023, 199.

837 Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. 2018, L 156/43.

838 Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie vom 12. Dezember 2019, BGBl. I 2602; hierzu *Glaab/Neu/Scherp* BB 2020, 322; *Feiler/J.-W. Kröger*, CCZ 2019, 262.

839 Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates, ABl. 2019, L 186/122.

wurden die Mitgliedstaaten verpflichtet, Vorschriften zu erlassen, die es den nationalen Sicherheitsbehörden erleichtern sollten, auf die Daten der FIU zur Bekämpfung schwerer Kriminalität zuzugreifen, also nicht nur zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung.[840] Aus dieser Zielsetzung ergab sich, dass der europäische Gesetzgeber offenbar bislang davon ausgegangen war, dass die auf Grundlage der GWRL erhobenen Informationen ausschließlich für diese Zwecke möglich war.[841]

Ausgehend von Art. 3 FinanzinformationsRL soll eine solche Übermittlung aber nur an ausdrücklich benannte Behörden zulässig sein. Darüber hinaus sieht die Richtline eine Reihe von Anforderungen, Art. 5, und Verfahrensvorschriften vor, etwa eine Protokollpflicht, Art. 6.

In Deutschland ist eine Umsetzung der FinanzinformationsRL durch die Einführung des § 32 Abs. 3a GwG erfolgt.[842] Als Behörde wurde das BKA benannt, § 3 Abs. 2a S. 2 BKAG. Weiterhin aber ist nach § 32 Abs. 3 Nr. 2 GwG eine Übermittlung auch zur Aufklärung sonstiger Gefahren und Bekämpfung sämtlicher Strafverfahren an die in § 32 Abs. 3 S. 1 GwG benannten Behörden (Strafverfolgungsbehörden, Bundesverfassungsschutz, BND und MAD) möglich. In Deutschland kann also keine Rede davon sein, dass erst im Rahmen der FinanzinformationsRL eine Übermittlung zu anderen Zwecken als der Bekämpfung von Geldwäsche und Terrorismusfinanzierung ermöglicht wurde.

Diese Diskrepanz weckt ernsthafte Zweifel an der Unionsrechtsmäßigkeit der Übermittlungsregeln des GwG (dazu Kap. G. III. 2. c. cc.).

840 Vgl. BT-Drs. 19/28164, S. 30.

841 Vgl. Erwägungsgrund Nr. 15, FinanzinformationsRL.

842 Gesetz zur europäischen Vernetzung der Transparenzregister und zur Umsetzung der Richtlinie 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Nutzung von Finanzinformationen für die Bekämpfung von Geldwäsche, Terrorismusfinanzierung und sonstigen schweren Straftaten (Transparenzregister- und Finanzinformationsgesetz) vom 25.06.2021 (BGB I, S. 2083); dazu BT-Drs. 19/28164, S. 54.

jj. Ein Blick in die Zukunft

Noch während der Bearbeitung dieser Arbeit, am 20. Juli 2021, hat die Kommission eine Vorlage für eine Geldwäscheverordnung vorgelegt.[843] Diese soll die GeldwäscheRL aber nur teilweise ablösen. [844] Die GeldwäscheRL soll stattdessen in Form der 6. GWRL ebenfalls neu gefasst werden.[845] Die Regeln zu den Verpflichteten und deren Sorgfaltspflichten sollen zukünftig in der Geldwäscheverordnung – GWVO geführt werden. Die Richtlinie enthält dann noch die allgemeinen Vorgaben zur supra- und nationalen Risikoanalyse sowie zu den verschiedenen Registern – außerdem die Vorgaben zu den FIUs.

Darüber hinaus will die Kommission die Grundlage für eine eigene EU-Behörde bzw. FIU mit dem Namen *Authority for Anti-Money Laundering and Countering the Financing of Terrorism* (AMLA) schaffen.[846] Auf diese sollen die Kompetenzen der Europäischen Bankenaufsichtsbehörde im Bereich der Geldwäsche- und Terrorismusfinanzierung übertragen werden.[847]

Die GeldtransferVO soll ebenfalls erneuert, allerdings nicht neu gefasst, sondern nur ergänzt werden.[848] Die Ergänzung erweitert den Anwendungsbereich der Verordnung auf den Transfer bestimmter Kryptowährungen.

Inhaltliche Änderungen der Überwachungs- oder der Aufzeichnungs- und Aufbewahrungspflicht finden sich in den Gesetzesvorschlägen nicht. Die Regelung der Überwachungspflicht als allgemeine Sorgfaltspflicht in

843 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, 20. Juli 2021, COM(2021) 420 final, 2021/0239 (COD).

844 Übersicht bei *Europäische Kommission,* Anti-money laundering and countering the financing of terrorism legislative package, 20.07.2021, https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en, zuletzt aufgerufen am 12.01.2025; dazu *Brian/Frey/Pelz*, CCZ 2021, 209.

845 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die von den Mitgliedstaaten einzurichtenden Mechanismen zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Aufhebung der Richtlinie (EU) 2015/849, 20. Juli 2021, COM(2021) 423 final, 2021/0239 (COD),

846 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung der Behörde zur Bekämpfung der Geldwäsche und Terrorismusfinanzierung und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010, 20. Juli 2021, COM(2021) 421 final, 2021/0240 (COD).

847 Idem, S. 29.

848 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte (Neufassung), 20. Juli 2021, COM(2021) 422 final, 2021/0241 (COD).

Art. 13 Abs. 1 lit. c) GWRL soll in Art. 16 Abs. 1 lit. (d) GWVO fast wortgleich übernommen werden. Die Änderungen sind redaktioneller Natur. Dem Umfang der Überwachungspflicht soll sich zwar künftig ein eigener Art. 21 GWVO widmen. Dieser betrifft aber vor allem die genauen Umstände über die Pflicht zur Aktualisierung der Kundendaten. Auf den Ablauf des Monitorings soll er sich offensichtlich nicht auswirken. Auch die Vorschrift des Art. 13 Abs. 3 GWRL, der eine Mindestpflicht zur Überwachung bei Anwendung vereinfachter Sorgfaltspflichten vorsieht, soll beibehalten werden und findet sich im neuen Art. 27 Abs. 1 UABs. 2 GWVO.

Die verstärkte Überwachungspflicht, bislang in Art. 18 Abs. 2 GWRL geregelt, bleibt ebenfalls erhalten, die risikoorientierte Anwendung wird aber spezifiziert. Im vorgeschlagenen Art. 28 Abs. 4 GWVO findet sich ein Katalog an Maßnahmen, die von den Verpflichteten in den Situationen, die eine verstärkte Sorgfaltspflicht auslösen, angewandt werden können. Der Wortlaut „apply any of these measures" impliziert dabei aber, dass nicht alle Maßnahmen kumuliert ergriffen werden müssen, sondern zur Auswahl der Verpflichteten stehen. Insoweit könnte die Pflicht zur verstärkten Überwachung abgeschwächt werden. Allerdings werden die verstärkten Sorgfaltspflichten bei Korrespondenzbankbeziehungen und PEP in eigene Artikel ausgegliedert (Art. 31 und 32) und sehen weiterhin strikt anzuwendende, verstärkte Sorgfaltspflichten vor.

Die Aufzeichnungs- und Aufbewahrungspflicht des Art. 40 GWRL ist wortgleich in Art. 56 GWVO enthalten.

Soweit sich aus dem aktuellen Anti-Geldwäscherecht eine umfassende Pflicht zur Speicherung von Kontoinhaltsdaten ergibt, ist also auch von den Gesetzesvorschlägen keine Änderung zu erwarten. Sie unterscheiden sich insofern nicht von dem aktuellen Regelwerk, das im folgenden Abschnitt erläutert werden soll.

b. Die Sorgfaltspflichten als Leitsystem des GwG: insbesondere *kontinuierliche Überwachung*

Der Kern des deutschen Anti-Geldwäscherechts ist (noch) das GwG. Ziel des GwG ist die Verhinderung von *Geldwäsche* und *Terrorismusfinanzierung*. Diese Begriffe werden in § 1 Abs. 1, 2 GwG legaldefiniert. Hinsichtlich der Geldwäsche wird auf § 261 StGB verwiesen. Dort findet sich der entsprechende Straftatbestand.

Die Terrorismusfinanzierung ist nach § 89c StGB ebenfalls strafbewehrt, allerdings geht die Definition des GwG über diesen Straftatbestand hinaus. So gilt nach § 1 Abs. 2 GwG nicht bloß die *Begehung einer Tat nach § 89c StGB* als Terrorismusfinanzierung, sondern auch das „*Bereitstellen oder Sammeln von Vermögensgegenständen mit dem Wissen oder in der Absicht, dass diese Vermögensgegenstände ganz oder teilweise dazu verwendet werden oder verwendet werden sollen*" eine Tat nach §§ 129a, 129b StGB oder Art. 3, 5-10 und 12 der Terrorismusbekämpfungsrichtlinie 2017[849] zu begehen.

Trotz mancher Divergenzen sind sämtliche in dieser Richtlinie aufgeführten Taten nach den §§ 89c, 129a, 129 StGB strafbewehrt, allerdings nicht immer explizit als terroristische Straftaten.[850] Durch den Verweis in § 1 Abs. 2 Nr. 1 lit. b) GwG auch auf die Terrorismusbekämpfungsrichtlinie wird der Begriff der Terrorismusfinanzierung mithin erweitert.[851] Auf die strafrechtlichen Feinheiten soll indes hier nicht eingegangen werden. Aufgrund der Verweisungen ist § 1 Abs. 2 GwG jedenfalls so weitreichend, dass sämtliche vollendete oder versuchte Vermögensabflüsse im Zusammenhang mit einer terroristischen Tat (im deutschen oder EU-Sinne) unter Terrorismusfinanzierung gefasst werden können.[852] Um diese Vermögensflüsse aufzudecken und somit Straftaten ermittelt oder verhindert werden können, versucht das GwG, den Geldfluss transparent zu machen, indem es die unmittelbar am Geldfluss Beteiligten zu bestimmten Maßnahmen verpflichtet.[853] Es handelt sich also um eine sicherheitsrechtliche Begrenzung der Heimlichkeit bestimmter wirtschaftlicher Vorgänge und somit der informationellen Selbstbestimmung (zur bisherigen Diskussion s. Kap. F. II.).[854]

Im vorangegangenen Abschnitt wurde die Entwicklung des GwG beschrieben. Dabei wurde an mancher Stelle bereits deutlich gemacht, dass

849 Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. 2017, L 88/6.

850 *Engelstätter*, GSZ 2019, 95 (97 ff.).

851 „konturenlos" nach *Häberle* in Erbs/Kohlhaas Nebengesetze, GWG § 1 Rn. 3.

852 *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 12 Rn. 6.

853 *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 179.

854 Allg. zu diesem Spannungsverhältnis *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 162 ff.; *Werner,* Geldwäsche, 1996, S. 94 ff.; *Kirchhof* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 79 (88 f.); *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95; *Häberle* in Erbs/Kohlhaas Nebengesetze, GWG, Vor. § 1 Rn. 1.

sich aus dem GwG eine umfangreiche Pflicht für Banken und andere Institute zur Speicherung von Kontoinhaltsdaten ergibt. Um diese Speicherpflicht einem verfassungs- und europarechtlichen Vergleich zu unterziehen, muss sie in ihrer aktuellen Fassung aber detaillierter erörtert werden. Daher soll in diesem Abschnitt die Wirkweise des zum Zeitpunkt der Bearbeitung gültigen GwG[855] beschrieben werden. Weiterhin liegt der Fokus dieser Arbeit auf der Betrachtung persönlicher Kontoinhaltsdaten, insbesondere Kontobewegungen. Das GwG soll daher sinnvollerweise nicht vollumfänglich, sondern nur in diesem Kontext erläutert werden.

Dreh- und Angelpunkt[856] des Gesetzes sind die in § 10 ff. GwG geregelten Sorgfaltspflichten. Diese basieren auf einem risikoorientierten Ansatz, dem „Risk-Based-Approach" und dem „Know-Your-Customer (KYC)"-Prinzip. Gemäß dem Risk-Based-Approach gilt, dass nicht alle Geschäftsbeziehungen oder Transaktionen gleich gefährlich sind. Dies ist abhängig von den betreffenden Umständen – etwa den beteiligten Personen, der Höhe des transferierten Betrages, dem Ziel der Transaktion etc.[857] Dieser am Risiko orientierte Ansatz setzt voraus, dass Risiken überhaupt erst erkannt werden. Um eine solche Analyse anzustellen, sind die Beteiligten darauf angewiesen, irreguläre Vorgänge zu identifizieren.[858] Dies gelingt nur, wenn sie ihre Kunden und deren reguläres Verhalten kennen. Insofern ergänzen sich der Risk-Based-Approach und das KYC-Prinzip.

Die risikoabhängigen Transparenzerfordernisse zeigen sich zunächst in einer Trichotomie von Sorgfaltspflichten, die die in § 2 GwG normierten Verpflichteten zu erfüllen haben. So gibt es vereinfachte Sorgfaltspflichten, § 14 GwG, allgemeine Sorgfaltspflichten, §§ 10-13 GwG und verstärkte Sorgfaltspflichten, § 15 GwG.

Diese Pflichten sollen im Folgenden nicht extensiv, sondern schwerpunktmäßig in Bezug auf die Pflicht zur kontinuierlichen Überwachung untersucht werden.

---

855 Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), zuletzt geändert durch Gesetz vom 10. August 2021 (BGBl. I S. 3436) geändert worden ist.

856 Vgl. schon *Achsnich/Mende/Mülhausen ua.* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 39 Rn. 30.

857 *Sotiriadis/Heimerdinger*, BKR 2009, 234 (234); *Costanzo* in Unger (Hrsg.), HdB Money Laundering, 2013, S. 349; *Gürkan,* Geldwäscheprävention, 2019, 95 ff.; *Herzog/Achtelik* in Herzog GwG, Einl. Rn. 86, 157; *Ross/Hannan*, J. of Money Laundering Control 10 (2007), 106 (107 ff.).

858 *Tuba/van der Westhuizen*, Int. J. of Public Law and Policy 4 (2014), 53 (59); *Spoerr* in BeckOK Datenschutzrecht, Grundlagen Syst. J. Rn. 150; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 209.

aa. Allgemeine Sorgfaltspflichten nach §§ 10 ff. GwG

Den Regelfall stellen die allgemeinen Sorgfaltspflichten nach § 10 GwG[859] dar. Diese werden nach dem Katalog des § 10 Abs. 1 Nr. 1-5 GwG im Einzelnen aufgeführt. Sie umfassen nach § 10 Abs. 1 Nr. 1 GwG die Pflicht, den Vertragspartner zu identifizieren; nach Nr. 2 die Pflicht abzuklären, ob hinter dem Vertragspartner ein abweichender wirtschaftlicher Berechtigter steht, der gegebenenfalls zu identifizieren ist; nach Nr. 3 die Pflicht, Informationen über den Zweck und die Art der angestrebten Geschäftsbeziehung einzuholen; nach Nr. 4 die Pflicht zur Feststellung, ob es sich bei dem Vertragspartner um eine politisch exponierte Person handelt bzw. ein Familienmitglied oder eine ihr nahestehende Person, und schließlich nach Nr. 5 die Pflicht zur kontinuierlichen Überwachung der Geschäftsbeziehung einschließlich der in ihrem Verlauf durchgeführten Transaktionen. Diese Pflicht steht im Zentrum dieser Untersuchung.

(1). Pflichtauslösende Umstände

Wann diese Sorgfaltspflichten zu erfüllen sind, bestimmt sich nach § 10 Abs. 3 Nr. 1-3 GwG. Dabei dürfte § 10 Abs. 3 Nr. 1 GwG – die Begründung einer Geschäftsbeziehung – den in der Praxis bedeutendsten Auslöser darstellen.[860] Er begründet die Pflicht zur Einhaltung von Sorgfaltspflichten gegenüber den Vertragskunden der Verpflichteten. Sorgfaltspflichten gegenüber Bank- insbesondere Girokunden müssen also nach § 10 Abs. 3 Nr. 1 GwG eingehalten werden.[861]

§ 10 Abs. 3 Nr. 2 GwG betrifft hingegen Gelegenheitskunden der Verpflichteten, die keine dauerhafte Rechtsbeziehung zu den Verpflichteten eingehen, sondern nur einzelne bare oder unbare Überweisungen vornehmen.[862] Die im regelmäßigen Geschäftsverkehr typische Transaktion, die über ein bestehendes Geschäftskonto abgewickelt wird, ist von § 10 Abs. 3 Nr. 2 GwG also nicht umfasst, sondern fällt unter § 10 Abs. 3 Nr. 1 GwG.[863]

859 Umsetzung von Art. 13 Abs.1 der 4. Geldwäscherichtlinie, s. BT-Drs. 18/11555, S. 116

860 Vgl. *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020.

861 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 26.

862 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Z. 9; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017; *Höche/Rößler*, WM 2012, 1505 (1507).

863 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Z. 9.

Zu den Begriffen des § 10 Abs. 3 Nr. 1 GwG bedarf es einiger Ausführungen. Die Formulierung „*bei der Begründung einer Geschäftsbeziehung*" ist nicht eindeutig.

Sie könnte so verstanden werden, dass die Sorgfaltspflichten nur *im Moment der Begründung* einer Geschäftsbeziehung umgesetzt werden müssen. Das wäre jedenfalls hinsichtlich der Identifizierungspflicht auch erst einmal sinnvoll. Die kontinuierliche Überwachungspflicht erstreckt sich aber nach § 10 Abs. 1 Nr. 5 GwG ausdrücklich auch auf Transaktionen, die *im Verlauf der Geschäftsbeziehung* getätigt werden. Gleichzeitig werden nach § 1 Abs. 4 GwG nur auf eine gewisse Dauer angelegte Geschäftsbeziehungen unter § 10 Abs. 3 S. 1 GwG subsumiert, wodurch sich diese von den gelegentlichen Transaktionen i. S. v. § 10 Abs. 3 S. 2 GwG abgrenzen. Bei dauerhaften Geschäftsbeziehungen, etwa einem Girovertrag, finden Transaktionen auch nicht im Moment der Begründung, sondern im späteren Verlauf statt. Schon aus der Überwachungspflicht ergibt sich deshalb, dass § 10 Abs. 3 S. 2 GwG nicht regelt, wann die Sorgfaltspflichten einzuhalten sind, sondern ab wann.[864]

Was unter *Begründung* der Geschäftsbeziehung verstanden wird, ergibt sich aus § 11 Abs. 1 GwG. Da § 11 Abs. 1 GwG die Identifizierungspflicht im Regelfall *vor* der Begründung verlangt, kommt als frühester Punkt nur der Vertragsschluss in Betracht, nicht die Zeit unmittelbar davor.[865]

(2). Kontinuierliche Überwachung nach §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG

Nach § 10 Abs. 1 Nr. 5 GwG haben die Verpflichteten ihre Geschäftsbeziehungen, einschließlich der in ihrem Verlauf durchgeführten Transaktionen, kontinuierlich zu überwachen. Im engen Zusammenhang mit dieser Vorschrift steht § 25h Abs. 2 KWG, wonach *Kreditinstitute unbeschadet der Überwachungspflicht aus § 10 Abs. 1 Nr. 5 GwG Datenverarbeitungssysteme zu betreiben und zu aktualisieren haben, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die relativ gesehen, besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen*. Die Vorschriften können gemeinschaftlich als Pflicht, insbe-

864 *Ackermann/Reder*, WM 2009, 158 (166).; s.a. BT-Drs. 16/9038, S. 34
865 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 451 f.

sondere für Banken, gelesen werden, die Transaktionen ihrer Kunden mit Datenverarbeitungssystemen zu überwachen.[866]

Was genau unter *Überwachung* verstanden werden soll, ergibt sich aus dem Gesetz nur unzureichend und sorgt beim ersten Zugriff für einige Verwirrung. Da § 15 GwG für bestimmte Fälle eine verstärkte Überwachung vorsieht, also einen qualitativen oder quantitativen Unterschied einfordert, könnte man annehmen, dass bei weniger riskanten Situationen nicht alle Transaktionen erfasst werden müssen.

Um Auslegungsproblemen des Geldwäscherechts zu begegnen, erlassen die Europäischen Finanzaufsichtsbehörden nach Art. 17, 18 Abs. 4 der 4. GWRL und Art. 16, 56 der ESA-Verordnungen[867] Leitlinien zu den Risikofaktoren, die die Verpflichteten im Rahmen der Sorgfaltspflichten zu beachten haben.[868] Diese werden von der BaFin grundsätzlich übernommen.[869]

In der aktuellen Leitlinie[870] heißt es in lfd. Mr. 4.7 lit. e), dass die Verpflichteten darlegen sollen, „welches Maß an Überwachung unter welchen Umständen Anwendung findet" und zwar nach lfd. Nr. 4.10 lit a) in Abhän-

866 Vgl. BT-Drs. 17/9038, S. 49 f.; BT-Drs. 18/11555, S. 176; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 343; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Ackermann/Reder*, WM 2009, 158 (164); *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (456).

867 Verordnungen über die Gründung der Europäischen Aufsichtsbehörden (European Supervisory Authorities – ESAs): Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission, ABl. 2010, L 331/12; Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission, ABl. 2010, L 331/48; Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission; ABl. 2010, L 331/84.

868 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung).

869 *BaFin,* Leitlinien und Q&As der ESA, https://www.bafin.de/DE/RechtRegelungen/Leitlinien_und_Q_and_A_der_ESAs/Leitlinien_und_Q_and_A_der_ESAs_node.html, zuletzt aufgerufen am 12.01.2025.

870 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung).

gigkeit des jeweiligen Risikos. Demnach variiert die Überwachungspflicht offenbar in ihrem Umfang.

Mit diesem Umfang setzen sich lfd. Nr. 4.72 ff. auseinander. Lfd. Nr. 4.73 legt zunächst fest, dass die Transaktionsüberwachung ermöglichen soll, ungewöhnliche oder verdächtige Transaktionen oder Transaktionsmuster zu erkennen. Das entspricht dem Wortlaut der § 25h Abs. 2 KWG und § 14 Abs. 2 S. 2 GwG. Gleichzeitig soll der Umfang der Überwachung nach lfd. Nr. 4.72 aber *angemessen* sein. Was angemessen ist, hängt nach lfd. 4.74 wiederum vom jeweiligen Risiko ab. So sollen die Verpflichteten nach lfd. Nr. 4.74 lit. a) etwa entscheiden können, ob und wann sie Transaktionen in Echtzeit überwachen und wann nur nachträglich.

Aus der Möglichkeit der Echtzeitüberwachung ergibt sich eine erste entscheidende Erkenntnis: Unter Überwachung versteht das GwG nicht nur die Vorgänge, die eine bestehende Datenbasis voraussetzen, sondern die Anlegung neuer Daten in Folge von Beobachtung. Dies bedarf einer vertieften Betrachtung:

§ 10 Abs.1 Nr. 5 GwG ließe sich zunächst so verstehen, dass das GwG vom Bestehen einer entsprechenden Datengrundlage *a priori* ausgeht und die Anlegung dieser Grundlage nicht der Pflicht zur Überwachung unterfällt. Ein solches Verständnis könnte man darauf stützen, dass die Verpflichteten sämtliche Transaktionen ohnehin wahrnehmen, denn sie sind es, die diese digital oder manuell ausführen. Auch Speicherpflichten bestehen außerhalb des GwG zur Genüge (zu den Speicherpflichten außerhalb des GwG siehe oben Kap. D. II).

Die *Überwachung* i. S. d. geldwäscherechtlichen Vorschriften erschöpfte sich nach diesem Verständnis in der nachträglichen Kontrolle der vorliegenden Daten, was die BaFin in Abgrenzung zum Screening (= Echtzeitüberwachung) als Monitoring bezeichnet.[871] Eine solche Kontrolle – ob mittels EDV oder individuell – könnte auch in verschiedenen Intensitätsstufen erfolgen, womit sich wiederum erklären lässt, dass im GwG verschiedene Intensitätslevel der Überwachungspflicht veranlagt sind.

Wenn aber die Auslegungshinweise von der Möglichkeit einer Echtzeitüberwachung[872] ausgehen, muss auch die Datenanlage bzw. die Wahrneh-

871 *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.

872 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.74 lit. a); *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.

mung der Transaktion von der Überwachungspflicht mitumfasst sein. Auch die DK-Hinweise sehen sowohl das „laufende Monitoring" als auch die „konkrete, anlassbezogene Transaktionskontrolle" von § 25h Abs. 2 KWG umfasst.[873] Dies impliziert, dass die Wahrnehmung aller Transaktionen zur Überwachungspflicht dazugehört und diese nicht auf die nachträgliche Kontrolle reduziert ist. Überwachung ist demnach Screening *und* Monitoring.

Insbesondere im digitalen Massenverkehr dürfen also keine automatisierten Transaktionsvorgänge etabliert werden, die dem Monitoringsystem verborgen bleiben. Unabhängig von der technischen Ausgestaltung ist auf abstrakter Basis zu verlangen, dass die Verpflichteten Kenntnis aller im Rahmen ihrer Geschäftsbeziehungen durchgeführten Transaktionen erhalten. Schon im Moment der Transaktion setzt somit die Überwachungspflicht an.[874]

Verstünde man die Überwachungspflicht hingegen ausschließlich als nachträgliche Kontrolle einer Datenbasis, von deren Bestehen man *a priori* ausgeht, folgte aber ohnehin aus der Aufzeichnungspflicht i. S. d. § 8 Abs. 1 Nr. 1 GwG auch eine Pflicht zur Wahrnehmung der Transaktionen. In § 8 Abs. 1 Nr. 1 GwG wird festgelegt, dass auch die *zur Erfüllung der Sorgfaltspflicht eingeholten Informationen* aufzuzeichnen sind. Da auch die Überwachung im Sinne einer bloß nachträglichen Transaktionskontrolle eine Datenbasis bedingt, ergibt sich die Pflicht zur Transaktionserkennung und Speicherung jedenfalls aus § 8 Abs. 1 Nr. 1 GwG .[875]

Die Pflicht zur Speicherung der Transaktionsdaten ist also unabhängig von der Frage, ob die Überwachung i. S. d. § 10 Abs.1 Nr. 5 GwG eine Pflicht zur Wahrnehmung der Transaktionen oder nur eine Pflicht zur nachträglichen Kontrolle enthält.

Überzeugend ist es, schon die Datenanlegung bzw. die Erstwahrnehmung etwaiger Transaktionen unter den Überwachungsbegriff zu subsumieren. Allerdings ist der Begriff damit nicht erschöpft. Nach lfd. Nr. 4.74 lit. c) der ESA-Leitlinien sollen die Verpflichteten schließlich die Häufigkeit der Transaktionsüberwachung bestimmen. Schon hier wird klar, dass mit *Überwachung* nicht mehr nur das reine Erfassen der Transaktion gemeint

873 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d) S. 69 f.

874 Vgl. *Degen,* Geldwäsche, 2009, 206 f.

875 So etwa *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463.); wohl auch *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18.

sein kann, denn ohne dies wäre auch ein nachträgliches Überwachen nicht möglich.

Der Überwachungsprozess gliedert sich vielmehr in mehrere graduelle Schritte auf. Am Anfang steht die Erfassung sämtlicher Transaktionen, also die Anlegung der Datenbasis. Danach erfolgt die Kontrolle dieser Daten, typischerweise durch einen automatisierten Abgleich mit bestehenden Daten. Dies geschieht teilweise im Rahmen einer Echtzeitüberwachung und teilweise nur im Rahmen einer nachträglichen, automatisierten Kontrolle. Die ausschließlich nachträgliche Überprüfung einer Transaktion auf Auffälligkeiten stellt in der Praxis den Standard dar. [876] Anstelle der ständigen Prüfung einzelner Transaktionen nimmt sich die Software einen ganzen Transaktionsverlauf eines Kunden in längeren, periodischen Abständen vor.[877]

Dass die Überwachung in jedem Fall eine Kontrolle der Daten beinhaltet, folgt aus § 25h Abs. 2 KWG und § 14 Abs. 2 S. 2 GwG. Dort wird festgelegt, dass selbst bei der geringsten Überwachungspflicht sämtliche Auffälligkeiten nachvollziehbar bleiben müssen. Soweit Leitlinie 4.74 lit. c) der ESA-Leitlinien von einer Reduzierung der Überwachungshäufigkeit spricht, ist nur die Quantität oder Qualität der nachträglichen Kontrolle gemeint, nicht der Umfang der Datenanlegung. Andernfalls würde eine Reduzierung der Häufigkeit dazu führen, dass bestimmte Transaktionen gar nicht registriert werden. Das Erkennen von Unregelmäßigkeiten i. S. d. § 25h Abs. 2 KWG und § 14 Abs. 2 S. 2 GwG wäre in diesem Fall nicht ständig gewährleistet.

Wenn im GwG bzw. dem Geldwäscherecht von *Überwachung* gesprochen wird, ist zusammenfassend also ein komplexer Prozess gemeint, der mehrere Einzelvorgänge von der digitalen Wahrnehmung bis zur manuell-individuellen Kontrolle von Transaktionen umfasst. Das prinzipielle Erfassen sämtlicher Transaktionen und die Durchführung eines regelmäßigen Abgleichs, zumindest digital, ist dabei das unterste Maß der Überwachung und muss immer gewährleistet sein. Keine Transaktion darf den Verpflichteten – etwa wegen der Verwendung automatisierter Systeme – verborgen bleiben. Auch im Rahmen des risikobasierten Ansatzes gilt folglich, unabhängig von der präzisen Einordnung im Gesetzestext, dass die Monitoring-

876 *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (455 f.).

877 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 57.

systeme der Verpflichteten sämtliche Transaktionsvorgänge wahrnehmen und in gewissen Abständen rastern müssen.[878] Dies ist für das Verständnis der unterschiedlichen Ausprägungen der Überwachungspflicht, insbesondere i. R. d. verstärkten Sorgfaltspflichten, höchst bedeutsam. Wenn also im Folgenden vom risikoorientierten Umfang der Sorgfaltspflichten bzw. der Überwachung gesprochen wird, darf nicht übersehen werden, dass sich dies nur auf die individuelle Überwachung bzw. Kontrolle – etwa durch Mitarbeiter – nicht auf das generelle Erfassen der Transaktionsdaten bezieht.

(3). Risikobasierter Umfang

Der konkrete Umfang der Sorgfaltspflichten bestimmt sich nach § 10 Abs. 2[879] GwG – ganz dem Risk-Based-Approach folgend[880] – nach dem jeweiligen Risiko einer Geschäftsbeziehung oder einzelnen Transaktion. Diese Vorschrift geht Hand in Hand mit § 5 GwG, der die Verpflichteten allgemein zur Risikoanalyse im Rahmen ihrer geldwäscherechtlichen Aufgaben verpflichtet, wobei die nationale Risikoanalyse[881] i. S. d. § 3a Abs. 2 GwG gem. § 5 Abs. 1 S. 2 GwG zu berücksichtigen ist. Bei der Risikobestimmung kommt den einzelnen Unternehmen ein Ermessenspielraum zu.[882]

Für Verpflichtete, die unter das KWG fallen, ergibt sich dieser Ermessensspielraum auch aus dem insoweit ergänzenden §§ 25h Abs. 1 KWG, der ein *angemessenes* Risikomanagement verlangt.[883] Um dieses Risiko zu bestimmen, enthält das GwG in den Anlagen 1 und 2 eine nicht abschließende Liste an Faktoren, die für ein potenziell niedriges oder erhöhtes Risiko sprechen. Stellen die Verpflichteten ein solches niedriges oder erhöhtes

878 BT-Drs. 16/9038, S. 50; *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 15; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462).

879 Umsetzung von Art. 13 Abs. 2 – 5 der 4. Geldwäscherichtlinie, s. BT-Drs. 18/11555, S. 116

880 *Figura* in Herzog GwG, §10 Rn. 38.

881 Zuletzt *Bundesministerium der Finanzen,* 1. Nationale Risikoanalyse 2018/19.

882 BT-Drs. 16/9038, S. 35 zu § 3 Abs. 4 GwG aF; *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 13 Rn. 179.

883 *Figura* in Herzog GwG, § 10 Rn. 40.

Risiko fest, haben sie in Anwendung der §§ 14, 15 GwG vereinfachte oder verstärkte Sorgfaltspflichten anzuwenden.

bb. Vereinfachte Sorgfaltspflichten nach § 14 GwG

Im Falle eines niedrigen Risikos gelten nach § 14 GwG vereinfachte Sorgfaltspflichten. Ob ein niedriges Risiko besteht, haben die Verpflichteten nach § 5 Abs. 1 GwG im Rahmen ihrer Risikoanalyse unter Anwendung anerkannter Risikofaktoren zu bestimmen – insbesondere der in Anlage 1 und 2 aufgeführten Kriterien. Die in den Anlagen 1 und 2 genannten Risikofaktoren sind nach § 14 Abs. 1 S. 2 GwG aber nur Indikatoren für ein gewisses Risiko und nicht abschließend zu verstehen[884]. Die Verpflichteten müssen im konkreten Fall auch stets das tatsächliche Bestehen eines geringen Risikos der Geldwäsche oder Terrorismusfinanzierung feststellen.

Eine schematische Anwendung findet i. R. d. § 14 GwG nicht statt. Einen Katalog mit Regelbeispielen zu Situationen, in denen vereinfachte Sorgfaltspflichten gelten, sucht man im Gesetz heute vergeblich (zur alten Gesetzeslage s. o. III. 2. a.). Vielmehr ist die Anwendung vereinfachter Sorgfaltspflichten immer denkbar, wenn es der Einzelfall denn zulässt.[885]

§ 14 GwG ist heute so ausgestaltet, dass er nicht mehr die grundsätzliche Anwendung der Sorgfaltspflichten entbehrlich macht, sondern nur den Umfang der in § 10 GwG aufgeführten Pflichten beschränkt. Wie diese Beschränkung im Einzelfall ausgestaltet werden soll, schreibt die Norm auch nicht vor, sondern überlässt es in § 14 Abs. 2 Nr. 1 GwG grundsätzlich den Verpflichteten, eine *angemessene* Reduzierung vorzunehmen. Die Verpflichteten sind bei der Reduzierung des Pflichtenumfangs aber nicht gänzlich sich selbst überlassen. Sie werden mit Auslegungshinweisen versorgt. In den ESA-Leitlinien sind beispielhaft Möglichkeiten aufgezählt, wie sich die allgemeinen Sorgfaltspflichten reduzieren lassen.[886] Das GwG selbst verweist zwar nicht auf die Art. 16, 56 ESA-Verordnungen bzw. dem hier-

884 BT-Drs. 18/11555, S. 63; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 59.

885 *Ruppert*, DStR 2012, 100 (101 f.).

886 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.41.

nach erlassenen Leitlinien. Allerdings stellt die Gesetzesbegründung (zum GwG 2017) den Bezug ausdrücklich her.[887]

So kann insbesondere die Häufigkeit und Intensität der Transaktionsüberwachung reduziert werden, indem die überwachten Transaktionen von einem gewissen Schwellenwert abhängig gemacht werden.[888] Dabei ist jedoch § 14 Abs. 2 S. 2 GwG zu beachten, nach dem die Verpflichteten in jedem Fall die Überprüfung von Transaktionen und die Überwachung von Geschäftsbeziehungen in einem Umfang sicherstellen, der es ihnen ermöglicht, ungewöhnliche oder verdächtige Transaktionen zu erkennen und zu melden. Dies setzt voraus, dass jede Transaktion zumindest grundsätzlich von den digitalen Sicherungsmechanismen erfasst wird und kontrolliert werden kann.[889]

cc. Verstärkte Sorgfaltspflichten nach § 15 GwG

Das Gegenstück zu den vereinfachten Sorgfaltspflichten stellen die verstärkten Sorgfaltspflichten dar, die in § 15 GwG geregelt sind. Sie sind nach § 15 Abs. 2 GwG anzuwenden, falls die Verpflichteten unter Berücksichtigung der in den Anlagen 1 und 2 genannten Faktoren ein *höheres Geldwäscherisiko* festgestellt haben – und zwar entweder im Rahmen ihrer Risikoanalyse i. S. d. § 5 Abs. 1 GwG oder im Einzelfall. Neben diesem generalklauselartigen Auslöser gibt § 15 Abs. 3 GwG einen Katalog bestimmter Fälle vor, in denen von einem erhöhten Risiko *insbesondere* auszugehen ist. Die Aufzählung ist im Zeichen des Risk-Based-Approach nicht abschließend zu verstehen.[890]

(1) Auslösende Umstände und allgemeiner Umfang

Schon aus § 15 Abs. 2 GwG ergibt sich, dass die Anwendung verstärkter Sorgfaltspflichten sich nicht nur generell aus bestimmten Umständen eines

887 BT-Drs. 18/11555, S. 120.

888 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.41 lit. e).

889 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 11, 13.

890 Vgl. *Ackermann/Reder*, WM 2009, 200 (202); *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 455.

Kunden ergeben, sondern auch von Umständen einzelner Transaktionen ausgelöst werden kann. Dieser Befund spiegelt sich auch im Beispielkatalog des § 15 Abs. 3 GwG wider.

§ 15 Abs. 3 Nr. 1 GwG etwa stellt allgemein auf den Kunden ab. Handelt es sich bei diesem oder dessen wirtschaftlich Berechtigtem um eine politisch exponierte Person (PEP), ein Familienmitglied einer PEP oder auch nur um eine Person, die einer PEP nahesteht, so sind stets verstärkte Sorgfaltspflichten anzuwenden.[891]

§ 15 Abs. 3 Nr. 2 GwG hingegen stellt auf Geschäftsbeziehungen oder Transaktionen ab und nimmt damit sowohl allgemeine Umstände einer Geschäftsbeziehung als auch Einzelumstände von Transaktionen in den Blick. Die Norm betrifft Vorgänge mit Beteiligung eines geldwäscheriskanten Drittstaats. Diese Drittstaaten „mit hohem Risiko" werden nach Art. 9 Abs. 2, 64 GWRL in einem Rechtsakt der Kommission bestimmt. Dies geschah erstmals im Jahr 2016 im Rahmen der Delegierten-Verordnung (EU) 2016/1675.[892] Die Liste wurde zuletzt im Jahr 2020 aktualisiert.[893]

Bei der Bestimmung orientiert sich die Kommission an den Erkenntnissen der FATF. Diese überwacht und bewertet in Kooperation mit regionalen FATF-ähnlichen Organisationen weltweit die Effizienz der Geldwäschebekämpfung in über 200 Staaten.[894]

Staaten mit erhöhtem Risiko werden in der Liste *„jurisdictions under increased monitoring"*[895] geführt. Staaten mit hohem Geldwäscherisiko, in denen ein unzureichendes Anti-Geldwäscheregime festgestellt wurde, kommen auf die sogenannte *black list (High-Risk Jurisdictions subject to a Call*

891 Zur Entwicklung *Herzog/Hoch*, WM 2007, 1997; *Kunz/Schirmer* BB 2015, 2435 (2439 f.).

892 Delegierte Verordnung (EU) 2016/1675 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates durch Ermittlung von Drittländern mit hohem Risiko, die strategische Mängel aufweisen, ABl. 2016, L 254/1; konsolidierte Fassung vom 07.02.2021: Document 02016R1675-20210207.

893 Delegierte Verordnung (EU) 2021/37 der Kommission vom 7. Dezember 2020 zur Änderung der Delegierten Verordnung (EU) 2016/1675 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates im Hinblick auf die Streichung der Mongolei aus der Tabelle unter Nummer I des Anhangs; ABl. 2021, L 14/1.

894 *FATF,* Annual Report 2019/2020, 37 ff.

895 Aktuelle Liste unter *dies.,* Jurisdictions under Increased Monitoring, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html, zuletzt aufgerufen am 12.01.2025

for Action).[896] Auf diese *black list* stellt § 15 Abs. 8 GwG ab, nach dem die BaFin über § 15 Abs. 4 GwG hinausgehende Maßnahmen erforderlich machen kann.[897] Ähnliches sieht § 15 Abs. 5a GwG vor, der aber nicht auf die FATF-Listen abstellt, sondern für alle von der Kommission festgelegten Drittstaaten im Einzelfall besonders intensive Pflichten vorsieht. Ausgehend von § 15 Abs. 5a GwG hat die BaFin für Nordkorea und den Iran Gebrauch gemacht und eine Meldepflicht für Geschäftsbeziehungen und Transaktionen mit dort ansässigen Personen angeordnet.[898]

Allein auf die Umstände einer einzelnen Transaktion, unabhängig vom jeweiligen Kunden, stellt § 15 Abs. 3 Nr. 3 GwG ab. Danach sind verstärkte Sorgfaltspflichten bei Transaktionen anzuwenden, die im Vergleich zu ähnlichen Fällen besonders komplex oder ungewöhnlich groß sind (lit. a), einem ungewöhnlichen Transaktionsmuster folgen (lit. b) oder keinen offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck haben (lit. c). Außerdem sind verstärkte Sorgfaltspflichten nach § 15 Abs. 3 Nr. 4 GwG bei Transaktionen von bestimmten Verpflichteten auszuüben, insbesondere Transaktionen von Kreditinstituten an deren Korrespondenzinstitute, wenn sich die Korrespondenzinstitute in einem Drittstaat oder in einem Staat des Europäischen Wirtschaftsraums befinden.

Wie auch bei den vereinfachten Sorgfaltspflichten gilt der Risk-Based-Approach ebenso bei den verstärkten Sorgfaltspflichten. So haben nach § 15 Abs. 1 S. 2 GwG die Verpflichteten prinzipiell selbst den konkreten Umfang der verstärkten Sorgfaltspflichten zu bestimmen. Anders als bei den vereinfachten Sorgfaltspflichten sehen § 15 Abs. 4 – 8 GwG aber für verschiedene Fälle nur Mindestpflichten vor, die zwar alle über die allgemeinen Sorgfaltspflichten hinausgehen, aber in unterschiedlicher Schärfe. Auf eine abschließende Aufzählung der Maßnahmen wurde bewusst verzichtet.[899]

---

896 Derzeit nur Nordkorea und Iran, *dies.,* High-Risk Jurisdictions, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2021.html, zuletzt aufgerufen am 12.01.2025.

897 Dazu *BaFin,* Rundschreiben 01/2019 (GW), 15.02.2019; Rundschreiben 03/2020 (GW), 13.05.2020, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2020/rs_03-2020_laenderliste_gw.html, zuletzt aufgerufen am 12.01.2025.

898 *BaFin,* Allgemeinverfügung zur Anordnung einer Meldepflicht bei Geschäftsbeziehungen und Transaktionen mit Bezug zur Demokratischen Volksrepublik Korea (Nordkorea), GZ: GW 1-GW 2002-2020/0002, 13.05.2020; *BaFin,* Allgemeinverfügung zur Anordnung einer Meldepflicht bei Geschäftsbeziehungen und Transaktionen mit Bezug zu Iran, GZ: GW 1-GW 2002-2020/0002, 13.05.2020.

899 *Zentes/Glaab* BB 2017, 67 (70).

Die Intensität der verstärkten Sorgfaltspflichten ist also nur nach oben hin unbegrenzt[900] und steht auch nur insoweit tatsächlich im Ermessen der Verpflichteten.

(2) Verstärkte kontinuierliche Überwachung

Auf die einzelnen Mindestpflichten, die § 15 Abs. 4-7 GwG für die verschiedenen auslösenden Situationen statuiert, soll nur kurz eingegangen werden. Da die kontinuierliche Überwachung der Geschäftsbeziehungen schon aufgrund der allgemeinen Sorgfaltspflichten gilt, ist sie natürlich erst recht im Rahmen der hochriskanten Situationen des § 15 GwG einzuhalten. Die verstärkten Sorgfaltspflichten intensivieren die Überwachungspflicht aber an einigen Stellen. Die Pflichten des § 15 Abs. 4-7 GwG in Bezug auf die Überwachung zeigen insofern, dass der Überwachungsbegriff im GwG uneinheitlich ist bzw. verschiedene Handlungen mitumfasst.

Für Geschäftsbeziehungen und Transaktionen, an denen PEP beteiligt sind, sehen etwa § 15 Abs. 4 Nr. 2 und 3 GwG vor, dass durch angemessene Maßnahmen die Herkunft der transferierten Vermögenswerte bestimmt wird und die Geschäftsbeziehung einer *verstärkten* kontinuierlichen Überwachung unterzogen wird. Hier wird deutlich, dass es im Rahmen der verstärkten Sorgfaltspflicht nicht ausreichend sein kann, dass sämtliche Transaktionen von der EDV erfasst und irgendwann einmal kontrolliert werden. *Überwachung* ist hier also nicht gleichbedeutend mit dem allgemeinen EDV-Monitoring. Vielmehr werden sich die Verpflichteten aktiv und individuell bzw. durch Einsatz ihrer Mitarbeiter mit den einzelnen Vorgängen regelmäßig beschäftigen müssen.[901] Der genaue Rahmen der Intensität ergibt sich aus dem Gesetz aber nicht.[902]

Die Verpflichteten sind insofern auf die Auslegungshinweise des ESA angewiesen. Dort heißt es: „*Die Unternehmen sollten nach Anzeichen für ungewöhnliche Transaktionen suchen und die ihnen vorliegenden Daten regelmäßig überprüfen, um sicherzustellen, dass alle neuen oder aufkommenden Informationen mit potenziellen Auswirkungen auf die Risikobewertung*

900 Vgl. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (193 ff.).

901 *Achtelik* in Herzog GwG, § 15 Rn. 25; *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 12 Rn. 244.

902 Schon *Herzog/Hoch*, WM 2007, 1997 (1998).

zeitnah identifiziert werden. Die Häufigkeit der Überprüfungen im Rahmen der fortlaufenden Überwachung sollte sich nach dem Risikograd der betreffenden Geschäftsbeziehung richten."[903] Die sektorspezifischen Leitlinien zur Unternehmensfinanzierung stellen daneben ausdrücklich fest: „*In diesem Zusammenhang* (der Unternehmensfinanzierung) *sollten Unternehmen, die automatisierte Transaktionsüberwachung einsetzen, diese mit den Kenntnissen und dem Fachwissen des die Tätigkeit ausübenden Personals kombinieren. Diese verstärkte Überwachung sollte zu einem klaren Verständnis führen, weshalb ein Kunde eine bestimmte Transaktion oder Tätigkeit durchführt; für diesen Zweck sollten Unternehmen dafür Sorge tragen, dass sein Personal sein Wissen über den Kunden, und was unter den gegebenen Umständen zu erwarten wäre, einsetzt, um ungewöhnliche oder potenziell verdächtige Transaktionen und Tätigkeiten zu erkennen.*[904]

Daraus ergibt sich doch recht eindrücklich, dass eine *verstärkte Überwachung* nur durch eine qualitative und/oder quantitative[905] Ausweitung der individuellen Kontrollen ausgeübt werden kann.

Die unterschiedliche Verwendung des Überwachungsbegriffs zeigt sich denn auch in § 15 Abs. 6 GwG, der die Pflichten bei Hochrisikotransaktionen i. S. d. § 15 Abs. 3 Nr. 3 GwG bestimmt. Nach § 15 Abs. 6 Nr. 1 GwG haben die Verpflichteten zunächst Informationen zu der Transkation einzuholen, um sodann das Risiko der Transkation oder Geschäftsbeziehung einschätzen und überwachen zu können. Nach § 15 Abs. 6 Nr. 2 GwG soll weiter, *wenn die Transaktion aus einer Geschäftsbeziehung stammt, die Geschäftsbeziehung verstärkt überwacht werden, um das Geldwäsche- oder Terrorismusfinanzierungsrisiko zu bestimmen und bei höherem Risiko zu überwachen.*

Mit dieser undankbaren Formulierung ist Folgendes gemeint: Zunächst soll also das Transaktionsverhalten im Rahmen der Geschäftsbeziehung individuell bzw. manuell erfasst und in angemessener Regelmäßigkeit überwacht werden. Daran anknüpfend soll die Risikoeinstufung im weiteren Verlauf, die wiederum für das Maß der individuellen Überwachung verantwortlich ist, regelmäßig und individuell kontrolliert werden. Die Überwachung des Risikos ist keine Überwachung im Sinne der Wahrnehmung bestimmter Vorgänge, sondern ein Kontrollvorgang hinsichtlich der eigenen

903 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.50. d).
904 Idem, lfd. Nr. 20.7. h).
905 Nur knapp *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 62.

Kundeninformationen. Sie baut aber auf der eigentlichen Überwachung bestimmter Vorgänge auf. Die Verwendung des Begriffs der „Überwachung" in § 15 Abs. 6 Nr. 2 GwG ist dahingehend undifferenziert.

dd. Ergebnis: Überwachung prinzipiell unabhängig von Sorgfaltspflichten

Es lässt sich damit feststellen, dass die Pflicht zur kontinuierlichen Überwachung prinzipiell unabhängig von den einschlägigen Sorgfaltspflichten besteht. Lediglich das Maß der *Überwachung* ändert sich.

Im Rahmen vereinfachter Sorgfaltspflichten besteht die Pflicht zur Überwachung, die es ermöglicht, ungewöhnlich hohe Transaktionen zu erkennen, § 14 Abs. 1 S. 2 GwG. Eine ungewöhnlich hohe Transaktion kann im Einzelfall verstärkte Sorgfaltspflichten auslösen, § 15 Abs. 3 Nr. 3 GwG.[906] Eine individuelle Überwachung der Transaktionen im Rahmen vereinfachter Sorgfaltspflichten wird nicht regelmäßig stattfinden müssen, sondern kann von Schwellenwerten abhängig gemacht werden.[907]

Dementsprechend geht die Praxis bei der Überwachung von Kunden so vor, dass sie grundsätzlich alle Transaktionen des Kunden in das Monitoring miteinbezieht.[908] Bei den vereinfachten Sorgfaltspflichten beschränkt sich die Überwachungspflicht also minimal darauf, dass ein EDV-System die Transkationen des Kunden registriert, speichert und im Rahmen bestehender Geschäftsbeziehungen mit den Transaktionsmustern des Kunden regelmäßig abgleicht. Bei Kunden mit geringem oder moderatem Risiko rastern die EDV-Systeme in gewissen Abständen die Transaktionsverläufe blockweise, anstatt sich jede Transaktion einzeln „anzusehen".[909] Bestimmte Transaktionsmuster werden jedoch automatisch eine individuelle Echtzeit- oder Nachprüfung einleiten, indem z. B. die Überweisungsmasken

906 *Vollmuth,* Geldwäscheprävention, 2020, S. 173; *Achtelik* in Herzog GwG, § 25h KWG Rn. 11 f.

907 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.41 lit. e).

908 *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463).

909 Vgl. *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020 mit Verweis auf *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d).

beim Online-Banking auf bestimmte Namen oder Länderkennungen reagieren.[910]

Diese Praxis erscheint sachgerecht und ist notwendig. Denn § 25h Abs. 2 KWG und § 14 Abs. 1 S. 2 GwG verlangen, dass auf der niedrigsten Risikostufe zumindest Abweichungen vom Risikoprofil registriert werden können. Die unter das KWG fallenden Institute kommen der vereinfachten Sorgfaltspflicht somit bereits durch den Einsatz ausreichender EDV-Systeme nach. Manuelle Prüfungen finden nur statt, wenn die EDV-Systeme bei einer Transaktion *anschlagen,*[911] und deshalb verstärkte Sorgfaltspflichten zu beachten sind.

c. Verdachtsmeldungen

Wenn die Verpflichteten im Rahmen der Ausführung ihrer Sorgfaltspflichten verdächtige Transaktionen oder andere Umstände aufspüren, müssen sie diese an die FIU melden, § 43 Abs. 1 GwG. Die Meldungen sind der Zweck der Überwachungsmaßnahmen der Verpflichteten[912] und stehen ganz im Zentrum der Geldwäschebekämpfung.[913]

Anders als etwa die Vorratsdatenspeicherung von TK-Verkehrsdaten nach § 176 TKG wurde und wird die Beobachtung der Finanzströme durch private Akteure nicht primär als Instrument zum Datensammeln und Bereithalten für staatliche Behörden verstanden. Vielmehr verwenden die Verpflichteten diese Daten selbst – zumindest im ersten Zugriff. Die Verpflichteten sollen selbstständig Verdachtsmomente aus dem Massengeschäft filtern und melden. Von Kritikern des Anti-Geldwäschesystems werden sie deshalb als „Erfüllungsgehilfen“[914], „verlängerter Arm der Staatsanwaltschaft“[915] oder gar als „Hilfssheriffs“ [916] bezeichnet.

910 Zum Prozess ausf. *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 40 ff; 54 ff.
911 Idem, Rn. 47, 54 ff.
912 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (204).
913 Vgl. nur. *Barreto da Rosa* in Herzog GwG, § 43 Rn. 1; *Greite* in Zentes/Glaab GWG, § 43 Rn. 2.
914 *Dahm/Hamacher*, wistra 1995, 206 (207).
915 *L. Schuster,* Geldwäsche, 1994, S. 21.
916 *Griebel* NZM 2012, 482.

Wie sich ihre Stellung in der Geldwäschebekämpfung rechtlich einsortieren lässt, war und bleibt umstritten.[917] Nach Ansicht des Gesetzgebers erfüllen die Verpflichteten schlicht eine gewerberechtliche Pflicht und sind weder Verwaltungshelfer noch Beliehene oder sonst hoheitlich ermächtigt.[918]

Dass die Sicherheitsbehörden im ersten Schritt der Geldwäschebekämpfung eine passive Funktion haben, zeigt sich schon im Wortlaut der geldwäscherechtlichen Vorschriften. Sowohl in der GWRL als auch dem GwG wird die FIU als zentrale *Melde*stelle bzw. als Zentralstelle für Finanztransaktionsuntersuchungen bezeichnet.[919] Schon dem Namen nach ist die FIU also auf eine passive Tätigkeit ausgerichtet, die auf ein proaktives Handeln der verpflichteten Akteure aufbaut. Die FIU selbst beschreibt ihre Tätigkeit auf ihrer Homepage als das *Entgegennehmen, Sammeln und Auswerten von Meldungen über auffällige Finanztransaktionen.*[920] Ob diese Selbsteinschätzung vor dem Hintergrund ihrer, zumindest auf dem Papier bestehenden, weiten rechtlichen Befugnisse überzeugen kann, ist zu bezweifeln.[921] (s. Kap. G. III. 3. b. bb.).

aa. Rechtsnatur und Verdachtsschwelle

Die Rechtsnatur der Verdachtsmeldungen ist bis heute nicht ganz klar.[922] Gemäß dem Gesetzgeber soll es sich jedenfalls nicht um Strafanzeigen i. S. d. § 158 StPO handeln,[923] sondern um eine *gewerberechtliche* Meldeverpflichtung.[924] Die Rechtswissenschaft scheint dies akzeptiert zu haben, wenngleich weiterhin auf die Gemeinsamkeiten der Verdachtsmeldung zur

917 Ausführlich hierzu *Degen,* Geldwäsche, 2009, S. 128 ff.
918 BT-Drs. 18/11928, S. 26; *Kaetzler*, CCZ 2008, 174 (174).
919 Der Begriff wird auch in dem Entwurf für eine EU-GeldwäscheVO verwendet, COM/2021/420 final
920 *Zoll,* Financial Intelligence Unit, https://www.zoll.de/DE/Der-Zoll/Aufgaben-des-Zolls/Schutz-fuer-Mensch-Wirtschaft-und-Umwelt/FIU-Aufgaben/fiu-aufgaben_node.html , zuletzt aufgerufen am 12.01.2025.
921 Dazu *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (249 f.); krit. auch *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21.
922 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5.
923 BT-Drs. 17/6804, S. 21, 35.; *Findeisen* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, § 85 Rn. 62; anders noch *Herzog* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 20, 32.
924 BT-Drs. 18/11928, S. 26.; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 76.

Strafanzeige hingewiesen wird.[925] Im Hintergrund dieser Frage steht offenbar der Verdachtsgrad, der im Rahmen des § 43 Abs. 1 GwG erreicht werden muss.[926]

(1) Keine Ableitung der Verdachtsschwelle aus der Rechtsnatur

In der Literatur wurde versucht, aus der Einordnung der Verdachtsmeldungen als Strafanzeige Erkenntnisse über die Verdachtsschwelle zu gewinnen.[927] Der Gesetzgeber stellte deshalb in der Begründung zum Geldwäscheoptimierungsgesetz aus dem Jahr 2011[928] fest, dass die Verdachtsmeldungen keinen Anfangsverdacht i. S. d. § 152 Abs. 2 StPO benötigen, *da sie keine Strafanzeigen darstellen*[929]. In der Begründung zum Gesetz zur Umsetzung der 4. GWRL wurde wiederum festgehalten, *dass der Verdachtsgrad, auf Basis dessen der Verpflichtete eine Meldung abgibt, unterhalb dem einer Strafanzeige liegt.*[930] Damit stellte der Gesetzgeber sich allgemein gegen eine stark vertretene Meinung in der Literatur, die unabhängig von der Frage der Rechtsnatur, den Verdachtsgrad des § 152 Abs. 2 StPO auf die Verdachtsmeldepflicht übertragen wollte.[931]

Die Ausführungen in den Gesetzesbegründungen zur Verquickung von Rechtsnatur und Verdachtsgrad der Strafanzeige irritieren. Die Strafanzeige nach § 158 StPO kennt überhaupt keine materiellen Voraussetzungen bzw. einen Verdachtsgrad, ab dem sie obligatorisch würde. Sie ist lediglich eine (private) Aufforderung an die Staatsanwaltschaft, einen Sachverhalt strafrechtlich zu prüfen.[932]

925 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5, der von einer Pflicht „sui generis" ausgeht.: zust. *Lenk*, JR 2020, 103 (105 Fn 15).

926 Dazu *Höche/Rößler*, WM 2012, 1505 (1509 f.).

927 In diese Richtung jedenfalls *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5 ff.; *Herzog/Achtelik* in Herzog GwG, 2. Aufl. 2014, Rn. 16; dazu krit. *Findeisen* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, § 85 Rn. 62.

928 Gesetz zur Optimierung der Geldwäscheprävention vom 22.12.2011 (BGBl. I, S. 2595).

929 BT-Drs. 17/6804, S. 21, 35.

930 BT-Drs. 18/11555, S. 144.

931 *Krais,* Geldwäsche, 2018, Rn. 510; *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (68); *ders.* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 18 ff.; *Klugmann*, NJW 2012, 641 (644); *Carl/Klos*, wistra 1994, 161 (162); *Bülte*, NZWiSt 2017, 276 (280 f.); *Degen,* Geldwäsche, 2009, S. 127 f.

932 *Köhler* in Meyer-Goßner/Schmitt StPO, § 158 Rn. 2.

Mit wenigen Ausnahmen, etwa Anzeigen von bekannten Querulanten und oder „Geistesgestörten“[933], ist die Staatsanwaltschaft grundsätzlich zur Prüfung verpflichtet.[934] Die Anzeigen werden registriert und sodann in den sogenannten „Vorermittlungen“ darauf geprüft, ob sie die Verdachtsschwelle des § 152 Abs. 2 StPO erreichen.[935] So dies der Fall ist, muss die Strafverfolgungsbehörde mit den formellen Ermittlungen beginnen, § 152 Abs. 2 StPO. Nicht die Strafanzeige, sondern nur die Reaktion der Staatsanwaltschaft hängt also von einem Verdachtsgrad ab.

Die primäre Folge der Anzeige ist also immer deren Prüfung, unabhängig von etwaigen Voraussetzungen. Die Umstände der Anzeige können aber dennoch weite Folgen nach sich ziehen. Wer leichtfertig eine objektiv unwahre Anzeige abgibt, muss die Kosten des – auch außergerichtlichen – Verfahrens und Auslagen des Beschuldigten tragen, § 469 Abs. 1 StPO. Im Falle der vorsätzlich erstatteten Falschanzeige kommt auch eine Strafbarkeit wegen falscher Verdächtigung nach § 164 StGB in Betracht bzw. ein darauf gestützter zivilrechtlicher Schadensersatzanspruch nach § 823 Abs. 2 BGB.[936]

Der Vergleich der Verdachtsmeldung mit der Strafanzeige sagt somit über die Verdachtsschwelle der Pflicht zur Verdachtsmeldung nicht unmittelbar etwas aus, da für den Strafanzeigenden eine solche Schwelle gar nicht existiert. Selbst wenn die Meldung analog zur Strafanzeige behandelt werden müsste, könnte man aus den §§ 152 Abs. 2, 160 Abs. 1 StPO nur ableiten, ab wann die FIU aufgrund der Meldung weitere Schritte einleiten muss, denn die FIU stellt im geldwäscherechtlichen Meldesystem das Pendant zur Staatsanwaltschaft im Rahmen der §§ 152 ff. StPO dar.

Wenn in den Gesetzesbegründungen und der Literatur um den Verdachtsgrad gestritten wird, kann es daher nicht darum gehen, ob der Verdachtsgrad für die meldenden Verpflichteten niedriger ist als der Verdachtsgrad eines Strafanzeigenden, sondern niedriger ist als der Grad, ab dem die Strafverfolgungsbehörden auf Grundlage einer Anzeige tatsächlich ermitteln muss. Dieser wiederum wird in § 152 Abs. 2 StPO bestimmt, wonach Ermittlungen eingeleitet werden *müssen*, wenn *zureichende tatsächli-*

933 Dazu *Kockel/Vossen-Kempkens*, NStZ 2001, 178.
934 *Köhler* in Meyer-Goßner/Schmitt StPO, § 158 Rn. 2.
935 *Kölbel* in MüKo StPO, § 158 Rn. 26.
936 Etwa AG Bremen, NJW-RR 2014, 207.

che Anhaltspunkte (bzgl. einer Straftat) vorliegen. Der Verdachtsgrad des § 152 Abs. 2 StPO ist im Übrigen der niedrigste, den die StPO kennt.[937]

(2) Konturen der Verdachtsschwelle

§ 43 GwG ist ähnlich formuliert wie § 152 Abs. 2 StPO. Ausweislich des hier abgekürzten Wortlauts sind Verdachtsmeldungen vorzunehmen, *wenn Tatsachen vorliegen, die darauf hindeuten, dass ein Vermögensgegenstand aus einer Vortat der Geldwäsche stammt, oder ein solcher Gegenstand, ein Geschäftsvorfall oder eine Transaktion im Zusammenhang mit Terrorismusfinanzierung steht*. Außerdem *wenn Tatsachen vorliegen, die darauf hindeuten, dass ein Geschäftspartner seinen wirtschaftlich Berechtigten, so er existiert, nicht offenbart hat.*

Die Voraussetzung erschöpft sich also in „hindeutenden Tatsachen". Diese Formulierung wird gemeinhin als ein Weniger zum strafprozessualen Anfangsverdacht i. S. d. § 152 Abs. 2 StPO verstanden[938], für den zwar ebenfalls schon „konkrete Anhaltspunkte" ausreichen sollen,[939] aber eben in Bezug auf das Vorliegen einer Straftat. Das soll bei den Verdachtsmeldungen gerade nicht mehr die Schwelle sein. Da es sich bei den Verpflichteten nicht um eine Strafverfolgungsbehörde handelt, müssten diese nicht die Vorstellung haben, dass möglicherweise eine Straftat begangen wurde oder begangen wird. Insbesondere sollen sie nicht den § 261 StGB tatbestandlich prüfen, sondern nur kontrollieren, ob die nach dem GwG erforderlichen Tatsachen vorliegen.[940] Das wiederum sei dann der Fall, wenn nach der subjektiven Ansicht des Verpflichteten bzw. dessen Mitarbeiter eine Ungewöhnlichkeit oder Auffälligkeit im spezifischen geschäftlichen Kontext

937 *Frister* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. F Rn. 122; *Herzog* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 19 ff.

938 BT-Drs. 17/6804, S. 35; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; Findeisen in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, Rn. 62; *Klugmann*, NJW 2012, 641 (644); *Greite* in Zentes/Glaab GWG, § 43 Rn. 10 ff.

939 Hierzu *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 152 Rn. 4; *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 15 mwN.

940 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; *Bundesministerium der Finanzen,* Auslegunsghinweise Verdachtsmeldewesen, 06. November 2014, S. 3; OLG Frankfurt a.M., Hinweisbeschluss vom 17. Dezember 2012 - 19 U 210/12; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (202).

vorliegt – etwa, weil ein ungewöhnlich großer oder unnötig komplexer Vorgang stattfindet.[941] Für die Verpflichteten besteht also ein Beurteilungsspielraum, der allerdings begrenzt sein kann, wenn bestimmte Indikatoren vorliegen.[942]

Diese Indikatoren kann nach § 43 Abs. 5 GwG die FIU bestimmen. Als die FIU noch beim BKA angesiedelt war, wurden diese Indikatoren in Newslettern veröffentlicht – etwa in dem Papier „Anhaltspunkte Geldwäsche"[943], auf das die BaFin noch heute hinweist.[944] Es finden sich aber auch Indikatoren in den ESA-Leitlinien.[945]

Der Beurteilungsspielraum erlaubt es den Verpflichteten nicht, den Sachverhalt durch eigene Nachforschungen eigens aufzuklären.[946]

Mit den Anforderungen an die Verdachtsmeldungen hat sich jünger auch das BVerfG kurz beschäftigt.[947] Anlass war eine Wohnungsdurchsuchung wegen Verdachts einer Geldwäschehandlung. Dieser ging eine Verdachtsmeldung voraus. Es fehlten im konkreten Fall aber Anhaltspunkte dafür, dass die transferierten Beträge, die in der Tat auffällig waren, aus einer Katalogtat des damaligen § 261 Abs. 1 StGB stammten. Nach Ansicht des Generalbundesanwalts waren solche Anhaltspunkte nicht nötig, da es im Rahmen der Verdachtsmeldepflicht i. R. d. § 43 Abs. 1 GwG auch nicht darauf ankäme.[948] Gegen diese Übertragung stellte sich das BVerfG und hob die Unterschiede zwischen strafprozessualem Anfangsverdacht und § 43 Abs. 1 GwG hervor. Im Rahmen der geldwäscherechtlichen Verdachtsanzeige sei es danach ausreichend, wenn *objektiv erkennbare Anhaltspunkte dafür sprechen, dass durch eine Transaktion illegale Gelder dem Zugriff*

941 BT-Drs. 17/6804, S. 35; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72 f.; *Bundesministerium der Finanzen,* Auslegungshinweise Verdachtsmeldewesen, 06. November 2014, S. 3.

942 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72.

943 Die Newsletter werden nicht mehr auf der Website der FIU veröffentlich, vgl. *Krais,* Geldwäsche, 2018, Rn. 507, zuletzt online aber hier verfügbar: *FIU,* Anhaltspunktepapier - Newsletter 11/2014, August 2014, https://geldwaesche-beauftragte.de/wp-content/uploads/2017/04/FIU_Newsletter_Ausgabe_Nr._11_-August_2014.pdf, zuletzt aufgerufen am 12.01.2025; zusammengefasst bei *Diergarten* in Hauschka/Moosmayer/Lösler (Hrsg.), Hdb. Haftungsvermeidung, 3. Aufl. 2016, § 34 Rn. 392; *Krais,* Geldwäsche, 2018, Rn. 717.

944 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72.

945 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 2.16 ff.

946 OLG Frankfurt, NStZ 2020, 173 (175).

947 BVerfG, NJW 2020, 1351 (1353, Rn. 43).

948 Ibid.

der Strafverfolgungsbehörden entzogen oder die Herkunft illegaler Vermögenswerte verdeckt werden sollen und ein krimineller Hintergrund im Sinne des § 261 StGB nicht ausgeschlossen werden kann.[949] Die vom Gesetzgeber vorgestellte Verdachtsschwelle unterhalb der Anforderungen des § 151 Abs. 2 StPO kann daher als akzeptiert angesehen werden.

(3) Kritische Würdigung

Die niedrige Verdachtsschwelle ist nicht ohne Kritik geblieben. Auf die dogmatische Nähe zur Strafanzeige wurde gerade eingegangen. Da jedoch für die Strafanzeige keine materiellen Voraussetzungen gelten, lässt sich aus der Frage der Rechtsnatur für den Verdachtsgrad des § 43 GwG nichts ableiten.

Aber auch unabhängig von der Rechtsnatur ist eine Übertragung des § 152 Abs. 2 StPO nicht einzusehen. Banken sind keine Ermittlungsbehörden und sollen es auch nicht sein. Das Geldwäscherecht soll die strafprozessuale Ermittlung nicht ersetzen, sondern die Informationen liefern, auf denen die Ermittlungen aufbauen können.[950]

Die Verdachtsmeldungen der Verpflichteten bzw. die Maßnahmen, mit denen diese Meldungen erst vorbereitet werden, stellen also *Vorfeldermittlungen*[951] dar. Ihr Sinn liegt (noch) nicht in einer strafrechtlichen Prüfung eines Sachverhalts, sondern der aktiven Gewinnung von Verdachtssituationen[952]. Diese sollen dann von den Strafverfolgungsbehörden auf einen Anfangsverdacht hin untersucht werden, wobei eine operative Analyse als Zwischenschritt durch die FIU erfolgt, § 28 Abs. 1 Nr. 2 GwG (zu deren Rechtsnatur unten Kap. E II. 2. c. bb. (2)).

Die Beurteilung dieser Pflicht als „gewerberechtlich" überzeugt indes nicht.[953] Es ist schon nicht klar, was hiermit überhaupt gemeint sein soll. Dass (auch) Gewerbebetriebe von der Pflicht erfasst sind, ändert nichts an

949 Idem, mit Verweis auf OLG Frankfurt a.M., Hinweisbeschluss vom 17. Dezember 2012 - 19 U 210/12.

950 *Werner,* Geldwäsche, 1996, S. 141; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72.

951 Ausf. *Weßlau,* Vorfeldermittlungen, 1989, S. 25 ff.; Abgrenzung zu „Vorermittlungen": *Zöller,* Informationssysteme, 2002, S. 127 ff.; *Rogall*, ZStW 1991, 907 (945 ff.); *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 17 f.

952 *Böse*, ZStW 2007, 848 (866 ff.).

953 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 7 f.

deren Funktion. Dass private Betriebe für staatliche Aufgaben eingesetzt werden, an denen sie nur mittelbar und mehr zufällig auch ein Eigeninteresse haben, ist der springende Punkt der Inpflichtnahme. Sie unterscheidet sich von anderen Spielarten der *Criminal Compliance* dadurch, dass die jeweiligen Unternehmen nicht bloß ihre unternehmensinternen Risiken bekämpfen sollen, sondern dass die spezifische Nähe bestimmter Wirtschaftsteilnehmer zu externen Gefahrenlagen (wie etwa Kreditinstitute zur Finanzkriminalität) ausgenutzt werden soll (s. o. Kap B. II. 2. B. b. (a)).[954] Die Motivation des Staates liegt nicht darin, von den Unternehmen ausgehende Risiken einzudämmen, sondern die Unternehmen zur Bekämpfung von Drittrisiken zu utilisieren. Dementsprechend muss sich der Staat auch die Handlungen dieser in die Pflicht genommenen Unternehmen als eigene Eingriffe gegenüber Dritten zurechnen lassen.[955]

Gerade im Bereich der Verdachtsgewinnung durch Massenüberwachung ist dieses Vorgehen mittlerweile typisch. Da der Staat selbst im Sicherheitsrecht grundsätzlich reaktiv handeln muss, lagert er die Vorermittlungen an Private aus und grenzt dann lediglich die Übermittlung der entsprechenden Informationen ein.

Die Bezeichnung der geldwäscherechtlichen Meldepflicht als „gewerberechtlich" kann nur als Versuch gedeutet werden, von der Tatsache abzulenken, dass es sich um eine massenhafte Verdachtsgewinnung i. R. d. Sicherheitsgewährleistung handelt. Tatsächlich sind die Maßnahmen der Verpflichteten primär sicherheitsrechtlich motiviert. Die reaktiven (Mindest-)Eingriffsschwellen bestimmter Sicherheitsbehörden sollen unterlaufen werden.[956]

In letzter Konsequenz dienen die Meldungen dabei faktisch vor allem der Ahndung von Strafdelikten, wenngleich die ermittelten Informationen auch zur Gefahrenabwehr genutzt werden können. Diese Frage hängt aber primär davon ab, wie die Aufgaben der FIU charakterisiert werden (s. Kap. E II. 2. c. bb. (2)).

Jedenfalls ist die Herabsetzung der Verdachtsschwelle mitnichten von der Entlastung der Verpflichteten motiviert, denen keine strafverfahrensrechtli-

954 Weiter Begriff der Criminal Compliance bei *Hilgendorf* in Rotsch (Hrsg.), Compliance Zukunft, 2013, S. 19 (21).

955 BVerfGE 125, 260 (310) – Vorratsdatenspeicherung; dazu *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff. mwN.; aA. *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 30.

956 *Krais,* Geldwäsche, 2018, Rn. 510; *Lenk,* JR 2020, 103 (107 f., insb, Fn 51); *Böse*, ZStW 2007, 848 (861, 866 ff.).

chen Pflichten – es fehlte ihnen auch die meist die Expertise – aufgebürdet werden sollen. Vielmehr ergibt sich aus der niedrigen Schwelle eine große Menge an Verdachtsmomenten und somit eine breitflächige Vorfeldermittlung[957], die der Staat wohl eigenständig weder vornehmen könnte noch dürfte.

Berechtigt sind im Übrigen auch die Einwände, die die praktischen Nachteile der niedrigen Schwelle betonen. Nach § 56 Abs. 1 Nr. 69 GwG handelt ordnungswidrig, wer entgegen § 43 GwG eine Verdachtsmeldung nicht abgibt. Das Erreichen des Verdachtsgrads führt also zu einer bußgeldbewährten Meldepflicht, der nachzukommen im finanziellen Interesse der Verpflichteten liegt. Dies hat wohl zwangsläufig den Effekt, dass ein Absenken des Verdachtsgrads zu einer Steigerung der Menge der gemeldeten Fälle führt.[958] Mit der zunehmenden Zahl an Verdachtsmeldungen geht aber keine steigende Anzahl erfolgreicher Strafverfahren einher.[959] In der Literatur wird dieses Phänomen mit „Masse statt Klasse" überschrieben und kritisch hervorgehoben.[960]

In der Tat wächst die Menge der Verdachtsmeldungen seit Jahren rasant. Waren es im Jahr 2009 noch knapp 10.000, gingen 2019 schon etwa 115.000 Meldungen bei der FIU ein.[961] Der Umstand, dass diese mit der Menge an Verdachtsmeldungen kaum zurechtkommt, zieht mittlerweile beträchtliche politische Kreise und hat sowohl im Rahmen des Wirecard-Skandals als auch im Wahlkampf zur Bundestagswahl 2021 eine (fragwürdige) Rolle gespielt.[962]

957 zum Begriff ausf. Weßlau, Vorfeldermittlungen, 1989, S. 25 ff.; Abgrenzung zu „Vorermittlungen": Zöller, Informationssysteme, 2002, S. 127 ff.; Rogall, ZStW 1991, 907 (945 ff.); Roxin/Schünemann, Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 17 f.

958 So auch *FIU*, (BKA), Jahresbericht, 2011, S. 11.

959 *T. Fischer,* StGB, 69. Aufl. 2021, § 261 Rn. 4 c; *FIU,* Jahresbericht, 2019, S. 21 bemerkt eine Steigerung zum Vorjahr von gerade einmal 2%, trotz immenser Steigerung der Meldungen von 2018 zu 2019, siehe dort S. 15.

960 *Höche/Rößler*, WM 2012, 1505 (1509 f.); *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 501; *Herzog* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 16; vgl. auch *Hein* in Schwark/Zimmer, KMRK, 4. Aufl. 2010, WpHG § 10 Rn. 21.

961 *FIU,* Jahresbericht, 2019, S. 15.

962 *Bartz/Böcking/Diehl ua.* – Deutschland, ein Paradies für Geldwäscher, Der Spiegel vom 27.08.2021, Ausgabe 35/2021.

bb. Form der Meldung

Die Meldung muss seit Juni 2016 gem. § 45 Abs. 1 S. 1 GwG elektronisch eingereicht werden. Die Verpflichteten müssen sich außerdem unabhängig von der Abgabe einer Meldung gem. § 45 Abs. 1 S. 2 GwG bei der FIU online registrieren. Eine Meldung auf dem Postweg ist nach § 45 Abs. 2 GwG nur in Ausnahmefällen möglich oder nach § 45 Abs. 1 S. 3 GwG, wenn die elektronische Datenübermittlung gestört ist.

Ein elektronisches Meldesystem hat die FIU, mit einiger Verzögerung[963], zum Februar 2018 durch die Bereitstellung des Meldeportals „goAML" implementiert.[964] Bei goAML handelt es sich um eine Software, die vom Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung (UNODC) entwickelt wurde und den FIUs der UNO-Mitglieder bereitgestellt wird.[965] Laut Angaben des UNODC wird goAML aktuell von 56 FIUs verwendet.[966]

Im goAML-Webportal können sich die Verpflichteten registrieren und auf zwei verschiedene Arten Meldungen einreichen. Sie können entweder eine XML-Datei mit vorgeschriebenen Elementen[967] hochladen oder eine Webmaske ausfüllen[968].

cc. Umfang der Meldepflicht

Gemeldet werden müssen alle i. S. d. § 43 Abs. 1 GwG verdächtigen baren und unbaren Transaktionen sowie andere Vermögensverschiebungen,

963 *Barreto da Rosa* in Herzog GwG, § 45 Rn. 1; *Greite* in Zentes/Glaab GWG, § 45 Rn. 3 ff.; bis zum Februar 2018 galt eine Übergangslösung, siehe *FIU,* Schreibem vom 09.01.2018, GZ: SV 6002-2018.RUN.800002-DVIII.D.12, verfügbar unter https://web.archive.org/web/20220522191027/https://www.coburg.ihk.de/media/merkblatt_der_generalzolldirektion.pdf, zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im Mai 2022).

964 *FIU,* goAML Web, https://goaml.fiu.bund.de/Home, zuletzt aufgerufen am 12.01.2025; s.a. *FIU,* Handbuch goAML Web Portal, https://www.zoll.de/DE/FIU/Software-goAML/Publikationen/publikationen_node.html, Stand 01.02.2024, https://www.zoll.de/DE/FIU/Software-goAML/Publikationen/publikationen_node.html, zuletzt aufgerufen am 12.01.2025

965 *UNODC,* goAML, https://unite.un.org/goaml/, zuletzt aufgerufen am 12.01.2025.

966 Ibid.

967 *FIU,* XML-Schema Dokumentation, Stand 20.08.2018.

968 Hierzu ausf. *FIU.,* Handbuch goAML Web Portal, Stand 27.01.2020.

unabhängig von ihrer Höhe und unabhängig davon, ob sie schon durchgeführt wurden, noch bevorstehen oder nach § 46 GwG abgelehnt wurden.[969] Für verdächtige Geschäftsbeziehungen gilt dasselbe. Sie sind auch dann meldepflichtig, wenn sie sich erst anbahnen.[970]

Die Meldung muss nicht nur den konkreten Vorgang, sondern auch die wesentlichen Umstände enthalten, aus denen sich das Verdachtsmoment ergibt. Bei einer ungewöhnlichen Transaktion, etwa einer sehr hohen Bargeldeinzahlung, müssen der Meldung deshalb Begleitinformationen beigefügt werden, aus denen sich die Auffälligkeit ableiten lässt, z. B. vergangene Umsätze.[971] In der Praxis wird außerdem der Sachverhalt in Form einer schriftlichen Begründung präsentiert, wobei sich der Gutachtenstil bewährt haben soll.[972]

Die konkreten Details der Meldung ergeben sich in der Praxis zwangsläufig aus der goAML-Webmaske bzw. den Anforderungen an die XML-Datei. Sämtliche der folgenden zusammengefassten Angaben sind dem Handbuch zur goAML-Webmaske[973] entnommen.

Bei der Meldung sind zunächst Informationen über den meldenden Verpflichteten wie Name, Adresse etc. und des meldenden Mitarbeiters einzutragen sowie die unmittelbaren Umstände der Meldung, etwa das Datum, das Aktenzeichen, der Meldungstyp und der Grund der Meldung. Sodann sind sämtliche Informationen über die Transaktion anzugeben, d. h. der Betrag, die Währung, die handelnde Person, interne Referenznummer, das Transaktionsverfahren, Datum, Ort (z. B. Filiale), Verwendungszweck sowie sonstige Informationen als Kommentar.

Hinsichtlich der ausführenden Person sind alle persönlichen Daten inklusive Legitimationsdokumente (etwa die Ausweisnummer) und – soweit vorhanden – die E-Mail-Adresse anzugeben. Bei Überweisungen sind sinnvollerweise all diese Informationen auch bzgl. des Empfängers und der beteiligten Personen und Institutionen anzugeben. Steht die Transaktion mit Gütern im Zusammenhang, sind alle verfügbaren Informationen über die entsprechenden Sachen anzugeben, wie z. B. Identifikationsnummern oder bei Immobilien die Adresse des Objekts.

969 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 71 f.
970 Idem, S. 72.
971 Idem, S. 76.; s.a. *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 77 f.
972 *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (394);
973 *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 30 ff.

Geht die Transaktion von einem Bankkonto aus, sind die Kontoinformationen anzugeben. Dazu zählen u. a. die Kontonummer, der Name, das Institut, BLZ oder BIC/Swift, die Kontoart, der Kontostand und die Berechtigten.

dd. Eingang, Speicherung und Verbleib der Meldung bei der FIU

Die Meldung geht bei der FIU ein, die sie nach § 30 Abs. 1 Nr. 1 GwG entgegennehmen und verarbeiten muss. Das weitere Schicksal der Meldung bestimmen die §§ 30 ff. GwG.

Die Grundaufgabe der FIU besteht darin, die Meldungen auf ihren Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung zu analysieren, § 30 Abs. 2 GwG, und dann nach § 32 ff. GwG an die zuständigen Stellen weiterzuleiten. Dies gilt prinzipiell für alle nach § 30 Abs. 1 GwG entgegenzunehmenden Meldungen. Der Datenverarbeitungsprozess der FIU hängt also prinzipiell nicht von der Art der Meldung bzw. von der Person des Verpflichteten ab.[974]

Aufgrund der Fülle der Verdachtsmeldungen (s. o. III. 2. c. aa. (3)) ist es praktisch nicht denkbar, dass die Meldungen kurzfristig oder gar in Echtzeit bzw. unmittelbar nach deren Eingang bearbeitet werden. Laut einer Antwort der Bundesregierung auf eine kleine Anfrage von Abgeordneten und der Fraktion Bündnis90/Die Grünen werden zwar alle Meldungen umgehend erstbewertet – insbesondere, um Fristfälle nach § 46 GwG herauszufiltern, Angaben zur Dauer der Bearbeitung der nicht-priorisierten Fälle konnte die Bundesregierung machen.[975]

Grundsätzlich werden sämtliche Verdachtsmeldungen zunächst gespeichert, unabhängig davon, ob sie zeitnah weitergegeben werden.[976] Die Ermächtigung der FIU zur Speicherung ergibt sich aus § 29 Abs. 1 GwG, der als Generalklausel zur Verarbeitung von Daten[977] im Rahmen ihrer Aufgaben nach § 28 GwG dient.[978]

974 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (226).
975 BT-Drs. 19/2263, S. 4.
976 BT-Drs. 18/11928, S. 26; *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 11; *Barreto da Rosa* in Herzog GwG, § 32 Rn. 26, § 37 Rn. 19.
977 i. S. d. §§ 3, 46 Nr. 2 BDSG bzw. Art. 4 Nr. 2 DSGVO, vgl. BT-Drs. 18/11555, S. 140; zur Identität der Legaldefinitionen *M. Lang* in Taeger/Gabel DSGVO - BDSG, § 3 BDSG Rn. 18.
978 Vgl. BT-Drs. 18/11555, S. 140.

Die Daten sind nach §§ 37 Abs. 2, 38 Abs. 2 GwG eigentlich zu löschen, sobald *die Kenntnis dieser Daten für die Aufgabenerfüllung nicht mehr erforderlich ist.* Grundsätzlich wäre dies nach Abschluss der operativen Analyse der Fall. Es sei denn, es bestehen Anhaltspunkte, dass die Daten in der Zukunft noch relevant werden.[979] Die Bundesregierung argumentiert jedoch für das Bestehen starrer Löschfristen unabhängig von der Notwendigkeit der Daten und beruft sich dabei auf §§ 37 Abs. 2-4, 39 Abs. 1 GwG.[980] Personenbezogene Daten, die durch die FIU bearbeitet wurden, obgleich sie weitergeleitet wurden oder nicht, werden hiernach erst drei Jahre nach Beendigung der operativen Analyse automatisch gelöscht.[981]

Diese Praxis könnte auf einem falschen Verständnis der Speicher- und Löschpflichten nach §§ 37 ff. GwG beruhen. § 39 Abs. 1 GwG regelt die Errichtung automatisierter Dateien bei der FIU, die jeweils einer Anordnung bedürfen. Der Anordnung muss das Bundesinnenministerium zustimmen, § 39 Abs. 1 S. 2 GwG. Welche Dateien die FIU bislang errichtet hat, bzw. wie sie sortiert sind, unterliegt der Geheimhaltung.[982]

Die Bundesregierung bezieht sich in ihrer oben angesprochenen Antwort, in der sie von starren Löschfristen ausgeht, überraschenderweise nicht auf § 39 Abs. 2 GwG. Diese Vorschrift müsste aber korrekterweise mitzitiert werden. Dort erst wird unter Nr. 8 festgelegt, dass auch Fristen in der Anordnung aufgeführt werden müssen, in denen die in der Datei gespeicherten Daten überprüft werden müssen. § 39 Abs. 2 GwG stellt somit auf § 37 Abs. 4 GwG ab, der besagt, dass die FIU ihre gespeicherten Daten bei der Einzelfallbearbeitung und in festgesetzten Fristen, die im Gesetz aber nicht im Einzelnen dargelegt werden, prüfen muss, *ob gespeicherte personenbezogene Daten zu berichtigen, zu löschen oder in der Verarbeitung einzuschränken sind.*

§ 37 Abs. 4 und § 39 Abs. 2 GwG stehen also in einem gemeinsamen Kontext. Sie regeln aber nicht das Eintreten der Löschpflicht, sondern das Mindest-Überprüfungsintervall der gespeicherten Daten. Die Löschpflicht tritt grundsätzlich unmittelbar nach der operativen Analyse mit negativem Ausgang ein – spätestens aber, wenn die Daten nicht mehr zur Aufgabenerfüllung notwendig sind, § 37 Abs. 2 GwG.

979 *C. Lang* in Zentes/Glaab GWG, § 37 Rn. 7 mit Verweis auf BVerwG, NJW 1994, 2499.
980 BT-Drs. 19/2263, S. 8 f.
981 Ibid.
982 *Barreto da Rosa* in Herzog GwG, § 29 Rn. 2.

§ 37 Abs. 4, § 39 Abs. 2 GwG beziehen sich also nur auf die Fälle, in denen nach der Analyse noch von einer Notwendigkeit ausgegangen wird, die Daten deshalb gespeichert werden und die Notwendigkeit dann zu einem späteren Zeitpunkt entfällt. Diese „Datenleichen" sind das Ziel der turnusmäßigen Überprüfung.

Die von der Bundesregierung geschilderte Praxis einer Speicherung sämtlicher bearbeiteten Meldungen für drei Jahre kann nur damit erklärt werden, dass die FIU nach jeder Analyse einfach prinzipiell annimmt, dass die Daten eventuell noch gebraucht werden, und sie deshalb speichert. Da die erste Kontrolle dann erst nach drei Jahren erfolgt, kommt es für diesen Zeitraum zu einer indifferenten Speicherung auch nicht notwendiger Daten. Die in § 37 Abs. 4 GwG eigentlich auch nach der Einzelfallbearbeitung vorgesehene Prüfung der Löschpflicht wird von der Bundesregierung ignoriert.

Für den Fall, dass die FIU im Rahmen der Analyse zu einem positiven Ergebnis gelangt, sie also von einem Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung ausgeht und den Fall weiterleitet, werden die gemeldeten Daten für fünf Jahre nach dem Abschluss der Analyse aufgehoben.[983]

ee. Ergebnis: Speicherung gefilterter Finanzdaten bei der FIU.

Wie soeben dargestellt, enthält jede Verdachtsmeldung eine Fülle an Finanzinformationen, da sie nicht nur die konkreten Umstände des verdächtigen Vorfalls enthalten, sondern auch jene, aus denen sich die Ausfälligkeit ergibt. Hierzu gehört insbesondere das Transaktionsverhalten bei Bankkunden, weshalb den Verdachtsmeldungen regelmäßig Umsatzlisten beigefügt werden dürften.[984] Jedenfalls im Rahmen der Verdachtsmeldungen wird also eine große Menge an sensiblen[985] persönlichen Daten verarbeitet.[986] Der Bundesregierung wurde im Rahmen einer kleinen Anfrage im Jahr 2018 die Frage gestellt, wie viele unterschiedliche Dateien die FIU

983 BT-Drs. 19/2263, S. 9.

984 *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 78; *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (S. 395).

985 Vgl. BVerfGE 120, 274 (346 ff.) [2008] – Online-Durchsuchung.

986 Übersicht bei *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (393 ff.); umfänglich *FIU,* Handbuch goAML Web Portal, Stand 27.01.2020, S. 30 ff.

führt, und wie viele Personen je Datei geführt werden. Die Antwort fällt knapp aus. Es würden aktuell in den Dateien der FIU unter Nutzung von goAML *149.285 natürliche und juristische Personen gespeichert.*[987] Ob es sich bei all diesen Personen um eigene Verdachtsmeldungen handelt, oder wie viele Meldungen im Schnitt auf diese Personen entfallen, bleibt unbeantwortet. Da in den Meldungen regelmäßig eine ganze Fülle an Personen genannt wird (ausführende Person, Empfänger, wirtschaftlich Berechtigter, beschäftigte Mitarbeiter etc.), lässt sich aus der Antwort der Bundesregierung nicht abschätzen, wie viele Daten bzw. einzelne Vorgänge oder Verdächtige gespeichert sind. Es ist noch nicht einmal klar, ob alle diese Daten aus Verdachtsmeldungen stammen. Aus der Antwort ergibt sich nur, dass die FIU von *149.285 verschiedenen* Personen, inklusive juristischen Personen, irgendwelche Daten besitzt.

Wenngleich diese Daten dazu bestimmt sind, einem sicherheitsrechtlichen Zweck zu dienen und insofern von den Verpflichteten vorgefiltert werden, ist die Schwelle, ab der diese Daten übermittelt werden, sehr niedrig. Sie wird unterhalb dem strafprozessualen Anfangsverdacht eingeordnet (s.o.). Gleichzeitig regt das Compliance System des GwG die Verpflichteten dazu an, möglichst umfangreich zu melden (s. o.), da sie sich anderenfalls bußgeldpflichtig machen können.[988]

Durch die Verdachtsmeldungen entsteht bei der FIU daher ein gewaltiger Datenpool, der sich aus sämtlichen Meldungen und den hierzu eingeholten Informationen speist.[989] Ausweislich von Angaben der Bundesregierung werden die Meldungen für mindestens drei Jahre gespeichert, da die eigentlich unmittelbar einsetzenden Löschpflichten erst im Rahmen der turnusmäßigen Datenprüfungen umgesetzt werden.[990] Es besteht damit ein Normenregime, das den Umgang mit diesen Daten einigermaßen streng reglementieren könnte, faktisch aber nicht angewandt wird.

Das GwG sieht aber nicht nur eine Speicherpflicht für die vorgefilterten Meldedaten bei der FIU nach §§ 29, 39 GwG vor, sondern auch eine umfassende Aufzeichnungs- und Aufbewahrungspflicht der Verpflichteten. Auf diese soll im folgenden Abschnitt eingegangen werden.

987 BT-Drs. 19/2263, S. 3.
988 Bspw. OLG Frankfurt, NStZ 2020, 173 (175).
989 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (228).
990 BT-Drs. 19/2263, S. 8 f.

d. Aufzeichnungs- und Aufbewahrungspflicht nach § 8 GwG

Die nach § 2 GwG Verpflichteten müssen gem. § 8 Abs. 1 GwG bestimmte Informationen aufzeichnen und aufbewahren. Das GwG verpflichtet insbesondere Banken und Zahlungsinstitute zur Vorhaltung massenhafter Kontoinhaltsdaten ihrer Kunden. Nicht nur Verdachtsmeldungen sind zu speichern, auch alle unauffälligen Transaktionsdaten unterfallen § 8 Abs. 1 GwG.

aa. Verdachtsmeldungen

Nicht nur die FIU, auch die Verpflichteten haben die Verdachtsmeldungen zu speichern. Nach § 8 Abs. 1 Nr. 4 GwG sind die *Erwägungsgründe und eine nachvollziehbare Begründung des Bewertungsergebnisses eines Sachverhalts hinsichtlich der Meldepflicht nach § 43 Abs.1 GwG* aufzuzeichnen und aufzubewahren. Diese Pflicht betrifft alle Fälle, in denen konkret geprüft wurde, ob eine Pflicht zur Meldung bestehen könnte – also auch jene, in denen von einer Meldung abgesehen wurde.[991] Ziel ist es, für die Aufsichtsbehörden nachvollziehbar zu halten, ob die Beurteilung sachgerecht erfolgt ist, bzw. auf richtigen Tatsachen und allgemeingültigen Bewertungsmaßstäben beruht.[992] Die Erwägungsgründe umfassen daher sinnvollerweise sämtliche Informationen, die im Rahmen der Verdachtsmeldung an die FIU übermittelt wurden, da auch im Rahmen der Verdachtsmeldung die Hintergründe der Auffälligkeit dargelegt werden müssen (s. o.). Der Datenbestand der Verdachtsmeldungen bei den Verpflichteten wird also im Falle einer erstatteten Meldung regelmäßig identisch mit der übermittelten Meldung sein, jedenfalls aber nicht dahinter zurückstehen. Die Aufbewahrungspflicht läuft in diesen Fällen letztlich darauf hinaus, dass sowohl bei der FIU als auch bei den Verpflichteten die Meldung aufbewahrt wird. Unterschiede bestehen allenfalls hinsichtlich der Frist (dazu unten).

991 BT-Drs. 18/11555, S.114; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 74 f.; *Täubner* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 377 (393).

992 *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 74 f.

bb. Allgemeine Transaktionsdaten aufgrund der Überwachungspflicht

Neben dieser immerhin von einem gewissen Verdachtsmoment geprägten Dokumentationspflicht enthält § 8 GwG in Abs. 1 Nr. 1 GwG eine generell formulierte Pflicht zur Aufzeichnung und Aufbewahrung *aller Informationen, die von den Verpflichteten im Rahmen der Erfüllung ihrer Sorgfaltspflichten erhoben oder eingeholt werden.*

Das betrifft nach § 8 Abs. 1 Nr. 1 lit. a) GwG zunächst die Informationen, die im Rahmen der Identifizierungspflicht i. S. d. § 10 Abs. 1 Nr. 1, §§ 11, 12 GwG eingeholt wurden. Insbesondere sind nach § 8 Abs. 2 S. 1 GwG die Art, die Nummer und die Behörde, die das zur Überprüfung der Identität vorgelegte Dokument ausgestellt hat, aufzuzeichnen. Von den vorgelegten Identifikationspapieren – insbesondere Ausweispapieren – müssen die Verpflichteten nach § 8 Abs. 2 S. 2 GwG Kopien anfertigen.

Auch wenn diese umfangreiche Speicherung von Identifikationsdaten, gerade auch in Kombination mit der Kontobestandsabfrage nach § 24c KWG, schon einen beachtlichen vorgehaltenen Datenbestand darstellt, soll der hier angelegte Fokus doch auf § 8 Abs. 1 Nr. 1 lit. b) GwG liegen. Dieser beinhaltet eine Aufzeichnungs- und Aufbewahrungspflicht für Informationen *über Geschäftsbeziehungen und Transaktionen, insbesondere Transaktionsbelege, soweit sie für die Untersuchung von Transaktionen erforderlich sein können*, die im Rahmen der Erfüllung der Sorgfaltspflichten erhoben und eingeholt werden.

(1) Überwachung als anfängliche Pflicht zum Erfassen aller Transaktionen

§ 8 Abs. 1 Nr. 1 lit. b) GwG muss im Kontext mit der Überwachungspflicht des § 10 Abs. 1 Nr. 5 GwG verstanden werden. Das GwG selbst beinhaltet keine präzisen Aussagen zum Umfang der Überwachungspflicht, geschweige denn, wie die *Überwachung* ausgestaltet werden soll. Erst der Blick auf § 25h Abs. 2 KWG und § 14 Abs. 1 S. 2 GwG bringt i. V. m. mit den ESA-Leitlinien die erhellende Erkenntnis, dass die Überwachungspflicht eine originäre Pflicht zur Wahrnehmung sämtlicher Transaktionen beinhaltet. Aus den Leitlinien ergibt sich,[993] dass die Verpflichteten in Abhängigkeit von den jeweiligen Umständen zwischen einer Echtzeit- oder einer nach-

993 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.74, 4.75.

träglichen Überwachung wählen können. Beides ist nur möglich, wenn die Sicherungsmaßnahmen der Verpflichteten zumindest alle Transaktionen wahrnehmen können. Das GwG kann also nicht davon ausgehen, dass die Datenbasis für die Transaktionsüberwachung ohnehin vorliegt, um sodann nur deren nachträgliche, verschiedentlich intensive Überprüfung anzuordnen. Ein solches Verständnis würde die Echtzeitüberwachung ausschließen. Vielmehr ist schon die Anlage dieser Datenbasis, auch wenn sie zwangsweise ohnehin entsteht, eine Pflicht des Geldwäscherechts (s. o. 2. b. aa. (2)).

Jedenfalls aber ist die Datenbasis in Form aller durchgeführten Transaktionen für die Überwachungspflicht unabdinglich. Sie kann deswegen auch aus der Aufzeichnungspflicht des § 8 Abs. 1 Nr. 1 GwG konstruiert werden, wenn man die Überwachungspflicht auf die Kontrollpflicht einer schon existierenden Datenbasis reduziert. Dies ergibt sich aus der Pflicht, sämtliche Transaktionen zu prüfen. Hierfür müsste der gesamte Datenbestand bzgl. der Kundentransaktionen als *Information einbezogen* werden und wäre folglich nach § 8 Abs. 1 Nr. 1 GwG in vollem Umfang aufzuzeichnen (s. o. 2. b. aa. (2)).[994]

(2) Unabhängige Pflicht zur Speicherung von Transaktionsbelegen in der GWRL und dem Auslegungsmaterial

Zu diesem Verständnis, dass sämtliche Transaktionsbelege im Rahmen einer Geschäftsbeziehung aufbewahrt werden müssen, gelangt man auch zwingend, wenn man zur Auslegung des § 8 Abs. 1 Nr.1 GwG den Art. 40 Abs. 1 lit. b) der GWRL heranzieht. Dessen Wortlaut enthält hinsichtlich der Aufbewahrungspflicht für Transaktionsbelege, anders als § 8 Abs. 1 Nr. 1 GwG, von vorneherein keine Anknüpfung an die Sorgfaltspflichten.

Stattdessen heiß es dort schlicht: *„Die Mitgliedstaaten schreiben vor, dass die Verpflichteten die nachstehenden Dokumente und Informationen im Einklang mit dem nationalen Recht für die Zwecke der Verhinderung, Aufdeckung und Ermittlung möglicher Geldwäsche oder Terrorismusfinanzierung durch die zentrale Meldestelle oder andere zuständige Behörden aufbewahren: a)… b) die Transaktionsbelege und -aufzeichnungen (…) für die Dauer von fünf Jahren nach Beendigung der Geschäftsbeziehung mit dem Kunden oder nach dem Zeitpunkt einer gelegentlichen Transaktion.“*

994 Für ein solches Verständnis etwa *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462), wohl auch *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18.

Die ESA-Leitlinien bestätigen dieses Bild. Dort wird in verschiedenen Bullet Points aufgeführt, dass Aufzeichnungen geführt werden müssen für: „*a) die für die Sorgfaltspflichten gegenüber Kunden relevanten Informationen; b) ihre Risikobewertungen; und c) Transaktionen.*"[995] Somit wird klargestellt, dass Transaktionsaufzeichnungen immer geführt werden müssen, unabhängig von der Frage, ob man sie auch als *zur Erfüllung der Sorgfaltspflichten notwendige Informationen* subsumieren könnte.

Auch die FATF-Empfehlungen[996] sind in dieser Hinsicht eindeutig. Unter der lfd. Nr. 11 wird im ersten Absatz verdeutlicht, dass alle notwendigen Transaktionsdaten aufbewahrt werden sollen, um Auskunftsersuchen staatlicher Stellen nachkommen zu können. Diese Aufbewahrungen müssen ausreichend sein, um individuelle Transaktionen rekonstruieren zu können. In einem weiteren eigenen Absatz wird sodann festgestellt, dass die Finanzinstitute alle Aufzeichnungen über Transaktionen aufbewahren sollen, die sie im Rahmen der Sorgfaltspflichten erlangt haben. Selbst wenn man die FATF-Empfehlungen nun so liest, dass sie aus der Erfüllung der Sorgfaltspflichten noch keine Pflicht zur Aufzeichnung sämtlicher Transaktionsdaten ableiten, so stellen sie dennoch ganz ausdrücklich klar, dass sämtliche Transaktionsbelege aufbewahrt werden müssen.

Das Geldwäschegesetz, das der Umsetzung der EU-Geldwäsche RL und mittelbar den FATF-Empfehlungen dient, muss also, ähnlich wie die §§ 25a KWG, 257 HGB, 22 UStG, 147 AO, eine Pflicht zur Speicherung sämtlicher Transaktionsdaten vorsehen.[997] Obwohl dies in der Literatur zum GwG nicht deutlich zum Ausdruck kommt, ergibt sich dies dort daraus, dass

995 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 5.1.

996 *FATF,* Recommendations 2012, konsolidierte Fassung März 2022.

997 Bzgl. Art. 40 Abs. 1 li.t b) 4. EU-GeldwäscheRL: *C. Kaiser,* Privacy in Financial Transactions, 2018, 102 ff. und *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (118 f; 123); vgl. auch *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 28, 29, S. 22 ff.; ohne konkreten Normbezug: *Ioannides,* Money Laundering, 2016, S. 135; *Flores/Angelopoulou/Self* J. of Internet Services & Information Security 3 (2013), 101 (111); vgl. auch *Basel Committee on Banking Supervision*, (Bank of Internationational Settlements), Guidelines AML, January 2014 (rev. July 2020), S. 11; offen gelassen bei *B. Vogel* in Vogel/

auf die unterschiedlichen Fristen der Transaktionsaufbewahrungspflichten aufmerksam gemacht wird.[998]

Auch der historische Gesetzgeber ließ erkennen, dass er den Umfang der Speicherpflicht erkannt hat. In der ersten Form des GwG anno 1993 wurde noch auf eine Aufbewahrungspflicht für Transaktionsbelege verzichtet. In der Gesetzesbegründung wurde dies ausdrücklich damit erklärt, dass eine solche Pflicht ja schon in § 257 HGB enthalten sei.[999] Man ging also davon aus, dass eine geldwäscherechtliche Aufbewahrungspflicht der Pflicht nach § 257 HGB inhaltlich entsprechen würde und deswegen obsolet wäre. Dieses Verständnis trägt noch immer. § 8 Abs. 1 GwG und § 257 HGB sind gleichlaufend. Sie sehen eigenständig eine umfangreiche Pflicht zur Aufbewahrung sämtlicher Transaktionsdaten (in Form von Kontoauszügen) vor.

(3) Umfang, Form und Speicherfrist – „Big Data".

Die Transaktionsbelege müssen ausreichend sein, um die geldwäscherechtlichen Pflichten zu erfüllen.[1000] Sie enthalten dazu mindestens den Kundennamen, die Kontonummer, Empfangs- und Versendungsinstitut, Empfangs- und Versendungsland, das Transaktionsdatum, den Betrag und die Währung sowie den Verwendungszweck.[1001]

Die Aufbewahrungspflicht für alle nach § 8 GwG notwendigen Aufbewahrungen beträgt gem. § 8 Abs. 4 S. 1 GwG fünf Jahre unbeschadet anderer gesetzlicher Vorschriften. Es handelt sich somit um eine Mindestfrist.[1002] Jedenfalls nach zehn Jahren sind die Unterlagen zu vernichten, § 8 Abs., 4 S. 2 GwG. Die Frist beginnt nach § 8 Abs. 4 S. 4 GwG für Transaktionsbelege mit Ablauf des Jahres, in dem die Angabe festgestellt wurde, d. in dem Jahr, in dem die Transaktion durchgeführt wurde.

Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (990); aA. *Krais,* Geldwäsche, 2018, S. 284.

998 *Herzog* in Herzog GwG, § 8 Rn. 1, 18; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438; Diergarten/Fraulob GWG, S. 228; *Stegmann/Meuer* in Bürkle (Hrsg.), Compliance, 3. Aufl. 2020, § 12 Rn. 230.

999 BT-Drs. 12/2704, S. 16.

1000 Vgl. *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d) S. 71.

1001 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 53; *Fiedler/Krumma/Zanconato ua.,* Geldwäscherisiko Glücksspiel, 2017, S. 38.

1002 Hierzu krit. *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 29.

Für Informationen, die zur Erfüllung der Pflichten nach § 10 Abs. 3 S. 1 GwG (insbesondere Identifizierung bei Begründung der Geschäftsbeziehung) eingeholt werden, beginnt die Pflicht hingegen erst mit dem Schluss des Kalenderjahres, in dem die Geschäftsbeziehung endet, § 8 Abs. 4 S. 3 GwG.

Zwischen Mindest- und Maximaldauer der Speicherung entscheiden die Verpflichteten nach Ermessen.[1003] Der Gesetzgeber ging davon aus, dass durch die mögliche Verlängerung (bis zu zehn Jahre) eine Angleichung an die §§ 257 Abs. 5 HGB, 147 Abs. 4 AO stattfinden sollte.[1004]

Bei den Transaktionsbelegen kommt es insofern zu einem Gleichlauf der Fristen. §§ 257 Abs. 5 HGB, 147 Abs. 4 AO sehen für Kontoauszüge eine Aufbewahrungspflicht von zehn Jahren vor[1005] und zwar, wie auch § 8 Abs. 4 S. 4 GwG, ab Ende des Kalenderjahres, in dem die Dokumente entstanden sind. Das Ermessen i. R. v. § 8 Abs. 1 GwG wird bei Kontoauszügen also leerlaufen.[1006]

Die aufbewahrungspflichtigen Daten können nach § 8 Abs. 3 GwG digital gespeichert werden, wenn sie mit den festgestellten Informationen übereinstimmen, während der Frist verfügbar bleiben und jederzeit in angemessener Zeit lesbar gemacht werden können. Im Hinblick auf die Feststellung, dass die Banken sämtliche Informationen über die Transaktionen ihrer Kunden archivieren müssen, ist diese Möglichkeit wohl auch kaum wegzudenken. Jedenfalls bei den größeren Banken, insbesondere den am Privatkundenmarkt beteiligten, liegen immense Datenmengen vor, deren Verwendung unter dem Stichwort „Big Data" auch in der IT-Wissenschaft diskutiert wird.[1007] Die Speicherung erfolgt längst nicht mehr nur in den Rechenzentren der Verpflichteten, sondern vermehrt in Kooperation mit großen Anbietern von Online- bzw. Cloud-Speichern.[1008] Transaktionsda-

1003 *Brian/Krais* in BeckOK GwG, § 8 Rn. 38.

1004 BT-Drs. 19/13827, S. 76.

1005 Vgl. *Schober*, BC 2013, 528 (532).

1006 *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438.

1007 Etwa *Skyrius/Giriūnienė/Katin ua.* in Srinivasan (Hrsg.), Big Data, 2018, S. 451 (452 ff., 458 ff.); *Turner/Schroeck/Shockley*, (IBM Institute for Business Value, Saïd Business School at the University of Oxford), IBM Paper Big Data, 2013; *Deutsche Bank*, Big Data Whitepaper, 2014; Sapozhnikova/*Gayanova/Vulfin ua.* in, ITNT, IV INT, 2018, S. 228 (229 f.); *Westermeier*, Information, Communication & Society 23 (2020), 2047 (2051 f.).

1008 Die Deutsche Bank hat eine große Kooperation mit Google angekündigt, siehe *Deutsche Bank,* Deutsche Bank & Goolge Cloud partnership, 4. Dezember, 2020,

ten dürften bei diesen Datenbeständen einen großen Anteil ausmachen[1009] und sollen laut einem der größeren Anbietern von Cloud-Speichern insbesondere zum Erkennen von Geldwäsche verwendet werden.[1010]

3. Zusammenfassend: Speicherung von Inhaltsdaten bei FIU und Privaten

In diesem Kapitel wurde dargestellt, wie sich aus der GeldtransferVO und dem GwG, das die GWRL umsetzt, eine Pflicht zur Speicherung von Kontoinhaltsdaten ergibt. Es konnten zwei Datenpools identifiziert werden, die als taugliches Objekt einer Untersuchung aus dem Blickwinkel der Rechtsprechung zur Vorratsdatenspeicherung infrage kommen.

a. Speicherung von Verdachtsmeldungen bei der FIU, §§ 28 ff., 43 Abs. 1 GwG

Zunächst agiert die Zentralstelle für Finanztransaktionsuntersuchungen bzw. Financial Intelligence Unit – FIU als Sammelstelle für Verdachtsmeldungen bzgl. Geldwäsche und Terrorismusfinanzierung nach § 28 Abs. 1 Nr.1, § 30 Abs. 1, 2, § 43 Abs. 1 GwG. Um dieser Aufgabe nachzukommen, darf sie persönliche Daten verarbeiten, § 29 GwG.

Die Verdachtsmeldungen werden unterhalb eines strafprozessualen Verdachtsgrads[1011] von privaten Akteuren an die FIU übermittelt. Die Verpflichteten werden danach nicht selbst als Strafverfolger oder Verfassungsschützer tätig, sondern lediglich als Lieferanten von Informationen, die

---

https://www.db.com/news/detail/20201204-deutsche-bank-and-google-cloud-sign-pioneering-cloud-and-innovation-partnership?language_id=1, zuletzt aufgerufen am 12.01.2025.

1009 *Turner/Schroeck/Shockley*, (IBM Institute for Business Value, Saïd Business School at the University of Oxford), IBM Paper Big Data, 2013, S. 6.

1010 *Stackowiak et al.*, (Oracle Corp.), Big Data in Financial Services and Banking, 2015, S. 7.

1011 BT-Drs. 18/11928, S. 26.; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; *Bundesministerium der Finanzen,* Auslegunsghinweise Verdachtsmeldewesen, 06. November 2014, S. 3; *Greite* in Zentes/Glaab GWG, § 43 Rn. 10 ff.; *Findeisen* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. II, 3. Auflage 2017, § 85 Rn. 62; krit.; *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5 ff., 24 ff.; *Degen,* Geldwäsche, 2009, 127 f.; *Krais,* Geldwäsche, 2018, Rn. 510 f.; *Klugmann*, NJW 2012, 641 (644); *Bülte*, NZWiSt 2017, 276 (280 f.).

eventuell, ausgehend von einer weiteren Analyse, durch die FIU an verschiedene Sicherheitsbehörden weitergeleitet werden können. Im Moment der Meldung ist somit gerade nicht klar, ob die an die FIU übermittelten Informationen eine sicherheitsrechtliche Relevanz aufweisen. Sie sind allenfalls *auffällig* im geldwäscherechtlichen Sinne.[1012]

Die FIU prüft die Meldungen nach Aussagen der Bundesregierung zwar umgehend, d. h. spätestens am Folgetag des Eingangs, allerdings nur sehr oberflächlich.[1013] Aufgrund des mittlerweile gewaltigen Meldeaufkommens[1014] wäre eine intensive Prüfung unmittelbar nach der Übermittlung auch nicht denkbar. Die Meldungen werden stattdessen von der FIU gespeichert und in einer Datei, für die nach § 39 GwG eine Errichtungsanordnung gilt, abgelegt. Dort liegen sie, nach Aussage der Bundesregierung, für mindestens drei Jahre nach Bearbeitung, auch wenn sie nicht weitergeleitet wurden.[1015] Bei der FIU liegen also massenhaft Kontoinhaltsdaten vor, bei denen unklar ist, ob sie sicherheitsrechtlich relevant sind, oder nicht.

b. Speicherung von Verdachtssachverhalten und Transaktionsdaten bei den Verpflichteten

Die noch weitaus größere Datensammlung, die im Rahmen der geldwäscherechtlichen Vorschriften angelegt werden muss, findet sich aber unmittelbar und dezentralisiert bei den Verpflichteten.

aa. Art. 16 GeldtransferVO

Die an einem Geldtransfer beteiligten Institute müssen schon nach Art. 16 Abs. 1, S. 2 GeldtransferVO alle Angaben, die nach den Art. 4-7, 11 Geld-

1012 BT-Drs. 18/11928, S. 26.; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 72; *Bundesministerium der Finanzen,* Auslegungshinweise Verdachtsmeldewesen, 06. November 2014, S. 3; *FIU,* Anhaltspunktepapier - Newsletter 11/2014, August 2014, https://geldwaesche-beauftragte.de/wp-content/uploads/2017/04/FIU_Newsletter_Ausgabe_Nr._11_-August_2014.pdf, zuletzt aufgerufen am 12.01.2025; Die FIU-Indikatoren für Auffälligkeit zusammengefasst bei zusammengefasst bei *Diergarten* in Hauschka/Moosmayer/Lösler (Hrsg.), Hdb. Haftungsvermeidung, 3. Aufl. 2016, § 34 Rn. 392; *Krais,* Geldwäsche, 2018, Rn. 717.

1013 BT-Drs. 19/2263, S. 4.

1014 *FIU,* Jahresbericht, 2019, S. 15 ff.

1015 BT-Drs. 19/2263, S. 8 f.

transferVO für den entsprechenden Geldtransfer bereitgestellt werden, fünf Jahre lang aufbewahren (s. o. 1. d.). Bei diesen Angaben handelt es sich um die entscheidenden Umstände eines Transfervorgangs – also die Namen der Beteiligten sowie die Kontonummern, außerdem die Anschrift des Auftraggebers, die Nummer eines Ausweisdokuments oder das Geburtsdatum und der Geburtsort des Auftraggebers. Die GeldtransferVO dient insofern ausdrücklich dem Nachvollzug der „Papierspur"[1016] unbarer Zahlungen.

Der Anwendungsbereich der Verordnung ist aber mit Blick auf das Massengeschäft überschaubar. Nach Art. 5 GeldtransferVO sind nämlich Zahlungen innerhalb der EU von den Übermittlungsanforderungen weitgehend ausgenommen. Es müssen lediglich die Konto- bzw. die Transaktionsnummern, bei Transaktionen außerhalb einer Geschäftsbeziehung (Einmalzahlungen), übermittelt werden. Die übrigen Daten können zwar vom Dienstleister des Begünstigten proaktiv abgefragt werden. Dieses Anfragerecht ist aber bei Transaktionen unterhalb von 1.000,00 € begrenzt auf die Namen von Auftraggeber und Begünstigten sowie die Konto- bzw. Transaktionsnummern nach Art. 5 Abs. 2 lit. b) GeldtransferVO. Außerdem sind Bareinzahlungen generell vom Anwendungsbereich gem. Art. 2 Abs. 2, 4 lit. a) GeldtransferVO ausgenommen.

bb. § 8 Abs. 1 Nr. 2 GwG (Art. 40 Abs. 1 lit. b) GWRL)

Brisanter als die GeldtransferVO hinsichtlich der Speicherung von Kontoinhaltsdaten sind daher § 8 Abs. 1 Nr. 2 GwG i. V. m. § 10 Abs. 1 Nr. 5 GwG und § 25h Abs. 2 S. 1 KWG.

Die in § 10 Abs. 1 Nr. 5 GwG, § 25h Abs. 2 S. 1 KWG vorgesehene kontinuierliche Überwachungspflicht wird in der Praxis obligatorisch durch ein umfassendes Kontenmonitoring und Einzelfall*screening* umgesetzt.[1017] Ins-

1016 *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25g KWG Rn. 3; *Schatz* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 525 (527); vgl. auch Erwägungsgrund 9, EU-GeldtransferVO.

1017 BT-Drs. 16/9038, S. 50; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *ders.* in Herzog GwG, § 25h Rn. 12 ff.; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462); *Jahn*, ZRP 2002, 109 (110); *Herzog/Christmann*, WM 2003, 6 (11).

besondere Banken, die sich am privaten Massenverkehr beteiligen, müssen hierfür ausdrücklich spezielle EDV-Systeme etablieren.[1018]

Die Überwachungspflicht setzt nach dem hier vorgetragenen Verständnis die Datenbasis in Form aller Transaktionen aller Kunden nicht einfach voraus, sondern konstituiert deren Anlegung. *Überwachen* bedeutet also nicht nur, dass die Banken ihre bestehenden Daten regelmäßig kontrollieren, sondern dass sie alle Transaktionen zumindest digital wahrnehmen und speichern. Es muss von der EDV an diesem Punkt nicht immer eine Auffälligkeit registriert werden, es kann auch eine nachträgliche Kontrolle erfolgen.[1019] Die abstrakte Pflicht zur Anlegung dieser Datenbasis bleibt vom Zeitpunkt der Rasterung aber unberührt.

Aus § 8 Abs. 1 Nr. 2 GwG folgt im Anschluss die Pflicht zur Aufbewahrung dieses Datensatzes. Selbst wenn man ausschließlich von Überwachung in Form einer nachträglichen Kontrolle ausgehen würde, müsste aber ohnehin eine Speicherung erfolgen, denn § 8 Abs. 1 GwG schreibt auch die Aufbewahrung solcher Informationen vor, die *zur* Erfüllung der Sorgfaltspflichten eingeholt wurden.[1020] Da das Kontenscreening bzw. -monitoring[1021] sämtliche Transaktionen erfasst[1022], muss die gesamte Transaktionsdatenbasis herangezogen werden und fällt spätestens jetzt unter die Aufbewahrungspflicht. Dieses Ergebnis wird vom Wortlaut des Art. 40

1018 BT-Drs. 16/9038, S. 50; dazu *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d.; *Langweg* in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, § 14 GWG Rn. 105; *Achtelik* in Herzog GwG, § 25h KWG Rn. 11 ff.; *ders.* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h KWG Rn. 16 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (456 f.); *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 50 ff.

1019 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.74 a); zur Praxis: *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 57; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (455 f.).

1020 So etwa *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h KWG Rn. 18; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463).

1021 Begriffe nach *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.

1022 BT-Drs. 16/9038, S. 50; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 4 Rn. 11; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (463); *Degen,* Geldwäsche, 2009, S. 206.

Abs. 1 lit. b) der 4. GWRL und den Auslegungsmaterialen[1023] gestützt, die unabhängig von den Sorgfaltspflichten eine Aufbewahrung der Transaktionsbelege anordnen.

§ 8 Abs. 1 Nr. 2 GwG reiht sich somit ein in die Vorschriften des Zahlungs-, Aufsichts-, Handels- und Privatrechts, die ebenfalls eine Pflicht zur Speicherung von Kontotransaktionsdaten etablieren. Wenngleich er aufgrund der inhaltlichen Überschneidung mit diesen Vorschriften faktisch nicht zu mehr gespeicherten Daten führt, ergänzt § 8 Abs. 1 Nr. 2 GwG aber doch die Zwecke der Speicherung um einen sicherheitsrechtlichen Aspekt.

Die Vorschrift begründet also durchaus, wie die Opposition im Bundestag schon im Jahr 2008 befürchtet hatte[1024], nichts Geringeres als die unbegrenzte Pflicht für Banken und andere geldwäscherechtlich Verpflichteten zur Speicherung sämtlicher Transaktionsdaten ihrer Kunden.[1025]

1023 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 5.1; *FATF,* Recommendations 2012, konsolidierte Fassung März 2022, lfd. Nr. 11.

1024 BT-Drs. 16/9647, S. 3.

1025 Vgl. *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 101 ff; 493 ff.; *Milaj/C. Kaiser* Int. Data Privacy Law 7 (2017), 115 (123); *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 28. 29, S. 22 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462); offen gelassen bei *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (990); aA. *Krais,* Geldwäsche, 2018, Rn. 284.

Kapitel E. Zugriff auf Kontodaten durch Sicherheitsbehörden

Im vorherigen Kapitel wurde dargestellt, welche Personen und Institutionen Kontodaten speichern und auf welcher Rechtsgrundlage dies jeweils erfolgt.

Zuvor wurde aufgezeigt, dass die bislang von der Rechtsprechung behandelten Überwachungsregimes, insbesondere die Vorratsdatenspeicherungen von TK-Verkehrsdaten, stets Daten betrafen, die sonst nicht in dieser Form bevorratet würden. Bedenklich an der Vorratsdatenspeicherung ist nicht, dass ein retrograder Zugriff auf die entsprechenden Daten ermöglicht wird, sondern, dass der Staat a priori von der etwaigen Notwendigkeit dieser Daten für Sicherheitszwecke ausgeht und deswegen die Kontrolle über das spätere Vorliegen sicherheitsrechtlich regelt (Kap. B. III. 2. a. aa.). Denn gewöhnlicherweise unterliegen Speicherungspflichten nur dem Wirtschaftsrecht und sind für die Sicherheitsbehörden gewissermaßen nur zufällig verwendbar. Bei der Vorratsdatenspeicherung gewährleistet das Sicherheitsrecht das Vorhandensein der Daten selbst.

Die Speicherung von Finanzdaten unterscheidet sich von den bisher von der Rechtsprechung behandelten Vorratsdatenspeicherungsregimen. Gerade für Kontoauszüge bestehen Aufbewahrungspflichten nicht nur im Sicherheits-, sondern auch im Wirtschafts- und Steuerrecht (s. Kap. D. II.).

Eine Verwendung der Finanzdaten kommt daher auch ohne spezifisches Überwachungsregime in Betracht. Es liegt die Vermutung nahe, dass die relativ geringe Aufmerksamkeit der geldwäscherechtlichen Überwachung damit zusammenhängt.

Um zu verstehen, weshalb die geldwäscherechtliche Überwachung überhaupt und auch hinsichtlich der Aufbewahrungs- und Zugriffsprobleme eine grundrechtliche Herausforderung darstellt, soll der allgemein sicherheitsrechtliche Zugriff auf diese Daten im Folgenden beschrieben werden.

Für die Übertragung bestehender Rechtsprechung zu Überwachungsmaßnahmen auf die Vorschriften des Geldwäscherechts ist dies nicht unmittelbar relevant. Die Darstellung dient mehr der Übersicht über die bisherige Rolle von Finanzdaten im Sicherheitsrecht und soll insofern darauf aufmerksam machen, dass spezifische Überwachungsregime auch bei solchen Daten noch grundrechtssensibel sein können, die nicht erst

aufgrund dieser Regime, sondern seit jeher im Rahmen der *klassischen* Sicherheitsgewährleistung eine Rolle spielen.

I. Offene Ermittlung von Kontodaten

Im ersten Kapitel wurde festgestellt, dass es der Kritik an der Vorratsdatenspeicherung im Kern darum geht, dass formelle Ermittlungsmaßnahmen umgangen werden. Der Bürger soll ganz konkret vor der Situation geschützt werden, dass eine Sicherheitsbehörde ihn überwacht, ohne dass dies in irgendeiner Weise nach außen hin sichtbar wird. Heimliche oder gar automatisierte Zugriffe wirken daher besonders schwer.[1026]

Um darzustellen, inwiefern durch gesetzliche Ermächtigungen zum heimlichen Abfragen von Kontodaten formelle bzw. „offene" Ermittlungsmaßnahmen umgangen werden, sollen diese übersichtlich erläutert werden. Da sich die Rechtsgrundlagen im Rahmen der offenen Ermittlungsmaßnahmen nicht nach der Art der Daten (Inhalts- oder Bestandsdaten) unterscheiden, kann an dieser Stelle auf eine diesbezügliche Differenzierung verzichtet werden.

1. Strafprozessuale Ermittlungsmaßnahmen

Im Strafprozess gilt hinsichtlich der Schuld- und Tatfrage das Strengbeweisverfahren.[1027] Soweit Daten in die Ermittlungen einbezogen werden sollen, müssen diese also auf Datenträgern im weitesten Sinne vorgelegt werden. Für Kontoumsätze oder Kontostammdaten werden sich grundsätzlich Urkunden anbieten, indem entsprechende Kopien in das Verfahren eingeführt werden. Denkbar wären gerade bei größeren Datenmengen aber auch digitale Datenträger im Wege der Inaugenscheinnahme.[1028] Eine solche Inaugenscheinnahme von *Urkunden* ist aber nur möglich, wenn es nicht auf den

1026 BVerfGE 130, 151 (196) – IP-Adressen; hierzu *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 178: Eingriffe bei Dritten sind „ambivalent".

1027 Siehe nur *B. Schmitt* in Meyer-Goßner/Schmitt StPO, StPO § 244 Rn. 6; *Kudlich* in MüKo StPO, Einl. Rn. 411.

1028 allg. *Trüg/Habetha* in MüKo StPO, § 244 Rn. 39; *Günther* in MüKo StPO, § 100a Rn. 161.

Inhalt der Urkunde ankommt.[1029] Können die Kontodaten also verschriftlicht werden, auch wenn sie ausschließlich digital vorhanden sind, § 249 Abs.1 S. 2 StPO, ist somit der Urkundenbeweis vorrangig.[1030] Kontoauszüge müssen daher wohl zwangsläufig im Wege des Urkundenbeweis nach § 249 StPO in das Verfahren eingeführt werden.[1031]

Im Strafverfahren stehen sich die Ermittlung der Wahrheit und die informationelle Selbstbestimmung der jeweiligen Beschuldigten in klassischer Weise gegenüber.[1032] Ermittlungen im Strafverfahren sind gerade dazu da, personenbezogene Informationen zu erhalten und tangieren somit zwangsweise die Privatheitsrechte der Betroffenen. Die strafprozessualen Maßnahmen können deshalb immer auch im Lichte der informationellen Selbstbestimmung erblickt werden. Daraus folgt zunächst, dass für sämtliche Ermittlungsmaßnahmen, die in dieses Recht eingreifen, eine Ermächtigungsgrundlage existieren muss.[1033]

Für die Ermittlung von Daten bei Privaten kommt im Strafprozessrecht lediglich § 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO als Generalklausel in Betracht.[1034] Dieser gestattet der Staatsanwaltschaft sowie der Polizei, „*Ermittlungen jeder Art*" vorzunehmen, „*soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln*". Ein Recht, „Auskunft zu verlangen", steht den Ermittlungspersonen gem. § 161 Abs. 1 S. 1 Hs. 1 Alt. 1 StPO dagegen nur gegenüber *Behörden* zu.

Soweit es sich bei Banken um Behörden i. S. d. § 161 Abs. 1 S. 1 Hs. 1 Alt. 1StPO handelt, ist also ein Auskunftsersuchen schon nach dem unmittelbaren Gesetzeswortlaut möglich. Unter den Begriff fallen alle Dienststellen des Bundes, der Länder, der Gemeinden und sonstigen Gebietskörperschaften sowie öffentlich-rechtliche Körperschaften.[1035] Die vorherrschende Ansicht bezieht daher auch öffentlich-rechtliche Kreditinstitute in den

1029 Vgl. BGH, NJW 2011, 3733 (3733); *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 249 Rn. 7 mwN.

1030 *Trüg,* StV 2016, 343 (344); *Eisenberg,* Beweisrecht, 10. Aufl. 2017, Rn. 2023 *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 249 Rn. 13.

1031 BGH, NJW 2011, 3733 (3733) Rn. 7; BGH Beschl. v. 06.05.1998, Az.: 1 StR 174/98.

1032 *Riepl,* Informationelle Selbstbestimmung, 1998, S. 11 ff., 172; *Singelnstein* in Barton/Kölbel/Lindemann (Hrsg.), Ermittlungsverfahren, 2015, S. 251 (253).

1033 *Frister* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. F Rn. 115 ff.

1034 BVerfG, NJW 2009, 1405 (1407) Rn. 26; *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 1a.

1035 *Sackreuther* in BeckOK StPO, § 161 Rn. 5; *Kölbel* in MüKo StPO, § 161 Rn. 24.

Adressatenkreis des Auskunftsverlangen mit ein.[1036] Das wird, aufgrund deren hohen Marktanteils, vor allem bei den nach § 40 KWG i. V. m. Landesgesetzen öffentlich-rechtlich organisierten[1037] Sparkassen relevant.[1038]

Manche Autoren wollen hier allerdings differenzieren. Soweit die öffentlich-rechtlichen Banken privatrechtlich bzw. -wirtschaftlich agieren, etwa im alltäglichen Kundengeschäft, sollen sie wie privatrechtlich organisierte Institute behandelt werden und folglich nicht dem Auskunftsrecht nach § 161 Abs. 1 S. 1 Hs. 1 Alt. 1StPO unterliegen (dazu gleich unten).[1039]

Jedenfalls aber folgt Arg. e. § 161 Abs. 1 S. 1 Hs. 1 StPO, dass gegenüber privaten Dritten kein Auskunftsrecht besteht. Die Ermittlungspersonen können bei diesen zwar um Informationen ersuchen, diese sind aber, anders als Behörden[1040], grundsätzlich nicht zur Antwort verpflichtet. Es handelt sich lediglich um eine formlose, schriftliche Zeugenvernehmung.[1041]

Dass die StPO keine allgemeinen Datenerhebungsklausel[1042] gegenüber Privaten enthält, überrascht, da private Akteure im 21. Jahrhundert den Staat als größten Datensammler abgelöst haben dürften.[1043] Durch die Datenspuren, die jeder Teilnehmer der Kommunikationsgesellschaft im Austausch mit anderen Privaten hinterlässt, entsteht ein gigantisches Potential für die Strafverfolgung.[1044] Diesem Umstand wird durch die StPO, die kein spezielles Regelungsregime für allgemeine Informationsanfragen an Private enthält, nicht ausreichend Rechnung getragen.[1045] Nur im Bereich der Telekommunikationsdaten wurden spezifische Normen für Auskunftsersuche

1036 *Weingarten* in KK-StPO, § 161 Rn. 8; *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 4; *Kretschmer*, wistra 2009, 181 (181).

1037 Dazu *R. Fischer/C. Müller* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 40 KWG Rn. 6; vgl. auch § 1 SpG BW.

1038 Vgl. *Kahler,* Kundendaten, 2017, S. 41.

1039 *Erb* in Löwe/Rosenberg StPO, § 161 Rn. 40; *Kahler,* Kundendaten, 2017, 41 f. *Reichling*, JR 2011, 12 (15); *Bär,* Computerdaten, 1992, 448 f.; ausf. *F. Jansen,* Bankauskunftsersuchen, 2010, S. 347, 252 ff; 263 ff.

1040 BVerfGE 141, 220 (337) – BKA-Gesetz; zu den Grenzen siehe etwa *Kölbel* in MüKo StPO, § 161 Rn. 30 ff.

1041 LG Hof, NJW 1968, 65 (65); *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 2; *Weingarten* in KK-StPO, § 161 Rn. 8; *F. Jansen,* Bankauskunftsersuchen, 2010, S. 46 f.; 227 f.; 445; *Reichling*, JR 2011, 12 (15); vgl. auch LG Frankfurt aM, NJW 1954, 688 (689), das jedoch eine Auskunftsverweigerung als unzulässig erachtete.

1042 Aus dem Polizeirecht etwa § 43 Abs. 1 LPolG BW.

1043 *Bung*, ZStW 2014, 536 (547).

1044 *Masing*, NJW 2012, 2305 (2309).

1045 Vgl. *Kölbel* in MüKo StPO, § 161 Rn. 26; *Kahler,* Kundendaten, 2017, S. 131; *Singelnstein*, NStZ 2012, 593 (603 f.).

geschaffen, vgl. §§ 100 g, j StPO, die mit entsprechenden Speicherfristen im TKG korrelieren („Doppeltürenprinzip").[1046]

Mangels einer eigenständigen Regelung müssen die Strafverfolgungsbehörden also auf die tradierten Ermittlungsmaßnahmen der StPO zurückgreifen, um an Kontoinformationen zu gelangen.

a. Förmliche Zeugenvernehmung

Möglich wäre etwa eine förmliche Zeugenvernehmung nach § 161a Abs. 1 StPO. Danach kann die Staatsanwaltschaft Zeugen laden und (mündlich) vernehmen. Eine solche Vernehmung kann auch mit Zwang durchgesetzt werden, § 161a Abs. 2 StPO. Voraussetzung für eine Zeugenvernehmung ist in materieller Hinsicht ein Anfangsverdacht i. S. d. § 152 Abs. 2 StPO.[1047] Soll die Zeugenvernehmung durch die Polizei als Ermittlungsperson der Staatsanwaltschaft erfolgen, richtet sich das Recht zur Ladung und die Aussagepflicht nach § 163 Abs. 3 StPO.

Nach ganz allgemeiner Auffassung können sich Kreditinstitute bzw. deren Mitarbeiter, die im Rahmen strafrechtlicher Ermittlungen als Zeuge geladen wurden, nicht auf ein „Bankgeheimnis" berufen.[1048] Soweit ein solches in der Bundesrepublik überhaupt besteht,[1049] ergibt sich daraus kein allgemeines Zeugnisverweigerungsrecht.[1050] Die Zeugnisverweigerungsrechte sind in den §§ 52 ff. StPO geregelt und gelten sowohl für das gerichtliche Verfahren als auch für das Ermittlungsverfahren, gem. den §§ 161 Abs. 1 S. 2, 163 Abs. 3 S. 2 StPO.

§ 52 StPO betrifft Familienangehörige und ist somit nur ausnahmsweise relevant. Die §§ 53, 53a StPO regeln die Auskunftsverweigerungsrechte der Berufsgeheimnisträger. Kredit-, Finanz- oder Zahlungsinstitute sind hier nicht genannt. Eine analoge Anwendung scheidet nach der Rechtsprechung aus.[1051]

1046 dazu BVerfGE 130, 151 (184) – Bestandsdatenauskunft I; E 155, 119 (167, 209 f.) – Bestandsdatenauskunft II.

1047 Vgl. *Frister* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. F. Rn. 29; *F. Jansen,* Bankauskunftsersuchen, 2010, S. 72 ff.

1048 Siehe nur *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 4; *Erb* in Löwe/Rosenberg StPO, § 161 Rn. 39 jeweils mwN.

1049 Hierzu *Tolani*, BKR 2007, 275; *Kahler,* Kundendaten, 2017, 42 ff.

1050 Ausf. *F. Jansen,* Bankauskunftsersuchen, 2010, S. 229 ff.

1051 LG Frankfurt a. M., NJW 1954, 688 (690); LG Hamburg, NJW 1978, 958.

Nach § 55 StPO besteht aber ein Zeugnisverweigerungsrecht, wenn sich der Zeuge mit der Aussage selbst belasten würde. Dies kann in Ausnahmefällen, wenn der geladene Mitarbeiter an der entsprechenden Tat mitgewirkt hat, relevant werden.

Für die öffentlich-rechtlichen Institute könnte sodann noch § 54 Abs .1 StPO zu beachten sein, wenn man der Auffassung folgt, dass diese nicht schon als Behörden nach § 161 Abs. 1 S. 1 Hs. 1 Alt. 1 StPO auskunftspflichtig sind und deren Mitarbeiter deshalb eventuell mit einer persönlichen Zeugenladung rechnen müssen.[1052] Danach könnten für ihre Mitarbeiter die Notwendigkeit einer Aussagegenehmigung durch ihre Vorgesetzten bestehen. Eine solche ist nach den einschlägigen Vorschriften aber grundsätzlich zu erteilen, wenn mit ihr nicht erhebliche Nachteile für Bund oder Land einhergehen, §§ 68 BBG, 37 Abs. 4 S.1 BeamtStG.[1053] Insofern dürfte die Geltung des § 54 Abs. 1 StPO praktisch kaum zu einer Vereitelung der Befragung führen.[1054]

Die Vernehmung von Mitarbeitern der (auch öffentlich-rechtlichen) Kreditinstitute ist also prinzipiell und in vollem Umfang möglich. Fraglich ist nur, ob sie auch praktikabel ist. Einzelne Mitarbeiter werden wohl kaum Kenntnisse über die Kontoinhaltsdaten eines bestimmten Kunden besitzen.[1055] Ein Zeuge muss sich auf die Vernehmung vorbereiten und dazu eventuell auch mithilfe der verfügbaren Unterlagen sein Gedächtnis auffrischen.[1056] Gem. § 64 Abs. 2 RiStBV soll der Zeuge sogar aufgefordert werden, bedeutende Schriftstücke oder andere Beweismittel bei der Vernehmung vorzulegen. Zur aktiven Nachforschung[1057] oder Herausgabe von Beweismitteln, etwa Umsatzlisten bzw. Kontoauszüge, sind sie im Rahmen der Vernehmung bzw. auf Grundlage des § 161a Abs. 1 StPO aber nicht

1052 gegen eine Anwendung des § 54 Abs. 1 StPO: *Reichling*, JR 2011, 12 (15); *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 54 Rn. 10 jeweils mit Verweis auf *Rogall* in SK-StPO, § 54 Rn. 25.; aA. etwa *Lilie*, NStZ 1981, 438 (440).

1053 Nach *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 54 Rn. 9 gelten diese auch für die Versagung der Aussagegenehmigung gegenüber Angestellten.

1054 So *C. Hirsch,* Kreditinstitute, 1991, S. 47 ff.; hierauf verweisend *Reichling*, JR 2011, 12 (15).

1055 *Reichling*, JR 2011, 12 (15).

1056 LG Bonn, BKR 2003, 914 (915); *Maier* in MüKo StPO, § 69 Rn. 15 mit Verweis auf BGHSt 1, 4 (5, 8).

1057 *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 8 Rn. 34; *Krehl*, NStZ 1991, 416 (416).

verpflichtet.[1058] Das Mitbringen von Akten oder Unterlagen ist also nicht obligatorisch[1059] und kann auch nicht erzwungen werden. Gerade auf diese Dokumente bzw. deren Inhalte wird es den Ermittlern bei der Vernehmung von Bankmitarbeitern aber ankommen.

b. Beschlagnahme und Herausgabeverlangen

Eine bessere Möglichkeit zum Erlangen von Kontodaten könnte daher die Ingewahrsamnahme nach § 94 Abs. 1 StPO bzw. bei Weigerung der Gewahrsam haltenden Person, die Beschlagnahme nach § 94 Abs. 2 StPO darstellen.[1060] Zwar bezieht sich diese nach ihrem Wortlaut nur auf *Gegenstände,* hierunter fallen aber nach allgemeiner Auffassung auch Daten bzw. digital gespeicherte Informationen.[1061] Kontoauszüge können also in Papier oder digital beschlagnahmt werden.

Bei den digital gespeicherten Informationen werden jedoch, da diese im Voraus oft nicht bestimmt werden können, zunächst die Datenträger beschlagnahmt, häufig im Rahmen von Durchsuchungen.[1062] Die Durchsicht der Medien richtet sich sodann nach § 110 Abs. 3 StPO. [1063] Werden beim Auslesen der Datenträger beweiserhebliche Daten gefunden, können diese dann wiederum selbstständig beschlagnahmt werden,[1064] etwa durch die Anfertigung von Kopien bei der Polizei oder der Staatsanwaltschaft.[1065] Bei einer Durchsuchung kann es unter Umständen aber auch möglich sein, noch vor Ort vollständige Kopien anzufertigen. Da diese Möglichkeit ein milderes Mittel darstellt, ist sie unter Verhältnismäßigkeitsaspekten vorzu-

1058 LG Bonn, BKR 2003, 914 (915); *Erb* in Löwe/Rosenberg StPO, § 161a Rn. 9; aA. wohl *Lilie*, NStZ 1981, 438 (440) mit Verweis auf § 64 Abs. 2 RiStBV.

1059 *Krepold* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 39 Rn. 225.

1060 *Reichling,* JR 2011, 12 (13).

1061 BVerfGE 113, 29 (50 ff.); E 124, 43 (54 ff.); *Köhler* in Meyer-Goßner/Schmitt StPO, § 94 Rn. 4, 13; aA. *Radtke*, FS Meyer-Goßner, 2001, S. 321 (327 f.).

1062 Vgl. *Bell,* Beschlagnahme, 2016, S. 11 ff.; *Radtke*, FS Meyer-Goßner, 2001 (321).

1063 BVerfG, NJW 2018, 3571 (3572 Rn. 25); *Park,* Durchsuchung und Beschlagnahme, 4. Aufl. 2018, Rn. 823 ff.

1064 Vgl. BVerfG, NJW 2007, 3343; VGH Mannheim, NVwZ-RR 2019, 901 (902 Rn. 21); VG Gelsenkirchen, Beschl. v. 06. Mai 2009 - 14 I 11/09; LG Nürnberg-Fürth, Beschl. v. 22.12.2017 - 18 Qs 49/17; für eine „unselbstständige" Beschlagnahme: *Bell,* Beschlagnahme, 2016, S. 15

1065 BVerfG, NJW 2003, 2669 (2670); *Bruns* in KK-StPO, § 110 Rn. 9; *Bär,* EDV-Beweissicherung, 2007, Rn. 415 ff.

ziehen.[1066] Die Beschlagnahme wird hierdurch auf die Daten reduziert, da die Datenträger am Ort belassen werden können. Dies wird vor allem dann relevant werden, wenn die gesuchten Kontounterlagen nur noch digital, eventuell sogar nur auf ausgelagerten (Cloud-)Servern, verfügbar sind. Die zwangsläufig mitbeschlagnahmten, aber beweisunerheblichen Daten sind dann unverzüglich nach der Durchsicht zu löschen.[1067]

In der Praxis spielen Bankdurchsuchungen und Beschlagnahmen allerdings offenbar keine große Rolle mehr.[1068] Oft erweisen sich Durchsuchungen und Beschlagnahmen, wenn es vorwiegend um Daten geht, aufgrund rechtlicher und tatsächlicher Hürden, etwa Datenschlüsseln, als schwierig.[1069] Überhaupt aber sind die Maßnahmen nur sinnvoll, wenn von vorneherein feststeht, dass sich das betroffene Institut sicher im Besitz der gewünschten Unterlagen befindet.[1070]

Dann aber wird meist ohnehin das Herausgabeverlangen praktikabel sein.[1071] Nach § 95 StPO sind *Gegenstände der vorbezeichneten Art* vom Gewahrsamsinhaber *vorzulegen und auszuliefern*. Die Gegenstände der vorbezeichneten Art sind die in § 94 Abs. 1, 2 StPO aufgeführten.[1072] Allerdings ist der Anwendungsbereich des § 95 StPO nach allgemeiner Auffassung auf Nichtbeschuldigte begrenzt.[1073] § 95 StPO ist also in strengem Zusammenhang mit der Beschlagnahme zu lesen, steht aber nach vorherrschender Ansicht eigenständig neben dieser.[1074]

Immer, wenn eine Beschlagnahme in Betracht kommt, ist demnach auch ein Herausgabeverlangen möglich.[1075] Der einzige Unterschied besteht in der Durchführung. Bei der Beschlagnahme eignen sich die Ermittlungsbehörden eigenständig den Gewahrsam an. Beim Herausgabeverlangen, das

1066 BVerfGE 113, 29 (53 f.); *Köhler* in Meyer-Goßner/Schmitt StPO, § 94 Rn. 18a; *Bell,* Beschlagnahme, 2016, S. 99 ff.; *Michalke*, NJW 2008, 1490 (1493).
1067 *Bär,* EDV-Beweissicherung, 2007, Rn. 425.
1068 *Reichling,* JR 2011, 12 (14).
1069 *Sieber,* Gutachten C DJ 69, 2012, S. 114 ff.; 119.
1070 Vgl. *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 8 Rn. 39.
1071 *Reichling,* JR 2011, 12 (14) *Park,* Durchsuchung und Beschlagnahme, 4. Aufl. 2018, Rn. 442; krit. Zu § 95 als Rechtsgrundlage *Sieber,* Gutachten C DJ 69, 2012, S. 115.
1072 Siehe nur *Greven* in KK-StPO, § 95 Rn. 1.
1073 *Köhler* in Meyer-Goßner/Schmitt StPO, § 95 Rn. 5; *Hauschild* in MüKo StPO, § 95 Rn. 12.
1074 LG Halle, NStZ 2001, 276; LG Lübeck, NJW 2000, 3148 (3149); zum Verhältnis zu § 94 StPO: *F. Jansen,* Bankauskunftsersuchen, 2010, 135 ff.
1075 *Köhler* in Meyer-Goßner/Schmitt StPO, § 95 Rn. 1; *Gerhold* in BeckOK StPO, § 95 Rn. 8.

nach § 95 Abs. 2 StPO mit den in § 70 StPO bezeichneten Zwangsmitteln durchgesetzt werden kann, wird der Gewahrsam durch eine Handlung des bisherigen Inhabers eingeräumt, wenn auch nicht *freiwillig*.

Auch das Herausgabeverlangen stellt sich für die Praxis aber nicht als optimale Lösung dar. Zwar können die Ermittlungspersonen über § 24c Abs. 2 Nr. 3 KWG schnell und einfach herausfinden, bei welchen Instituten die verdächtige Person ein Konto führt, und dann beim entsprechenden Institut die Herausgabe der Unterlagen verlangen. Oftmals werden sich aber erst aus den Unterlagen die genauen Umstände ergeben. Vor deren Sichtung ist also nicht klar, welche Unterlagen überhaupt benötigt werden. Eine Anforderung (aller) „schriftlicher Kontounterlagen" bestimmter Konten in einem bestimmten Zeitraum soll aber aufgrund mangelnder Bestimmtheit unzulässig sein.[1076] Soweit also im Voraus nicht klar ist, welche spezifischen Unterlagen beschlagnahmt werden sollen, müsste zunächst umfangreich durchsucht und nach § 110 StPO durchsichtet werden. Die Verfahrenshindernisse für solch ein Vorgehen sind rechtlich und faktisch enorm.

c. Informelles Auskunftsersuchen und Abwendungsauskunft

In der Praxis hat sich daher das informelle Auskunftsersuchen etabliert.

aa. Allgemeine Ermittlungsklausel des § 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO

Dieses kann nach gefestigter Auffassung auf § 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO gestützt werden, der zu *Ermittlungen jeder Art* ermächtigt.[1077] Es handelt sich dabei letztlich um eine formlose, schriftliche Zeugenvernehmung.[1078] Anders als bei der förmlichen (mündlichen) Vernehmung nach

1076 OLG Koblenz, NStZ 2007, 285 (286).

1077 BVerfG, NJW 2009, 1405 (1407); LG Hof, NJW 1968, 65 (65); *Erb* in Löwe/Rosenberg StPO, § 161 Rn. 22; *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 4; *Kölbel* in MüKo StPO, § 161 Rn. 27; *Reichling*, JR 2011, 12 (16); *F. Jansen,* Bankauskunftsersuchen, 2010, S. 30 ff; 228; aA. *Singelnstein*, NStZ 2012, 593 (602 f.); krit. auch EGMR, Urt. v. 27.4.2017, 73607/13 – Sommer/Deutschland, Rn. 58 ff. = NJOZ 2019, 455; *Petri*, StV 2007, 266 wenn ein hausinterner Datenabgleich erfolgt (vgl. BVerfG, NJW 2009, 1405 (1407)).

1078 AG Halle., DuD 2007 (464 (467); LG Frankfurt aM, NJW 1954, 688 (689); *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 2; *Weingarten* in KK-StPO, § 161 Rn. 8; *F. Jansen,* Bankauskunftsersuchen, 2010, S. 30 ff., 228.

§ 161a Abs. 1 StPO, die an eine spezifische natürliche Person gerichtet sein muss[1079], kann das Auskunftsersuchen nach § 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO unmittelbar an die Institute bzw. Firmen gerichtet werden. Es spielt dann keine Rolle, welche natürliche Person für das befragte Unternehmen auf die Anfrage antwortet.

§ 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO ist allerdings auf die Erteilung von Auskünften bzw. Informationen beschränkt. Da es sich um eine Generalklausel handelt[1080], sind die speziellen Ermittlungsmaßnahmen vorrangig zu beachten.[1081] § 161 Abs. 1 S. 1 Hs. 2 StPO enthält deshalb den Vorbehalt *„soweit nicht andere gesetzliche Vorschriften ihre Befugnisse besonders regeln"*. Werden in dem Ersuchen Unterlagen angefordert, dürfte es sich daher stets um ein Herausgabeverlangen i. S. d. § 95 StPO handeln. Die Ermittlungsgeneralklausel sollte bei Verlangen nach Kontoauszügen also eigentlich von den §§ 94 ff. StPO gesperrt werden.[1082]

Anders als das Herausgabeverlangen nach § 94 Abs. 2, § 95 Abs. 2 StPO, die förmliche Vernehmung nach § 161a Abs. 1, 2 StPO oder die Behördenauskunft nach § 161 Abs. 1 Hs. 1 S. 1 Alt. 1StPO, sieht die allgemeine Ermittlungsklausel keine *Pflicht* der Privaten zur Auskunftserteilung und folglich auch keine zwangsweise Durchsetzung vor.[1083] Damit die Auskunftsersuche nicht aus diesem Grund leerlaufen, werden sie in der Praxis mit der Androhung einer formalen Zeugenladung i. S. d. § 161a StPO oder einer Durchsuchung nach § 103 StPO verbunden.[1084] Die Institute bzw. deren Mitarbeiter werden damit vor die Wahl gestellt, entweder Informationen *freiwillig* zu erteilen oder formalen Ermittlungsmaßnahmen ausgesetzt zu werden. Die Auskünfte werden deshalb auch als *Abwendungsauskünfte*[1085] bezeichnet. Das geht so weit, dass die Staatsanwaltschaften im Voraus Durchsuchungsbeschlüsse beantragen und den Instituten dann die Möglichkeit geben

1079 Vgl. *Bader* in KK-StPO, vor § 48 Rn. 5.
1080 Ausf. *Hefendehl*, StV 2001, 700 (703 ff.).
1081 BVerfG, NJW 2009, 2876 (2877) Rn. 20; *Kölbel* in MüKo StPO, § 161 Rn. 7; *Hilger*, NStZ 2000, 561 (563 f.).
1082 *F. Jansen,* Bankauskunftsersuchen, 2010, S. 362 ff, 374, 445; *Singelnstein*, NStZ 2012, 593 (603); *ders.* in Barton/Kölbel/Lindemann (Hrsg.), Ermittlungsverfahren, 2015, S. 251 (254 ff.); *Weingarten* in KK-StPO, § 161 Rn. 8; aA. BVerfG, NJW 2009, 1405 (s.u.)
1083 LG Hof, NJW 1968, 65 (65); *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 4 *Kahler,* Kundendaten, 2017, S. 42 *F. Jansen,* Bankauskunftsersuchen, 2010, S. 42 f.
1084 *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 39 Rn. 40; *Reichling*, JR 2011, 12 (16).
1085 Ibid.

kann, die Durchführung durch Herausgabe der Informationen abzuwenden.[1086]

bb. Ermächtigung zur massenhaften Datenerhebung? Die „Operation Mikado"

Das Bundesverfassungsgericht hat die auf § 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO gestützte Praxis in einem beachtenswerten Beschluss zur „Operation Mikado" gebilligt.[1087] Dem Beschluss lag folgender Sachverhalt zugrunde:[1088] Eine Staatsanwaltschaft hatte von einer Internetseite erfahren, die zahlungspflichtig kinderpornografisches Material anbot, und versuchte, die Namen der Kunden der Seite zu ermitteln, da diese im Verdacht standen, sich nach § 184b StGB strafbar gemacht zu haben. Die Ermittler kannten den Namen und die Merchant-ID des Unternehmens sowie die Bank, bei der die Zahlungen eingingen. Sie wussten auch um den Geldbetrag von 79,99 $, der für den Zugang zu der Seite zu bezahlen war.

Diese Informationen gab die Staatsanwaltschaft an verschiedene Banken und Kreditkartenanbieter weiter und forderte sie auf, ihre gesamten Datenbestände nach entsprechenden Zahlungsvorgängen zu durchsuchen. Andernfalls würden Mitarbeiter der Banken nach § 161a StPO als Zeugen geladen. Die angeschriebenen Banken durchsuchten daraufhin die Konten von etwa 22 Mio. Bürgern und landeten bei 322 Personen einen Treffer. Die Identität der entsprechenden Personen wurde an die Staatsanwaltschaft weitergeleitet.

Das AG Halle ging davon aus, dass die Anfrage durch die Staatsanwaltschaft von der Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 Alt. 1 StPO

1086 Vgl. *Oberste Finanzbehörden der Länder,* AStBV (St) 2019, 01. Dezember 2018, Nr. 146 Abs. 2, https://datenbank.nwb.de/Dokument/769703/, zuletzt aufgerufen am 12.01.2025; *Reichling*, JR 2011, 12 (16).

1087 BVerfG, NJW 2009, 1405

1088 AG Halle, DuD 2007, 464; Ausf. *DSB SA,* VIII. Tätigkeitsbericht, 2007, S. 122 ff.; *Kahler,* Kundendaten, 2017, 20 ff.; *Schnabel*, DuD 2007, 426 (426 f.).

gedeckt war.[1089] Insbesondere läge keine Rasterfahndung i. S. d. § 98a StPO vor.[1090] Das BVerfG hat diese Auffassung bestätigt.[1091]

Der Abgrenzung zur Rasterfahndung dürfte zuzustimmen sein. Der Sinn der Rasterfahndung liegt darin, dass sich die Ermittlungsbehörden verschiedene Datensätze aushändigen lassen, um diese zu vergleichen und eine Schnittmenge zu erstellen.[1092] Dabei ist meist im Voraus ein bestimmter Täter gesucht. Das ergibt sich schon aus dem Wortlaut des § 98a Abs. 1 S. 1 StPO: *„auf den Täter vermutlich zutreffende Prüfungsmerkmale"*. Sucht die Staatsanwaltschaft etwa eine Person, von der sie weiß, dass sie einen schwarzen Mercedes fährt und in Berlin wohnt, lässt sie sich entsprechende Namenslisten beim Meldeamt und der KFZ-Zulassungsstelle aushändigen. Der Abgleich wird dann eine Liste möglicher Verdächtiger ergeben. Erhält sie weitere Informationen, kann die Staatsanwaltschaft diese nunmehr mit der schon engeren Liste abgleichen und so das Netz immer enger spinnen.[1093] Die Rasterfahndung ist also von vornherein darauf ausgelegt, dass in ihrem Verlauf auch Nichttreffer erzielt, werden[1094], die sich aus den Abgleichslisten ergeben – zunächst mehr, dann immer weniger. Wird lediglich ein einzelner Datenspeicher anhand bestimmter Merkmale nach einer Person oder Personengruppe durchsucht, liegt deshalb nach herrschender Auffassung keine Rasterfahndung vor.[1095]

Bei der Abfrage von Daten im Rahmen einer hausinternen Suche werden lediglich Treffer an die Staatsanwaltschaft herausgegeben. Alle Namen, die sie erhält, sind unmittelbar tatverdächtig. Nach Auffassung des BVerfG wird deshalb – anders als bei der Rasterfahndung[1096] – auch nur (unmittelbar) in die Grundrechte dieser Personen eingegriffen.[1097]

1089 AG Halle, DuD 2007, 464 (467).

1090 Idem, (467 f.); zust. *Kahler,* Kundendaten, 2017, S. 37 f.; *Petri*, StV 2007, 266, die aber eine Anwendung des § 161 Abs. 1 S. 1 Hs. 2 StPO iE. ablehnen; aA. *Schnabel*, DuD 2007, 426 (427 f.): „mittelbare Rasterfahndung"; *Brodowski*, JR 2010, 543 (547 f.).

1091 BVerfG, NJW 2009, 1405 (1406 f.).

1092 BVerfGE 115, 320 (321) – Rasterfahndung; OLG Köln, NStZ-RR 2001, 31 (31)

1093 Vgl. *Gerhold* in BeckOK StPO, § 98a Rn. 9 ff.

1094 BVerfG, NJW 2009, 1405 (1406).

1095 Idem (1406 f.), OLG Stuttgart, NStZ 2001, 158 (159); OLG Köln, NStZ-RR 2001, 31 (32); *Köhler* in Meyer-Goßner/Schmitt StPO, § 98a Rn. 8; *Kahler,* Kundendaten, 2017, S. 37; aA. *Schnabel*, DuD 2007, 426 (427 f.); *Brodowski*, JR 2010, 543 (547 f.).

1096 Vgl. BVerfGE 115, 320 (343) – Rasterfahndung.

1097 BVerfG, NJW 2009, 1405 (1406); aA. *Buermeyer,* Informationelle Selbstbestimmung, 2019, 152 f.; *Brodowski*, JR 2010, 543 (547).

Auch von den Stimmen, die mit der Rechtsprechung keine Rasterfahndung in der Veranlassung einer hausinternen Datenbankdurchsuchung erkennen wollen, wird die Anwendung des § 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO als Rechtsgrundlage für Massenabfragen aber kritisiert.[1098] Durch das Auskunftsersuchen würden die Privaten faktisch gezwungen[1099], im Rahmen einer Datenverarbeitung[1100] mittelbar in die Grundrechte massenweiser nichtverdächtiger Personen einzugreifen. Dadurch bediene sich die Staatsanwaltschaft letztlich des gesamten Datenbestandes der betroffenen Institute.[1101]

Weiter läge kein (notwendiger) Anfangsverdacht in Bezug auf die gesamte Kundschaft vor. Die Staatsanwaltschaft hatte nur Kenntnis darüber, dass auf der entsprechenden Website Kinderpornografie angeboten wurde. Dass diese dann auch tatsächlich in Deutschland konsumiert wurde, war zwar zu erwarten, reale Anhaltspunkte gab es aber nicht, schon gar nicht bzgl. bestimmter Personen. Diese konkreten Verdachtsfälle seien erst durch das Auskunftsersuchen geschaffen worden.[1102] Darüber hinaus zeige schon § 98c StPO, der ebenfalls einen Datenabgleich an nur einem Datensatz regelt, dass der Gesetzgeber prinzipiell von der Notwendigkeit eines Spezialgesetzes für hausinterne Datenabfragen ausgegangen sei.[1103]

d. Strafprozessuale Kontoermittlungen als offene Maßnahmen

Allen vorangegangenen Maßnahmen ist gemein, dass es sich um offene Ermittlungsmaßnahmen handelt. Unter offenen Ermittlungsmaßnahmen werden nach dem Verständnis dieser Arbeit alle Maßnahmen erfasst, die dem Beschuldigten nicht zwingend verborgen bleiben. Auch Maßnahmen, die zunächst nur einem Dritten unmittelbar zur Kenntnis gelangen, sollten als „offen" bezeichnet werden, wenn der Dritte nicht zur Verschwiegenheit verpflichtet ist.

In der Rechtsprechung herrscht ein anderes Verständnis vor. Eine Maßnahme soll dann „offen" erfolgen, wenn der Betroffene bzw. Beschuldigte

1098 *Kahler,* Kundendaten, 2017, S. 123 ff., 182; *Petri*, StV 2007, 266 (268 f.).
1099 *Singelnstein*, NStZ 2012, 593 (603); *Petri*, StV 2007, 266 (268).
1100 Dazu ausf. *Kahler,* Kundendaten, 2017, S 55 ff.
1101 Idem, S. 127 f.; *Brodowski,* JR 2010, 543 (547).
1102 *Schnabel*, DuD 2007, 426 (427 f.); aA. *Brodowski*, JR 2010, 543 (546).
1103 *Petri*, StV 2007, 266 (268).

sich rechtzeitig mit rechtlichen Mitteln zur Wehr setzen kann.[1104] Das ist insbesondere dann der Fall, wenn Benachrichtigungspflichten in unmittelbarem zeitlichem Zusammenhang zur Maßnahme bestehen oder er die informationserhebende Maßnahme von vornherein wahrnehmen kann. Ob sich eine Maßnahme nach diesen Merkmalen als „heimlich" oder „verdeckt"[1105] erweist, ist aber nicht immer so leicht zu bestimmen, wie es in der Rechtsprechung meist anklingt.[1106]

aa. Beschlagnahme und Herausgabeverlangen

Für die Beschlagnahme folgt die Offenheit in jedem Fall aus der Notwendigkeit einer gerichtlichen Anordnung nach 98 Abs. 1 StPO. Bevor diese stattfindet, muss der Betroffene zwar regelmäßig wegen einer Gefährdung des Durchsuchungszwecks nicht angehört werden, §§ 33 Abs. 1, 4 StPO. Er ist aber stets nach §§ 33 Abs. 2, 35 Abs. 2 StPO zu benachrichtigen.[1107] Die gerichtlich angeordnete Beschlagnahme ist also nicht nur offen in dem Sinn, dass sie dem Beschuldigten durch Dritte sanktionslos bekannt und in den Akten eingesehen werden kann, §§ 168b, 147 Abs. 1, 2 StPO.[1108] Die Information muss ihm sogar angetragen werden. Es besteht also eine Offenbarungsobligation. Für die Durchsuchung gilt dasselbe nach § 105 Abs. 2 StPO.

(1) Geheime Beschlagnahme nach § 95a StPO

Die Gesetzeslage zur Rückstellung der Benachrichtigung hat sich allerdings jüngst aufgrund des Gesetzes zur Fortentwicklung der Strafprozessordnung

1104 Vgl. BVerfG 115, 166 (194 f.); BGHST 51, 211.
1105 Zu den Begrifflichkeiten *Tanneberger,* Sicherheitsverfassung, 2014, S. 247, der mwN. auf die synonyme Verwendung in der Rspr. Hinweist; unterschiedliche Verwendung bei *Gusy* in Huster/Rudolph (Hrsg.), Präventionsstaat, 2008, S. 120 (124).
1106 S.a. *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 4 ff.
1107 Vgl. nur BGH, NJW 2010, 1297 (1298).
1108 *Schlothauer* in Müller/Schlothauer/Knauer (Hrsg.), MAH Strafverteidigung, 3. Aufl. 2022, § 3 Rn. 47.

und zur Änderung weiterer Vorschriften[1109] geändert. Insbesondere wurde § 95a StPO neu eingeführt.

Bislang konnte die Benachrichtigung über die Anordnung zwar zurückgestellt werden, musste aber spätestens bis zu dem Zeitpunkt, an dem die Durchführung der Maßnahme beginnt, erfolgen.[1110] § 95a Abs. 1, 2 StPO lässt nunmehr unter gewissen Voraussetzungen auch eine bis zu sechs Monate währende Zurückstellung zu, wenn andernfalls der Untersuchungszweck gefährdet würde. Der Grundsatz der Offenheit der Beschlagnahme gilt also nicht mehr ausnahmslos. Mit § 95a StPO wurde folglich nichts Geringeres als eine „geheime Beschlagnahme" eingeführt.[1111] Daran zeigt sich einerseits, dass sich spezielle Überwachungsregime abseits des klassischen Sicherheitsrechts, wozu auch die StPO zählt,[1112] nicht mehr unbedingt durch ihre Heimlichkeit absetzen, sondern strukturell. Andererseits wirft die sensitive grundrechtliche Betrachtung bestimmter sicherheitsrechtlicher Überwachungsmaßnahmen (auch) aufgrund deren Heimlichkeit die Frage auf, ob die sicherheitsverfassungsrechtlichen Prinzipien auch bzgl. der StPO kohärent Anwendung finden (dazu unten Kap. G. I. 2.).

(2) Bekanntgabe von Eilentscheidungen nach § 98 Abs. 2 StPO

Erfolgt die Beschlagnahmeanordnung nicht aufgrund einer gerichtlichen Verfügung, sondern als Eilanordnung durch die Staatsanwaltschaft oder Polizei, gilt § 35 Abs. 2 StPO nicht unmittelbar.[1113] In diesem Fall muss aber nach § 98 Abs. 2 StPO eine gerichtliche Bestätigung eingeholt werden, wenn

1109 Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25. Juni 2021 (BGBl. I 2021, 2099).

1110 BGH, NStZ 2015, 704; BGH, NJW 2017, 2359 (2359 f.); *Greven* in KK-StPO, § 98 Rn. 21.

1111 *Burhoff*, StRR (9) 2021, 6 (6); krit. auch *Vassilaki*, MMR 2022, 103; *Gallus/Zeyher*, NStZ 2022, 462.

1112 *Danne,* Prävention und Repression, 2022, S. 21 ff.; *Dietrich* in Dietrich/Fahrner/Gazeas ua. (Hrsg.), Hdb. Sicherheits- und StaatsschutzR, 2022, § 6 Rn. 49; *Götz* in Isensee/Kirchhof (Hrsg.), HdB StR Bd. IV, 3. Aufl. 2006, § 85 Rn. 5 f. *Gärditz*, GSZ 2017, 1 (2) mit Verweis in Fn 12 auf *Bäcker,* Kriminalpräventionsrecht, 2015; *Zöller,* Informationssysteme, 2002; aA *Graulich*, DVBl 2013, 1210, der allein auf den Zuständigkeitsbereich des 6. Senats des Bundesverwaltungsgerichts abstellt.

1113 *Valerius* in MüKo StPO, § 35 Rn. 2.

der von der Beschlagnahme *Betroffene* bzw. ein erwachsener Angehöriger nicht anwesend ist oder ihr widerspricht. Die gerichtliche Bestätigung stellt eine *eigene Entscheidung* des Gerichts dar und hat somit den Charakter einer (gerichtlichen) Anordnung,[1114] für die dann wiederum § 35 Abs. 2 StPO gilt. Die Beschlagnahme bzw. Herausgabe von Kontodaten findet regelmäßig bei den Finanz- bzw. Kreditinstituten, also bei Dritten, statt. Da es sich bei diesen um die jeweiligen Gewahrsamsinhaber handelt, sind zunächst sie die Betroffenen.[1115]

Widerspricht der oder die Betroffene allerdings nicht, kommt es nach § 98 Abs. 2 StPO nicht zu einer gerichtlichen Entscheidung. Wie sich dies auf die Bekanntgabe auswirkt, lässt das Gesetz offen. Der neue § 95a Abs. 1 StPO erlaubt eine Zurückstellung nur in den Fällen der gerichtlichen Anordnung oder Bestätigung. Das wirft die Frage auf, ob es bei einer freiwilligen Herausgabe eines Dritten überhaupt zu einer Bekanntgabe gegenüber dem Beschuldigten kommen muss. Dies würde dem Grundsatz der offenen Beschlagnahme unabhängig von § 95a StPO widersprechen. In der Literatur wird dieses Problem überraschenderweise nicht intensiver behandelt. Es finden sich lediglich pauschale Aussagen, dass im Falle einer Eilanordnung zumindest eine mündliche Unterrichtung des Beschuldigten durch die Staatsanwaltschaft erfolgen muss.[1116] Die Grundlage dieser Pflicht wird nicht herausgestellt.

Eine Offenbarungsobligation, darauf weist auch die Bundesregierung hin[1117], ergibt sich aber bei genauem Hinsehen aus § 98 Abs. 2 S. 2, 5 StPO. Danach ist *der Betroffene* über seine Rechte zu belehren, auch über die Möglichkeit, jederzeit eine gerichtliche Entscheidung einzuholen, selbst wenn der Beschlagnahme zunächst nicht widersprochen wurde, vgl. § 98 Abs. 2 S. 2 StPO.[1118]

Der Beschuldigte müsste danach belehrt werden, wenn er von der Maßnahme *betroffen ist.* Das ist nach gängiger Definition immer dann der Fall,

1114 *Schnarr*, NStZ 1991, 209 (214).
1115 KG Berlin, NJW 1999, 2979 (2980).
1116 *Burhoff*, StRR (9) 2021, 6 (6); *Schlothauer* in Müller/Schlothauer/Knauer (Hrsg.), MAH Strafverteidigung, 3. Aufl. 2022, § 3 Rn. 109 zur Durchsuchungsanordnung bei Gefahr im Verzug, deren Regeln auch für die Beschlagnahme gelten, vgl. *Ignor/K. Peters* in Hamm/Leipold (Hrsg.), Beck'sches Formular-Hdb., StV, 6. Aufl. 2018, Teil III. Kap. H 1. b.).
1117 Vgl. BT-Drs. 19/27654, S. 65.
1118 BVerfG, NJW 2007, 3343(3343); *Köhler* in Meyer-Goßner/Schmitt StPO, § 98 Rn. 20.

wenn der Beschuldigte Rechte oder rechtlich geschützte Interessen an dem jeweiligen Gegenstand hat, wobei seine Stellung als Beschuldigter allein nicht ausreichen soll.[1119] Betroffen ist also jeder, in dessen Privatheitsgrundrechte eingegriffen wird.[1120]

Das Recht nach 98 Abs. 2 S. 2 StPO, jederzeit eine gerichtliche Entscheidung zu beantragen, steht allen Betroffenen zu. Konsequenterweise sind also auch alle Betroffenen nach § 98 Abs. 2 S. 5 StPO zu belehren. [1121] In dem Fall, dass der Beschuldigte von einer freiwilligen Herausgabe eines Dritten (mit)betroffen ist, muss er also über sein Recht nach § 98 Abs. 2 S. 2 StPO belehrt werden und erfährt hierdurch von der Maßnahme.

Bei der Beschlagnahme von Kontoauszügen dürfte dies regelmäßig der Fall sein.[1122]Da durch die Einsicht eine Datenerhebung stattfindet, wird der Beschuldigte in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt. Darüber hinaus könnte man argumentieren, dass § 98 Abs. 2 S. 1 StPO schon dann greift, wenn nur einer der Betroffenen bzw. dessen Angehöriger nicht anwesend ist. Die Beschlagnahme von Kontodaten bei einer Bank wäre hiernach nicht einmal dann freiwillig, wenn die Bank der Herausgabe nicht widerspricht, da auch der Kontoinhaber anwesend und mit der Beschlagnahme einverstanden sein müsste. Gerade das wird aber kaum der Fall sein. Entsprechend müsste bei der Beschlagnahme von Kontodaten in Abwesenheit des Kontoinhabers immer eine gerichtliche Entscheidung nach § 98 Abs. 2 S. 1 StPO beantragt werden. Jedenfalls aber muss der Kontoinhaber als Betroffener über sein Recht auf gerichtliche Entscheidung nach § 98 Abs. 2 S. 2, 5 StPO belehrt werden, auch wenn seine Bank der Beschlagnahme nicht widersprochen hat.

bb. Förmliche Zeugenvernehmung und informelles Auskunftsersuchen

Weder die förmliche Zeugenvernehmung noch das informelle Auskunftsersuchen, das selbst nicht im Gesetz geregelt ist,[1123] sehen eine gerichtliche Anordnung vor. Eine Bekanntgabe gegenüber dem Beschuldigten nach

1119 BGH, Beschluss vom 09.12.1992 – StB 16/92, 2 BJs 16/92 – 6 – StB 16/92; *Hauschild* in MüKo StPO, § 98 Rn. 22.
1120 *Singelnstein*, NStZ 2012, 593 (603).
1121 Vgl. BVerfGE 124, 43 (71) Rn. 95.
1122 KG Berlin, NJW 1999, 2979 (2980).
1123 Hierzu *F. Jansen,* Bankauskunftsersuchen, 2010, 14 ff.

§§ 33 Abs. 2, 35 Abs. 2 StPO scheidet daher von vornherein aus. Anders als bei der richterlichen Vernehmung nach § 168c Abs. 2, 5 StPO, hat der Beschuldigte bei der Vernehmung durch die Staatsanwaltschaft oder Polizei auch kein Anwesenheitsrecht und muss folglich nicht über den Termin benachrichtigt werden.[1124]

(1) Keine Bekanntgabepflicht

Das bedeutet, dass der Bankkunde im Falle einer Zeugenvernehmung in förmlicher oder informeller Weise auf die Akteneinsicht oder eine Information durch das entsprechende Institut angewiesen ist.[1125] Das macht die Maßnahme aber nicht heimlich im Sinne der StPO. Dass die Polizei und Staatsanwaltschaft sich im Rahmen ihrer Ermittlungen einen Wissensvorsprung, ein „element of surprise"[1126], erarbeiten dürfen, wird zwar gelegentlich kritisiert, ist aber als Grundkonzept der Ermittlung anerkannt.[1127] Ob der Beschuldigte erst durch seine obligatorische Vernehmung nach §§ 136, 163a StPO oder aufgrund Art. 6 Abs. 3 lit. a) EMRK über das Ermittlungsverfahren informiert werden muss, ist irrelevant, da in beiden Fällen nur über den Zeitpunkt gestritten wird, ab wann die Information bzw. die Vernehmung obligatorisch wird.[1128] Auch wenn der (Bank)Kunde nicht selbst informiert wird, erfährt er also zu einem bestimmten Zeitpunkt zwangsweise von der Zeugenvernehmung bzw. dem schriftlichen Auskunftsersuchen.

Im Strafverfahrensrecht gilt der Grundsatz der freien Gestaltung des Ermittlungsverfahrens. Dieses lebt davon, dass manche Maßnahmen zunächst ohne Wissen des Beschuldigten erfolgen.[1129] Der Beschuldigte wird durch das Akteneinsichtsrecht[1130] und die obligatorische Beschuldigtenvernehmung nach §§ 136, 163 StPO ausreichend geschützt. Bei der Definition

1124 *Erb* in Löwe/Rosenberg StPO, § 161a Rn. 31; *Monka* in BeckOK StPO, § 168c Rn. 2; zur Verfassungsmäßigkeit BVerfGE 96, 68 (96).
1125 Vgl.; *Ransiek*, wistra 1999, 401 (408); *Reichling*, JR 2011, 12 (16).
1126 *Stavros,* Guarantees, 1993, S. 75.
1127 *Gaede,* Fairness, 2010, S. 601; *ders.* in MüKo StPO, EMRK Art 6 Rn. 145; krit. *Wohlers/A. Helena Albrecht* in SK-StPO, § 163a Rn. 9: nur bei Verdunkelungsgefahr; ähnlich *Ambos*, ZStW 2003, 583 (598).
1128 *Fincke*, ZStW 1983, 918 (965).
1129 BVerfG, NJW 2009, 1405, (1407) Rn. 28.
1130 Hierzu *Gaede,* Fairness, 2010, S. 243 f.; 301 ff.; 305 ff.; 828 ff.; *Schlegel*, HRRS 2004, 411.

der Offenheit ist dieser Maßstab zu respektieren. Das Fehlen der Mitteilungsverbote in Verbindung mit der verfahrensrechtlichen Stellung des Beschuldigten und seines Verteidigers durch die Akteneinsicht ist ausreichend, um die Maßnahme als offen zu qualifizieren.

(2) Kein Mitteilungsverbot

Etwas anderes würde allenfalls gelten, wenn die Informationsweitergabe durch die jeweiligen Institute bzw. Zeugen verboten wäre.

Ein Mitteilungsverbot könnte sich zunächst aus §§ 257, 258 StGB ergeben, wenn sich die Mitarbeiter der betroffenen Institute bei einer Information ihres Kunden wegen Begünstigung oder Strafvereitelung strafbar machen würden.[1131] Hier droht aber ein Zirkelschluss.

Nach herrschender Auffassung kann prozessrechtlich erlaubtes Verhalten keine strafbewehrte Informationsweitergabe sein. § 258 StGB verweist vielmehr auf das Prozessrecht.[1132] Ob im Strafprozess ein Mitteilungsverbot eines Beteiligten vorliegt, kann also gerade nicht aus den Strafgesetzen abgeleitet werden.[1133] Halten sich die Beteiligten hinsichtlich der ihnen zugehenden Informationen an die Vorschriften des Strafprozessrechts, muss für sie eine Strafbarkeit wegen Strafvereitelung ausscheiden.[1134] Davon abgesehen wird eine Strafbarkeit betroffener Mitarbeiter nach §§ 257, 258 StGB in den allermeisten Fällen ausscheiden, da die Information über eine Ermittlungsmaßnahme kaum allein die Strafe vereiteln wird, sondern nur auf das Verhalten des Kunden einwirkt.[1135]

Dass eine einfachgesetzliche Regelung für ein Mitteilungsverbot im Rahmen des Verfahrens notwendig ist, zeigt etwa § 47 GwG. Danach ist es

1131 Dazu *Park,* Durchsuchung und Beschlagnahme, 4. Aufl. 2018, Rn. 981 ff.; *A. Allgayer* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 11 Rn. 632 ff.; *Diergarten* in Hauschka/Moosmayer/Lösler (Hrsg.), Hdb. Haftungsvermeidung, 3. Aufl. 2016, § 34 Rn. 407; *Geurts/C. Koch/Schebesta ua.,* Bankgeheimnis, 6. Aufl. 2000, Rn. 29.

1132 BGH, NJW 2006, 2421 Rn. 9; *T. Fischer,* StGB, 69. Aufl. 2021, § 258 Rn. 17; *Hecker* in Schönke/Schröder StGB, § 258 Rn. 19.

1133 *Ransiek*, wistra 1999, 401 (404) mit Verweis auf *Lüdersen* in Löwe/Rosenberg, 24. Aufl. 1988, vor Rn. 102, 112.

1134 Vgl. für den Fall der Aussageverweigerung *Popp*, JR 2014, 418 (422 ff.); *Weidemann*, JA 2008, 532 (533).

1135 Ausf. *A. Allgayer* in Ellenberger/Bunte (Hrsg.), Bankrechts-Hdb, 6. Aufl. 2022, § 11 Rn. 632 ff.

den geldwäscherechtlich Verpflichteten unter Androhung eines Bußgelds gem. § 56 Abs. 2 Nr. 7 GwG verboten, *„den Auftraggeber der Transaktion und sonstige Dritte in Kenntnis zu setzen über 1.) eine beabsichtigte oder erstattete Meldung nach § 43 Abs. 1 GwG, 2.) ein Ermittlungsverfahren, das aufgrund einer Meldung nach § 43 Abs. 1 GwG eingeleitet worden ist, und 3.) ein Auskunftsverlangen nach § 30 Abs. 3 S. 1 GwG."* Für diese Fälle ging der Gesetzgeber also davon aus, dass er eine Verschwiegenheitspflicht erst anordnen muss und sich diese nicht schon aus §§ 257, 258 StGB ergibt. Man muss daraus folgern, dass in den Fällen, die § 47 GWG nicht beschreibt, gerade kein Informationsverbot besteht.[1136] Dafür spricht auch, dass die klassischen Ermittlungsmaßnahmen des Strafprozessrechts prinzipiell von Offenheit geprägt sind.[1137] Zwar ist das Ermittlungsverfahren an sich bis zum Entgegentreten im Rahmen der obligatorischen Beschuldigtenvernehmung geheim,[1138] das heißt aber nur, dass der Beschuldigte nicht alles wissen muss – nicht, dass er es nicht wissen darf.

Der Grundsatz des offenen Strafverfahrens zeigt sich etwa darin, dass in § 101 Abs. 2 StPO speziell angeordnet wird, dass Informationen aus und über die verdeckten Maßnahmen erst bei Eintreten der Bekanntmachungspflicht zu den Akten genommen werden § 101 Abs. 2 S. 2 StPO. Der Gesetzgeber ist sich in der StPO selbst also ganz offensichtlich des Umstandes bewusst, dass Informationen prinzipiell frei verfügbar sind, und schafft an einigen Stellen Regelungen, um sie einzufangen. Wo er das nicht tut, müssen die Ermittlungspersonen mit der Offenheit ihrer Handlungen leben.

Für die förmliche Zeugenvernehmung und das schriftliche Auskunftsverlangen bestehen keine solchen Regelungen, aus der sich eine Geheimhaltungspflicht der Zeugen bzw. Befragten ergeben würde. In der Praxis soll zwar regelmäßig eine Geheimhaltung mit Verweis auf die §§ 257, 258 StGB angeordnet werden, dafür gibt es aber keine Rechtsgrundlage.[1139] Es handelt sich also eher um eine zwanglose Bitte nach Diskretion, die nahe an den Bereich willkürlicher Strafandrohung heranrückt.

1136 *Geurts/C. Koch/Schebesta ua.,* Bankgeheimnis, 6. Aufl. 2000, Rn. 29; gegen eine solche Analogie: *Ransiek*, wistra 1999, 401 (404); *J. Petersen,* Bankgeheimnis, 2005, S. 88.

1137 *Zöller*, ZStW 2012, 411 (415, 424 ff.).

1138 BGHSt 42, 139 (150); *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, Rn. 29.

1139 *Ransiek*, wistra 1999, 401 (407); zust. *Park,* Durchsuchung und Beschlagnahme, 4. Aufl. 2018, Rn. 987; *Reichling*, JR 2011, 12 (16).

2. Polizeirechtliche Ermittlungen

Offene Bankauskunftsbegehren können auch im Bereich der Gefahrenabwehr stattfinden.[1140] Dieser Bereich stellt aber ganz offenbar einen Nebenschauplatz dar. Anders als im Bereich des Strafprozessrechts lassen sich Literatur oder Rechtsprechung zur polizeirechtlichen Bankauskunft nur spärlich finden.

Das dürfte sich damit erklären lassen, dass Kontodaten oder andere Inhaltsdaten, die vornehmlich bei Privaten liegen, meist dann notwendig werden, wenn schon ein Tatverdacht vorliegt. Insbesondere bei Transaktionen wird es aufgrund der weit gefassten Tatbestände der Geldwäsche und Terrorismusfinanzierung (s. o.) nur wenige Fälle geben, auf die ausschließlich gefahrenabwehrrechtlich reagiert werden kann. Aus der Rechtsprechung ist nur ein einziger Fall bekannt, in dem es um eine Anfrage bei der Schufa ging.[1141]

Die folgenden Ausführungen zum Landes- und Bundespolizeirecht sind daher weniger abschließend als jene zur StPO. Anstatt ausdrücklich für alle denkbaren Situationen in Bezug auf Auskunftsersuchen bei Kreditinstituten die konkrete Rechtsgrundlage in den jeweiligen Gesetzen zu bestimmen, sollen die Unwägbarkeiten, die sich in den verschiedenen Polizeigesetzen finden, in den Vordergrund gestellt werden.

a. Landespolizeigesetze

Die Rechtsgrundlagen für eine gefahrenabwehrrechtliche Auskunft durch die Landespolizeibehörden und den jeweiligen Polizeivollzugdienst finden sich in den Polizeigesetzen der verschiedenen Bundesländer. Da sie sich aber inhaltlich in Bezug auf die Bankauskunft nicht unterscheiden, orientieren sich die folgenden Ausführungen vornehmlich am Recht des Landes Baden-Württemberg. Auf Ausnahmen wird jeweils hingewiesen.

1140 *Wonka*, NJW 2017, 3334 (3337 f.); OVG Koblenz, NVwZ 2002, 1529.

1141 VG Trier, NJW 2002, 3268 und in zweiter Instanz OVG Koblenz, NVwZ 2002, 1529.

aa. Allgemeine Datenerhebungsklausel

Allen Polizeigesetzen ist gemein, dass eine Ingewahrsamnahme von Gegenständen zu Beweiszwecken ausscheidet.[1142] Sie kennen nur die *Sicherstellung* zur Abwehr einer Gefahr für die entsprechende Sache und von Gefahren, die von der Sache ausgehen. Das Baden-Württembergische Polizeigesetz trennt diese Varianten ausdrücklich in Sicherstellung und Beschlagnahme auf, §§ 37, 38 LPolG BW, und unterscheidet sich insofern von den restlichen Bundesländern.[1143]

Anders als in der StPO ist der Gegenstandsbegriff in den Polizeigesetzen auf körperliche Gegenstände begrenzt.[1144] Nur in Bayern ist neuerdings die Sicherstellung von Daten speziell geregelt worden, Art. 25 Abs. 3 BayPAG.[1145] Kontodaten können außerhalb von Bayern also nur polizeirechtlich sichergestellt oder beschlagnahmt werden, wenn sie verkörpert sind, etwa auf ausgedruckten Kontoauszügen oder auf einem Datenträger.

Die polizeirechtliche Sicherstellung bzw. Beschlagnahme setzt allerdings stets voraus, dass die Gefahr gerade darin besteht, dass der Pflichtige den Gewahrsam ausübt,[1146] die Gefahr soll durch den Entzug der Sachherrschaft gebannt werden. Das wird bei Finanzdaten im Gewahrsam der Finanzinstitute nicht der Fall sein. Diese sind nicht polizeipflichtig. Die Ingewahrsamnahme von (verkörperten) Finanzdaten wird vielmehr als Beweis oder als Möglichkeit zum Auffinden von mutmaßlich polizeipflichtigen Personen notwendig sein. Diese Variante kennt die polizeirechtliche Sicherstellung bzw. Beschlagnahme aber klassischerweise nicht. Im oben angesprochenen Fall der Schufa-Daten[1147] wurde eine Sicherstellung bzw. Beschlagnahme auch gar nicht erst angesprochen.

Für Auskunftsersuchen an Banken und andere Institute kommen im Polizeirecht daher vor allem die allgemeinen Datenerhebungsklauseln in

1142 *Reinhardt* in BeckOK BWPolG, § 37 Rn. 1.
1143 Vgl. etwa § 43 PolG NRW; Art. 25 BayPAG, hierzu auch *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 18 Rn. 1.
1144 *F. Michl*, NVwZ 2019, 1631 (1631); *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 698; *Reinhardt* in BeckOK BWPolG, § 37 Rn. 5; auch Tiere vgl. VGH Mannheim, VBlBW 2014, 377.
1145 Dazu ausf. *F. Michl*, NVwZ 2019, 1631; s.a *Löffelmann*, GSZ 2020, 244 (249 f.)
1146 Vgl. zu Daten aus „Smart-Home" Geräten *Löffelmann*, GSZ 2020, 244 (249 f.).
1147 VG Trier, NJW 2002, 3268; OVG Koblenz, NVwZ 2002, 1529.

Betracht.[1148] Die Datenerhebungsklauseln sind als Generalklauseln ausgestaltet und finden sich in allen Polizeigesetzen.[1149] Sie erfüllen zweierlei Aufgaben. Einmal dienen sie als Rechtsgrundlage für den Eingriff in die informationelle Selbstbestimmung des Betroffenen, der jeder Ermittlungshandlung immanent ist.[1150] Sie betreffen also zunächst das Verhältnis der Behörde zu der Person, von der die Gefahr mutmaßlich ausgeht und über die Informationen eingeholt werden sollen[1151], etwa Kontodaten. Gleichzeitig dienen sie unter Umständen auch als Ermächtigung für den Erhebungsvorgang an sich und beeinträchtigen damit auch die Person, von der die Information eingeholt wird. Diese kann als Adressat bezeichnet werden.[1152] Das können stets auch Dritte bzw. Nichtstörer sein, wenn dies unter Verhältnismäßigkeitsaspekten statthaft ist, § 14 Abs. 1 BWPolG.[1153]

Auch in die Rechte der Adressaten wird durch den Erhebungsvorgang eingegriffen.[1154] Das gilt trotz der Tatsache, dass die allgemeinen Datenerhebungsklauseln keine Pflicht zur Auskunftserteilung begründen,[1155] da schon in der Konfrontation mit dem Verlangen eine grundrechtsrelevante Duldungspflicht erblickt werden kann.[1156]

Die allgemeine Datenerhebungsklausel in Baden-Württemberg findet sich in § 43 Abs. 2 BWPolG. Danach kann die Polizei *personenbezogene Daten erheben, „soweit dies zur Abwehr einer Gefahr oder zur Beseitigung einer Störung der öffentlichen Sicherheit oder Ordnung erforderlich ist und die Befugnisse der Polizei nicht anderweitig geregelt sind"*. Informatorische

1148 *Wonka*, NJW 2017, 3334 (3337 f.); OVG Koblenz, NVwZ 2002, 1529 .

1149 *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 12 Rn. 9.

1150 Vgl. *Di Fabio* in Dürig/Herzog/Scholz GG, Art. 2 Abs. 1 Rn. 176; *Weiner* in BeckOK NdsPOG, § 31 Rn. 5 ff.; zum Strafprozess *Riepl,* Informationelle Selbstbestimmung, 1998, S. 172; *Singelnstein* in Barton/Kölbel/Lindemann (Hrsg.), Ermittlungsverfahren, 2015, S. 251 allg. BVerfGE 65, 1 (41 ff.) – Volkszählung; für spezialgesetzliche Auskunftsverlangen gegenüber Online-Unternehmen: VG Berlin, NVwZ-RR 2021, 934 (936) Rn. 35.

1151 Vgl. *M. Koch,* Datenerhebung, 1999, S. 69.

1152 Differenzierung zwischen „Adressat" und „Betroffener" bei *Heckmann* VBlBW 1992, 164 (167).

1153 Vgl. *Son,* Heimliche Eingriffe, 2011, 93 f.

1154 *Graulich* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. E Rn. 312.

1155 BVerfGE 130, 151 (201) – Bestandsdatenauskunft I; *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 12 Rn. 10.

1156 *Graulich* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. E Rn. 312; *Röcker* in BeckOK BWPolG, § 43 Rn. 2; *Gusy*, NVwZ 1991, 614 (616); aA. *Schmidbauer* in Schmidbauer/Steiner BayPAG, Art. 12 Rn. 2.

Befragungen bzw. Auskunftsersuchen lassen sich auf diese Grundlage stützen. Bei diesen besteht nach heute gefestigter Auffassung aber keine Auskunftspflicht.[1157] Da sie keine verpflichtende Wirkung entfalten, handelt es sich auch nicht um Verwaltungsakte. Das gilt erst recht gegenüber dem Betroffenen, da ihm die Maßnahme nicht bekanntgegeben wird.[1158] Auskunftsersuchen, die sich auf die allgemeine Datenerhebungsklauseln stützen, sind daher sowohl in Richtung des Adressaten als auch für den Betroffenen nur Realakte.

Bei den allgemeinen Datenerhebungsklauseln muss stets beachtet werden, dass die speziellen Datenerhebungsklauseln vorrangig anzuwenden sind.[1159] Ob Auskunftsersuchen allein auf diese Norm gestützt werden können, ist daher fraglich, wenn Auskunftsverlangen in Spezialgesetzen geregelt sind.

bb. Herausgabeverlangen und -pflicht, insbesondere bei der *Befragung*?

Ein Unterfall der Datenerhebung ist die im Polizeirecht typische *Befragung.* Diese ist meist als eigene Ermächtigungsgrundlage ausgestaltet, da sie – anders als die allgemeine Datenerhebung – teilweise mit Antwortpflichten einhergeht, bspw. § 43 Abs.1 PolG BW.

Ermächtigungen der Polizei zur Erhebung von Informationen bei Personen gehen typischerweise nicht mit einer Pflicht dieser Person zur Erteilung einer Auskunft einher. Die Ermächtigungsgrundlagen beziehen sich nur auf die Handlung der Polizei. Pflichten der Betroffenen im Zusammenhang mit den Ermittlungshandlungen müssen gesetzlich festgelegt werden. Ebenso wenig wie eine Auskunftspflicht ergibt sich aus dem Polizeirecht aber ein Auskunftsverbot. Freiwillige Herausgaben von Informationen – etwa durch Aushändigung von Kontoumsätzen – sind grundsätzlich möglich. Etwas anderes könnte sich lediglich aus dem Datenschutzrecht ergeben.

Da das Polizeirecht die Pflichten und Rechte der Erhebungsadressaten nicht regelt, ist allein fraglich, ob die Polizei konkret nach der Herausgabe

1157 BVerfGE 130, 151 (201) – Bestandsdatenauskunft I; *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 651; *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 12 Rn. 10.

1158 *Son,* Heimliche Eingriffe, 2011, S. 96 ff.; *Deutsch,* Informationen, 1992, S. 279 f.; *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI §1 Rn. 14.

1159 *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht,Rn. 610.

von verkörperten Daten verlangen darf, und wenn ja, auf welcher Rechtsgrundlage dies beruhen kann.

Aus den vorherigen Ausführungen lässt sich ableiten, dass bei einem schriftlichen Verlangen nach Unterlagen – je nach Auslegung – von vornherein nur die Datenerhebungsklauseln in Betracht kommen. Diese sehen grundsätzlich keine Auskunftspflicht vor. Schon deswegen kann eine Herausgabe bestimmter Daten oder Datenträger nicht auf deren Grundlage verlangt werden. Etwas anderes kommt nur bei solchen Auskunftsverlangen in Betracht, die eine *Befragung* darstellen, da mit ihnen teilweise Auskunftspflichten einhergehen.

In § 43 Abs. 1 S. 3 BWPolG etwa werden die Betroffenen zur Abgabe *sachdienlicher Angaben verpflichtet, die über die Personendaten des § 43 Abs. 1 S. 2 BWPolG hinausgehen, wenn die Befragung der Abwehr einer Gefahr für Leben, Gesundheit oder Freiheit einer Person oder für bedeutende fremde Sach- oder Vermögenswerte dient.*

Dabei ist aber schon fraglich, ob eine Befragung überhaupt schriftlich erfolgen darf.[1160] In einigen Polizeigesetzen ergibt sich aus der Formulierung der Ermächtigung, dass offensichtlich nur spontane, mündliche Ansprachen gemeint sein sollen, da die Befragten für die Dauer der Befragung *angehalten* werden dürfen, § 43 Abs. 1 S. 1l BWPolG, § 9 Abs. 2 S. 2 NRW-PolG. Art. 12 S. 3 BayPAG. Soweit diese Gesetze Antwortpflichten bei der Befragung vorsehen, kann dies nicht für schriftliche Anfragen gelten, denn diese stellen eben keine Befragung dar.

Bei den Polizeigesetzen, die eine schriftliche Befragung nicht ausschließen, stellt sich ein aus der StPO bekanntes Problem: Sowohl in einem schriftlichen als auch mündlichen Auskunftsverlangen wird es praktisch sein, Datensätze herauszugeben. Wie bereits dargelegt, können unmittelbare Auskünfte von Personen Kontoinformationen nur begrenzt wiedergeben. Sie sind zu komplex. Viel eher wird sich anbieten, dass die Kontodaten schriftlich herausgegeben werden.

Für die StPO wurde festgestellt, dass ein Verlangen nach verkörperten Daten keine formlose oder förmliche Zeugenvernehmung i. S. d. § 161 Abs. 1 S. 1 Hs. 1 Alt. 2, § 161a Abs. 1 StPO, sondern – nach korrekter Ansicht – ein

1160 *Waechter* in BeckOK NdsPOG, § 12 Rn. 32; *Schenke* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BPolG § 22 Rn. 9.

Herausgabeverlangen i. S. d. § 95 Abs.1 StPO darstellt.[1161] Die Polizeigesetze der Länder beschreiben aber keine Rechtsgrundlage, die § 95 Abs. 1 StPO entsprechen würde, sondern eben nur die allgemeine Datenerhebung und Befragung.

Wenn ausschließlich die verkörperten Kontodaten sachdienlich sind, könnte sich die polizeirechtliche Befragung faktisch als konkretes Herausgabeverlangen nach solchen Daten darstellen. An diesem Punkt stellt sich dann die Frage nach der Bestimmtheit der Norm.[1162] Ließe man eine Auslegung zu, die die Auskunftspflicht in bestimmten Fällen zu einer Herausgabepflicht reduziert, hätte man in der Befragung letztlich eine Spezialermächtigung zu einer ganz anderen, dem § 95 StPO entsprechenden, Handlung.[1163] Diesem Ergebnis steht das verfassungsrechtliche Bestimmtheitsgebot entgegen.[1164]

Die Polizei ist also auch bei der Befragung auf eine freiwillige Herausgabe von Daten angewiesen. Eine Regelung, die sich zu § 95 StPO äquivalent verhält, findet sich im Polizeirecht nicht.

b. Datenerhebung und Befragung im Polizeirecht des Bundes

Eine Datenerhebungsgeneralklausel und eine Ermächtigung zur Befragung finden sich auch in den bundesrechtlichen Vorschriften zur Gefahrenabwehr. Für die Bundespolizei sind sie in §§ 21, 22 BPolG geregelt. Das Bundeskriminalamt wird in den §§ 39, 41 BKAG ermächtigt.

Nur die Ermächtigungsgrundlagen zur Befragung sehen in § 22 Abs. 2 S. 2 BPolG und § 41 Abs. 2 S. 2 BKAG eine Auskunftspflicht auch für Nichtstörer bzw. Dritte vor, soweit die Voraussetzungen des polizeilichen Notstands i. S. d.. § 20 BPolG vorliegen. Auf Maßnahmen, die auf die allgemeinen Datenergebungsklauseln gestützt werden, müssen die Betroffenen

1161 *F. Jansen,* Bankauskunftsersuchen, 2010, S. 445; *Singelnstein*, NStZ 2012, 593 (603); *ders.* in Barton/Kölbel/Lindemann (Hrsg.), Ermittlungsverfahren, 2015, S. 251 (254 ff.).
BVerfG, NJW 2009, 1405 (1407).

1162 Hierzu *Lepsius* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 12 Rn. 75.

1163 Vgl. VGH Mannheim Urt. v. 07.12.2017 - 1 S 2526/16 Rn. 42, 43 zum Gefährderanschreiben; *Schmidbauer* in Schmidbauer/Steiner BayPAG, Art 10 Rn. 2 ff.

1164 Vgl. dazu *Cremer*, NVwZ 2001, 1218 (1221); *Gassner*, DÖV 1996, 18 (23).

keine Auskünfte erteilen.[1165] Das ergibt sich aus § 21 Abs. 4 S. 2 BPolG, § 39 Abs. 3 i. V. m. § 9 Abs. 3 S. 3 BKAG. Danach ist der Betroffene bei der Datenerhebung auf die Freiwilligkeit der Auskunft hinzuweisen, wenn keine Auskunftspflicht besteht. Die Auskunftspflicht muss also erst im Einzelfall geschaffen werden.[1166]

Das Herausgabeverlangen ist im BPolG und im BKAG ebenfalls nicht geregelt. Eine Ermächtigungsgrundlage für die Erteilung von Auskünften durch die Übergabe bestimmter Sachen enthalten also auch die bundespolizeilichen Regeln nicht. Ihre Auskunftsersuchen müssen also darauf beschränkt werden, dass allgemein die Erteilung bestimmter Informationen verlangt wird.

c. Polizeirechtliche Auskunftsersuchen als offene Maßnahmen

Alle Polizeigesetze enthalten eine Klausel, wonach die Datenerhebung grundsätzlich *offen* zu erfolgen hat, bspw. § 14 Abs. 1 BWPolG, § 21 BPolG Abs. 3 S. 1, § 39 Abs. 3 i. V. m. § 9 Abs. 2 S. 1 BKAG. Dieser Grundsatz drückt das traditionelle Verständnis der nach rechtsstaatlichen Grundsätzen agierenden Polizei aus, die gerade kein Nachrichtendienst sein soll.[1167]

Unmittelbar definiert wird diese grundsätzliche Offenheit nicht, dafür aber das Gegenteil. In § 14 Abs. 2 S. 2 BWPolG etwa wird die „*verdeckte*" Ermittlung als Maßnahme umschrieben, „*die nicht als polizeiliche Maßnahme erkennbar sein soll*". Die übrigen Polizeigesetze sind identisch, etwa § 30 Abs. 2 S. 2 NdsPOG, oder fast identisch formuliert, wie z. B. Art. 31 Abs. 4 S. 1 BayPAG § 21 Abs. 3 S. 3 BPolG und § 9 Abs. 2 S. 4 BKAG.

Der Begriff *verdeckt* bedeutet dabei nichts anderes als heimlich. Teilweise wurde versucht, verdeckte und heimliche Maßnahmen voneinander abzugrenzen bzw. die verdeckten Maßnahmen als Unterfall der heimlichen Ermittlung einzustufen.[1168] Verdeckte Maßnahmen sollten danach nur solche sein, die zwar gegenüber dem Betroffenen erfolgen, für diesen aber nicht als

1165 *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 12 Rn. 10.

1166 *Schenke* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BKAG § 9 Rn. 48; BPolG § 21 Rn. 18.

1167 BVerfGE 133, 277 (328 f.) – Antiterrordatei; *Graulich* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. E Rn. 678.

1168 Übersicht bei *Zöller*, ZStW 2012, 411 (419 f.); *R.-G. Müller,* Datenerhebungn, 1997, S. 118.

Polizeimaßnahmen erkennbar sind.[1169] Ein klassisches Beispiel hierfür wäre der verdeckte Ermittler. Die verdeckten Maßnahmen sollten ihre Intensität daraus ziehen, dass der Betroffene getäuscht wird und sich in falscher Sicherheit wähnt.[1170] Diese Differenzierungsversuche haben sich aber nicht durchgesetzt. Das BVerfG erblickt die Intensität der Heimlichkeit darin, dass der Betroffene sich mangels Kenntnis nicht mit rechtlichen Mitteln wehren kann,[1171] und zwar auch dann, wenn es selbst von verdeckten Maßnahmen spricht.[1172] Daher besteht zwischen den verdeckten und heimlichen Maßnahmen kein qualitativer Unterschied. Sie sind identisch zu behandeln.[1173]

Für verdeckte allgemeine Datenerhebungen gelten meist strengere Voraussetzungen als nach § 14 Abs. 2. BWPolG. In manchen Bundesländern ist sie sogar gesetzlich untersagt, etwa nach § 9 Abs. 5 NRWPolG. Daher muss dringend geklärt werden, ob ein polizeirechtliches Auskunftsverlangen bei Dritten als verdeckte oder offene Maßnahme anzusehen ist.

Hierzu ist zunächst festzustellen, dass keine Norm der Polizeigesetze es der Polizei verwehren würde, selbst für die Offenheit zu sorgen. Informiert die Polizei den Betroffenen über ihre Maßnahme, erfolgt sie *offen*.

Eine Benachrichtigungspflicht sehen die Polizeigesetze, etwa § 86 BWPolG, hingegen für Maßnahmen nicht vor, die verdeckt aber auf der Grundlage der allgemeinen Datenerhebungsgeneralklausel oder als Befragung erfolgen. Ausgehend von Art 13 Abs. 1, 2 der JI-RL ist der Betroffene aber über bestimmte Basisinformationen bei der Datenverarbeitung zu informieren. Die Unterrichtung kann zwar aus Gründen des Art. 13 Abs. 3 JI-RL zurückgestellt werden, eine solche Zurückstellung findet aber bei den offenen Maßnahmen gerade nicht statt.[1174]

Art. 13 JI-RL ist z. B. in § 85 BWPolG umgesetzt. Hier wird zwar nicht zwischen offenen und verdeckten Maßnahmen differenziert, es ergibt sich aber aus der Logik der verdeckten Maßnahmen, dass die Basisinformationen erst mit der Benachrichtigung erteilt werden. Besser ausgestaltet ist

1169 Etwa *Kniesel/Vahle*, DÖV 1990, 646 (646) für § 9 NRWPolG 1990.
1170 *Makrutzki,* Ermittlungen, 2021, S. 51.
1171 BVerfGE 107, 299 (321); E 115, 320 (353) – Rasterfahndung; *Tanneberger,* Sicherheitsverfassung, 2014, S. 247 mwN.
1172 BVerfGE 122, 342 (373).
1173 *Tanneberger,* Sicherheitsverfassung, 2014, S. 248; *Bode,* Ermittlungsmaßnahmen, 2012, S. 13 *R.-G. Müller,* Datenerhebung, 1997, S. 118; *Zöller*, ZStW 2012, 411 (420).
1174 Vgl. *M. W. Müller/Schwabenbauer* in Lisken/Denninger Hdb PolR, 6. Aufl. 2018, Kap G Rn. 1055.

Art. 31 Abs. 4 S. 2 BayPAG, der diesen Umstand klarstellt. Es fehlt allerdings in beiden Vorschriften an einem zeitlichen Anknüpfungspunkt. Man steht somit vor einem Zirkelschluss. Wenn die datenschutzrechtliche Informationspflicht nur für offene Maßnahmen besteht, kann sich die Offenheit nicht aus dieser Informationspflicht ergeben. Man kommt um die Frage, ob ein Auskunftsersuchen bei Dritten bzw. eine Zeugenbefragung ohne Verschwiegenheitspflicht als originär heimliche Maßnahme einzustufen ist, also nicht herum.

Ausgehend von den Ausführungen des BVerfG zur Heimlichkeit muss die Möglichkeit des Betroffenen, sich zur Wehr zu setzen, im Vordergrund der Auslegung stehen. Im Strafprozessrecht etwa wird die Offenheit, wenn keine Offenbarungspflicht besteht, durch das Akteneinsichtsrecht und die frühestmögliche Beschuldigtenvernehmung gewährleistet (s. o. I. 1. d.). Die Zeugenvernehmung wird daher ganz klassischerweise nicht als verdeckte Maßnahme beurteilt, auch wenn der Beschuldigte davon erst nachträglich erfährt, d. h. die Informationsbeschaffung also für einen bestimmten Zeitraum ohne seine Kenntnisnahme erfährt.

Der Maßstab der StPO ist aber auch ein anderer. Die freie Gestaltung des Ermittlungsverfahrens erlaubt heimliche Ermittlungen, da dieses ohne sie schlicht nicht auskommt.[1175] Eine Grundsatznorm der offenen Datenerhebung findet sich in der StPO nicht. Trotzdem wird durch die Akteneinsicht und die obligatorische Beschuldigtenvernehmung eine gewisse Waffengleichheit hergestellt.[1176] Im Polizeirecht dienen hierzu eben nur der Grundsatz der Unmittelbarkeit, der nichts weiter ist als ein Ausfluss der allgemein geltenden Erforderlichkeit[1177], und das Offenheitsprinzip. Letzteres muss ernstgenommen werden. Mangels des Strafprozesses entsprechender Verfahrenssicherungen ist der Betroffene bei Datenerhebungen stärker dem Zufall ausgeworfen, wenn es darum geht, von den Ermittlungen bei Dritten zu erfahren. Um Betroffene zu schützen, muss der Offenheitsgrundsatz entsprechend eng ausgelegt werden. Eine Offenheit liegt daher nur vor, wenn der Betroffene von einer Datenerhebung bei Dritten umgehend informiert wird.

Etwas Anderes lässt sich nur dann vertreten, wenn man nicht das Erschweren des Rechtsschutzes durch die Heimlichkeit in den Vordergrund

1175 BVerfG, NJW 2009, 1405, (1407) Rn. 28.
1176 BVerfGE 63, 45 (61 f.); *Gaede,* Fairness, 2010, S. 243 f.; 301 ff.; 305 ff.; 828 ff.; zur Akteneinsicht *Schlegel*, HRRS 2004, 411 .
1177 Vgl. *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 12 Rn. 17.

stellt, sondern deren Täuschungscharakter. Geht es darum, eine Verschleierung der polizeilichen Maßnahme vor dem Adressaten zu vermeiden, ließe sich auch gut argumentieren, dass es für die Offenheit ausreicht, wenn die Polizei gegenüber dem Adressaten offen auftritt.[1178]

Mit der Judikatur des BVerfG, die das Erschweren von Rechtsschutz in den Vordergrund stellt,[1179] lässt sich dieser Ansatz aber nicht in Einklang bringen. Im Polizeirecht ist eine Datenerhebung daher nur dann offen, wenn sie sowohl gegenüber dem Adressaten als auch dem Betroffenen offen erfolgt.[1180] In den Polizeigesetzen, die keine verdeckte allgemeine Datenerhebung vorsehen, ist die Benachrichtigung damit obligatorisch. In den anderen Gesetzen gelten, bei Ausbleiben der Benachrichtigung, die jeweils verschärften Voraussetzungen.

II. Heimliche Maßnahmen

Die *offenen* Maßnahmen der Sicherheitsbehörden sind somit abschließend beschrieben. Im Folgenden soll nunmehr eine Übersicht der Normen angeboten werden, die einen verdeckten bzw. heimlichen Zugang zu Kontodaten ermöglichen.

Bei Auskünften von Finanzinstituten besteht ein Dreiecksverhältnis. Unmittelbar von der Maßnahme adressiert wird das Institut bzw. deren Mitarbeiter. Betroffener im Lichte der informationellen Selbstbestimmung ist hingegen auch bzw. vorrangig der Kontoinhaber. Es wurde bereits gezeigt, dass eine Maßnahme nicht schon deshalb verdeckt ist, weil sie im Moment ihres Geschehens vom Betroffenen unbemerkt bleibt, etwa durch eine Zeugenvernehmung. Andererseits ist die polizeiliche Befragung, über die der Betroffene nicht informiert wird, eine verdeckte Maßnahme im Sinne der Polizeigesetze. Die Definition der Heimlichkeit ist also abhängig vom gesetzlichen Kontext. Die Auslegung ergibt sich anhand der Rechtsprechung des BVerfG, das die intensivierende Eigenart der Heimlichkeit

1178 So *Röcker* in BeckOK BWPolG, § 14 Rn. 22.

1179 BVerfGE 107, 299 (321); E 115, 320 (353) – Rasterfahndung; *Gärditz* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 13 Rn. 98 ff.; *Tanneberger,* Sicherheitsverfassung, 2014, S. 247 mwN.

1180 So wohl *Heckmann*, VBlBW 1992, 164 (168 Fn 36); iE, auch *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 7.

primär in ihrer nachteiligen Wirkung für den Rechtsschutz des Betroffenen erkennt.[1181]

Stets heimlich ist eine Maßnahme danach, wenn die Informationsgewinnung ohne Kenntnisnahme des Dritten erfolgt, etwa aufgrund einer automatisierten Einrichtung, oder wenn er zur Verschwiegenheit über die Maßnahme gesetzlich verpflichtet wird. Solche Verschwiegenheitspflichten wirken besonders intensiv, wenn sie strafbewährt sind.

1. Bestandsdatenauskunft

Zunächst soll der heimliche Zugriff der Sicherheitsbehörden auf die Kontobestandsdaten (s. o. Kap. D. I. 2) beschrieben werden. Bei Kontobestandsdaten, die meist Stammdaten genannt werden[1182], handelt es sich allgemein um Daten, die unmittelbar mit der Einrichtung eines Kontos bzw. mit den vertraglichen Rahmenbedingungen zusammenhängen. Sie entsprechen damit den Bestandsdaten im Sinne des § 3 Nr. 6, §§ 172 ff. TKG.[1183] Das umfasst etwa die Personendaten und die Kontonummer. Auf europäischer Ebene wurden die Regeln der automatischen Bestandsdatenauskunft, nachdem diese durch Art. 32a der 5. EU GeldwäscheRL verpflichtend geworden war, in der Finanzinformationsrichtlinie (FinanzinformationsRL)[1184] harmonisiert.

Die Institute müssen ihre Dateisysteme gem. § 24c Abs. 1 S. 6 KWG so einrichten, dass ihnen die Abrufe nicht zur Kenntnis gelangen. Da die Zugriffe mithin noch nicht einmal dem unmittelbaren Maßnahmenadressaten offenkundig werden, handelt es sich bei der Bestandsdatenabfrage

1181 BVerfGE 107, 299 (321); E 115, 320 (353) – Rasterfahndung; *Tanneberger,* Sicherheitsverfassung, 2014, S. 247 mwN.

1182 BVerfGE 118, 168 – Kontostammdaten; *Achtelik* in Herzog GwG, KWG § 24c Rn. 2; *Tolani*, BKR 2007, 275 (276 ff.).

1183 *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 38; *Gnüchtel*, NVwZ 2016, 13 (16); zum Inhalt des § 3 TKG siehe nur *Ricke* in Spindler/Schuster/Anton (Hrsg.), Elektronische Medien, 4. Auflage 2019, TKG § 3 Rn. 6.

1184 Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates, ABl. 2019 L 186/122.

definitiv um eine heimliche Maßnahme.[1185] Das Gesetz sieht auch keine Benachrichtigungspflicht vor. Lediglich die Protokollierung der Abrufe ist nach § 24c KWG Abs. 4 vorgeschrieben.

Zum Zugriff auf das Dateisystem sind nach § 24c Abs. 1 KWG, § 93b, § 93 Abs. 7 AO und § 31 Abs. 6 GWG unmittelbar nur die BaFin, die FIU und das BZSt berechtigt. Sowohl die BaFin als auch das BZSt sind dabei ausdrücklich berechtigt, Daten aus dem System aufgrund von Auskunftsersuchen an verschiedene Stellen zu übermitteln.

Die zu übermittelnden Daten unterscheiden sich geringfügig zwischen den Abfragen von BaFin und FIU einerseits und dem BZSt andererseits. Da die Institute nur ein einheitliches Dateisystem führen sollen, aber die Abfragen nicht bemerken können, wird die Abfrage über das ITZBund als gemeinsames Rechenzentrum von BaFin und BZSt gesteuert, das zwischen den verschiedenen Abfragen differenziert und dafür sorgen soll, dass nur die jeweils zulässigen Daten übermittelt werden.[1186] Die Ermächtigungen zur Abfrage aufgrund von Auskunftsersuchen führen dazu, dass auch Sicherheitsbehörden über Zwischenstellen heimlich auf das Kontobestandsdatensystem zugreifen können.

a. Behörden der Strafverfolgung

Auskunftsersuchen der Strafverfolgung richten sich nach § 24c Abs. 3 S. 1 Nr. 2 KWG. Danach erteilt die BaFin auf Ersuchen Auskunft aus dem Dateisystem, das *„[den] für die Leistung der internationalen Rechtshilfe in Strafsachen sowie im Übrigen für die Verfolgung und Ahndung von Straftaten zuständigen Behörden oder Gerichten, soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.“*

Eine spezifische Ermächtigungsgrundlage, die die Strafverfolgungsbehörden zu solchen Auskunftsersuchen ausdrücklich ermächtigen würden, findet sich in der StPO nicht. In der Literatur wurde schon früh bemerkt, dass § 24c Abs. 3 Nr. 2 KWG nur die BaFin adressiert und sich die Rechtmäßigkeit der Auskunftsersuchen nach dem Recht der jeweils anfragenden

1185 BVerfGE 118, 168 (197 ff.) – Kontostammdaten; *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 129*Tolani*, BKR 2007, 275 (277); *Herzog/Christmann*, WM 2003, 6 (10); *Zubrod*, WM 2003, 1210 (1214).

1186 BT-Drs. 18/12127, S. 51.

Behörde richten müsste.[1187] Mit dieser Problematik hat sich das BVerfG in seiner Entscheidung zur Kontostammdatenabfrage aber nicht weiter auseinandergesetzt.[1188] Heute wäre die Argumentation aber hoch aktuell. Sie entspricht der aktuellen Rechtsprechung des BVerfG vom „Doppeltürenmodell".[1189] Diese stellt die Notwendigkeit einer Ermächtigung sowohl für die weitergebende Behörde zur Übermittlung als auch der ersuchenden Behörde für die Anfrage fest.[1190]

Der Gesetzgeber selbst ging bei der Schaffung der Kontobestandsdatenabfrage davon aus, dass die Strafverfolgungsbehörden nach den „allgemeinen Regeln" erst beim Vorliegen eines Anfangsverdachts ein Auskunftsersuchen stellen dürfen und verwies auf die §§ 152 Abs. 2, 160 StPO.[1191] Zur Frage, auf welche Norm Auskunftsersuchen konkret zu stützen sind, äußerte er sich nicht. Berücksichtigt man, dass 24c KWG im Jahr 2002 eingeführt wurde, ist das Fehlen einer solchen Auseinandersetzung nachvollziehbar. Das „Doppeltürenprinzip" wurde vom BVerfG erst zehn Jahre später etabliert.[1192] Nach der Rechtsprechung des BVerfG sind seither sämtliche Einzelhandlungen bei der Datenabfrage differenziert zu betrachten.

Bei der automatisierten Abfrage von Bestandsdaten steht sowohl im Regelungsgefüge der Kontobestandsdaten als auch im TKG eine Aufsichtsbehörde zwischen den Sicherheitsbehörden und der privaten Stelle, die die Daten führt. Jeweils vier Schritte lassen sich bei diesen Normkomplexen identifizieren. Zuerst wird eine gesetzliche Speicherpflicht in einem automatisierten System geschaffen. Sodann wird die vermittelnde Stelle zum automatisierten Zugriff auf diese Dateien ermächtigt. Im nächsten Schritt wird die vermittelnde Stelle befugt, die Daten an Sicherheitsbehörden zu übermitteln. Dieser Schritt entspricht nun der ersten Hälfte der Doppeltür.[1193] Den letzten Schritt stellt das Auskunftsersuchen dar, das die zweite Hälfte der Doppeltür öffnet. Hierzu hat das BVerfG festgestellt, dass die all-

1187 *Zubrod*, WM 2003, 1210 (1214).
1188 BVerfGE 118, 168 – Kontostammdaten.
1189 BVerfGE 130, 151 (184) – Bestandsdatenauskunft I; E 155, 119 (167, 209 f.) – Bestandsdatenauskunft II.
1190 Zusammenfassend statt vieler *Graulich* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BKAG § 10 Rn. 9 f.; *ders.*, NVwZ-Beilage 2020, 47.
1191 BT-Drs. 14/8017, S. 123.
1192 BVerfGE 130, 151 (184) – Bestandsdatenauskunft I.
1193 Idem (193) für § 112 TKG a.F.

gemeinen Datenerhebungsklauseln grundsätzlich infrage kommen,[1194] die Ermächtigung aber auch in derselben Norm mit der ersten Tür geregelt werden könnte.[1195]

§ 24c Abs. 3 Nr. 2 KWG käme daher prinzipiell als Ermächtigungsgrundlage für die Öffnung der zweiten Tür, also für die Auskunftsverlangen der Strafverfolgungsbehörden, in Betracht. Es wurde aber auch schon früh die Ermittlungsgeneralklausel des § 161 Abs. 1 StPO als Ermächtigungsgrundlage bzw. als zweite Tür vorgeschlagen.[1196] Zu letzterem Ergebnis kommt auch die Rechtsprechung[1197] und dürfte wohl vom BVerfG intendiert sein. Auch wenn sich der Entscheidung „Bestandsdatenauskunft I" keine ausdrückliche Bestimmung der zweiten Tür zu § 112 TKG aF. entnehmen lässt, winkt das BVerfG dort gewissermaßen mit dem Zaunpfahl.[1198]

Der Wortlaut des § 24c Abs, 3 KWG ist eindeutig auf die Übermittlungshandlung gerichtet. Das Auskunftsersuchen wird als Voraussetzung formuliert und gerade nicht als Handlung, die erst ermöglicht werden sollte. Daher kommt als Ermächtigungsgrundlage für die zweite Tür tatsächlich nur § 161 Abs. 1 S. 1 Hs. 1 Alt. 1 StPO in Betracht[1199], der zur verpflichtenden[1200] Datenerhebungen bei Behörden ermächtigt.

Die Voraussetzungen der Bestandsdatenabfrage lassen sich nur aus § 24c Abs. 3 Nr. 2 KWG und § 161 Abs. 1 Hs. 1 Alt. 1 StPO ziehen. § 24c Abs. 3 Nr. 2 KWG schreibt vor, dass die Auskunftserteilung an die Strafverfolgungsbehörden erfolgt, *„soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist."* Unmittelbar adressiert wird von dieser Vorschrift nur die BaFin. Diese muss die Zulässigkeit der Übermittlung nur prüfen, *„soweit hierzu besonderer Anlass besteht"*, § 24c Abs. 3 S. 3 KWG. *„Die Verantwortung für die Zulässigkeit der Übermittlung trägt die ersuchende Stelle"*, § 24c Abs. 3 S. 4 KWG.

Die Anforderungen der Strafverfolgungsbehörden ergeben sich aus § 161 Abs. 1 Hs. 1 Alt. 1 StPO, der allerdings nur einen Anfangsverdacht voraus-

1194 Idem (192).
1195 BVerfGE 155, 119 (184.) – Bestandsdatenauskunft II.
1196 *Zubrod*, WM 2003, 1210 (1214).
1197 OLG Stuttgart, NStZ, 48 (48).
1198 BVerfGE 130, 151 (193 ff.) – Bestandsdatenauskunft I; *Meinicke*, MMR 2012, 410 (416).
1199 Ausdrücklich *Dalby,* Strafverfolgung, 2016, S. 68, der solch eine Festlegung auch bei *Bär*, MMR 2013, 700 (702) erkennen will.
1200 *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 1a.

setzt.[1201] § 24c Abs. 3 Nr. 2 adressiert die ersuchende Behörde zwar nicht, der dort zum Ausdruck kommende Erforderlichkeitsgrundsatz gilt als Teil der Verhältnismäßigkeitsprüfung jedoch generell für alle Sicherheitsbehörden. Aus den anzuwendenden Vorschriften lassen sich als Voraussetzungen für ein Auskunftsersuchen der Strafverfolgungsbehörden also nur die Geltung des Verhältnismäßigkeitsprinzips und die Notwendigkeit eines Anfangsverdachts ableiten. Formelle Voraussetzungen sucht man vergeblich.

b. Polizeivollzugsbehörden

Die Übermittlung von Kontobestandsdaten an die Polizeivollzugsbehörden des Bundes und der Länder für den Bereich der Gefahrenabwehr ist in §§ 93 Abs. 8 S. 1 Nr. 2, 93b AO geregelt und erfolgt durch das BZSt. Der Umfang der zu übermittelnden Daten richtet sich nach § 93b Abs. 1a, § 154 Abs. 2a, 2d AO, Art. 97 § 26 Abs. 5 Nr. 3, 4 EGAO und unterscheidet sich somit von der Abfrage der Strafverfolgungsbehörden nach § 24c Abs. 3 S. 1 Nr. 2 KWG insofern, dass auch die Adresse des Kontoinhabers übermittelt wird (s.o. Kap. D. I. 2.).

Die Regelung in § 93. Abs. 8 AO a.F. war in ihrer Ursprungsgestalt von 2002[1202] vom BVerfG zunächst für verfassungswidrig erklärt worden.[1203] Sie ermächtigte damals noch zur Übermittlung an Behörden, die für ein Gesetz zuständig sind, das an *Begriffe des Einkommenssteuergesetz anknüpft*. Diese Formulierung hielt das BVerfG für zu unbestimmt.[1204] Durch die konkrete Nennung der berechtigten Behörden wurde dieser Missstand im Jahr 2008 beseitigt.[1205] Die Polizeivollzugsbehörden waren im Rahmen dieser Novelle aber nicht genannt. Sie wurden erst im Jahr 2017 in den Kreis der Ermächtigten aufgenommen.[1206]

Nach § 93b Abs. 3 AO trägt der Ersuchende die Verantwortung für die Zulässigkeit des Datenabrufs. Eine Regel entsprechend § 24c Abs. 3 S. 3

1201 BVerfG, NJW 2009, 1405 (1407); OLG Stuttgart, NStZ 2016, 48 (48); *Kölbel* in MüKo StPO, § 161 Rn. 1.

1202 Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003, BGBl. I, S. 2928.

1203 BVerfGE 118, 168 (188 ff.) – Kontostammdaten.

1204 Ibid.

1205 Unternehmenssteuerreformgesetz 2008 vom 14. August 2007, BGBl. I, S. 1912.

1206 Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni2017, BGBl. I S. 1822.

KWG, wonach eine Prüfung der Zulässigkeit durch die BaFin bei besonderem Anlass besteht, findet sich in der AO nicht. § 93b Abs. 4 AO erklärt nur die § 24c Abs. 1 S. 2-6, Abs. 4-8 KWG für entsprechend anwendbar. Es findet also in keinem Fall eine Zulässigkeitsprüfung durch das BZSt statt. Das ist vor dem Hintergrund, dass § 93b Abs. 8 AO den Zugang für eine Vielzahl verschiedener Verwaltungsbehörden eröffnet, auch verständlich. Allein für die Polizeivollzugsbehörden braucht es aufgrund der Kompetenz der Länder für die Landespolizei 18 verschiedene Ermächtigungsgrundlagen für die Auskunftsersuchen zum BZSt.

Wie auch in der StPO finden sich in den Polizeigesetzen von Bund und Ländern aber keine Normen, die spezifisch das Auskunftsersuchen im automatisierten Verfahren regeln. Hier kommen also ausschließlich die allgemeinen Datenerhebungsklauseln in Betracht.[1207]

Die Auskunftsersuchen nach § 93 Abs. 8 AO unterliegen grundsätzlich speziellen Verfahrensvorschriften, die in § 93 Abs. 9 AO geregelt sind. Nach § 93 Abs. 9 S. 1 AO müssen betroffene Personen vor dem Abrufersuchen auf die Möglichkeit des Abrufersuchens hingewiesen worden sein, *was auch durch ausdrücklichen Hinweis in amtlichen Vordrucken und Merkblättern* geschehen können soll. § 93 Abs. 9 S. 2 AO sieht eine Benachrichtigungspflicht des Betroffenen durch den Ersuchenden vor. Die § 93 Abs. 9 S. 1, 2 AO gelten nach 93 Abs. 9 S. 6 aber nicht in den Fällen des § 93 Abs. 8 S. 1 Nr. 2, 3 AO. Das Auskunftsersuchen durch die Polizeivollzugsbehörden bleibt damit geheim.

c. Nachrichtendienste der Länder

Die Kontobestandsdatenabfrage der Landesverfassungsschutzämter richtet sich nach § 93 Abs. 8 S. 1 Nr. 3 AO. Anders als bei § 93 Abs. 8 S. 1 Nr. 2 AO schreibt § 93 Abs. 8 S. 1 Nr. 3 AO vor, dass die Übermittlung nur zulässig ist, wenn *„dies durch Landesgesetz ausdrücklich zugelassen ist"*. Dieser Zusatz soll zunächst verdeutlichen, dass es sich nicht um eine Erhebungsbefugnis handelt.[1208] Legt man den Zusatz systematisch aus, muss man aber erkennen, dass eine Anfrage der Landesverfassungsschutzämter darüber hinaus nicht auf deren allgemeine Datenerhebungsklauseln[1209] gestützt wer-

1207 BVerfGE 130, 151 (193 ff.) – Bestandsdatenauskunft I.
1208 BT-Drs. 18/11555, S 170.
1209 Übersicht bei *J. Franz Lindner* in BeckO PolR Bayern, BayVSG Art. 5 Rn. 6.

den kann. Wäre die Voraussetzung nur als deklaratorischer Verweis auf das Doppeltürenprinzip gedacht, erschließt sich nämlich nicht, wieso auf diesen Zusatz im Rahmen von § 93 Abs. 8 S. 1 Nr. 2 AO verzichtet wurde. Das Doppeltürenprinzip gilt schließlich auch für den Polizeivollzugsdienst. Angesichts dessen ergibt der Wortlaut also nur Sinn, wenn damit eine spezifische Ermächtigungsgrundlage der Landesverfassungsschutzämter gesetzlich gefordert wird. Von der Notwendigkeit einer speziellen Regelung gingen offensichtlich auch die Landesgesetzgeber aus und haben spezifische Grundlagen geschaffen, etwa § 5c Abs. 3 BWVSG, § 13 Abs. 1 S. 2 RPVerfSchG, § 20 Abs. 4 NdsVerfSchG oder Art. 16 Abs. 2 BayVSG.

In den Ländern, in denen entsprechende Regeln fehlen, etwa in Nordrhein-Westfalen, Hamburg oder Schleswig-Holstein, ist ein automatisiertes Vorgehen über § 93 Abs. 8 S. 1 Nr. 3 AO folglich nicht zulässig. Auf Ermächtigungsgrundlagen, die zu Auskunftsersuchen gegenüber Kreditinstituten berechtigen, wie z. B. § 5 Abs. 2 Nr. 13 NRWVSG oder § 10 Abs. 2 Nr. 2 HVSG, kann die Anfrage zum BZSt nicht gestützt werden. Das Erfordernis des § 93 Abs. 8 S. 1 Nr. 3 AO ist insofern eindeutig und erfordert eine Ermächtigung, die sich ausdrücklich auf das dort normierte automatische Verfahren bezieht.

Wie auch für die Polizeivollzugsbehörden gilt § 93 Abs. 9 AO nicht für die Nachrichtendienste der Länder, § 93 Abs. 9 S. 6 AO. Es sind jedoch spezielle Verfahrensrechte in den Gesetzen der Länder vorgesehen, etwa in den §§ 13 ff. BWVSG. Anders als § 8b Abs. 1 BVerfSchG sehen aber weder § 5c Abs. 3 BWVSG noch § 13 Abs. 1 S. 2 RPVerfSchG oder Art. 16 Abs. 2 BayVSG eine Antragspflicht für die Kontobestandsdatenabfrage vor. Begründet wird dies mit der vermeintlich niedrigen Intensität der Maßnahmen[1210] Die Zulässigkeit der Abfragen wird demnach nicht von einer dritten Stelle geprüft.

Das ist auch deshalb bedenklich, da die Landesverfassungsschutzgesetze keine Benachrichtigungspflicht enthalten. § 5c Abs. 5 BWVSG etwa sieht eine Benachrichtigungspflicht nur für manuelle Bestandsdatenauskünfte von TK-Daten i. S. d. § 173 TKG vor. Auch der Art. 17 Abs. 2 BayVSG, der die Benachrichtigungspflichten über einen Verweis auf den strengen[1211] § 12 G-10 regelt, gilt für die Bestandsdatenabfrage nach Art. 16 Abs. 2 BayVSG gerade nicht. Der Betroffene ist daher auf die allgemeinen Vorschriften der Landesverfassungsschutzgesetze verwiesen, die aber eine Auskunft nur auf

1210 Hierzu BayLT-Drs. 17/19628, S. 54

1211 *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 57.

Antrag hin vorsehen, bspw. § 13 Abs. 1 BWVSG, Art. 23 Abs. 1 BayVSG, § 29 Abs. 1 RPVerfSchG.

d. Nachrichtendienste des Bundes

Fast sechs Jahre, bevor für die Polizeivollzugsbehörden und Landesverfassungsschutzbehörden nach § 93 Abs. 8 S. 1 Nr. 2, 3 AO die Möglichkeit zur Kontobestandsdatenabfrage eröffnet wurde, schuf der Gesetzgeber eine entsprechende Rechtsgrundlage für die Nachrichtendienste des Bundes in § 8a Abs. 2a BVerfSchG a.F.[1212], die sich heute wortgleich in § 8a Abs. 2 BVerfSchG findet. Auf den § 8a Abs. 2 BVerfSchG verweisen die §§ 3 Abs. 1 BNDG, 4a MADG.

Möglich war die Einbeziehung der Nachrichtendienste des Bundes auf Grundlage des § 93 Abs. 8 S. 2 AO, der schon damals eine Erweiterung des Kreises auskunftsberechtigter Behörden durch das Bundesgesetz zuließ.[1213] Nachdem sich die Ermächtigungsgrundlage bei den Nachrichtendiensten des Bundes als sinnvoll erwiesen hatte, drängten diese darauf, auch eine Möglichkeit für die Landesbehörden zu schaffen.[1214]

Eingriffsvoraussetzung für eine Kontobestandsdatenabfrage ist die Erforderlichkeit des Auskunftsersuchens für die Sammlung und Auswertung von Informationen i. S. d. § 3 Abs. 1 BVerfSchG, wenn *Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren* für die dort genannten Schutzgüter vorliegen. § 4a MADG übernimmt diese Formulierung mit der Maßgabe, dass an die Stelle der Schutzgüter aus § 3 Abs. 1 BVerfSchG die in § 1 Abs. 1 MADG genannten Schutzgüter treten.

Nach § 3 Abs. 1 BNDG ist eine Kontobestandsdatenabfrage möglich 1.) zur Erfüllung der Aufgaben nach § 1 Abs. 2 BNDG oder 2.) zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände oder Quellen des BND gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten. Voraussetzung ist nach § 3 Abs. 1 S. 2 BNDG, dass im Falle des § 3 Abs. 1 S. 1 Nr. 1 BNDG eine schwerwiegende Gefahr für die in § 5 Abs. 1 S. 3 Nr. 1-4 BNDG und § 6 G-10 genannten Gefahrenbereiche besteht oder im Falle des § 3 Abs. 1

1212 Gesetz zur Änderung des Bundesverfassungsschutzgesetzes vom 07. Dezember 2011, BGBl. I, S. 2576.

1213 Vgl. BT-Drs. 17/6925, S. 13; *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 39.

1214 Vgl. BT-Drs. 18/5935, S. 40; *Gnüchtel*, NVwZ 2016, 13 (16).

S. 1 Nr. 2 BNDG eine schwerwiegende Gefahr im Sinne des § 3 Abs. 1 Nr. 2 BVerfSchG existiert.

§ 93 Abs. 9 S. 6 AO erlaubt einen Ausschluss der Pflichten aus § 93 Abs. 9 S. 1, 2 AO, wovon der Bundesgesetzgeber in § 8a Abs. 2 S. 2 BVerfSchG Gebrauch gemacht hat. Sinnvollerweise ist also auch die Kontobestandsdatenabfrage durch die Nachrichtendienste des Bundes geheim. Es bestehen aber spezifisch nachrichtendienstliche Verfahrensvorschriften nach § 8b BVerfSchG, auf den § 4a MADG und § 3 Abs. 1 S. 3 BNDG verweisen.

Nach § 8b Abs. 1 BVerfSchG müssen Anordnungen nach § 8a Abs. 1, 2 BVerfSchG beim Innenministerium beantragt werden. Für Anträge des MAD ist das Verteidigungsministerium, § 3 MADG, für Anträge des BND das Kanzleramt zuständig, § 4 Abs. 1 S. 3 BNDG. In der Praxis werden zumeist sogenannte Kombi-Anträge eingereicht. Bei diesen werden gleichzeitig die Kontobestandsdatenabfrage und für den Fall, dass ein Konto gefunden wird, das Auskunftsersuchen an die entsprechende Bank bzgl. der Kontoinhalte nach § 8a Abs. 1 Nr. 2 BVerfSchG beantragt[1215] (dazu gleich). Von 21 Kontostammdatenabfragen zwischen November 2013 und November 2014 erfolgten 19 als Kombi-Antrag.[1216]

Über die Anordnungen muss nach § 8b Abs. 2 S. 1 BVerfSchG noch vor deren Vollzug die G-10-Kommission unterrichtet werden, es sei denn, es besteht Gefahr im Verzug. In diesem Fall soll auch eine Unterrichtung nach Vollzug möglich sein, § 8b Abs. 2 S. 2 BVerfSchG. Die G-10 Kommission prüft nach § 8b Abs. 2 S. 3, 4 BVerfSchG i. V. m. § 15 Abs. 5 G-10 die Zulässigkeit und Notwendigkeit der Einholung von Auskünften und zwar bzgl. der gesamten Datenverarbeitung. Erklärt sie die Anordnung für unzulässig, sind sie vom Innenministerium aufzuheben, § 8b Abs. 2 S. 5 BVerfSchG. Erhobene Daten sind dann umgehend zu löschen, § 8b Abs. 2 S. 6 BVerfSchG. Im Übrigen gelten die Lösch- und weitere Datenverarbeitungspflichten des § 4 G-10 gem. § 8b Abs. 2 S. 7 BVerfSchG.

Der Betroffene ist nach § 8b Abs. 7 BVerfSchG i. V. m. § 12 G-10 über die Maßnahme zu benachrichtigen in dem Moment, in dem der Zweck der Maßnahme durch die Benachrichtigung nicht mehr gefährdet wird.[1217]

1215 BT-Drs. 18/5935, S. 25, 32, 40

1216 Idem, S. 25.

1217 Hierzu *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 57.

2. Inhaltsdaten

Die Regeln zum automatisierten und damit heimlichen Zugriff auf Kontobestandsdaten sind damit beschrieben. Im Folgenden soll nun erläutert werden, wo der Gesetzgeber einen heimlichen Direktzugriff auf Kontoinhaltsdaten geregelt hat. Es kann kaum überraschen, dass sich solche Regeln weder in der StPO noch in den Polizeigesetzen finden. Letztere sind gerade von der offenen Datenerhebung geprägt. Das trifft zwar auf strafprozessuale Ermittlungsmaßnahmen in diesem Rahmen nicht zu.[1218] Dort soll aber Waffengleichheit zwischen dem Beschuldigten und den Ermittlungsbehörden herrschen, was insbesondere durch Bekanntgabepflichten, etwa §§ 33 Abs. 2, 35 Abs. 2 StPO,[1219] und die obligatorische Beschuldigtenvernehmung[1220] i. V. m. dem Akteneinsichtsrecht[1221] gewährleistet wird. Hinsichtlich der Untersuchung der polizeirechtlichen und strafprozessualen Ermittlungsmaßnahmen musste deshalb festgestellt werden, dass es sich um strukturell offene Maßnahmen handelt (s. o. I. 1. d. & I. 2. c.)

a. Nachrichtendienstliche Auskunftsverlangen

Heimliche Auskunftsersuchen finden sich allerdings in den Gesetzen der Nachrichtendienste.[1222] Dort werden sie als *besondere Auskunftsverlangen* bezeichnet.

aa. Übersicht

In § 8a Abs. 1 Nr. 2 BVerfSchG, auf den die §§ 4a MADG und 3 Abs. 1BNDG verweisen, heißt es z. B.: „*Das Bundesamt für Verfassungsschutz darf im Einzelfall Auskunft einholen bei Kreditinstituten, Finanzdienstleistungsinstituten, Wertpapierinstituten und Finanzunternehmen zu Konten, Kontenin-*

1218 BGHSt 42, 139 (150); *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, Rn. 29.

1219 Vgl. BGH, NJW 2010, 1297 (1298).

1220 *Erb* in Löwe/Rosenberg StPO, § 163a Rn. 35; *Kölbel* in MüKo StPO, § 163a Rn. 13; *Fincke*, ZStW 1983, 918 (955 ff., 964 ff.).

1221 BVerfGE 63, 45 (61 f.); *Gaede,* Fairness, 2010, S. 243 f; 301 ff; 305 ff; 828 ff; zur Akteneinsicht *Schlegel*, HRRS 2004, 411.

1222 Übersicht aller heimlichen Informationserhebungen bei *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 26 ff.

habern und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge."

Quasi identische Vorschriften enthalten die Gesetze der Landesverfassungsschutzbehörden, etwa in § 5b Abs. 1 Nr. 1 BWVSG, Art. 16 Abs. 1 Nr. 1 BayVSG oder § 13 Abs. 1 RPVSG. Die Vorschriften erfassen sämtliche Kontodaten, d. h. sowohl Bestands- als auch Inhaltsdaten.[1223]

Die besonderen Auskunftsverlangen unterscheiden sich von den staatsanwaltschaftlichen oder polizeilichen Auskunftsersuchen in zweierlei bedeutsamer Hinsicht. Der erste Unterschied besteht in der gesetzlichen Verpflichtung der Institute zur Verschwiegenheit, die in allen Gesetzen über die Nachrichtendienste enthalten sind, bspw. § 8b Abs. 4 S. 2 BVerfSchG, § 5b Abs. 6 S. 1 BWVSG, Art. 17 Abs. 2 S. 1 BayVSG i. V. m. § 17 Abs. 3 G-10. Es handelt sich also, wie im Recht der Nachrichtendienste üblich, um heimliche Maßnahmen. Die Verschwiegenheitspflicht ist grundsätzlich sanktionsfrei,[1224] es sei denn, eine solche Sanktion wird angeordnet. Das ist bislang nur bei den Gesetzen der Fall, die auf die §§ 17, 18 G-10 verweisen, etwa Art. 17 Abs. 2 S. 1 BayVSG.

Der zweite große Unterschied besteht darin, dass die Institute – anders als im Rahmen von § 161 Abs. 1 S. 1 Hs. 1 Alt. 2 StPO – bei nachrichtendienstlichen Auskunftsersuchen zur Übermittlung der Information verpflichtet sind. Für die Nachrichtendienste des Bundes ist dies ausdrücklich in § 8b Abs. 6 BVerfSchG festgehalten, der laut dem Gesetzgeber aber nur eine klarstellende Funktion haben soll. Die Pflicht soll sich stattdessen unmittelbar aus der Ermächtigung zum Auskunftsverlangen ergeben.[1225]

Diese Ansicht muss angesichts der Rechtsprechung vom Doppeltürenprinzip aber als kontrovers empfunden werden und gewinnt an Bedeutung, wenn man sich die einzelnen landesgesetzlichen Regelungen ansieht. Denn nur in manchen von diesen findet man eine vergleichbar eindeutige Regelung wie jene des § 8b Abs. 6 BVerfSchG. Hier kommt die Frage also durchaus zum Tragen, ob die Verpflichtung der Anfrage inhärent ist oder die Übermittlungspflicht im Gesetz geregelt sein muss.

1223 *Mallmann* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BVerfSchG § 8a Rn. 11 für Art. 16 BayVSG BayLT-Drs. 17/10014, S. 36; *K.-A. Schwarz* in BeckO PolR Bayern, BayVSG Art. 16 Rn. 12 f.

1224 *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 63.

1225 BT-Drs. 17/6925, S. 16.; *Fremuth*, AöR 2014, 32 (53).

Dabei bedarf es nicht zwingend einer ganz ausdrücklichen bzw. alleinstehenden Regelung. Es dürfte ausreichen, wenn sich per Auslegung ergibt, dass der jeweilige Gesetzgeber eine Verpflichtung regeln wollte.[1226] In § 20 Abs. 5 NdsVSG z. B. heiß es etwa „*Auskünfte nach den Abs. 1, 3 sind* (herv. durch Verf.) *unentgeltlich zu erteilen*". In Art. 17 Abs. 2 BayVSG oder § 13 Abs. 6 RPVerfSchG ist ebenfalls von dem „Verpflichteten" bzw. den „verpflichteten Unternehmen" die Rede. Auch im Rahmen der Landesverfassungsschutzgesetze, die eine Klarstellung der Übermittlungspflicht vermissen lassen, wird also meist von einer Auskunfts*pflicht* ausgegangen. Es ist aber durchaus fraglich, ob die Landesgesetze, die die Verpflichtung der Adressaten nicht klar bestimmen, dem verfassungsrechtlichen Doppeltürenprinzip entsprechen.[1227]

Um diesen Missstand auszuräumen, sollte auch in den Landesgesetzen eine Deklaration entsprechend § 8b Abs. 6 BVerfSchG aufgenommen werden. Sofern es an einer solchen Klarstellung fehlt, ist offen, ob die Landesgesetze den verfassungsrechtlichen Anforderungen des Doppeltürenprinzips standhalten.

Die nachrichtendienstlichen Auskunftsverlangen gehen insbesondere hinsichtlich der materiellen Anforderungen deutlich über die Ermittlungsgeneralklausel der Strafverfolgungsbehörden (Anfangsverdacht) oder die allgemeinen Datenerhebungsklauseln der Polizei (konkrete Gefahr) hinaus.

Nach § 8a Abs. 1 S. 2 BVerfSchG müssen „*Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Abs. 1 genannten Schutzgüter vorliegen*". Hintergrund dieser vergleichsweise detaillierten Regelungen ist die Heimlichkeit der Maßnahmen.

Die besonderen Auskunftsverlangen der Dienste müssen insofern der systematischen Rechtsprechung des BVerfG zu heimlichen Überwachungsmaßnahmen entsprechen und lagen dort auch schon zur Prüfung vor.[1228] Das Gericht befand, dass es sich angesichts der Sensibilität der Kontodaten um Überwachungsmaßnahmen von „erheblicher Intensität" bzw. „erhöhtem Gewicht" handle, was wohl der mittleren Stufe des etablierten

1226 Vgl. BVerfGE 155, 119 (209 ff.) – Bestandsdatenauskunft II; E 130, 151 (202 ff.) – Bestandsdatenauskunft I.

1227 Vgl. *Mallmann* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BVerfSchG § 8b Rn. 7.

1228 BVerfGE 120, 274 (346 ff.) – Online-Durchsuchung.

Stufenmodells des BVerfG entsprechen dürfte (s. oben Kap. B. III. 1.).[1229] Dementsprechend forderte es, dass nur bei qualifiziertem Anlass sowohl hinsichtlich des geschützten Rechtsguts als auch des Grades der Beeinträchtigung und nur bei Schaffung ausreichender Verfahrensvorkehrungen zur (internen) Rechtmäßigkeitskontrolle eine solche Maßnahme erlaubt sei.[1230]

Aufgrund dieser verfassungsrechtlichen Absegnung bestehen gegen die aktuelle Ausgestaltung der besonderen Auskunftsverlangen in den Verfassungsschutzgesetzen, abgesehen von der Doppeltürenproblematik, keine durchschlagenden Bedenken. Sie können vielmehr als Richtanker für die Befugnisse der operativen Sicherheitsbehörden gesehen werden, da für jene traditionell höhere Anforderungen an (heimliche) Überwachungsmaßnahmen gestellt werden.[1231]

bb. Durchsetzbarkeit

Die Auskunftsersuchen stellen aufgrund der Verpflichtung – jedenfalls, soweit eine solche im Gesetz vorgesehen ist – gegenüber den unmittelbaren Maßnahmeadressaten Verwaltungsakte dar.[1232] Dasselbe gilt für die Landesgesetze, die eine Anordnung durch einen Landesminister vorsehen, wie etwa § 5b Abs. 4 S. 3 BWVSG. Gegenüber dem Betroffenen, also dem Dateninhaber, liegt hingegen mangels Bekanntgabe weiterhin nur ein Realakt vor.[1233]

1229 Dazu *Rusteberg*, KritV 2017, 24 (29 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 89 ff.; krit. *Tanneberger,* Sicherheitsverfassung, 2014, S. 234 f.

1230 BVerfGE 120, 274 (348 ff.) – Online-Durchsuchung.

1231 Vgl. BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.); NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Poscher/Rusteberg* KJ 2014, 57 (60 ff.); *Gärditz*, JZ 2013, 633 (634); *Gusy*, GA 1999, 319 (325 ff.); *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 245 ff.

1232 *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, Vi § 1 Rn. 11, der den VA aber in der Anordnung des BMI erkennt; aA. wohl VG Berlin, Urt. v. 23. 05.2013 – 1 K 194.11 (Feststellungsklage).

1233 *Son,* Heimliche Eingriffe, 2011, S. 96 ff.; *Deutsch,* Informationen, 1992, S. 279 f.; *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI §1 Rn. 14 jeweils mwN auch zur aA.

Die Durchsetzbarkeit der Auskunftsverlangen ist trotz VA-Qualität hoch umstritten.[1234] Mit Verweis auf das Trennungsprinzip[1235] wird vielfach davon ausgegangen, dass zwar eine Auskunftspflicht aufgrund der Auskunftsverlangen entsteht, eine Durchsetzung aber nicht möglich sei, da das Verlangen sonst den Charakter einer polizeilichen Maßnahme erhielte.[1236] Eine solche sollen die Nachrichtendienste aber gerade nicht durchführen können, § 8 Abs 3 BVerfSchG.

Nach § 8b Abs. 1 S. 1 BVerfSchG ergehen die Auskunftsersuchen nach Anordnung des Innenministeriums. Die Beamten der Nachrichtendienste müssen diese Anordnung beantragen. Es stellt sich daher die Frage, ob überhaupt ein Verwaltungsakt der Nachrichtendienste vorliegt, oder ob nicht die Anordnung durch das Innenministerium die Grundlage für das Auskunftsersuchen darstellt.[1237] Für diese gilt das Trennungsprinzip grundsätzlich nicht, weshalb eine Durchsetzung nach dem Vollstreckungsrecht des Bundes infrage käme. Dafür, dass die ministeriale Anordnung den Verwaltungsakt darstellt, lässt sich § 8b Abs. 4 BVerfSchG ins Feld führen, wonach, die Anordnung auch dem Verpflichteten mitgeteilt werden muss. Man könnte annehmen, dass die Auskunftspflicht erst durch die Mitteilung der Anordnung i. S. d. § 41 VwVfG bekanntgegeben wird. Die Nachrichtendienste agierten insofern nur als Boten des Innenministeriums.[1238]

Der Gesetzgeber ging bei der Schaffung der Auskunftsermächtigungen im Jahr 2001 aber ausdrücklich davon aus, dass die Auskunftsverlangen nicht mit Verwaltungszwang durchsetzbar sein sollten.[1239] Allerdings wird hiergegen durchaus scharfsinnig vorgetragen, dass die Anordnungen ursprünglich noch gem. § 8 Abs. 9 BVerfSchG aF[1240] vom Präsidenten des

1234 Ausf. *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 14 ff.

1235 Hierzu allg. *Gusy* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, IV § 1 Rn. 28 ff.; *ders.*, GSZ 2021, 141 (144 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 79 f.; *Poscher/Rusteberg* KJ 2014, 57 (58 ff.).

1236 *Mallmann* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BVerfSchG §8a Rn. 3; *Droste,* Hdb. VerfSchR, 2007, S. 233.

1237 *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 15; *Droste,* Hdb. VerfSchR, 2007; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 27.

1238 Ibid.

1239 BT-Drs. 14/7386, S. 39

1240 Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 11. Januar2002, BGBl. I, S. 361.

Bundesverfassungsschutzes erlassen wurden. Aus der Gesetzesbegründung von 2001 lässt sich somit in der Tat nichts für die Gegenwart herleiten, da zu diesem Zeitpunkt in jedem Fall von einem Verwaltungsakt des Bundesverfassungsschutzes ausgegangen werden musste.[1241] Ob das heute noch gilt, ist gerade fraglich. In der Gesetzesbegründung[1242] zum Terorrismusbekämpfungsergänzungsgesetz von 2007[1243], durch das die Anordnungskompetenz zum Innenministerium überging, wurde das Problem nicht mehr angesprochen, ebenso wenig in den jüngeren Gesetzesänderungen aus den Jahren 2011[1244] und 2020[1245].

Die Zuordnung der Auskunftsverlangen als Verwaltungsakte des Innenministeriums, vermag indes nicht zu überzeugen. Durch § 8a BVerfSchG wird ausdrücklich der Bundesverfassungsschutz ermächtigt, *im Einzelfall Auskunft einzuholen*. Die Stellung unmittelbar hinter § 8 BVerfSchG, der die (allgemeinen) „*Befugnisse*" des Bundesverfassungsschutzes regelt, zeigt auf, dass es sich bei § 8a BVerfSchG um spezielle Ermächtigungen des Nachrichtendiensts handelt. Auch § 8b Abs. 10 BVerfSchG spricht von den „*Befugnissen*" (der Dienste).[1246] § 8b BVerfSchG selbst ist hingegen als Verfahrensregel tituliert. Entsprechend ordnet § 8b Abs. 4 BVerfSchG nicht nur die Übermittlung der Anordnung an, sondern auch deren Form. Sie soll so ausführlich sein, „*als dies erforderlich ist, um ihm* (dem Dienst) *die Erfüllung seiner Verpflichtung zu ermöglichen*".

Die Anordnung des Innenministeriums stellt sich in dieser Systematik also nicht als konstituierendes Merkmal der Auskunftspflicht dar, sondern als deren formelle Voraussetzung.[1247] Ein Blick auf die Rechtsprechung zu Anordnungen anderer nachrichtendienstlicher Maßnahmen spricht ebenfalls für diesen Befund. Das BVerwG hat die Anordnung einer strategischen Telefonüberwachung nach §§ 5, 10 G-10 durch den BND als innerdienstliche Weisung qualifiziert, auch wenn es die Frage für individuelle Anordnungen offenlassen will.[1248]

1241 So *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 16.
1242 BT-Drs. 16/2921
1243 Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes (Terrorismusbekämpfungsergänzungsgesetz) vom 10. Januar 2007, BGBl. I., S. 2.
1244 BT-Drs. 17/6925
1245 BT-Drs. 19/25294
1246 Darauf weist *Fremuth*, AöR 2014, 32 (54) hin.
1247 Vgl. *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 29 f.
1248 BVerwG, NJW 2008, 2135 (2137).

Die Einordnung der Auskunftsersuchen als Verwaltungsakte der Nachrichtendienste führt auch nicht zu einem Widerspruch mit der Mitteilungspflicht des § 8b Abs. 4 BVerfSchG. Die Verpflichteten sollen nicht auf rechtswidrige Ersuchen antworten. Daher sind sie auf die Mitteilung der ministerialen Anordnung, ohne die das Auskunftsverlangen nicht rechtmäßig sein kann, angewiesen. In der Gesetzesbegründung von 2001 wurde die Mitteilungspflicht als Parallelregelung zu § 10 Abs. 6 G-10 verstanden.[1249] Dort heißt es: „*Die Anordnung ist dem (…) Verpflichteten insoweit mitzuteilen, als dies erforderlich ist, um ihm die Erfüllung seiner Verpflichtungen zu ermöglichen*". Auch hier ist ganz offensichtlich, dass die Anordnungsmitteilung eine verfahrenssichernde Wirkung hat und nicht selbstständig den bekanntgegebenen Verwaltungsakt darstellen soll.

Die Zuständigkeit des Innenministeriums für die Anordnung der Auskunft ändert daher nichts an der Einordnung dieser als Maßnahme des jeweiligen Nachrichtendienstes.[1250] Es handelt sich somit um Verwaltungsakte derselben.

Um die Frage, ob das Trennungsgebot einer Anwendung des Vollstreckungsrechts entgegensteht, käme man daher nicht herum. Jedenfalls für die klassischen Polizeimaßnahmen, denen per se ein Zwangsmoment innewohnt, ist das Verbots einer Anwendung durch die Nachrichtendienste jedenfalls einfachgesetzlich anerkannt, z. B. für Festnahmen, Vernehmungen, Beschlagnahmen oder Durchsuchungen.[1251] Ob die Durchsetzung von Informationsansprüchen damit ebenfalls ausgeschlossen sein soll, ist aber weiterhin unklar, denn anders als die genannten Maßnahmen ist die Informationsbeschaffung originäre Aufgabe der Nachrichtendienste.[1252] Einigkeit besteht allenfalls darin, dass die Nachrichtendienste ihre Informationen nicht selbst zur Gefahrenabwehr durch Zwangsmaßnahmen einsetzen dürfen.[1253] Die pauschale Aussage, dass den Nachrichtendiensten Ver- oder Gebotsverfügungen untersagt seien,[1254] lässt sich schon mit § 8b Abs. 6 BVerfSchG, der ja eine Pflicht deklariert, nicht mehr in Einklang bringen.

1249 BT-Drs. 16/2921, S. 15.
1250 So auch *Fremuth*, AöR 2014, 32 (54).
1251 BVerfG, NJW 2011, 2417 (2420); *Roggan/Bergemann*, NJW 2007, 876 (876); zur Frage des Verfassungsrangs nur *Ibler* in Dürig/Herzog/Scholz GG, Art. 87 Rn. 143.
1252 *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 20 ff.; *Poscher/Rusteberg* KJ 2014, 57 (59 ff.)
1253 *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 19; *Poscher/Rusteberg* KJ 2014, 57 (58).
1254 *Droste,* Hdb. VerfSchR, 2007, S. 294.

Schon deshalb kann aus ihr nicht hergeleitet werden – selbst, wenn man sie für zutreffend erachtet –, dass Informationspflichten nicht zwangsweise durchgesetzt werden könnten.[1255]

Die Frage ist indes zu groß, um in dieser Arbeit abschließend beantwortet werden zu können. Einer abschließenden Stellungnahme bedarf es hier auch nicht. Für die Bewertung der Informationserhebungs- und Weiterleitungsbefugnisse der FIU im Rahmen der Geldwäschebekämpfung, die im Fokus dieser Untersuchung steht, kommt es ohnehin auf das anerkannte informationelle Trennungsprinzip[1256] an (dazu Kap. G. III. 3.).

Auch das Bundesverfassungsgericht scheut seit jeher eine vertiefte Auseinandersetzung mit dem Trennungsgebot. Daher ist bis heute nicht klar, welchen Rang es im Verfassungsgefüge einnimmt und welche Folgen für den Gesetzgeber daraus konkret erwachsen.[1257]

Neben dem Verwaltungszwang wird eine weitere Durchsetzungsvariante in den Raum geworfen. Selbst wenn man die Auskunftsersuchen schon nicht für einen Verwaltungsakt oder für einen nicht-durchsetzbaren Verwaltungsakt hielte, bleibt stets die Frage offen, ob die von § 8b Abs. 6 BVerfSchG deklarierte Pflicht einfach gerichtlich einklagbar sein könnte.[1258] Ob diese Möglichkeit aber praxistauglich ist, darf bezweifelt werden. Durch die (öffentliche) Klage eines Nachrichtendienstes würde die Heimlichkeit der Maßnahme verlorengehen. Das Vorgehen dürfte sich für die Nachrichtendienste daher als zu riskant erweisen, da mit der Offenkundigkeit ein erheblicher Nachteil für die weiteren Ermittlungen einhergehen dürfte.

cc. Fazit

Festzuhalten ist, dass heimliche Zugriffe auf Kontoinhaltsdaten durch Auskunftsersuchen der Nachrichtendienste möglich sind und in der Praxis

1255 Offen auch bei *Poscher/Rusteberg* KJ 2014, 57 (58).

1256 BVerfGE 133, 277 – Antiterrordatei I ;E 156, 11 – Antiterrordatei II;, NJW 2022, 1583 (Rn. 171 ff.) – Bayerisches Verfassungsschutzgesetz; dazu nur *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 260 ff.; *Gärditz*, JZ 2013, 633; *Unterreitmeier*, DÖV 2021, 659; *Löffelmann*, GSZ 2021, 25 (33 ff.); *Gusy*, GSZ 2021, 141.

1257 Vgl. nur *Banzhaf,* Verfassungsschutz, 2021, 197 ff. *Gusy*, GSZ 2021, 141 (144 ff.).

1258 so *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 20 f.

stattfinden.[1259] Die Regelungen in manchen Ländern weisen aber die Unzulänglichkeit auf, dass sie die Verpflichtung der Institute zur Auskunftserteilung nicht ausdrücklich deklarieren. Es könnte daher an der erforderlichen *zweiten Tür* fehlen.[1260] Es stellt sich außerdem die Frage, ob die Institute sich weigern können, den Auskunftsersuchen nachzukommen. Eine Antwort auf diese Frage ließe sich allerdings nur aus einer vertieften Auseinandersetzung mit dem Trennungsgebot von Nachrichtendiensten und Polizei generieren. Eine solche kann und soll hier aber nicht geliefert werden.

Auch fehlt es in einigen Gesetzen an einer Sanktion, wenn die Institute gegen die Geheimhaltungspflicht verstoßen.[1261] Eine solche Pflicht findet sich indes in §§ 47 Abs. 1 Nr. 3 i. V. m. 56 Abs. 2 Nr. 7 GwG für Mitteilungen über Auskunftsverlangen nach § 30 Abs. 3 S. 1 GWG. Dieser Vorschrift soll sich im folgenden Abschnitt zugewandt werden.

b. Zugriffsrechte der FIU

Nach § 30 Abs. 3 S. 1GwG kann die FIU *„unabhängig vom Vorliegen einer Meldung Informationen von Verpflichteten einholen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.“* Durch diese Vorschrift wurde der FIU eine weitreichende, ausdrückliche Ermächtigung zum Abruf von Informationen bei Verpflichteten eingeräumt – noch bevor[1262] eine solche Vorschrift durch Einführung des Art. 31 Abs. 9 der 5. EU-GeldwäscheRL obligatorisch wurde. Der Gesetzgeber wollte mit § 30 Abs. 3 GwG den Art. 31 Abs. 3 S. 4 der 4. EU-GeldwäscheRL umsetzen.[1263] Da Art. 31 Abs. 3 S. 4 der 4. EU-GeldwäscheRL aber im Zusammenhang mit Verdachtsmeldungen steht, dürfte § 30 Abs. 3 GwG eine überschießende Umsetzung dargestellt

1259 BT-Drs. 18/5935, S. 25 ff; *InGFA*, (Bundesministeriums des Innern, für Bau und Heimat), Evaluation Terrorismusbekämpfungsgesetz, Juli 2018, S. 27 ff. *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 27, der auf einen Bericht der Bundesregierung hinweist, nach dem bis 2013 kein Auskunftsersuchen abgelehnt wurde

1260 Vgl. *Mallmann* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BVerfSchG § 8a Rn. 7.

1261 Dazu krit. *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1 Rn. 63.

1262 Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017 (BGBl I. S. 1822).

1263 BT-Drs. 18/11555, S. 141.

haben.[1264] Erst mit Art. 31 Abs. 9 der 5. EU-GeldwäscheRL hat der europäische Gesetzgeber eine Verpflichtung der Mitgliedstaaten zur Etablierung einer verdachtsunabhängigen Zugriffsnorm geschaffen.

Die Auskunftsersuchen der FIU dürften sich auf umfassende Informationen beziehen. Der Begriff der Informationen in § 30 Abs. 3 GwG ist mangels einschränkender Umschreibungen weit zu verstehen und schließt sämtliche Kontobestands- und Inhaltsdaten mit ein.[1265]

Weder § 30 Abs. 3 S. 1GwG noch die Finanzinformations-RL enthalten spezifische Voraussetzungen für die Ersuchen der FIU an die verpflichteten Institute – außer dass die Informationen für die Aufgaben der FIU *notwendig* sein müssen. Damit scheinen sämtliche Aufgaben gemeint – jedenfalls aber alle in § 28 GwG genannten. Da nach § 28 Abs. 1 S. 1 GwG nicht nur die *Erhebung und Analyse von Informationen im Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung,* sondern auch die *Weitergabe dieser Informationen an die zuständigen inländischen öffentlichen Stellen* zur Aufgabe der FIU gehört, dürfte auch § 32 Abs. 3 GwG als Aufgabe i. S. d. § 30 Abs. 3 S. 1 GwG zu verstehen sein.

Danach übermittelt die FIU *auf Ersuchen Daten aus Finanzinformationen und Finanzanalysen – auch, soweit sie personenbezogene Daten enthalten, an die Strafverfolgungsbehörden, das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst oder den MADG*. Es wäre also denkbar, dass die FIU Informationen bei den Instituten anfragt, um ein solches Ersuchen zu beantworten, wenn sie selbst die notwendigen Informationen noch nicht besitzt. In den Gesetzen für die Geheimdienste ist ein solches Vorgehen ausdrücklich verboten, § 17 Abs. 1 BVerfSchG, § 10 Abs. 3 BNDG, § 10 Abs. 4 MADG.

Gerade aber, weil der Gesetzgeber die FIU nicht mit den Geheimdiensten gleichsetzen wollte (dazu Kap. G. III. 3. b. (2)), lässt das Fehlen einer vergleichbaren Vorschrift im GwG durchaus den Schluss zu, dass die FIU aktiv Informationen erstmals einholen darf, nach denen sie von anderen Behörden ersucht wurden.

Verschiedene Sicherheitsbehörden inklusive der Staatsanwaltschaft könnten nach dieser Interpretation also über §§ 30 Abs. 3, 32 Abs. 3 GwG mittelbar auf Informationen der Verpflichteten zugreifen. Dies ist problematisch, da die Verpflichteten nach §§ 47 Abs. 1 Nr. 3 i. V. m. 56 Abs. 2 Nr. 7 GwG über die Ersuchen der FIU stillschweigen müssen. Den Sicher-

1264 *Barreto da Rosa* in Herzog GwG, § 30 Rn. 17.
1265 Idem, Rn. 19.

heitsbehörden könnten über §§ 32 Abs. 3, 30 Abs. 3 GwG also mittelbar die Ermächtigung zu heimlichen Auskunftsersuchen bei etlichen Privaten eingeräumt worden sein.

Über § 161a Abs. 1 S. 1 Alt. 2 StPO könnte die Staatsanwaltschaft zwar ohnehin die FIU zu Auskünften verpflichten. Erst durch § 32 Abs. 3 GwG würde aber die FIU ermächtigt, aufgrund der Anfragen der Sicherheitsbehörden eigene Auskunftsersuchen an die Verpflichteten zu richten.

§ 32 Abs. 3 GwG enthält keine spezifischen materiellen oder formellen Voraussetzungen für die Weiterleitung von Finanzdaten durch die FIU an die in der Vorschrift bezeichneten Sicherheitsbehörden. Solche Voraussetzungen sind vom europäischen Gesetzgeber auch nicht vorgesehen. Dieser hatte nach Erlass der 5. Geldwäsche-RL zwar eigens die Finanzinformations-RL für die Verwendung von Finanzdaten im Sicherheitsrecht erlassen. In Art. 7 der Finanzinformations-RL, der das Recht auf Ersuchen von Sicherheitsbehörden bei der FIU determiniert, finden sich aber ebenfalls keine spezifischen Voraussetzungen für die Anfragen.

Die Vereinbarkeit von § 30 Abs. 3 S. 1GwG bzw. Art. 31 Abs. 9 der 5. EU-Geldwäsche-RL mit höherrangigem Recht ist daher sehr zweifelhaft. Durch die Vorschriften wird einer staatlichen Behörde unmittelbar die Möglichkeit eingeräumt, Private zu einer Auskunft über sensible personenbezogene Daten zu verpflichten –Daten, die die Privaten aufgrund desselben Normenkomplexes für mindestens fünf Jahre aufbewahren müssen.

Da die FIU die Daten an verschiedene Sicherheitsbehörden weitergeben muss bzw. aufgrund derer Anfragen tätig werden kann, wird diesen mittelbar Zugriff auf einen vorgehaltenen Datenpool eingeräumt. Es bestehen daher mit Blick auf den Zugriff insbesondere der Staatsanwaltschaft über § 32 Abs. 3 GwG unübersehbare Parallelen zur Vorratsdatenspeicherung von TK-Verkehrsdaten.[1266]

Dass §§ 30 Abs. 3, 32 Abs. 3 GwG deshalb unter Anwendung des Art. 2 Nr. 5 EU-FinanzinformationsRL einschränkend auszulegen sind, soll später gezeigt werden. Darüber hinaus wirft die Übermittlung der FIU Fragen hinsichtlich der informationellen Trennung von Nachrichtendiensten und anderen Sicherheitsbehörden auf (zu beiden Fragen unten Kap. G. III 2. & 3.)

1266 Vgl. *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71 f.); *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 481 ff.; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (242 ff.) *ders.* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (896 ff.).

III. Zusammenfassung: Übersicht der Zugriffsrechte

Im vorangegangenen Kapitel wurden die Zugriffsrechte der Sicherheitsbehörden auf Finanzinformationen dargestellt, erläutert und analysiert. Es hat sich gezeigt, dass der Zugriff auf Kontodaten sowohl im Hinblick auf Bestands- als auch Inhaltsdaten schon seit geraumer Zeit ein typisches Ermittlungsinstrument darstellt.[1267]

Dabei erfolgt die Ermittlung klassischerweise individuell bezogen und offen. Sie unterscheidet sich insofern nicht von irgendeiner anderen Form der gefahrenabwehrrechtlichen oder strafverfahrensrechtlichen Informationsgewinnung. Allerdings liegen Finanzdaten naturgemäß massenhaft vor. Dieser Umstand hat in der jüngeren Vergangenheit zu Verschiebungen in der Gesetzgebung und Ermittlungspraxis geführt.

So hat der Gesetzgeber, noch bevor dies europarechtlich obligatorisch wurde, trotz erheblicher Kritik (s. Kap)[1268], die automatisierte und somit heimliche Abfrage von „Kontostammdaten" eingeführt, was vom BVerfG im ersten eigentlichen Bestandsdatenurteil gebilligt wurde.[1269]

Die Staatsanwaltschaft nutzt aber nicht nur Bestandsdaten, sondern greift auch auf Kontoinhaltsdaten zu. Das BVerfG hat es ihr sogar gestattet, Auskunftsersuchen an Kreditinstitute zu richten, die nicht auf eine bestimmte Person gerichtet sind, sondern Verdachtspersonen durch Rastern der Datensätze erst zutage fördert.[1270] Immerhin erfolgt die Massenabfrage von Kontoinhaltsdaten nach der Ermittlungsgeneralklausel nicht heimlich, sondern nach den allgemeinen Regeln der Waffengleichheit im Strafverfahren.[1271] Im Polizeirecht gilt äquivalent der Grundsatz der Offenheit polizeirechtlicher Ermittlungen. Heimliche Auskunftsersuchen bei Kredit- und anderen Finanzinstituten stehen daher allein den Nachrichtendiensten zu, etwa nach § 8a Abs.1 Nr. 2 BVerfSchG.[1272]

Der Ausschluss heimlicher Ermittlungen von Kontoinhaltsdaten im Rahmen der klassischen Sicherheitsgesetze wird durch die Regeln des Anti-

1267 *Kahler,* Kundendaten, 2017, S. 31 ff.; *Reichling*, JR 2011, 12; *Wonka*, NJW 2017, 3334 (3337 f.).
1268 Übersicht bei *Pfisterer*, JöR 2017, 393; *Degen,* Geldwäsche, 2009, S. 273 ff.
1269 BVerfGE 118, 168 – Kontostammdaten
1270 BVerfG, NJW 2009, 1405
1271 *Ransiek*, wistra 1999, 401.
1272 Zu diesen etwa *Fremuth*, AöR 2014, 32 (53 ff.); *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 27; *Gärditz* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, VI § 1.

Geldwäscherechts durchbrochen. Die FIU analysiert nicht nur Meldungen der Geldwäscheverpflichteten nach § 43 Abs. 1 GwG, sondern kann nach § 30 Abs. 3 GwG auch ohne vorherige Meldung bei den Verpflichteten Auskünfte zu sämtlichen[1273] Finanzinformationen abfragen. Über solche Auskunftsersuchen haben die adressierten Institute unter Bußgeldandrohung Stillschweigen zu bewahren, §§ 47 Abs. 1 Nr. 3 i. V. m. 56 Abs. 2 Nr. 7 GwG.

Das Auskunftsrecht der FIU geht einher mit der Möglichkeit von Staatsanwaltschaften, bei der FIU um Auskünfte zu ersuchen, § 32 Abs. 3 S. 1 GwG. Somit besteht die Möglichkeit, dass Staatsanwaltschaften mittelbar einen heimlichen Zugang zu bei Privaten gespeicherten Finanzinformationen erhalten. Die Ermittlungsprinzipien der StPO drohen insofern umgangen zu werden. Wie dieses Problem grundrechtlich zu lösen sein könnte, soll später besprochen werden (Kap. G. III. 2. c.)

1273 *Barreto da Rosa* in Herzog GwG, § 30 Rn. 19.

Kapitel F: Diskussion der massenhaften Speicherung und Nutzung von Finanzdaten zu sicherheitsrechtlichen Zwecken

Über die Speicherung von Finanzdaten, deren Verwendung bei den Instituten und den Zugriff der Sicherheitsbehörden auf diese Daten wird bereits seit geraumer Zeit diskutiert (zur Gesetzeshistorie oben Kap. D. III. 2. a.) Die jeweiligen Änderungen an den entsprechenden Gesetzen wurden fachbereichsübergreifend sowohl im banken- als auch im sicherheitsrechtlichen Kontext kommentiert.

Dabei wurden immer wieder verfassungs- und europarechtliche Zweifel gegenüber der Bestandsdatenspeicherung und dem Geldwäscherecht erhoben. In diese Kritik wird sich diese Arbeit einreihen und die jüngsten strukturellen und konkreten Entwicklungen des Sicherheitsverfassungsrechts ergänzen (s. Kap. G).

Da sie insofern an Vorarbeiten bzw. frühere Kritiken anschließt und nicht in Anspruch nehmen will, erstmals allgemeine rechtliche Zweifel an den geldwäscherechtlichen Überwachungsmaßnahmen zu formulieren, soll die historische Diskussion über die verschiedenen Speicherpflichten und Zugriffsrechte im Anti-Geldwäscherecht in vollem Umfang chronologisch dargestellt und kommentiert werden.

I. Kontobestandsdaten

Zunächst soll die Diskussion über die Bestandsdatenauskunft nach § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO dargestellt werden. Anders als bzgl. der Speicherung von Kontoinhaltsdaten hat das BVerfG hierzu bereits in einem Beschluss aus dem Jahr 2007 Stellung bezogen.[1274] Diese Rechtsprechung soll für die Darstellung der Kommentierung als Anker dienen. Die folgenden Abschnitte sind daher chronologisch in die Zeit bis zum Beschluss und jener danach aufgeteilt.

1274 BVerfGE 118, 168 – Kontostammdaten

1. Diskussion bis zur Klärung durch das BVerfG

§ 24c KWG war gleich bei seiner Einführung und in den unmittelbar darauffolgenden Jahren auf breite Kritik aus verschiedenen Fach- und Rechtsbereichen gestoßen. Die Beeinträchtigung der informationellen Selbstbestimmung durch die Bestandsdatenabfrage sah bereits der Bundesrat kritisch.[1275] In seiner Stellungnahme zum Regierungsentwurf stellte er den Umfang der zu speichernden Daten und das Fehlen einer Kontrollinstanz beim Datenzugriff, etwa durch Richtervorbehalt, infrage.[1276] Außerdem sollte die Bundesregierung prüfen, ob durch die Möglichkeit des Auskunftsersuchen durch die Strafverfolgungsbehörden bei der BaFin nicht Voraussetzungen der StPO, die bestimmte Auskunftsersuchen auf schwere Straftaten begrenzt, umgangen würden.[1277]

Trotz dieser Zweifel regte der Bundesrat aber auch Änderungen an, die den Umfang der Bestandsdatenauskunft erweiterten.[1278] So war im Regierungsentwurf noch vorgesehen[1279], dass eine Auskunft nicht solchen Behörden erteilt werden darf, die Steuerstraftaten verfolgen. Der Bundesrat fürchtete einerseits eine Auslegung dieser Einschränkung dahingehend, dass somit alle Strafverfolgungsbehörden ausgenommen werden könnten, die zumindest auch Steuerstraftaten verfolgen. Da dies den gesamten Strafverfolgungsapparat beträfe, könnte die Norm leerlaufen.[1280] Andererseits würden bei der intendierten Auslegung, die nur die spezifischen Behörden zur Verfolgung von Steuerstraftaten adressierte, Steuerstraftaten privilegiert, was der Bundesrat ebenfalls ablehnte. Er schlug daher vor, die Bereichsausnahme für Steuerstraftaten zu streichen.[1281]

Auch aus der Finanzwirtschaft wurde schon im Zuge der Gesetzeseinführung Kritik laut. Der Zentrale Kreditausschuss (heute: „Deutsche Kreditwirtschaft" – DK) machte in seiner Stellungnahme zum Gesetzesentwurf darauf aufmerksam, dass von der Regelung über 400 Millionen Konten betroffen wären.[1282] Auf diese könnte die BaFin – und über sie die Strafver-

1275 BT-Drs. 14/8017, S. 168
1276 Ibid.
1277 Ibid.
1278 Vgl. *Zubrod*, WM 2003, 1210 (1211).
1279 BT-Drs. 14/8017, S. 48, 168.
1280 Idem, S. 169.
1281 Ibid.
1282 *ZKA,* Stellungnahme zum 4. Finanzmarktförderungsgesetz, AZ: 413-FPLD, 13. Februar 2002, S. 8.

folgungsbehörden – ohne Anfrage, ohne Kenntnismöglichkeit und gänzlich ohne Kontrollmechanismen zugreifen.[1283] Das Verfahren sei letztlich eine „Outsourcing-Variante" des gesellschaftlich umstrittenen Kontenzentralregisters und greife unverhältnismäßig in die Rechte der betroffenen Kunden ein.[1284] Die Bestandsdaten seien auch an sich nutzlos und dienten nur einer Verkürzung der Verfahrensdauer, da im Anschluss an das Auffinden eines Konto ja weiterhin noch im Einzelfall die Umsatzdaten angefragt werden müssten. Eine Kontaktaufnahme mit den ca. 2.900 Kreditinstituten gleichzeitig zur Feststellung, ob und wo eine bestimmte Person ein Konto führt, sei aber derzeit technisch gar kein Problem mehr. Es bestünde sogar schon ein internes System, mit dem das BKA Suchanfragen automatisch an alle Institute weiterleiten könne.[1285] Das (voll-)automatisierte System mit heimlichem Zugriff direkt durch eine staatliche Stelle sei daher nicht erforderlich.[1286]

Lehnhoff, Mitglied des Vorstands des Bundesverbandes der Deutschen Volks- und Raiffeisenbanken, meldete ebenfalls verfassungsrechtliche Kritik an.[1287] Die Möglichkeit von Auskunftsersuchen an die Kreditinstitute stelle den milderen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Kontoinhaber dar. Dass diese so zeitaufwendig wären, läge an der ineffizienten Verwaltung.[1288] Dies sei aber nicht das Problem der Bürger, sondern des Staates und dürfe deshalb nicht zulasten der Grundrechtsträger gelöst werden.[1289] Die automatisierte geheime Abfrage bedeute, dass jeder Bürger ständig mit einem Eingriff in seine Daten rechnen müsse. Insofern würden die Bürger unter einen Generalverdacht gestellt.[1290] Weiter sei es rechtsstaatlich bedenklich, dass die Prüfung der Legitimität eines Auskunftsersuchens bei der BaFin nur im Ausnahmefall kontrolliert würde.[1291]

Vergleichbare Äußerungen wurden auch von rechtswissenschaftlicher Seite vorgetragen. Aufgrund der fehlenden Kontrollmechanismen, der Heimlichkeit des Eingriffs und der breiten Betroffenheit der Bevölkerung

1283 Ibid.
1284 Ibid.
1285 Idem, S. 8 f.
1286 Idem, S. 9.
1287 *Lehnhoff*, WM 2002, 687.
1288 Ibid.
1289 Ibid.
1290 Ibid.
1291 Ibid.

wurde die Maßnahme von einigen Autoren ebenfalls als unverhältnismäßig erachtet.[1292] Teilweise war dieses Ergebnis aber auf bestimmte Einzelregelungen begrenzt, etwa auf den erweiterten Kreis der abfrageberechtigten Behörden in § 93 Abs. 8 AO, und nicht generell auf die Bestandsdatenabfrage i. S. d. § 24c KWG.[1293]

Diejenigen Autoren, die die Bestandsdatenabfrage umfänglich für einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung erachteten, stützten diesen Befund auf die fehlenden Eingriffsvoraussetzungen. Das KWG selbst sah und sieht keine besonderen Voraussetzungen vor. Die Ersuchen richten sich stattdessen nach den Vorschriften der jeweiligen Behörden (s. Kap. D. I. 2.). Für die Staatsanwaltschaften kommt dabei nur die Generalklausel für behördliche Ersuchen des § 161 Abs. 1 S. 1 Hs. 1 Alt. 1 StPO in Betracht.[1294] Diese erfordert lediglich einen Anfangsverdacht.

Von den Kritikern wurde nun vorgebracht, dass diese Anforderung nicht der intensiven Wirkung der Bestandsdatenabfrage gerecht würde. Diese sei nicht mit einer gewöhnlichen Auskunft zu vergleichen, sondern mit einer Rasterfahndung oder Telekommunikationsüberwachung, da sie flächendeckend und heimlich erfolge und in eine vertrauliche Beziehung eingreife.[1295]

Vonseiten einiger Datenschutzbeauftragter wurde des Weiteren das Fehlen datenschutzrechtlicher Standards angemahnt. Insbesondere erfordere das Transparenzgebot, dass die Betroffenen über eine Anfrage informiert würden. Entsprechende Schutzvorschriften wurden jedenfalls für § 93 Abs. 7, 8 AO gefordert.[1296]

Neben der Verhältnismäßigkeit nahmen verschiedenen Beiträge auch die Bestimmtheit der Vorschriften, insb. des § 93 Abs. 8 AO, ins Visier. In

1292 *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.); aA. *Kokemoor*, BKR 2004, 135; *Rüpke* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 55 Rn. 8 ff., 13.

1293 *Göres*, NJW 2005, 253 (256).

1294 *Zubrod*, WM 2003, 1210 (1214).

1295 *Samson/Langrock,* Gläserner Bankkunde, 2005, 17 ff., 78 ff.; *Degen,* Geldwäsche, 2009, S. 293 ff.; *Zubrod*, WM 2003, 1210 (1214); *Widmaier*, WM 2006, 116 (118 ff.); *Hamacher*, DStR 2006, 633 (637).

1296 *DSB BW,* 25. Tätigkeitsbericht, 2004, S. 141; *DSB NRW,* 17. Datenschutzbericht, 2004, S. 145.

seiner Ursprungsfassung aus dem Jahr 2003 sah § 93 Abs. 7, 8 AO[1297] noch vor, dass nur Finanzbehörden über das BZSt eine Bestandsdatenabfrage entsprechend § 24c KWG vornehmen können. Nach § 93 Abs. 8 AO 2003 sollten aber alle Behörden, die für ein Gesetz zuständig sind, das an *„Begriffe des EstG anknüpft"*, ein Finanzamt um Auskunft erbeten können, das dann über das BZSt eine Bestandsdatenabfrage durchführt.

Diese Formulierung wurde in der Literatur umgehend kritisiert. Es sei nicht klar, wann ein Gesetz an *„Begriffe des EStG anknüpfen"* würde, da schon nicht festgeschrieben wurde, welche Begriffe damit gemeint sein sollten. Der Gesetzgeber hatte zwar in der Gesetzesbegründung einige Beispielsbegriffe genannt, etwa „Einkünfte, Einkommen oder zu versteuerndes Einkommen",[1298] die Aufzählung war aber nicht abschließend. Da das EStG eine Vielzahl weiterer vergleichbarer Begriffe enthielt, die zwangsläufig in anderen Gesetzen vorkamen, wurde der Kreis der berechtigten Behörden als zu unbestimmt kritisiert.[1299] Um Abhilfe bei der Auslegung zu schaffen, erließ das Finanzministerium einen Anwendungserlass (AEAO).[1300] In Nr. 3.2. AEAO wurde festgestellt, dass sich § 93. Abs. 9 AO 2003 ausschließlich auf Sozialbehörden und Sozialgerichte bezieht.

Dieser Anwendungserlass führte immerhin dazu, dass das BVerfG einem Eilantrag gegen § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO nicht stattgab.[1301] Zwar erkannte es ebenfalls, dass § 93 Abs. 8 AO nicht zu entnehmen ist, welche Behörden und Gerichte bei den Finanzbehörden anfragen dürfen. Aufgrund des Anwendungserlasses sei aber anzunehmen, dass diese nur auf Anfragen der in Nr. 3.2. AEAO bezeichneten Behörden reagieren würden. Die mangelnde Bestimmtheit würde sich daher faktisch nicht negativ auswirken, weshalb im Rahmen der Folgenabwägung (noch) zugunsten des Gesetzgebers entschieden werden müsste.[1302]

1297 Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003, BGBl. I, S. 2928

1298 BT-Drs. 15/1309, S. 12; BR-Drs. 542/03, S. 19.

1299 *Göres*, NJW 2005, 253 (255); *Kühling*, ZRP 2005, 196 (198 f.) *DSB NRW,* 17. Datenschutzbericht, 2004, S. 145; *DSB BW,* 25. Tätigkeitsbericht, 2004, S. 141; krit. auch *Widmaier*, WM 2006, 116 (117).

1300 *BFM*, Anwendungserlass zur Abgabenordnung (AEAO); Regelungen zu §§ 92 und 93 AO (Auskunftsersuchen; Kontenabruf) vom 10.03.2005, BStBl. I, S. 422.

1301 BVerfGE 112, 284.

1302 Idem, (301 f.); krit. *Florian*, BKR 2005, 202 (204).

2. Die Entscheidung des BVerfG im Jahr 2007

In der Hauptsache stellte das BVerfG dann jedoch fest, dass § 93 Abs. 8 KWG 2003 in der Tat unbestimmt und daher nichtig sei.[1303] Eine weite Auslegung der Vorschrift würde dazu führen, dass bei jeder begrifflichen Übereinstimmung eines Gesetzes mit dem EStG der Anwendungsbereich des § 93 Abs. 8 KWG eröffnet würde. Da das EStG alle möglichen Begriffe beinhalte, wäre die Menge der nach § 93. Abs. 8 KWG berechtigten Behörden letztlich unübersehbar.[1304] Das würde selbst dann gelten, wenn man § 93 Abs. 8 KWG eng auslegte und nur auf spezifisch steuerrechtliche Begriffe abstellen würde, wie es die Gesetzesbegründung nahelegte[1305], da auch diese in allen möglichen Gesetzen vorkämen.[1306] Dem Gesetzgeber wäre es ohne weiteres möglich gewesen, die berechtigten Stellen einfach aufzuzählen, wie es letztlich in Nr. 3.2. AEAO denn auch geschehen war.[1307] Die gesetzliche Unbestimmtheit würde durch den Anwendungserlass auch nicht geheilt.[1308]

a. Verhältnismäßigkeit

Im Übrigen stellte das BVerfG keine Unverhältnismäßigkeit der Bestandsdatenabfrage nach § 24c KWG, §§ 93b, 93. Abs. 7AO fest.

Die automatisierte Bestandsdatenabfrage wäre erforderlich im Sinne eines mildesten Mittels. Zwar befand auch das BVerfG, dass Einzelabfragen bei sämtlichen Instituten prinzipiell möglich wären, da sie aber aufwendiger seien und in ihrem Rahmen sämtliche Banken und andere Institute Kenntnis von den Ermittlungen erhielten, seien Einzelabfragen weder gleich geeignet noch ein milderes Mittel.[1309] Hierbei ist bemerkenswert, dass das BVerfG in der Heimlichkeit aufgrund der Automatisierung nach § 24c Abs. 1 S. 6 KWG nicht nur ein intensivierendes Merkmal, sondern einen Umstand erkannte, der sich als schützend für die Rechte des Betroffenen herausstellte. Auf diese Ambivalenz der Heimlichkeit bei Auskunftser-

1303 BVerfGE 118, 168 (188 ff.) – Kontostammdaten.
1304 Idem, (189).
1305 BT-Drs. 15/1309, S. 12.
1306 BVerfGE 118, 168 (189.) – Kontostammdaten.
1307 Idem, (190) mit Verweis auf *Kühling*, ZRP 2005, 196 (199).
1308 BVerfGE 118, 168 (191) – Kontostammdaten.
1309 Idem, (194 f.)

suchen gegenüber privaten Dritten ging das Gericht aber nicht vertiefend ein.

Die Kontobestandsdatenabfrage sei auch nicht unangemessen. Sowohl die funktionierende Strafverfolgung, die Herstellung von Steuergerechtigkeit als auch das Bekämpfen von Betrug bei Sozialleistungen seien Gemeinwohlbelange von erheblicher Bedeutung.[1310] Dazu stünde der Eingriff in das Recht auf informationelle Selbstbestimmung der von den Auskünften Betroffenen nicht außer Verhältnis. Bei der Prüfung dessen Intensität berücksichtigte das BVerfG die Heimlichkeit, den Charakter der erlangten Daten und die Wahrscheinlichkeit des kausalen Eintretens weiterer Nachteile aufgrund der Datenabfrage.

Die Heimlichkeit bewertete das BVerfG dabei anders als noch im Rahmen der Erforderlichkeit pauschal als intensivierend.[1311] Das war mit Blick auf die frühere Rechtsprechung auch nur konsequent.[1312] Es stellte fest, dass aufgrund der heimlichen Erhebung eine Benachrichtigung des Betroffenen notwendig sein kann, da diesem ansonsten ein effektiver Rechtsschutz verwehrt bliebe. Insofern ging es auf die Kritik der Datenschützer ein, die auf das Fehlen von Benachrichtigungspflichten aufmerksam gemacht hatten. Zum Zeitpunkt des Beschlusses war jedenfalls für § 93 AO auch schon die Einführung einer Benachrichtigungspflicht vorgesehen (heute § 93 Abs. 9 S. 2 AO).[1313]

Aber auch die zum Zeitpunkt der Entscheidung bestehenden Fassungen der § 93 Abs. 7,8 AO und § 24c KWG, der noch heute keine Benachrichtigungspflicht vorsieht, hielt das BVerfG nicht wegen fehlender Benachrichtigungspflichten für unverhältnismäßig. Eine Benachrichtigungspflicht würde sich stattdessen nach dem jeweils einschlägigen Verfahrensrecht bestimmen. Die Behörden könnten ausgehend vom Verhältnismäßigkeitsprinzip im Einzelfall eigenständig entscheiden, ob sie ihr Vorgehen nachträglich offenbaren würden oder nicht. Dies hielt das BVerfG für ausreichend und verlangte nicht, dass eine grundsätzliche Benachrichtigungspflicht eigens deklariert werden müsste.[1314]

1310 Idem, (195 f.).
1311 BVerfGE 118, 168 (197 f.) – Kontostammdaten.
1312 BVerfGE 115, 166 (194); E 141, 220 (269 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 247 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 165 ff.; *Löffelmann*, GSZ 2019, 16 (19) jeweils mwN.
1313 BT-Drs. 16/4841, S. 23.
1314 BVerfGE 118, 168 (200, 210 ff.) – Kontostammdaten.

Aus dem Charakter der Daten und aufgrund der Auskunft drohender weiterer Nachteile folgerte das Gericht keine gesteigerte Intensität. Stattdessen stellte es fest, dass es sich bei Kontobestandsdaten prinzipiell um die am wenigsten sensiblen Daten im Finanzbereich handelt. Es sei fast ausgeschlossen, dass sie allein zu einem Ermittlungserfolg führen. Vielmehr dienten sie lediglich als Bestimmung des Ortes, an dem dann Inhaltsdaten erhoben werden können, etwa Kontobewegungen. Das bedeute zwar, dass die Bestandsdaten stets zu weiteren Ermittlungen und damit zu einem Nachteil führen, dieser Nachteil sei aber gerade der offensichtliche Zweck der Erhebung. Die Rechtmäßigkeit der darauffolgenden Erhebung sei davon abzugrenzen und eigenständig zu berücksichtigen.[1315]

b. Das Urteil aus heutiger Sicht

Das Verhältnis der verschiedenen in § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO enthaltenen Ermächtigungen wurde in dem Beschluss zu den Kontobestandsdaten nur rudimentär behandelt. Blickt man mit dem heutigen Kenntnisstand bzw. mit dem von der Rechtsprechung entwickelten Modell der „Doppeltür"[1316] auf die Vorschriften, erkennt man in den Normen drei separate Teilregelungen.

Zunächst ergibt sich aus § 24c Abs. 1 KWG und § 93b Abs. 1 AO die Pflicht verschiedener Institute, eine automatisch zugängliche Datei über Kontobestandsdaten für die BaFin und das BZST bereitzuhalten. Diese Pflicht wird heute durch § 27 Abs. 2 ZAG und § 28 Abs. 1 S. 2 KAGB auf weitere Institute ausgedehnt. § 24c Abs. 2 KWG, § 93 Abs. 2 S. 1 Hs. 1 AO ermächtigen sodann die BaFin und das BZSt, auf dieses Dateisystem zuzugreifen und Daten abzurufen. Aus diesen Vorschriften ergibt sich aber noch nicht das Recht, diese Daten an verschiedene Behörden weiterzuleiten. Dieses folgt erst aus § 24c Abs. 3 KWG, §§ 93b Abs. 2 S. 1 HS. 2, 93 Abs. 7, 8 AO.

Was die § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO nicht regeln, ist das Recht der einzelnen Behörde, bei der BaFin oder dem BZSt um Auskunft zu ersuchen. Dieser vierte Schritt wird in dem Recht der jeweiligen Behörde geregelt. Diese Erkenntnis hatte das BVerfG im Jahr 2007 jedenfalls noch

1315 Idem, (198 f.).

1316 BVerfGE 130, 151 (184, 193 ff.) – Bestandsdatenauskunft I; E 155, 119 (142 ff.) – Bestandsdatenauskunft II; dazu *Graulich*, NVwZ-Beilage 2020, 47 (48 f.).

nicht vollständig erlangt. So stellte es fest: *„§ 24 c Abs. 3 Satz 1 Nr. 2 KWG ermächtigt (…) die zur Verfolgung und Ahndung von Straftaten zuständigen Behörden und Gerichte dazu, Abrufersuchen zu stellen*".[1317] Offenbar ging das Gericht also davon aus, dass §24c Abs. 3 KWG auch als Ermächtigung der anfragenden Behörde für das Ersuchen gegenüber der BaFin bzw. dem BZSt zu verstehen ist. Das wäre heute nicht mehr haltbar. Gleichzeit erkannte es aber, dass § 24c Abs. 3 KWG die Auskunftserteilung davon abhängig mache, dass das Ersuchen aus Sicht der anfragenden Behörde erforderlich ist.[1318] Daraus leitete es eine (Rechtsgrund-)Verweisung des § 24c Abs. 3 auf das jeweilige Verfahrensrecht der Behörde ab und stellte fest, dass ein Ersuchen der Staatsanwaltschaft ein konkretes Ermittlungsverfahren voraussetzt.[1319] Es ging aber nicht den entscheidenden Schritt einer Festlegung der Ermächtigungsgrundlage in der StPO, obwohl schon der Gesetzgeber in der Gesetzesbegründung erkannt hatte, dass sich das Ersuchen aus Sicht der Staatsanwaltschaft nach den allgemeinen Regeln der §§ 152 Abs. 2, 160 StPO richten müsste.[1320] Wie auch das Gericht ging er also von einer Art hybriden Konstellation aus, nach der § 24c Abs. 3 KWG zwar eine Ermächtigung u. a. der Staatsanwaltschaft enthielt, die Voraussetzungen aber aus der StPO folgen würden.

Dogmatisch korrekt wäre es (jedenfalls nach dem heutigen Erkenntnisstand) gewesen, die Ermächtigungsgrundlage für das Ersuchen an die BaFin in § 161 Abs. 1 S. 1 Alt. 1 StPO zu verorten. Diesen finalen Schritt ist der Gesetzgeber aber wie auch das BVerfG nicht gegangen.

In der Literatur war dieses – heute gängige[1321] – Ergebnis hingegen schon früh vorgeschlagen worden[1322]. Sie blieb insofern aber vom BVerfG unberücksichtigt.

c. **Reaktion**

Seit dem Beschluss des BVerfG ist die Diskussion über die Kontostammdatenauskunft verständlicherweise etwas eingeschlafen. Dabei geben die

1317 BVerfGE 118, 168 (191) – Kontostammdaten.
1318 Ibid.
1319 Ibid.
1320 BT-Drs. 14/8017, S. 123.
1321 OLG Stuttgart, NStZ 2016, 48 (48); *T. Knierim* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 10 Rn. 55.
1322 *Zubrod*, WM 2003, 1210 (1214).

Beschlüsse zur Bestandsdatenauskunft im Bereich der Telekommunikation durchaus Anlass, die Entscheidung aus dem Jahr 2007 einer Revision zu unterziehen.

Die unmittelbaren Reaktionen auf den Beschluss zu den Kontobestandsdaten waren zunächst ernüchtert. Teilweise wurde die Entscheidung als Erweiterung der gesetzlichen Spielräume zu heimlichen Überwachungsmaßnahmen eingeschätzt, die weitere Eingriffe in die Persönlichkeitsrechte im Rahmen der Terrorismusbekämpfung und Steuererhebung befürchten ließen.[1323] Manche sahen durch die Aufrechterhaltung von § 24c KWG und §§ 93b, 93 Abs. 7, 8 AO gar den „gläsernen Bankkunden" zur Realität werden.[1324]

Erwartungsgemäß wurden in der Urteilskritik die schon zuvor diskutierten Verhältnismäßigkeitsaspekte vorgebracht. Dem Gericht wurde vorgeworfen, die aufgrund der Streubreite und Heimlichkeit sehr hohe Eingriffsintensität verkannt zu haben und deshalb fälschlicherweise auf notwendige Voraussetzungen sowohl in materieller als auch verfahrensrechtlicher Hinsicht verzichtet zu haben.[1325]

In einer späteren Betrachtung wurden die strukturellen Aussagen des Beschlusses kritisiert. Durch die Darstellung der Bestandsdatenabfrage als prinzipiell geringfügigen Eingriff würde eine Datenkategorisierung vorgenommen und damit von der ehemaligen Vorstellung des BVerfG abgerückt, sodass die Art der Daten sich auf deren Aussagekraft nicht mehr auswirken könne.[1326] Anders als das BVerfG meint, sei die Bestandsdatenerhebung nicht isoliert von den Maßnahmen zu betrachten, die auf ihrer Basis erst ermöglicht würden. Gerade in der komplexen Betrachtung von Daten bzw. deren Verarbeitungs- und Verknüpfungsmöglichkeiten[1327] habe die Originalität des Volkszählungsurteils gelegen.[1328] Die Abkehr von diesem Blickwinkel sei unbefriedigend.[1329] Insgesamt zeige das BVerfG danach die Bereitschaft, eine breite Präventivzugänglichkeit von Daten in Abhängigkeit

1323 *Gregor*, EWiR 2008, 189 (190).
1324 *Tolani*, BKR 2007, 275 (281); so schon *Samson/Langrock,* Gläserner Bankkunde, 2005.
1325 Ausf. *Reichling,* Kontenabfrage, 2010, S. 129 ff.
1326 *Pfisterer*, JöR 2017, 393 (412 ff.).
1327 BVerfGE 65, 1 (45) – Volkszählung.
1328 *Pfisterer*, JöR 2017, 393 (413).
1329 Ibid.

der Datenart zuzulassen, wobei den Finanzdaten nicht der angemessene Persönlichkeitswert zuteil würde.[1330]

3. Klärung durch den EuGH? *Ministerio Fiscal.*

Auch der EuGH hat sich mit der Zulässigkeit sicherheitsrechtlicher Abfragen von (Telekommunikations-)Bestandsdaten befasst. Die Wertung des Gerichtshofs kann aufgrund der Vergleichbarkeit der Datensätze auf die Kontobestandsdatenabfrage übertragen werden.

In der Sache *Ministerio Fiscal*[1331] hatte ein spanisches Gericht dem EuGH die Frage vorgelegt, ob das EU-Recht ein polizeiliches Auskunftsersuchen nach Vertragsdaten bei Telekommunikationsprovidern unter die Voraussetzung stellt, dass die Abfrage der Verfolgung oder Verhütung einer schweren Straftat dient. Bei dem Verfahren ging es damit ausdrücklich nicht um die Speicherpflicht der Bestandsdaten, sondern allein um die Voraussetzungen, unter denen das nationale Sicherheitsrecht der Mitgliedstaaten einen Zugriff von Bestandsdaten zulassen dürfe.[1332]

In den Entscheidungen zur Vorratsdatenspeicherung von TK-Verkehrsdaten hatte der EuGH darauf bestanden, dass eine retrograde Abfrage solcher Daten nur zur Bekämpfung schwerer Straftaten zulässig sei.[1333] Dies folge aus Art. 15 der ePrivacy-RL (s. o. Kap. C. II. 1. a. bb.).[1334] Ob diese Rechtsprechung auf Bestandsdaten zu übertragen sei, war Gegenstand der Vorlagefrage.

In seiner Antwort stellte der Gerichtshof diesbezüglich klar, dass Art. 15 der ePrivacy-RL nicht in jedem Fall den Zugang zu Telekommunikationsdaten auf den Bereich der schweren Kriminalität begrenze. Die Norm eröffne vielmehr grundsätzlich die Möglichkeit zur Beeinträchtigung der Privatheitsrechte im Bereich der Telekommunikation durch das nationa-

1330 *Hartmann* KJ 2007, 2 (17 f.); *Pfisterer*, JöR 2017, 393 (421).
1331 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal) = NJW 2019, 655.
1332 Idem, Rn. 49.
1333 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 115 ff. = NJW 2017, 717; EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 27 ff. = NJW 2021, 2103.
1334 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, ABl. 2002, L 201/37.

le Sicherheitsrecht. Die besonderen Voraussetzungen für den Zugang zu Verkehrs- oder Standortdaten ergäben sich erst aus der Anwendung des Verhältnismäßigkeitsgrundsatzes.[1335] Ursächlich für die gesteigerten Anforderungen an die Abfrage von Verkehrsdaten sei die Erheblichkeit des damit verbundenen Eingriffs. Für diese wiederum kommt es nach dem EuGH darauf an, wie ausführlich sich die privaten Lebensumstände einer Person aus den entsprechenden Daten ableiten lassen („profiling", dazu auch Kap. III. 1. b. bb. (1)).[1336]

Unter Rückgriff auf diese Maßstäbe kam der EuGH in *Ministerio Fiscal* zu dem Ergebnis, dass der Zugriff von Sicherheitsbehörden auf Bestandsdaten, d. h. Daten, aus denen sich allein die Identität eines SIM-Karteninhabers, bzw. Geräte- oder Nummerninhabers ergebe, keine schwere Beeinträchtigung der Grundrechte aus Art. 7, 8 EU-GRC darstelle. Aus solchen Daten ließen sich keine weitergehenden Rückschlüsse auf das Privatleben des Betroffenen erzielen.[1337] Konsequenterweise verlange das EU-Recht bzw. Art. 15 der ePrivacy-RL in Verbindung mit Art. 7, 8 EU-GRC nicht, dass die nationalen Gesetzgeber die Abfrage von TK-Bestandsdaten nur zur Verhütung schwerer Kriminalität erlauben.[1338]

Ähnlich wie das BVerfG stellt der EuGH also keine spezifischen materiellen Voraussetzungen an den heimlichen sicherheitsrechtlichen Zugang zu (TK-)Bestandsdaten. Der Gerichtshof teilt die Auffassung, dass es sich bei Bestandsdaten um wenig sensible Informationen handelt, deren Abfrage allgemein zur Kriminalitätsverhütung möglich sein kann.

Mehr Gehalt lässt sich aus der Entscheidung nicht ziehen. Der EuGH beantwortete ausschließlich die Vorlagefrage, ob die Bestandsdatenabfrage allein zur Verhütung schwerer Kriminalität zulässig sein kann. Zur konkreten Ausgestaltung der Zugangsnormen, insbesondere hinsichtlich der Bestimmtheit und der Notwendigkeit eigenständiger Rechtsgrundlagen, zur Unterscheidung von automatisierten- und manuellen Abfrageverfahren

1335 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 55 = NJW 2019, 655 mit Verweis auf Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 115 = NJW 2017, 717.

1336 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 27 f. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 99 f. = NJW 2017, 717 EuGH, Urt. v. 6.10.2020 – C-511/18, C-512/18, C-520/18, *La Quadrature du Net* = NJW 2021, 531, Rn. 117; Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 35 f. = NJW 2021, 2103; s.a. *M. W. Müller/Schwabenbauer*, NJW 2021, 2079 (2084).

1337 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 58 ff. = NJW 2019, 655.

1338 Idem, Rn. 62 f.

oder zur Notwendigkeit datenschutzrechtlicher Formvorschriften, etwa Berichts-, Protokoll- oder Benachrichtigungspflichten, äußerte sich der Gerichtshof nicht.

4. Zusammenfassung und Stellungnahme

Obwohl die Kontobestandsdatenabfrage vor und unmittelbar nach ihrer Einführung stark kritisiert wurde[1339], hat sich das Instrument – ebenso wie die Überwachung von TK-Bestandsdaten – mittlerweile etabliert. Das BVerfG hatte in seiner Entscheidung von 2007 keine grundsätzlichen Bedenken geäußert.[1340]

Auch die Speicherung und Abfrage von TK-Bestandsdaten beanstandete die Rechtsprechung in den folgenden Jahren nicht prinzipiell.[1341] Da es sich bei den Bestandsdaten um wenig sensible Daten handelt, die nur als Türöffner für weitere Ermittlungen dienen, stellt die Abfrage durch Sicherheitsbehörden grundsätzlich einen leichter zu rechtfertigenden Grundrechtseingriff dar.[1342]

Im Zuge der Entscheidungen zur TK-Bestandsdatenspeicherung stellte das BVerfG aber bedeutende Grundsätze fest, die analog auf die Kontostammdatenabfrage anzuwenden sind und 2007 noch keine Berücksichtigung fanden. Dazu gehört insbesondere das Prinzip der Doppeltür,[1343] wonach die Ermächtigungen zu Auskunftsersuchen und entsprechender Übermittlung eigenständig geregelt werden müssen.

1339 *ZKA,* Stellungnahme zum 4. Finanzmarktförderungsgesetz, AZ: 413-FPLD, 13. Februar 2002, S. 8 f.; *Degen,* Geldwäsche, 2009, S. 273 ff.; *Samson/Langrock,* Gläserner Bankkunde, 2005; *Lehnhoff*, WM 2002, 687; *Zubrod*, WM 2003, 1210 (1210); *Herzog/Christmann*, WM 2003, 6 (12 f.); *Göres*, NJW 2005, 253 (256 f.); *Widmaier*, WM 2006, 116 (118 ff.); *Hamacher*, DStR 2006, 633 (637 f.); *ders.* Die Bank 09/2006, 40; kritisch auch der *Bundesrat,* BT-Drs. 14/8017, S. 168; aA. *Kokemoor*, BKR 2004, 135; *Rüpke* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 55 Rn. 8 ff., 13.

1340 BVerfGE 118, 168 (188 ff.) – Kontostammdaten; krit. *Reichling,* Kontenabfrage, 2010, S. 129 ff.; *Pfisterer*, JöR 2017, 393 (421); *Hartmann* KJ 2007, 2 (17 f.); *Tolani*, BKR 2007, 275 (281); *Gregor*, EWiR 2008, 189 (190).

1341 BVerfGE 130, 151– Bestandsdatenauskunft I; E 155, 119 – Bestandsdatenauskunft II.

1342 so auch EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 58 ff. = NJW 2019, 655.

1343 BVerfGE 130, 151 (184, 193 ff.) – Bestandsdatenauskunft I; E 155, 119 (142 ff.) – Bestandsdatenauskunft II; dazu *Graulich*, NVwZ-Beilage 2020, 47 (48 f.).

Die Auskunftsanfragen müssen dabei aber nur im Rahmen von manuellen Übermittlungen, d. h., die die unmittelbar durch die Privaten ergehen, in spezifischen Ermächtigungen geregelt werden. Bei automatisierten Auskünften, die auf bestimmte Vertragsdaten begrenzt sind, reichen die allgemeinen Datenerhebungsklauseln aus.[1344]

Dass die Kontobestandsabfrage in den meisten Sicherheitsgesetzen nicht spezifisch normiert wurde, dürfte daher unproblematisch sein. Allerdings bedürfte die unterschiedliche Behandlung von automatisierter und manueller Bestandsdatenabfrage einer tiefergehenden Untersuchung.

II. Kontoinhaltsdaten

Anders als die Bestandsdatenauskunft, ist der heimliche staatliche Zugriff auf Kontoinhaltsdaten nicht zentral geregelt. Mangels umfassender Zahlen lässt sich keine Aussage darüber treffen, auf welche Grundlage sich staatliche Sicherheitsbehörden in der Praxis primär stützen, wenn sie auf solche Finanzdaten zugreifen wollen. Bankenauskunftsersuchen der Staatsanwaltschaften nach § 161 Abs. 1 S. 1 Alt. 1 StPO gehören jedenfalls zu deren Standardrepertoire (s. o. Kap. E. I. 1. c.).[1345]

1. Einleitung: Abgrenzung von individuellen Auskunftsersuchen und Geldwäscheprävention

Zu individuellen bzw. individualisierten Auskunftsersuchen nach Kontodaten hat sich das BVerfG schon mehrfach verhalten. Besondere Aufmerksamkeit erlangte die Entscheidung im „Mikado"-Fall, in dem die Staatsanwaltschaft Kreditkartenunternehmen aufforderte, ihre Datenbestände nach bestimmten Zahlungsvorgängen zu rastern. Das BVerfG erklärte dieses Vorgehen, das auf die Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 Alt. 2 StPO gestützt wurde, für verfassungsgemäß.[1346]

1344 BVerfGE 130, 151 (184, 193 ff.) – Bestandsdatenauskunft I; *Bär* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 28 Rn. 113 f.

1345 Siehe nur *F. Jansen,* Bankauskunftsersuchen, 2010, S. 1 ff.; *Reichling*, JR 2011, 12 (12).

1346 BVerfG, NJW 2009, 1405; krit. *Buermeyer,* Informationelle Selbstbestimmung, 2019, 152 f.; *Brodowski*, JR 2010, 543 (547); *Singelnstein*, NStZ 2012, 593 (603); *Petri*, StV 2007, 266 (268).

Auch zu den nachrichtendienstlichen Auskunftsverlangen, die ausdrücklich zur heimlichen Abfrage von Kontodaten ermächtigen (s. o. E. II. 2. a.), hat das BVerfG Stellung genommen. Solche Auskünfte würden zwar erheblich in die informationelle Selbstbestimmung der Betroffenen eingreifen, da es sich um besonders sensible Daten handle. Bei entsprechender Ausgestaltung durch Anknüpfung an „qualifizierte Gefährdungstatbestände" und verfahrensrechtliche Sicherungen seien solche Zugriffe aber zulässig.[1347]

Gegenstand dieser Untersuchung ist nicht die Verhältnismäßigkeit individueller Abfragen von Kontoumsätzen, sondern das Normgefüge, mittels dessen diese traditionellen Ermittlungswege umgangen werden können: das Anti-Geldwäscherecht.

Substanzielle grundrechtliche Kritik an den Vorschriften des Anti-Geldwäscherechts gab es dabei schon seit dessen Einführung und wird auch aktuell noch vorgetragen. Die kritische Besprechung lässt sich in fünf Phasen unterteilen, bei denen verschiedene Aspekte der Geldwäschebekämpfung im Fokus der Auseinandersetzung standen.

Zunächst wurden – das Geldwäscherecht war in dieser ersten Phase noch rudimentär ausgestaltet – die unmittelbaren Pflichten der Verpflichteten zur Identifizierung und anschließenden Zusammenarbeit mit staatlichen Behörden besprochen, die zwar als Beeinträchtigung der informationellen Selbstbestimmung erkannt wurden, aber allgemein auf wenig Widerstand stießen. Erst als Mitte der 1990er Jahre das EDV-Monitoring etabliert wurde, keimten erste beachtliche Zweifel an der Vereinbarkeit des Geldwäscherechts mit den Privatheitsgrundrechten auf, wobei vor allem die Suche nach einer rechtlichen Grundlage der Datenverarbeitungsmaßnahmen im Zentrum stand.

Zu einem Versuch, das EDV-Monitoring in Gesetzesform zu gießen, kam es nämlich erst nach der Jahrtausendwende. Hierdurch wurde die dritte Phase der Kritik ausgelöst, in der zwar weiterhin ganz zentral über das Monitoring gestritten wurde, nun aber unter breiterem Interesse und mit stärkerem Fokus auf die Verhältnismäßigkeit der gesetzlichen Regelung.

Die vierte Phase ist von der Einführung des Anti-Geldwäscherechts in der Struktur der 3. GWRL geprägt. Erstmals war in den Gesetzen nun ausdrücklich von einer Überwachungspflicht der Institute die Rede. Gleichzeitig war das Monitoring mittlerweile gängige Praxis, weshalb die Diskussion um die Implikationen der Überwachung trotz der damals intensiven Dis-

1347 BVerfGE 120, 274 (348 ff.) – Online-Durchsuchung.

kussion um die TK-Vorratsdatenspeicherung weniger kontrovers geführt wurde.

In der fünften und aktuellen Phase wird das Monitoring zwar noch immer kritisiert. Der Fokus insbesondere der europäischen Literatur liegt aber primär auf den vorgehaltenen Datenbeständen der Banken und den Zugriffs- und Analyserechten der FIU.

Diese fünf Phasen sollen im Folgenden chronologisch erläutert und im Einzelnen kommentiert werden. Die Darstellung folgt somit der zuvor vorgenommenen historischen Darstellung der Entwicklung des Anti-Geldwäscherechts (s. Kap. D. III. 2. a.) und bezieht sich vornehmlich auf die deutsche Perspektive der Debatte.

Zuletzt sollen dann noch die knappen Ansätze der Rechtsprechung zum Verhältnis des Anti-Geldwäscherechts und der informationellen Selbstbestimmung bzw. den Privatheitsgrundrechten kurz beleuchtet werden.

2. Verdachtsmeldepflichten und „Bankgeheimnis"

In seiner ursprünglichen Form aus dem Jahr 1993 sah das GwG noch keine ausdrückliche Pflicht zur Überwachung, sondern lediglich Identifizierungspflichten und eine Meldepflicht bei Verdachtsmomenten vor. Diese Pflichten gingen mit einer Aufzeichnungs- und Aufbewahrungspflicht einher.

a. Erste Annäherungen bei der FES-Tagung zur Geldwäsche 1994

Die Beeinträchtigung der informationellen Selbstbestimmung der Bankkunden durch das GwG war dementsprechend unmittelbar nach der Einführung des Gesetzes noch ein untergeordnetes Thema. Zumeist wurde lediglich festgestellt, dass die geldwäscherechtlichen Pflichten mit dem Bankgeheimnis kollidieren würden.[1348] Dass dieses – soweit es in der Rechtsordnung überhaupt Ausdruck findet –[1349] aber keinen absoluten

1348 Etwa *Reifner*, JZ 1993, 273 (277 f.); *Carl/Klos*, wistra 1994, 161 (162).

1349 Hierzu übersichtlich *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 8 Rn. 4 ff.

Schutz genießt, sondern allgemein bei der Strafverfolgung durchbrochen wird, war dabei schon anerkannt.[1350]

So stellten zwei Regierungsjuristen etwa fest, dass durch die flächendeckende Mitteilung von Informationen der Banken an den Staat tief in die Privatsphäre der Bürger eingegriffen würde.[1351] Aber anstatt diesen Umstand verfassungsrechtlich zu prüfen, kritisierten sie, dass die aufgrund des Geldwäschegesetzes erlangten Informationen nicht bzw. nicht unmittelbar für die Steuerbekämpfung genutzt werden könnten.[1352]

Erste kritische Töne waren indes bereits auf einer Tagung der Friedrich-Ebert-Stiftung zum Geldwäschegesetz im Oktober 1993 laut geworden.[1353] Hier machten der Vorsitzende der Berliner Anwaltskammer[1354] auf die Beeinträchtigung der Geheimhaltungspflichten der Berufsgeheimnisträger und der Hessische Datenschutzbeauftragte auf Implikationen mit der Privatsphäre der Bankkunden[1355] aufmerksam.

Zwar wurde von beiden auf eine unmittelbare verfassungsrechtliche Einschätzung verzichtet. Sie legten jedoch gewissermaßen den Grundstein der aufkeimenden Diskussion, indem sie die verschiedenen durch das Anti-Geldwäscherecht betroffenen Rechtspositionen kompakt darstellten. Diese sind einerseits die wirtschaftlichen Rechte der verpflichteten Institute und Personen, die aber nicht Thema dieser Arbeit sind, sowie das Recht auf informationelle Selbstbestimmung der betroffenen Kunden.

b. Frühe Betrachtungen von GwG und informationeller Selbstbestimmung

Mit diesem setzte sich die erste umfassende Kommentierung des GwG von *Aepfelbach* und *Fülbier* im Hinblick auf die Melde-, Aufzeichnungs- und Aufbewahrungspflicht nach § 10 GwG 1993 auseinander.[1356] Hinsichtlich der Meldepflicht wurde zunächst ein Vergleich mit dem US-Recht ange-

1350 LG Frankfurt, NJW 1954, 688 (690); *R. Müller*, NJW 1963, 831 (836 ff.); *Carl/Klos*, DStZ 1994, 68 (70); ausf. *Sichtermann,* Bankgeheimnis, 2. Aufl. 1966, S. 289 ff.
1351 *Carl/Klos*, DStZ 1994, 68 (68).
1352 Idem, (71 ff.).
1353 *Kahlert* (Hrsg.), Friedrich-Ebert-Stiftung, Tagung Geldwäsche, 1994.
1354 *Dombek* in Kahlert (Hrsg.), Friedrich-Ebert-Stiftung, Tagung Geldwäsche, 1994, S. 103.
1355 *Hassemer* in Kahlert (Hrsg.), Friedrich-Ebert-Stiftung, Tagung Geldwäsche, 1994, S. 123.
1356 *Fülbier* in Aepfelbach/Fülbier GwG, 1. Aufl., 1993, S. 126 ff.

strengt, das eine allgemeine Meldepflicht für Bartransaktionen ab einem gewissen Schwellenwert vorsah. Solch eine Meldepflicht wäre aber eine Informationserhebung auf Vorrat und ins Blaue hinein, weshalb sie mit deutschem Verfassungsrecht nicht in Einklang zu bringen wäre.[1357] Zurecht hätte sich die EG daher für eine Verdachtsmeldepflicht entschieden. Diese würde zwar ebenfalls in das Recht auf informationelle Selbstbestimmung eingreifen, aufgrund der Filterung auf verdächtige Fälle jedoch nur in einem geringen Maße, das mit dem gesellschaftlichen Interesse an Strafverfolgung gerechtfertigt werden könnte.[1358]

Hinsichtlich der Aufzeichnungs- und Aufbewahrungspflicht wurde ebenfalls bemerkt, dass Private durch das GwG dazu verpflichtet werden, Informationen zu erheben und dem Staat zur Verfügung zu stellen.[1359] Auf eine Prüfung der Verhältnismäßigkeit anhand des deutschen Verfassungsrechts wurde jedoch verzichtet, da die Informationserhebung auf europäischem Recht beruhte.[1360] Nur soweit die Daten zu anderen als geldwäscherechtlichen Zwecken verwendet werden sollten, wäre das deutsche Verfassungsrecht einschlägig, da nach der Präambel der 1. GWRL die Datenverwendung auf geldwäscherechtliche Zwecke begrenzt sei.[1361] Hier wurde wohl übersehen, dass das Verwertungsverbot nicht nur in der Präambel, sondern ausdrücklich in Art. 6 Abs. 3 der 1. GWRL normiert wurden. Nach Art. 6 Abs. 3 S. 2 der 1. GWRL sollte es den Mitgliedstaaten aber möglich bleiben, die nach dem Anti-Geldwäscherecht zu speichernden Daten auch für andere Zwecke zu öffnen.

Das GwG 1993 sah dementsprechend in § 10 noch eine Verwertungsbeschränkung auf Strafverfahren vor, in denen wegen Geldwäsche i. S. d. § 261 StGB[1362] oder einer der Vortaten des § 261 StGB ermittelt wurde. Unter diese Vortaten fielen Verbrechen, Vergehen nach § 29 Abs. 1 Nr. 1 BtMG oder Vergehen des Mitglieds einer kriminellen Vereinigung i. S. d. § 129 StGB. Damit war die Verwertungsbeschränkung also gerade nicht auf Geldwäschedelikte beschränkt. Vielmehr durften die nach dem GwG gespeicherten Daten auch zur Aufklärung von Verbrechen genutzt werden,

1357 Idem, S. 138 ff.
1358 Idem, S. 140.
1359 Idem, S. 126; s.a. BT-Drs. 12/2704, S. 16 f.
1360 Grundlegend BVerfGE 73, 339 – Solange II.
1361 *Fülbier* in Aepfelbach/Fülbier GwG, 1. Aufl., 1993, S. 127; siehe BVerfG, NJW 1990, 974
1362 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15.7.1992, BGBl. I 1302.

ohne dass zusätzlich wegen Geldwäsche ermittelt wurde.[1363] Insofern hätte die Datenverarbeitung an deutschem Verfassungsrecht gemessen werden müssen.

Wenige Jahre später wurde die grundrechtliche Dimension des GwG auch in Zeitschriftenbeiträgen angesprochen.[1364] Von *Dahm* wurde bemerkt, dass die Geldwäschebekämpfung auf der Verarbeitung ganz besonders sensibler Daten beruht.[1365] Da in Form der Strafverfolgung ein staatlicher Zweck verfolgt würde, verlangte er die grundsätzlich unmittelbare Anwendung des Verfassungsrechts. Dabei ging er so weit, die Banken als Beliehene anzusehen.[1366] Dieser Ansatz erweist sich aber als Fehlsubsumption und konnte sich nicht durchsetzen, da die Banken gegenüber Dritten nicht hoheitlich tätig werden.[1367] Sie verarbeiten lediglich Daten, die aus einem privatrechtlichen Verhältnis stammen.

Im Mittelpunkt seiner Untersuchung steht *Dahms* früher Versuch, die geldwäscherechtlichen Pflichten der Banken und anderer Institute mit unmittelbar staatlichen Überwachungsmaßnahmen zu vergleichen und die dazu vorliegende Rechtsprechung des BVerfG als Maßstab für das GwG vorzuschlagen. Hierfür bot sich der 1995 ergangene Gerichtsbeschluss[1368] zur Auslandsfernmeldeaufklärung durch den BND an.[1369] In diesem hatte das BVerfG die Auswertung von Kommunikationsinhalten, die der BND im Rahmen der verdachtslosen Rasterung erhalten würde, vorläufig außer Vollzug gesetzt. Die Nachteile, die eine Auswertung anlasslos abgefangener Kommunikation für die unverdächtigen Betroffenen hätte, seien zu groß.[1370]

Dahm schlug nun vor, diese kritische Betrachtung anlassloser Datensammlung zur Sicherheitsprävention auf das GwG übertragen.[1371] Zwar war im Jahr 1996 noch nicht näher geklärt, auf welchem Wege die Verpflichteten verdächtige Transaktionen entdecken sollten. Es war jedoch bekannt geworden, dass das Bundesaufsichtsamt für das Kreditwesen (BAKred)

1363 *Carl/Klos*, DStZ 1994, 68 (71); vgl. auch BT-Drs. 12/2704, S. 17.
1364 *Dahm*, WM 1996, 1285; *Herzog*, WM 1996, 1753.
1365 *Dahm*, WM 1996, 1285 (1289).
1366 *Dahm/Hamacher*, wistra 1995, 206 (213 f.); *Dahm*, WM 1996, 1285 (1288); auch *Findeisen*, wistra 1997, 121 (124 f.) .
1367 Vgl. nur *Degen,* Geldwäsche, 2009, S. 130 ff.
1368 BVerfGE 93, 181.
1369 *Dahm*, WM 1996, 1285 (1290).
1370 BVerfGE 93, 181 (191).
1371 *Dahm*, WM 1996, 1285 (1290).

das anglo-amerikanische „Know-Your-Customer" System implementieren wollte, wonach die Banken alle verdächtigen Transaktionen zu untersuchen hätten (dazu gleich unten). Daraus wurde gefolgert, dass die Banken eine Art Rasterfahndung durchführen müssten, um solche verdächtigen Transaktionen zu identifizieren, wodurch sie letztlich den Geschäftsverkehr aller Kunden überwachen müssten. Die Rechtsprechung des BVerfG stünde dieser Bestrebung entgegen. Noch nicht einmal die Strafverfolgung selbst wäre zu einer solchen Vorfeldaufklärung berechtigt,[1372] Private sollten es erst recht nicht sein.[1373]

Eine weitere differenzierte Besprechung der Auswirkungen des GwG auf die informationelle Selbstbestimmung findet sich in der Dissertation von *Werner* aus dem Jahr 1996.[1374] Die bestehenden geldwäscherechtlichen Pflichten wurden hier allerdings nicht separat, sondern als einheitlicher Eingriffskomplex dargestellt. Dieser sei trotz des vordergründigen Tätigwerdens von Privaten aufgrund der gesetzlichen Anordnung und des klar definierten Zwecks der Strafverfolgung dem Staat zuzurechnen.[1375] Die Pflichten wurden einer hypothetischen Verhältnismäßigkeitsprüfung im Sinne des deutschen Verfassungsrechts unterzogen – hypothetisch, da im Voraus ebenfalls bemerkt wurde, dass dieses nach der Rechtsprechung des BVerfG aufgrund der dahinterliegenden Richtlinie keine Anwendung finden würde.[1376] Diese Prüfung kam zu dem Ergebnis, dass der Eingriff in die informationelle Selbstbestimmung gerechtfertigt wäre. Die Identifizierungspflicht sei schon kein erheblicher Eingriff, da Transparenz im Wirtschaftsverkehr normal und erwünscht sei.[1377] Die Aufzeichnungspflichten wären durch die Verwendungsbeschränkung und die Meldepflicht durch das Verdachtsmoment ausreichend eingehegt.[1378]

3. Diskussion um die Einführung des Konten-Monitorings ab Mitte der 1990er Jahre

Die Diskussion wurde intensiviert, nachdem Mitte der 1990er Jahre Überlegungen des BAKred zur Überwachung von Transaktionen durch die Geld-

1372 Ibid.
1373 Ibid.
1374 *Werner,* Geldwäsche, 1996, S. 94 ff.
1375 Idem, S. 96.
1376 Idem. S. 91 f.
1377 Idem, S. 102 f.
1378 Idem, S. 103.

wäscheverpflichteten bekannt wurden. Gemäß Art. 5 der 1. GWRL sollten die Mitgliedstaaten sicherstellen, dass die Verpflichteten alle Transaktionen, die einen Verdacht der Geldwäsche besonders nahelegten, sorgfältig prüfen würden. Eine solche Pflicht fand sich aber im GwG nicht ausdrücklich. Dieses sah in § 14 Abs. 2 Nr. 2 GwG 1993 lediglich generalklauselartig vor, dass bestimmte Verpflichtete, insbesondere Kreditinstitute, interne Grundsätze, Verfahren und Kontrollen zur Verhinderung der Geldwäsche entwickeln.

Das BAKred war deshalb besorgt, das Art. 5 der 1. GWRL nicht ausreichend umgesetzt war. Bei einer Tagung der CDU/CSU-Bundestagsfraktion stellten dessen Beamte deshalb vor, wie dieser vermeintliche Umsetzungsmangel behoben werden sollte.[1379] Aus der Verpflichtung zur Entwicklung interner Sicherungsmaßnahmen wollte man ableiten, dass die Banken zur Rasterung der Kundentransaktionen nach einem bestimmten Verfahren verpflichtet sind. Diesen Prozess bezeichnete man als „*Kontenresearch*"[1380]. Konkret vorgeschlagen wurde zunächst aber nur die Überwachung („Monitoring") bestimmter Kunden, wenn bei diesen Transaktionen gefunden wurden, die zwar auffällig waren, aber noch nicht die Schwelle zur Verdachtsmeldung überschritten.[1381] Für diesen Prozess sollten die Banken ihre hauseigene EDV nutzen, um anhand konkreter Suchparameter Auffälligkeiten bei Kundentransaktionen zu entdecken, die sodann im Sinne des Art. 5 der 1. GWRL besonders sorgfältig geprüft werden sollten.[1382] Das heute standardmäßige EDV-Monitoring war damit quasi geboren.

a. Erste Kritik von *Felix Herzog*

Der Vorstoß des BAKred wurde zeitnah von *Felix Herzog* besprochen, der die Beeinträchtigungen der informationellen Selbstbestimmung durch das

1379 *Artopeus/Findeisen*, (BAKred), Entwurfspapier Anhörung CDU/CSU im Bundestag, 21.08.1995, S. 10 ff. aus der Anhörung selbst zitieren *Dahm*, WM 1996, 1285 (1290) und *Herzog*, WM 1996, 1753 (1755 ff.).

1380 Vgl. *BAKred,* Jahresbericht, 1998, S. 92 f.; *Herzog*, WM 1996, 1753 (1755).

1381 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, Ziff. 30; abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.

1382 So jedenfalls *Herzog*, WM 1996, 1753 (1755 ff.); *Dahm*, WM 1996, 1285 (1290) jeweils mit Verweis auf die Anhörung der BAKred durch die CDU/CSU-Fraktion am 25.08.1995. Aus dem Entwurfspapier der BAKred (oben Fn 1380) und der Verlautbarung (oben Fn 1867 1382) ergibt sich das nicht in dieser Ausdrücklichkeit.

Anti-Geldwäscherecht seitdem immer wieder infrage gestellt hat. In einem 1996 erschienen Aufsatz unterzog er die Vorschläge des BAKred einer datenschutz- und verfassungsrechtlichen Prüfung.[1383] Die unmittelbar zuvor von *Dahm* vorgebrachten *Vorbehalte*[1384] erhielten dadurch erstmals echte Substanz. Der Aufsatz behandelt bereits alle Punkte, die auch aus heutiger Perspektive dringlich erscheinen und soll daher an dieser Stelle recht umfassend zusammengefasst werden.

Herzog befand, dass ein EDV-Monitoring von Kundendaten durch die Banken als Eingriff in die informationelle Selbstbestimmung zu werten wäre. Dabei verstand er diese begrifflich ganz im Sinne des Volkszählungsurteil als Quasi-Eigentum[1385] an Daten bzw. dem Recht jeder Person zu wissen, was andere über sie wissen.[1386] In dieses Recht würde eingegriffen, auch wenn die Datenverarbeitung durch die Banken als Private stattfinde. Schon in der Speicherung der Daten identifizierte *Herzog* eine Beeinträchtigung der informationellen Selbstbestimmung der Kunden,[1387] unterließ insofern aber eine rechtliche Prüfung.

Diese beschränkte er auf die übrigen EDV-Prozesse. Aufgrund der staatlichen Anordnung und dem staatlichen Zweck würde das Bank-Kunde-Verhältnis (bei der Suche nach geldwäscherechtlichen Auffälligkeiten) transformiert und damit zu einem öffentlich-rechtlichen.[1388] *Herzog* ordnete die Banken aber deswegen nicht als Beliehene oder Verwaltungshelfer ein. Auch käme es nicht darauf an, ob das Handeln der Banken eine mittelbare oder unmittelbare Grundrechtsbeeinträchtigung sei, da jedenfalls die Verpflichtung der Banken auf den Staat zurückzuführen ist und damit in jedem Fall unmittelbar dem Verfassungsrecht unterliegt.

Ausgehend von dieser Feststellung warf *Herzog* die Frage auf, ob ein Kontenmonitoring gestützt auf § 14 Abs. 2 Nr. 2 GwG 1993 nach dem damals geltenden Datenschutzrecht zulässig sein könnte. Dieses sah in § 4 Abs. 1 BDSG 1990[1389] bereits vor, dass jede Datenverarbeitung eine Einwilligung oder gesetzliche Grundlage voraussetzt. Für gesetzliche Eingriffe in die informationelle Selbstbestimmung hatte das BVerfG spezifische Be-

1383 *Herzog*, WM 1996, 1753 (1756 ff.).
1384 *Dahm*, WM 1996, 1285 (1290).
1385 Vgl. nur *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (132 f.).
1386 *Herzog*, WM 1996, 1753 (1757) mit Verweis auf BVerfGE 65, 1 (43) – Volkszählung.
1387 Idem, (1757).
1388 Idem, (1757).
1389 Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990, BGBl. I, S. 2954

stimmtheitsanforderungen formuliert. Danach müssen die Art, Umfang und Zweck der Datenverarbeitung präzise und bereichsspezifisch festgelegt werden.[1390] Diese Bestimmtheitsanforderungen sah *Herzog* von § 14 Abs. 2 Nr. 2 GwG 1993 nicht erfüllt, da die Vorschrift keine Voraussetzungen für eine Datenerhebung artikulierte.[1391]

Auch § 28 Abs. 1 Nr. 2 BDSG 1990 sah er nicht als taugliche Ermächtigungsgrundlage. Nach dieser Vorschrift dürften Private nur für eigene Zwecke Daten erheben. Die Bekämpfung der Geldwäsche sei primär aber nicht für die Imagepflege des Finanzstandorts Deutschlands, sondern für die Strafverfolgung gedacht und widmet sich damit einem genuin öffentlichen Zweck.[1392] Dennoch nähmen die Institute keine hoheitlichen Aufgaben i. S. d. § 2 Abs. 4 S. 2 BDSG 1990 wahr, weshalb auch die gesetzlichen Grundlagen des BDSG für die Datenverarbeitung durch öffentliche Stellen nicht einschlägig seien.[1393] Sie seien lediglich in die Pflicht genommene Private. Damit stellte sich *Herzog* gegen *Dahms* Einschätzung[1394], dass die Banken verwaltungsrechtlich als Beliehene anzusehen wären. Seine Meinung hat sich heute weitestgehend durchgesetzt. Die geldwäscherechtlichen Pflichten werden gemeinhin als gewerberechtliche Pflichten oder Pflichten *sui generis* und nicht als Kompetenzübertagung angesehen.[1395]

Obwohl es damit schon an einer Rechtsgrundlage für das Monitoring fehlen würde, nahm *Herzog* eine recht umfassende Verhältnismäßigkeitsprüfung anhand des Rechts auf informationelle Selbstbestimmung vor. Einen unionsrechtlichen Vorrang sprach er dabei nicht an.

Mit dem Zweck der Strafverfolgung – insbesondere der Aufklärung schwerer Straftaten – läge ein wesentlicher Auftrag des staatlichen Gemeinwesens vor.[1396] Allerdings erfasse das Kontenmonitoring aufgrund des groben Rasters notwendigerweise eine Unzahl unauffälliger Transaktionen des allgemeinen Lebens. Selbst die vom Raster erfassten „Vorverdachtsfälle" würden in den allermeisten Fällen noch keinen Anfangsverdacht begrün-

1390 BVerfGE 65, 1 (44 ff.) – Volkszählung.
1391 *Herzog*, WM 1996, 1753 (1758).
1392 Ibid.
1393 Idem, 1758 f.
1394 *Dahm/Hamacher*, wistra 1995, 206 (213 f.) *Dahm*, WM 1996, 1285 (1288).
1395 Übersicht bei *Degen,* Geldwäsche, 2009, S. 130 ff.; Für eine gewerberechtliche Pflicht BT-Drs. 18/11928, S. 26; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 76; *Kaetzler*, CCZ 2008, 174 (174); „Pflicht sui generis": *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5; *Lenk*, JR 2020, 103 (105 Fn 15).
1396 *Herzog*, WM 1996, 1753 (1759) mit Verweis auf BVerfG, JZ 1987, 1118 (1119).

den.[1397] Dennoch sollten diese Fälle festgehalten und von der Aufsichtsbehörde kontrollierbar, dem Staat also zugänglich, sein. Eine solche Vorfeldaufklärung bedürfe einer besonders strengen Verhältnismäßigkeitskontrolle.[1398]

Schon im Rahmen der Erforderlichkeitsprüfung bestünden erhebliche Zweifel. Ein gleich geeigneter Zweck könnte auch dann erreicht werden, wenn die Überwachung des Finanzverkehrs von materiellen und formellen Voraussetzungen abhängig wäre und durch bestimmte Verfahrensvorschriften eingehegt – wie etwa die Überwachung des Fernmeldeverkehrs.[1399] In diesem Fall wäre die Beeinträchtigung deutlich milder.

Im Übrigen sei das Monitoring nicht angemessen.[1400] Es teile Charakteristika staatlicher Überwachungsmaßnahmen wie der Rasterfahndung oder Telefonüberwachung. Massenhaft würden Daten verarbeitet, die alltägliches legales Verhalten beträfen. Jeder betroffene Bürger befinde sich im *Vorhof des Verdachts*.[1401] Wie auch *Dahm* verglich *Herzog* das EDV-Monitoring mit der Auslandsfernmeldeaufklärung durch den BND. Diese sei vom BVerfG zutreffend als verdachtslose Rasterfahndung gewertet worden.[1402]

Dass Private zu einer Datensammlung auf Vorrat in die Pflicht genommen würden, sei dabei noch skeptischer zu betrachten als vergleichbare Sammlungen durch die Polizei. Die Indienstnahme führe zu einer umfassenden Strukturveränderung im staatlichen Sicherheitsgefüge.[1403]

Weiter würde der Grundsatz der Offenheit des Strafverfahrens unterlaufen. Die vorrätige Datensammlung und geheime Verdachtsanzeigen würden dazu führen, dass die Strafverfolgungsbehörden auf eine Inkulpation verzichten könnten, falls sich ein Anfangsverdacht nicht erhärtet. Die Betroffenen würden daher nie von den Ermittlungen im Vorfeld erfahren und wären faktisch vom Rechtsschutz ausgeschlossen.[1404]

Aufgrund dieser Umstände könne das Interesse der Strafverfolgung den Eingriff in die informationelle Selbstbestimmung nicht rechtfertigen. Die massenhafte Inanspruchnahme Unverdächtiger sei mit rechtsstaatlichen Grundsätzen nicht vereinbar. Selbst wenn eine ausreichende gesetzliche

1397 *Ders.*, WM 1996, 1753 (1759).
1398 Idem, (1760).
1399 Idem, (1760 f.).
1400 Idem, (1761 f.).
1401 Idem, (1761).
1402 Idem, (1761) mit Verweis auf BVerfGE 93, 181 (182).
1403 Idem, (1762).
1404 Ibid.

Grundlage geschaffen würde, wäre fraglich, ob sie sich in den Grenzen des Verfassungsrechts halten könne.[1405]

Herzogs Kritik stieß zwar zunächst nicht auf größeres Echo, erhielt aber durchaus Zustimmung. *Dittrich/Trinkhaus* etwa sahen ebenfalls datenschutzrechtliche Probleme bei der Ermächtigung zur Speicherung von Verdachtsmeldungen.[1406] Sie teilten auch die Vorbehalte gegenüber dem EDV-Monitoring. Weder § 14 Abs. 2 Nr. 2 GwG 1993 noch § 28 Abs. 1 Nr. 2 BDSG 1990 seien ausreichende Grundlagen für eine solch umfassende Verarbeitung der Kundendaten zum Primärzweck der Strafverfolgung.[1407] Zur prinzipiellen verfassungsrechtlichen Zulässigkeit des Monitorings äußerten sie sich aber nicht.

b. Verteidigung des (EDV-)Research und -Monitorings durch *Michael Findeisen*

Die Lesart des § 14 Abs. 2 Nr. 2 GwG 1993 als Verpflichtung zur Errichtung interner Sicherheitsmaßnahmen einschließlich EDV-Monitoringsysteme wurde von *Findeisen*, dem zuständigen Referatsleiter bei dem BAKred, verteidigt.[1408] Die Vorschrift sei nicht nur ein Annex der konkreten Pflichten aus dem GwG, sondern bringe das Präventionsprinzip als eigene Säule des Anti-Geldwäscherechts zum Ausdruck.[1409]

Zur Inhaltsbestimmung verwies *Findeisen* auf die grundlegenden Normen der internationalen Geldwäschebekämpfung. § 14 Abs. 2 Nr. 2 GwG 1993 setzte Art. 11 der 1. EG-Geldwäscherichtlinie um und dieser wiederum die FATF-Empfehlungen von 1990.[1410]

Der Erkenntnisgewinn dieser Rechtsverweisung ist überschaubar. Weder Art. 11 der 1. EG-Geldwäscherichtlinie noch Nr. 20 der FATF-Empfehlungen 1990 schrieben konkrete Sicherungsmaßnahmen vor. Sie verpflichteten allenfalls zur Bereitstellung geeigneter bzw. adäquater Systeme und lesen sich somit wie Parallelvorschriften zu § 14 Abs. 2 Nr. 2 GwG 1993. Dennoch wollte *Findeisen* aus der Verpflichtung zur internen Sicherung die Pflicht

1405 Idem, (1763).
1406 *Dittrich/Trinkhaus*, DStR 1998, 342 (346).
1407 Idem, (347).
1408 *Findeisen*, wistra 1997, 121.
1409 Idem, (123 f.)
1410 *FATF*, 40 Recommendations, 1990.

zur Auswertung und Analyse der bei den Banken vorhandenen Datenbanken herleiten.[1411] Die aus dem GwG Verpflichteten hätten gravierende Erkennungsprobleme. Die Mehrzahl der Transaktionen im Geschäftsverkehr würden unbar durchgeführt und wären oberflächlich nicht auffällig. Auf diese Transaktionen seien die Identifizierungspflicht und die starren Schwellenwerte für Bargeschäfte nicht ausgerichtet. Diese orientierten sich vielmehr am klassischen Geschehen vor dem Bankschalter, das in der Praxis aber keine Relevanz mehr habe.[1412] Daher müsse stattdessen mit „Research" und „Monitoring" gearbeitet werden. Die Nutzbarmachung von Datenbanken zur Risikoprävention gehöre zum gewöhnlichen Sicherungsmanagement der Banken und sei daher auch für die Geldwäschebekämpfung fruchtbar zu machen. Das Research führe nicht zur Ausforschung des Kunden im Interesse der Strafverfolgungsbehörden, sondern diene dem Selbstschutz der Kreditinstitute. Insofern sei es datenschutzrechtlich unbedenklich.[1413]

c. Einführung des EDV-Monitorings durch Verlautbarung der BAKred im Jahr 1998 und anschließende Diskussion

Als ersten greifbaren Schritt hin zum verpflichtenden EDV-Monitoring wurde die Verlautbarung vom 30. März 1998[1414] verstanden.[1415] Nach Ziffer 30 der Verlautbarung („Abbruch der Geschäftsbeziehung") sollten Kreditinstitute Geschäftsbeziehungen längerfristig überwachen, wenn zuvor eine einzelne Transaktion zwar noch keinen Verdacht ausgelöst hatte, die Verdichtung eines Verdachts durch weitere Transaktionen aber möglich erschien. Nach Ziffer 34 (Bestellung eines Geldwäschebeauftragten) lit d.) sollten weiter durch den Geldwäschebeauftragten interne Organisationsanweisungen geschaffen werden, die gewährleisteten, dass solche Transaktionen mit besonderer Aufmerksamkeit behandelt werden, die bereits in der Vergangenheit aus dem Blickwinkel der Geldwäschebekämpfung auffällig geworden waren. Die Art und Weise dieser Sicherstellung wurde den Insti-

1411 *Findeisen*, wistra 1997, 121 (128).
1412 Ibid.
1413 Ibid.
1414 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.
1415 Etwa *Langweg* in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, § 14 Rn. 101.

tuten freigestellt. Rein faktisch dürfte es aber, wie *Findeisen* selbst bemerkt hatte[1416], schon damals nicht möglich gewesen sein, Auffälligkeiten in unbaren Transaktionen ohne die Verwendung einer EDV-Rasterung zu finden. Auch wenn in der Verlautbarung nicht ausdrücklich von EDV-Research bzw. – Monitoring gesprochen wurde, waren diese Prozesse durchaus intendiert.

aa. Erläuterung durch das BAKred bzw. *Michael Findeisen*

Dies wurde spätestens klar, als das BAKred noch im selben Jahr ein „Geldwäsche-Typologienpapier"[1417] als Rundschreiben an die deutschen Kreditinstitute versandte. In diesem wurden erstmals typische Auffälligkeiten beschrieben, die den geldwäscherechtlich Verpflichteten bei der Erkennung von Verdachtsfällen helfen sollten. Hier wurde erstmals ausdrücklich davon gesprochen, dass es sich um „*(EDV-gestützte Systeme) zur Sichtbarmachung geldwäscherelevanter Sachverhalte*"[1418] handle, die in Ziffer 34 lit. d) der Verlautbarung vom 30. März 1998 angesprochen würden.

Die Verlautbarung des BAKred vom 30. März 1998 wurde abermals vom Referatsleiter *Findeisen* in einem Fachbeitrag[1419] erläutert. Neue Argumente lieferte der Aufsatz zwar nicht, beschrieb aber erstmals in einigermaßen konkreter Form, wie sich das BAKred den Research- und Monitoring-Prozess bei den Kreditinstituten vorstellte. Im Rahmen der Bonitätsprüfung der Kunden würden Banken schon länger *Scoringsysteme* verwenden, bei denen aus den bankeigenen Datenbeständen Informationen extrahiert und zu einem Kundenwert verdichtet würden. Außerdem würden die gesammelten Massendaten mithilfe von Data-Mining-Algorithmen analysiert und in der Folge für Akquisitionszwecke genutzt.[1420]

Dieses Modell des „*Data Based Marketing*" ließe sich auf die Geldwäschebekämpfung übertragen. Aus den Transaktionen der Kunden könnten Sekundärinformationen gewonnen werden, die sich zu einem Kundenprofil vervollständigen ließen. Durch eine EDV-Analyse der Kundentransaktio-

1416 *Findeisen*, wistra 1997, 121 (128); *ders.*, WM 1998, 2410.
1417 *BAKred,* Rundschreiben 19 / 1998, Typologienpapier-Geldwäsche, 02.11.1998.
1418 Idem, S. 49.
1419 *Findeisen*, WM 1998, 2410.
1420 Idem, (2418).

nen anhand dieser Profile könnten die Grenzen des Massengeschäfts überwunden werden.[1421]

Das Research-Vorgehen würde im Ausland bereits eingesetzt. Dort hätten die Banken Computerprogramme entwickelt, die Listen mit ungewöhnlichen Transaktionen ausdrucken könnten. Die Ungewöhnlichkeit ergebe sich eben aus den im Rahmen des Research gewonnenen Kundenprofilen.[1422]

bb. Erneute Kritik von Felix Herzog

Kritik an der Verlautbarung kam abermals von *Felix Herzog*,[1423] der sein Vorbringen aus dem Jahr 1996 wieder aufgriff und insbesondere auch auf die fachlichen Erläuterungen von *Findeisen* einging. In seinem Beitrag sprach *Herzog* zunächst formelle bzw. Fragen des allgemeinen Verwaltungsrechts in Bezug auf die Verlautbarung an. Deren Rechtscharakter sei fraglich. Anders als *Findeisen* meine[1424], sei die Einordnung als faktisch bindende norminterpretierende Verwaltungsvorschrift nicht unproblematisch, da eine solche Bindung nur intern stattfinden kann, d. h. innerhalb des Verwaltungsapparats.[1425] Die Verlautbarung möchte das Gesetz aber faktisch[1426] bindend für Private auslegen und sieht recht konkrete Handlungspflichten vor. Sie ähnelte damit mehr einer Allgemeinverfügung, da die angestrebte Bindungswirkung nach außen zielt. Andererseits sei die Verlautbarung aber nicht unmittelbar zwangsbewehrt, was gegen den Charakter einer Allgemeinverfügung spräche. *Herzog* konstatierte daher, dass die Verlautbarung einer rechtlich strittigen, neuartigen Form von Verwaltungshandeln zuzuordnen sei, nämlich den „normkonkretisierende[n] Verwaltungsvorschriften, die Außenwirkung für sich beanspruchen."[1427] Die rechtliche Einordnung der Verlautbarungen bzw. Rundschreiben des BAKred und nun der BaFin konnte auch bis heute nicht abschließend geklärt werden.[1428]

1421 Ibid.
1422 Ibid.
1423 *Herzog*, WM 1999, 1905.
1424 *Findeisen*, WM 1998, 2410 (2410 f.).
1425 *Herzog*, WM 1999, 1905 (1911); dazu *Sennekamp* in Mann/Sennekamp/Uetrichtz VwVfG, 2. Aufl., § 9 Rn. 15.
1426 *Findeisen*, WM 1998, 2410 (2411).
1427 *Herzog*, WM 1999, 1905 (1911) mit Verweis auf *Wolf*, DÖV 1992, 849.
1428 *Bauernfeind*, DÖV 2020, 110; *Fekonja,* Verlautbarungen, 2013, S. 91 ff., 181 ff.

Schon *Herzog* erkannte aber, dass es für die Bewertung des Verlautbarungsinhalts auf deren Rechtscharakter letztlich nicht ankommen kann, da jedes belastende Verwaltungshandeln mit Außenwirkung ohnehin an höherrangigem Recht, insbesondere den Grundrechten, zu messen sei.[1429]

Ausgehend von dieser Prämisse prüfte er zunächst, ob das GwG eine ausreichende Zuständigkeitsbestimmung des BAKred zum Erlass solcher Verlautbarungen vorsah. *Findeisen* hatte sich für das BAKred insofern auf § 6 Abs. 2 KWG und § 16 Nr. 2 GwG 1993 berufen.[1430] Nach diesen Vorschriften war das BAKred mit der Durchführung des GwG betraut und sollte Missständen im Kredit- und Finanzdienstleistungswesen entgegenwirken, welche u. a. die ordnungsmäßige Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen. Nach *Herzog* handelte es sich um reine Aufgabenzuweisungen, aus denen keine Ermächtigungen zum Erlass von grundrechtsbeeinträchtigenden Verlautbarungen hervorgehen würden.[1431]

Außerdem würde die Verlautbarung gegen den Vorbehalt des Gesetzes bzw. verfassungsrechtlichen Wesentlichkeitsgrundsatz verstoßen, nach dem der Gesetzgeber wesentliche Entscheidungen selbst treffen muss.[1432] Auch diese Grundsatzfrage hinsichtlich der Verlautbarungspraxis des BAKred bzw. der BaFin wird noch heute diskutiert.[1433]

Im Rahmen der Wesentlichkeitsbestimmung wird regelmäßig auf die „Grundrechtsrelevanz" des geregelten Sachbereichs abgestellt.[1434] Kurz gesagt bedeutet das, dass die Wesentlichkeit und damit die Notwendigkeit einer Regelung durch Gesetz steigt, je intensiver die Materie in Grundrechte eingreift.[1435]

1429 *Herzog*, WM 1999, 1905 (1912); siehe allgemein *Starck* in v. Mangoldt/Klein/Starck GG, Art. 1 Rn. 227; ausf. zu Verwaltungsvorschriften als Grundrechtseingriff und Rechtsschutz *Sauerland,* Verwaltungsvorschrift, 2005, S. 391 ff., 417 ff.

1430 *Findeisen*, WM 1998, 2410 (2410 f.).

1431 *Herzog*, WM 1999, 1905 (1912).

1432 Idem, (1915) mit Verweis auf BVerfGE 61, 260 (275)

1433 *Fekonja,* Verlautbarungen, 2013, S. 194 ff.; *F. A. Schäfer* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 6 Rn. 16 ff.

1434 BVerfGE 49, 89 (126 f.); *Kotzur* in v. Münch/Künig GG, GG Art. 20 Rn. 157; *Kalscheuer/Jacobsen*, DÖV 2018, 523 (525).

1435 *Maurer/Waldhoff,* Verwaltungsrecht, 20. Aufl. 2020, § 6 Rn. 14; *Sauerland,* Verwaltungsvorschrift, 2005, S. 304 Fn 513 mit Verweis auf *Horn,* Verwaltung, 2020, S. 85 f. Fn 239.

Im Rahmen dieser Darstellung bezog er sich auf seine Ausführungen aus dem Jahr 1996,[1436] die er durch die Verlautbarung als bestätigt ansah. Das EDV-Research und -Monitoring käme in den Ziff. 18, 30 und 34 lit. d) zum Ausdruck.[1437] Die Vorgänge beeinträchtigten die informationelle Selbstbestimmung der Kunden. Zwar würde schon die Speicherung der Inhaltsdaten, deren Rechtsgrund nicht erwähnt wird, die informationelle Selbstbestimmung berühren, deren Verarbeitung sei aber ein „qualitativer Sprung" und somit eine eigenständig zu wertende Belastung.[1438]

Da ein Grundrechtseingriff vorliegt, greife der Vorbehalt des Gesetzes in Verbindung mit der Wesentlichkeitstheorie. Eine gesetzliche Grundlage für die in der Verlautbarung geforderten Maßnahmen gäbe es aber nicht. Weder § 14 Abs. 2 Nr. 2 GwG 1993 noch § 28 Abs. 1 BDSG 1990 kämen infrage. Eine hypothetische Verhältnismäßigkeitsprüfung der EDV-Prozesse unter der Prämisse einer geeigneten gesetzlichen Grundlage nahm *Herzog* in dem Beitrag nicht mehr vor.

Im Grunde zustimmend, aber differenziert äußerte sich *Kaufmann*[1439] zu den Argumenten *Herzogs.* Bei der bankinternen Datenrasterung handele es sich in der Tat um einen erheblichen Eingriff, da sich aus der Summe der Transaktionen eines Kunden ein wirtschaftliches Tätigkeits- und Leistungsprofil der Person ergeben würde.[1440] Solange der Eingriff aber bankintern bliebe, hätte er aufgrund des Privatrechtsverhältnisses keine Grundrechtsrelevanz. Erst die Verdachtsmeldung bilde die Schnittstelle zum hoheitlichen Tätigwerden.[1441] Würden die Banken eine Tätigkeit melden, deren Verdacht sich aus dem EDV-Research ergeben hätte, würde aufgrund der Meldung eine Verbindung zur Strafverfolgung hergestellt. Der gesamte Prozess würde dadurch einen staatlichen Charakter erhalten. Dies hätte zur Folge, dass der Staat sich bankinterne Daten beschafft hätte. So ein Vorgehen wäre aber in der StPO nicht vorgesehen und bräuchte eine spezifische Ermächtigungsgrundlage. Hierfür käme § 14 Abs. 2 Nr. 2 GwG aufgrund dessen Unbestimmtheit nicht infrage.[1442] Nach Ansicht *Kaufmanns* durften Banken die Daten ihrer Kunden also grundsätzlich rastern, die Ergebnisse

1436 *Herzog*, WM 1996, 1753 (1757 ff.).
1437 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.
1438 *Herzog*, WM 1999, 1905 (1916).
1439 *Kaufmann,* Geldwäsche, 2001, S. 174 ff.
1440 Idem, S. 176 f.
1441 Idem, S. 177.
1442 Ibid.

dieser Recherche aber nicht an die Staatsanwaltschaft übermitteln. Diese Vorstellung kann angesichts der Synergie bzw. der Wechselwirkung von Datenverarbeitungsschritten im Rahmen von Überwachungsmaßnahmen nicht überzeugen (s. Kap. B. I. 1. c.).

cc. Diskussionsbeiträge aus der Bankwirtschaft

Auch von Autoren aus der Bankwirtschaft wurde die Einführung des EDV-Research bzw. Monitoring mitunter kritisch besprochen. Der Geldwäschebeauftragte der Citibank *Bergles* und der Rechtsreferent beim Bankenfachverband *Schirnding* veröffentlichten gemeinsam einen Beitrag zur Umsetzung der EDV-Systeme in der Praxis.[1443] Auch sie begriffen die Ziff. 30 und 34 d der BAKred-Verlautbarung vom 30.03.1998 als Grundlage für die Anforderung zur Implementierung bankinterner Research-Systeme. Dabei versuchten sie zunächst, Ordnung in die bislang meist noch undifferenziert verwendeten Begriffe des „Research" und „Monitoring" zu bringen.[1444] Unter Research verstanden sie die personenunabhängige Recherche nach Auffälligkeiten im Datensatz der Banken. Als Monitoring bezeichneten sie die Überwachung eines konkreten Kontos.

Im Folgenden versuchten sie die Funktionsweise eines Research-Systems, das aus der großen Masse der Bankkonten die geldwäscheverdächtigen Fälle herausfiltert, näher zu umschreiben.[1445] Zunächst sollten in periodischen Abständen alle Konten auf zuvor definierte „Auffälligkeiten" untersucht werden. Die „Auffälligkeiten" müssten dann von dem Geldwäschebeauftragten oder einem Mitarbeiter kontrolliert und das entsprechende Konto einer Überwachung, also dem Monitoring, unterzogen werden. Falls sich kein Verdacht ergibt, sollte dies dem System klar gemacht werden, damit das Konto bei der nächsten periodischen Prüfung nicht unnötigerweise wegen den schon kontrollierten Kontobewegungen erneut gemeldet wird. Ergibt sich hingegen ein Verdacht, würde dieser nach § 11 GwG 1993 gemeldet.

Die Auffälligkeiten könnten nach relativen oder starren Mustern erkannt werden – also entweder an den regelmäßigen Bewegungen des geprüften Kontos oder festgelegten Schwellenwerten. Zentral sei die Höhe einer

1443 *Bergles/Schirnding*, ZBB 1999, 58.
1444 Idem, (59).
1445 Idem, (60 f.).

Transaktion. Es müssten aber weitere elektronisch greifbare Indikatoren hinzukommen – etwa ein Auslandsbezug, die Nationalität des Kunden, der Wohnort, ein Abbruch der Geschäftsbeziehung schon kurz nach Eröffnung des Kontos, die Anzahl der in Anspruch genommenen Bankprodukte und weitere.[1446]

Eine Betrachtung der Verfassungsmäßigkeit der von ihnen vorgeschlagenen Funktionsweise des EDV-Research und –Monitoring nahmen *Bergles/Schirnding* nicht vor. Sie wiesen lediglich auf die Kritik durch *Herzog* hin, ohne diese zu bewerten.

Einen Anschluss an dessen Argumente findet man jedoch in einer ausführlichen Besprechung des GwG samt den Verlautbarungen des BAKred durch die Mitarbeiter der Sparkasse Bonn *Lang/Schwarz/Kipp*.[1447] Aufbauend auf der Klarstellung von *Bergles/Schirnding* definierten sie die Begrifflichkeiten der EDV-Prozesse noch konkreter. *Lang/Schwarz/Kipp* verzichteten erstmals auf den Begriff des Research, der auch heute kaum mehr verwandt wird,[1448] und unterschieden stattdessen verschiedene Formen bzw. Phasen des Monitorings. Das bislang als Research bekannte Suchen nach Auffälligkeiten in nicht näher konkretisierten Datenbeständen bezeichneten sie als „Monitoring ohne Verdacht". Das Überwachen von Konten, bei denen eine Auffälligkeit entdeckt wurde, definierten sie hingegen als „Monitoring mit Verdacht". Bei diesem gäbe es einen speziell zu betrachtenden Unterfall, wenn der Verdacht auf einer externen Anfrage etwa einer Staatsanwaltschaft beruht. Diese dritte Kategorie bezeichneten sie als „Monitoring aufgrund externer Anfrage".[1449]

Die so identifizierten drei Varianten des Monitorings unterzogen sie in der Folge einer umfassenden verfassungsrechtlichen Prüfung. Am kritischsten wurde dabei das Monitoring ohne Verdacht beleuchtet.[1450]

Herzogs Ansicht[1451], dass schon die Speicherung der Kontoinhaltsdaten das Recht auf informationelle Selbstbestimmung tangiert, wollten sie in dieser Pauschalität nicht gelten lassen. Die Speicherung im Rahmen einer Geschäftsbeziehung erfolge mit Wissen und Wollen des jeweiligen Kunden,

1446 Idem, (61) mit Verweis auf *BAKred,* Rundschreiben 19/1998, Typologienpapier-Geldwäsche, 02.11.1998.
1447 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 610 ff.
1448 Vgl. *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14 lfd. Nr. 6.1.
1449 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff., Rn. 8.77.
1450 Idem, S. 644 ff., Rn. 8.4.2.X
1451 Idem, (1757).

da die Durchführung des Bankvertrags andernfalls nicht möglich wäre.[1452] Dabei verkannten sie aber offenbar, dass *Herzog*[1453] nicht von einer Verletzung des Rechts auf informationelle Selbstbestimmung durch die Speicherung gesprochen hatte, sondern nur von einer „Berührung".

Hinsichtlich der Verarbeitung der Datenbestände durch das anlasslose Monitoring teilten *Lang/Schwarz/Kipp* die verfassungsrechtlichen Bedenken *Herzogs*. Der Wortlaut des § 14 Abs. 2 Nr. 2 GwG 1993 spräche keinesfalls dafür, dass es sich um eine gesetzliche Grundlage für einen Eingriff in das Recht auf informationelle Selbstbestimmung handelte. Ebenso wenig wäre eine solche Grundlage nach Art. 5 der 1. EG-GWRL notwendig gewesen, denn auch deren Wortlaut erfordere nur die Prüfung beim Vorliegen von Auffälligkeiten und verpflichte nicht zur Vorfeldsuche.[1454] Differenzierter betrachteten die Autoren die Frage, ob sich eine gesetzliche Grundlage aus dem Datenschutzrecht und dort aus § 28 Abs. 1 Nr. 2 BDSG 1990 zur „Wahrung berechtigter Interessen" ergeben könnte.[1455] Die Früherkennung von Geldwäschefällen wäre schon deshalb im Interesse der Banken, da § 261 Abs. 5 StGB 1992[1456] das leichtfertige Nichterkennen von Geldwäsche unter Strafe stellte, was vor allem Bankmitarbeiter beträfe. Allerdings müsse das berechtigte Interesse i. S. d. § 28 Abs. 1Nr. 2 BDSG 1990 in Abwägung der entgegenstehenden Interessen ausgelegt werden.[1457] Diese Abwägung könnte nur zugunsten der Kunden ausfallen, da die Rasterung theoretisch aller Kundendaten schon aufgrund der Vielzahl der Kunden einen erheblichen Eingriff darstellte, dem ein höchst unsicheres Ergebnis gegenüberstünde.[1458] Dieser Datennutzung würde der Kunde, wenn er entscheiden könnte, sicher widersprechen. Auch sei zu berücksichtigen, dass Kunden als auffällig erkannt werden könnten, die tatsächlich mit Geldwäsche nichts zu tun haben. Dies würde das Vertrauensverhältnis zwischen Bank und Kunde zerrütten.[1459] Die Ansicht des BAKred, dass das anlasslose Monitoring auf

1452 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 650 Rn. 8.100.
1453 *Herzog*, WM 1996, 1753 (1757).
1454 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 651 Rn. 8.103.
1455 Idem, S. 654 ff., Rn. 8.106 ff.
1456 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15. Juli 1992, BGBL. I, S. 1302
1457 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 658 f. Rn. 8.109 mit Verweis auf BGH, NJW 1986, 2505 (2506).
1458 Iden, S. 661 Rn. 8.111.
1459 Idem. S. 662, Rn. 8.111.

§ 28 Abs. 1 Nr. 2 BDSG 1990 gestützt werden könne, sei deshalb unzutreffend.[1460]

Dem anlasslosen Monitoring stünde weiter entgegen, dass ein *hinreichender Anlass* von der Rechtsprechung als notwendige Mindestvoraussetzung von Eingriffen in die informationelle Selbstbestimmung gefordert würde. Je erheblicher ein solcher Eingriff sei, desto enger müsste er auf bestimmte Anlässe begrenzt sein.[1461] Über diesen Umstand herrsche aufgrund mehrerer Entscheidungen des BVerfG Einigkeit.[1462] Ermittlungen, die erst einen Anfangsverdacht zutage fördern sollten, verstießen deshalb gegen den Grundsatz der Verhältnismäßigkeit.[1463] Um genau so eine anlasslose Ermittlungsmaßnahme handle es sich aber bei dem EDV-Research, das das BAKred in der Verlautbarung vom 30.03.1998[1464] gefordert hatte.[1465]

Wie auch *Herzog* (s.o.)[1466] befanden *Lang/Schwarz/Kipp*, dass es sich bei der Durchführung des EDV-Monitoring nicht um eine hoheitliche Tätigkeit handeln könne.[1467] Es müsse sich schon deshalb lediglich um eine Inpflichtnahme Privater handeln, da die geforderte Maßnahme einer hoheitlich handelnden Behörde gar nicht zustehe.[1468] Gleichzeitig könne es aber nicht angehen, dass Private zu einem Eingriff aufgefordert werden, der dem Staat selbst nicht zustünde, da andernfalls der Grundrechtsschutz umgangen würde. Die Inpflichtnahme zum anlasslosen EDV-Monitoring sei insofern nicht zu rechtfertigen.[1469]

Etwas anderes gelte für das anlassbezogene Monitoring.[1470] Hier fehle die notwendige Voraussetzung eines hinreichenden Anlasses gerade nicht. Auch könnte man hier durchaus von einer Datenverarbeitung im berechtigten Interesse der Verpflichteten ausgehen, denn wenn eine Auffälligkeit bekannt ist, liefen die jeweils betrauten Mitarbeiter tatsächlich Gefahr, einer

1460 Idem, S. 661 ff., Rn. 8.111 f.
1461 Idem, S. 666. ff., Rn. 8.119 ff.
1462 Idem, S. 668 ff., Rn. 8.122 ff. mit Verweis vor Allem auf BVerfG, WM 1994, 691 = NJW 1994, 2079 und BVerfG ZIP 1995, 100 = NJW 1995, 2839.
1463 Idem, S. 680, Rn. 8.151 mit Verweis auf BVerfG, NJW 1997, 2163; Hamacher, WM 1997, 2149 (2151).
1464 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.
1465 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 683 Rn. 8.156.
1466 *Herzog,* WM 1996, 1753 (1758).
1467 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 685 Rn. 8.159 f.
1468 Idem, S. 685 Rn. 8.160.
1469 Ibid.
1470 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 690 ff., Rn. 8.172 ff.

Strafverfolgung wegen § 261 Abs. 5 StGB 1992 ausgesetzt zu werden.[1471] Außerdem seien die Institute an einer hohen „Qualität" der Verdachtsanzeigen interessiert. Sie wollen fehlerhafte Meldungen vermeiden. Hierzu können konkrete Nachforschungen im Wege eines anlassbezogenen Monitorings nützlich sein.[1472]

Das anlassbezogene Monitoring soll dabei auch dann möglich sein, wenn der Verdacht von außen herangetragen wird – etwa von einer Staatsanwaltschaft.[1473] Diese „dritte Kategorie"[1474] des Monitorings sollte aber von spezifischen Voraussetzungen abhängig gemacht werden. So müsse der Name des Verdächtigten genannt werden, denn eine Anregung zum Monitoring „ins Blaue hinein" sei aus den zuvor genannten Gründen zum anlasslosen Monitoring unzulässig.[1475]

4. Gesetzliche Einführung des EDV-Monitoring im Jahr 2002

Die Diskussion um das Kontenmonitoring ging weiter, nachdem § 14 Abs. 2 Nr. 2 GwG durch das Geldwäschebekämpfungsgesetz[1476] abgeändert und § 25a Abs. 1 Nr. 4 KWG mit dem vierten Finanzmarktförderungsgesetz[1477] neu eingefügt wurde.

Anstatt zur *„Entwicklung interner Grundsätze, Verfahren und Kontrollen zur Verhinderung der Geldwäsche"* waren die betroffenen Institute nunmehr nach § 14 Abs. 2 Nr. 2 GwG 2002 verpflichtet, *„interne Grundsätze, angemessene geschäfts- und kundenbezogene Sicherungssysteme und Kontrollen zur Verhinderung der Geldwäsche und Finanzierung terroristischer Vereinigungen"* zu entwickeln. In § 25a Abs. 1 Nr. 4 KWG 2002 hieß es zudem: *„Ein Institut muss über angemessene (…) Sicherungssysteme (…) verfügen; bei Sachverhalten, die aufgrund des Erfahrungswissens über die Methoden der Geldwäsche zweifelhaft oder ungewöhnlich sind, hat es diesen vor dem*

1471 Idem, S. 690 ff., Rn. 8.175 ff.
1472 Idem, S. 694 ff., Rn. 8.182.
1473 Idem, S. 698 ff., Rn. 8.190 ff.
1474 Idem, S. 642 ff. Rn. 8-77 ff., insb. S. 644 Rn. 8.78, 8.80.
1475 Idem, S. 699 ff., Rn. 8.193 ff.
1476 Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz) vom 08. August 2002 (BGBl. I S. 3105).
1477 Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) vom 21 Juni 2002 (BGBl. I, S. 2010).

Hintergrund der laufenden Geschäftsbeziehung und einzelner Transaktionen nachzugehen."

Die Einführung dieser *Sicherungssysteme* wurde in den Gesetzesmaterialien zu § 25a Abs. 1 Nr. 4 KWG 2002 ausdrücklich als gesetzliche Verankerung der EDV-Monitoringsysteme verstanden.[1478] Aus Sicht der Bundesregierung waren die Regelungsgehalte von § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002 aber, anders als der Bundesrat meinte, unterschiedlicher Natur.[1479]

Offenbar wich die Bundesregierung damit von der Vorstellung des BAKred ab, dass sich die Pflicht zum EDV-Monitoring aus § 14 Abs. 2 Nr. 2 GWG 1993 ergeben würde, und bevorzugte eine Regelung im KWG, damit ausschließlich Banken betroffen waren. Die Kritik an der zuvor vom BAKred geäußerten Rechtsauffassung, insbesondere bzgl. des Fehlens einer ausdrücklichen Ermächtigung zur Datennutzung, wurde aber bei der Schaffung des § 25a Abs. 1 Nr. 4 KWG 2002 nicht berücksichtigt. Auch diese Norm ließ eine entsprechende Klarstellung noch vermissen.

a. Stellungnahme des ZKA

Der ZKA hatte zu der Einführung des § 25a Abs. 1 Nr. 4 KWG 2002 durch das vierte Finanzmarktförderungsgesetz im Rahmen des Gesetzgebungsprozesses ausführlich Stellung genommen.[1480] Mit dem BAKred sei man sich prinzipiell einig, dass bei entsprechendem Anlass (sic), der kunden- oder transaktionsbezogen sein könne, alle Maßnahmen zur Aufklärung getroffen würden – auch die Verwendung der bankinternen EDV.[1481] Das sei aber schon auf Grundlage der aktuellen Gesetzeslage möglich. Eine Gesetzesänderung wäre also nur notwendig, wenn vom Gesetzgeber eine anlassunabhängige (sic) bzw. permanente Überwachung der Bürger für notwendig erachtet würde.[1482] Dies aber stellte eine Instrumentalisierung der Institute zu Zwecken der Strafverfolgung dar und ginge mit einem erheblichen Vertrauensverlust bei ihren Kunden einher. Auch würde § 25a

1478 BT-Drs. 14/8017, S. 125.
1479 BT-Drs. 14/9043, S. 11; aA. der Bundesrat idem, S. 5 f.
1480 *ZKA,* Stellungnahme zum 4. Finanzmarktförderungsgesetz, AZ: 413-FPLD, 13. Februar 2002.
1481 Idem, S.10.
1482 Ibid.

Abs. 1 Nr. 4 KWG 2002 die Anforderungen an eine gesetzliche Grundlage für eine solche permanente Rasterung nicht erfüllen. Die Vorschrift sei schon nicht bestimmt genug und hätte darüber hinaus aufgrund des Sachzusammenhangs im GwG normiert werden müssen.[1483]

b. Diskussion in der Literatur

In der Literatur war umstritten, ob die gesetzlichen Neuregelungen als endgültige Pflicht der Kreditinstitute bzw. der übrigen nach dem GwG Verpflichteten zum anlasslosen (EDV-)Monitoring verstanden werden mussten.[1484] Der damalige FAZ-Wirtschaftsredakteur *Jahn* verstand jedenfalls § 25a Abs. 1 Nr. 4 KWG 2002 als ausdrückliche gesetzliche Verpflichtung der Kreditinstitute zur aktiven und systematischen Durchforschung ihrer Kundendaten nach Geldwäschefällen.[1485] Eine verfassungsrechtliche Prüfung dieser Pflicht nahm er zwar nicht vor. *Jahn* stellte jedoch fest, dass die *„flächendeckende Präventivkontrolle und Datenspeicherung von Finanztransaktionen ein Ausmaß erreicht hätten, dass sich die Bürger eines Rechtsstaats in keinem anderen Lebensbereich bieten lassen würden.*"[1486]

Der Rechtsanwalt *Escher* hingegen war der Meinung, dass sich eine Pflicht zur anlasslosen Überwachung aus den § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002 nicht ergeben würde. Die betroffenen Institute müssten vielmehr ein Scoring-Verfahren etablieren, wonach bestimmte Transaktionen bzw. Transaktionstypen oder Kundentypen auf Auffälligkeiten durch die EDV zu prüfen wären und gegebenenfalls individuelle Nachforschungen angestellt werden sollten.[1487] Wie aber die so bestimmten Transaktionen gefunden werden sollten, wenn nicht alle verfügbaren Daten in die Rasterung einbezogen würden, ließ er offen.

Differenzierter sahen es Autoren aus der Bankwirtschaft selbst. So meinten *Bergles/Eul* etwa, dass sich aus der gesetzlichen Formulierung zwar

1483 Idem, S. 11.
1484 Siehe *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 52, der sich aber klar positionier und auf die Widersprüchlichkeit eines „anlassbezogenen" Monitorings hinweist; offen dagegen noch immer bei *Hartmann* KJ 2007, 2 (16 f.): „angedeutete Präventivkontrolle und Datenspeicherung".
1485 *Jahn*, ZRP 2002, 109 (110).
1486 Idem, (111).
1487 *Escher*, BKR 2002, 652 (661 f.).

nicht unmittelbar eine Pflicht der Kreditinstitute zur anlasslosen Überwachung ihrer Kunden ergäbe. Durch die neuen gesetzlichen Regelungen würden sie aber mehr denn je zu solch einer „Rasterung" gedrängt.[1488] Derweil waren sie der Auffassung, dass die geänderten bzw. neu gefassten Vorschriften § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002 nichts an der bisher vorgetragenen Kritik hinsichtlich der Normbestimmtheit ändern würden.[1489] Die neuen Begrifflichkeiten, insbesondere die Einführung „angemessener Sicherungssysteme", seien *„wenig geeignet allgemeine akzeptierte Datenschutzgrundsätze zu überschreiben."*[1490]

Allerdings käme § 28 Abs. 1 Nr. 2 BDSG 1991, der eine Datennutzung zu eigenen Zwecken erlaubt, hierzu durchaus in Betracht. Die im Rahmen des Research ermittelten Daten würden nicht unmittelbar und uneingeschränkt an die Sicherheitsbehörden übergeben, sondern wären Teil eines Riskmanagements, das den Banken im Vorfeld erlaube, ihre eigenen Risiken zu erkennen. Erst dieses Management erlaube eine effektive Geldwäschebekämpfung und mithin eine Verhinderung negativer Publicity, an der die Kreditinstitute ein eigenständiges wirtschaftliches Interesse hegten, wofür *Bergles/Eul* einige Beispiele aus der Presse anführten.[1491]

Ob dieses Interesse aber ein EDV-„Research/Screening" rechtfertigten könnte, sei fraglich. Im Rahmen des Durchlaufs der Transaktionsdaten könnten Bankkunden in einen falschen Verdacht geraten. Die Systeme bzw. deren Parameter müssten daher so konfiguriert werden, dass der Kreis der Personen, über den nach dem EDV-Programm weitere Nachforschungen angestellt werden, möglichst klein bliebe.[1492] Andererseits träte ein Vertrauensverlust bei den Kunden ein, den die Institute mit den Aktivitäten zur Verhinderung der Geldwäsche gerade zu verhindern suchten. Da insofern kein klarer Ausgang der Interessenabwägung im Rahmen des § 28 Abs. 1 Nr. 2 BDSG 1991 möglich sei, wäre der rechtliche Konflikt zwischen dem EDV-„Research/Screening" weiterhin ungelöst.[1493]

Der Anwalt *Scherp* betrachtete die Einwände gegen die „Researchpflicht", die er einheitlich mit § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG

1488 *Bergles/Eul*, BKR 2002, 556 (556); *Eul* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, S. 1085 (1098 ff.).
1489 *Bergles/Eul*, BKR 2002, 556 (562 f.).
1490 Idem, (562).
1491 Idem, (562 f.).
1492 Idem, (563).
1493 Idem, (564).; ausf. *Eul* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, S. 1085 (1100 ff.).

2002 überschrieb, als unschlüssig.[1494] Durch deren Einführung sei zunächst dem Argument, es bestünde keine taugliche Rechtsgrundlage, der Boden entzogen.[1495] Damit sei zwar noch nichts über die verfassungsrechtliche Zulässigkeit gesagt, auch hier könnten sich die kritischen Argumente aber nicht durchsetzen. Insbesondere kritisierte *Scherp* den Vergleich mit der Rasterfahndung i. S. d. § 98a StPO. Beim Kontenresearch würden nicht verschiedene Datenbanken abgeglichen, sondern nur die des jeweiligen Instituts. Betroffen seien somit nur Daten, die die Kunden freiwillig herausgegeben hätten. Die Daten seien in den Häusern vorhanden und deshalb dürften die Institute damit auch zu Zwecken der Geldwäschebekämpfung arbeiten.[1496] Bevor die Ergebnisse des Research analysiert und eventuell zu einer Meldung an staatliche Behörden führten, wäre lediglich das private Verhältnis von Bank und Kunde betroffen. Hier entfalteten die Grundrechte nur eine Ausstrahlungswirkung, weshalb die informationelle Selbstbestimmung nur begrenzt tangiert sei.[1497] Angesichts dessen sei das Research verhältnismäßig. Eine effektive Geldwäsche funktioniere nur durch einen risikoanalytischen Ansatz, der auf verschiedenen Risikograden und davon abhängenden Maßnahmen basierte. Durch die anschließenden Folgemaßnahmen würde gerade verhindert, dass es zu flächendeckenden Verdachtsmeldungen käme.[1498]

Von einer „tatbestandlichen Grundlage des Kontenscreening" sprachen auch *Herzog/Christmann*.[1499] Ihrer Meinung nach waren die § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002, die sie ebenfalls komplementär verstanden, eine ausdrückliche Ermächtigung der Banken zur digitalen Kontrolle der Transaktionen ihrer Kunden. Die Vorschriften würden aber den verfassungsrechtlichen Anforderungen an solch einen Eingriff in die informationelle Selbstbestimmung nicht gerecht werden.[1500] Ob die Banken durch die Vorschriften verpflichtet würden, ließen sie offen.

Bemerkenswert ist, dass *Herzog/Christmann* nicht nur die Ermächtigung der Banken ansprachen, sondern das Monitoring in einen Kontext mit den weiteren Änderungen des GwG stellten. Sie erkannten, ohne sich auf die ausdrückliche Auszeichnungs- und Aufbewahrungspflicht in § 9 GwG 2002

1494 *Scherp*, WM 2003, 1254 (1257 f.).
1495 Idem, (1257)
1496 Idem, (1257 f.).
1497 Idem, (1258).
1498 Ibid.
1499 *Herzog/Christmann*, WM 2003, 6 (11).
1500 Ibid.

zu berufen, dass die Banken aufgrund des *Kontenmonitoring „auf Vorrat Informationen für eine durch die Auskunftsbehörde oder Strafverfolgungsbehörden nach Bedarf einzuholende Auskunft verfügbar"* halten mussten. Ferner könne die neu geschaffene FIU im BKA nach § 5 Abs. 3 S. 2 GwG 2002 i. V. m. § 7 Abs. 2 BKAG 2002[1501] auf Daten bei den Banken zugreifen.[1502] Dem BKA käme durch diese Befugnis eine „Vorermittlungskompetenz" zu, die der Gesetzgeber eigentlich nicht einführen wollte.[1503]

Auch auf dem Bankrechtstag 2003, dokumentiert in einem Tagungsband[1504], wurde über die Auswirkungen des neuen Geldwäscherechts auf die informationelle Selbstbestimmung diskutiert. *Herzog* trug hier erneut vor, dass durch die *„Geldwäschebekämpfungsstrategie des Monitoring und Kontenscreening"* der Weg für eine umfassende Rasterung der Kontotransaktionen sämtlicher Bankkunden geebnet würde.[1505] Außerdem betonte er abermals, dass schon die Speicherung der Bankkundendaten einen Eingriff in die informationelle Selbstbestimmung der Kunden darstelle, da die weitere Datenverarbeitung zu verschiedenen Zwecken darauf aufbaue.[1506] Mit einem Verweis auf *Benda*[1507] machte *Herzog* aber klar, dass für ihn die Sammlung der Daten an sich kein Problem darstelle. Erst die (anschließende) Verarbeitung der Daten, die dem Betroffenen nicht gewahr wird, insbesondere durch staatliche Ermittlung, bedürfe einer gesonderten Ausgestaltung zur Wahrung des Verhältnismäßigkeitsprinzips.[1508] Eine solche Ausgestaltung verlangte eigentlich, dass im Rahmen des „Research" nur ein kleiner Kreis von Transaktionen ausgefiltert würde. Die Gesetzesbegründung des § 25a Abs. 1 Nr. 4 KWG 2002 sei aber so zu verstehen, dass zum Auffinden verdächtiger Transaktionen im Massengeschäft eine Vielzahl von

1501 Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 09. Januar 2002 (BGBl. I, S. 361).
1502 *Herzog/Christmann*, WM 2003, 6 (12).
1503 Ibid. mit Verweis auf BT-Drs. 14/9043, S.9
1504 *Hadding/Hopt/Schimansky* (Hrsg.), Bankrechtstag 2003, Basel II, 2004; zusammenfassend *C. Lange/Höche*, WM 2003, 1645.
1505 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (72); s.a. *ders.*, FS Kohlmann, 2003, S. 427 (448 ff.).
1506 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (59).
1507 *Benda* in Benda/Mailhofer/Vogel (Hrsg.), Hdb. Verfassungsrecht, 1984, S. 107 (123 f.).
1508 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (59 f.).

Transaktionen in den Verdachtsbereich gekehrt würden.[1509] Die umfangreiche Einbeziehung Unverdächtiger und deshalb geringe Trefferquote des Monitorings seien bei der Bewertung der Verhältnismäßigkeit zu berücksichtigen.[1510]

Verteidigt wurden § 25a Abs.1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 auf dem Bankrechtstag von *Findeisen*.[1511] Die Vorschriften verstünden sich im Lichte des international forcierten Paradigmenwechsels[1512] hin zu einem risikoorientierten, strukturpräventiven Ansatz (s. o. Kap. D. III. 2. a. ee.) bei der Geldwäschebekämpfung.[1513] Monitoring und Screening bestehender bzw. laufender Geschäftsbeziehungen erlaubten eine beständige Einschätzung des jeweiligen Kundenrisikos. Solche Risikoprofile erlaubten es wiederum, die Überwachung risikoarmer Kunden zu beschränken. Erst wenn der Abgleich eines Kundenrisikos mit dem Transaktionsmuster Ungewöhnlichkeiten hervorbrächte, wären weitere Aufklärungsschritte erforderlich. [1514] Die Bankenaufsicht würde dabei nur prüfen, ob ein solches System überhaupt integriert sei. Eine vollumfängliche Rasterung der Kundendaten und deren Herausgabe an staatliche Stellen verlange sie gerade nicht.[1515]

Dass ein vollumfänglicher Datensatz für das Funktionieren eines solchen Systems, insbesondere für den regelmäßigen Abgleich des Risikoprofils, notwendig ist, ließ aber auch *Findeisen* nicht unerwähnt. Die Verwendung und Aufbewahrung der Transaktionsdaten zu Zwecken der Geldwäschebekämpfung hielt er jedoch für verfassungs- bzw. datenschutzrechtlich unbedenklich. § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 seien Teil einer konsequenten „Customer Due Diligence-Politik" und taugliche Rechtsgrundlage des nunmehr etablierten EDV-Monitorings.[1516] Die Bank dürfe mit den aufgrund der Bankverträge vorhandenen Kundendaten arbeiten, um Reputations-, Organisations- und Rechtsrisiken zu vermeiden.

1509 Idem, (73).
1510 Ibid.
1511 *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95.
1512 *FATF,* 40 Recommendations, 2003, Nr. 5, 15; *Basler Ausschuss für Bankenaufsicht,* Sorgfaltspflichten, Oktober 2001, lfd. Nr. 53.
1513 *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (113 ff.).
1514 Idem, S. 115.
1515 Idem, S. 116.
1516 Idem, S. 117

Die bankinterne Geldwäschebekämpfung sei keine staatliche Fahndungsmaßnahme, sondern verantwortungsbewusste Risikominderung der jeweiligen Häuser.[1517] Interessant an den Ausführungen *Findeisens* ist, dass er ebenfalls – anders als der Gesetzgeber (s.o.) – § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 als einheitlich zu verstehende Rechtsgrundlage des Kontenmonitorings verstand.

Eine umfassende verfassungs- und menschenrechtliche Prüfung des – inhaltlich unveränderten – § 25a Abs. 1 S. 3 Nr. 6 KWG 2005[1518] findet sich in der Dissertation von *Degen.*[1519] Dieser begriff die Vorschrift als *„Verpflichtung, alle Kundendaten auf Verdachtsmomente bzgl. der Geldwäsche zu überprüfen"*.[1520] Dieses „Konten-Screening" stelle einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Die Kundendaten seien zwar vom Kunden in dem Wissen an die Bank übertragen worden, dass sie dort verarbeitet werden. Sie würden dazu jedoch nicht zu Daten der Bank, sondern seien weiterhin dem Kunden zuzuordnen.[1521] Mit Verweis auf *Herzog* erkannte *Degen*, dass schon durch die Speicherung der Grundstein für eine mögliche außervertragliche Verwendung gelegt würde. Erst aber, wenn diese Verwendung auch stattfindet, sei der Schutzbereich in verstärktem Maß berührt. [1522] Auch *Degen* äußerte somit an der Speicherung an sich keine grundrechtlichen Zweifel. Seine Kritik zielte allein auf die Monitoring-Pflicht. Diese hielt er – aufgrund einer ausführlichen Prüfung, die hier nur ganz knapp wiedergegeben werden kann, – im Ergebnis für verfassungs- und menschenrechtswidrig.[1523]

Zunächst sei § 25a Abs. 1 S. 3 Nr. 6 KWG 2005 unbestimmt, da weder die typologisierten Geldwäscheverdachtsmomente noch eingriffsbegrenzende Merkmale und die Anforderungen an die Systeme hinreichend konkretisiert wurden.[1524] Auch sei die Vorschrift unverhältnismäßig. Die Rasterung massenhafter Daten mit Sozialbezug, die die Schaffung eines Persönlichkeitsbildes theoretisch zuließen, ohne individuellen Anlass stelle letztlich

1517 Idem, S. 118
1518 Gesetz zur Umsetzung der Richtlinie 2002/87/EG des Europäischen Parlaments und des Rates vom 16 Dezember 2002 (Finanzkonglomeraterichtlinie-Umsetzungsgesetz) vom 21. Dezember 2004 (BGBl. I. S. 3610).
1519 *Degen,* Geldwäsche, 2009, S. 196 ff.
1520 Idem, S. 197.
1521 Idem, S. 200.
1522 Idem, S. 200 mit Verweis auf *Herzog*, WM 1999, 1905 (1916).
1523 Idem, zusammenfassend S. 270 ff.
1524 Idem, S. 205 ff., zusammenfassend S. 216.

eine Pauschalüberwachung dar, die den Wesensgehalt der informationellen Selbstbestimmung tangierte.[1525] Unabhängig vom Ausgang einer Güterabwägung sei das Konten-Screening daher verfassungswidrig. Auch dies ginge aber zulasten des Staates aus. Das Konten-Screening führe zu einer systematischen Überwachung einer großen Zahl Unbeteiligter, die keine Chance auf einen effektiven Rechtsschutz hätten. Da die Geldwäschevortaten mittlerweile auch Bagatelldelikte einschließen, sei das Screening nicht mehr auf Schwerstkriminalität begrenzt. Das Gemeininteresse an der Maßnahme sei daher reduziert und könne den schwerwiegenden Eingriff nicht rechtfertigen.[1526] Alles zu § 25a Abs. 1 S. 3 Nr. 6 KWG 2005 Gesagte gelte im Übrigen auch für § 14 Abs. 2 Nr. 2 GwG, da diese als Parallelnorm dieselbe Verpflichtung enthalte.[1527] Beide Normen seien überdies auch nicht mit Art. 8 Abs. 1 EMRK in Einklang zu bringen, da es auch hier an der Verhältnismäßigkeit bzw. der Notwendigkeit i. S. d. Art 8 Abs. 2 EMRK fehlte.[1528]

c. Kritik der Datenschutzbeauftragten

Wie die Literatur, stuften auch Datenschutzbeauftragte die § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 als Versuch einer Etablierung des Kontenmonitoring im Gesetz ein.[1529] Der Bundesbeauftragte stellte im Jahresbericht 2001-2002 (nur) in Bezug auf § 25a Abs. 1 Nr. 4 KWG 2002 zwar fest, dass die Analyse von Transaktionen mittels EDV *„doch erheblich in die Persönlichkeitsrechte der Betroffenen“* eingreife. Die Analyse und Kontrolle sei aber auf den Zweck der Geldwäschebekämpfung und Terrorismusfinanzierung begrenzt und daher akzeptabel.[1530] Hinsichtlich der Verwendung umfassender Datensätze und der Notwendigkeit deren Anlegung zu einem sicherheitsrechtlichen Zweck äußerte sich der Bundesdatenschutzbeauftragte nicht. Auch die Frage nach der spezifischen Rechtsgrundlage für das Vorgehen der verpflichteten Institute beantwortete er nicht ausdrücklich, wenngleich es in dem Bericht so klingt, als ob § 25a Abs. 1 Nr. 4 KWG 2002 selbst als Rechtsgrundlage angesehen würde.

1525 Idem, S. 222 ff.
1526 S. 227 ff.
1527 S. 236 ff.
1528 S. 245 ff.
1529 *DSB Bund,* 19. Tätigkeitsbericht, 2001-2002, S. 67; *DSB Berlin,* Jahresbericht, 2005, S. 51 ff.
1530 *DSB Bund,* 19. Tätigkeitsbericht, 2001-2002, S. 67.

Deutlich kritischer äußerte sich der Berliner Datenschutzbeauftragte im Jahresbericht 2005. Dieser hatte zuvor schon die Forderungen des BAKred nach EDV-Monitoring-Maßnahmen in Zweifel gezogen[1531] und nahm die gesetzliche Verankerung zum Anlass einer erneuten Besprechung.[1532]

Der Berliner Datenschützer besprach § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 einheitlich als „Rasterfahndung zur Bekämpfung der Geldwäsche". Allerdings seien diese Normen keine tauglichen Rechtsgrundlagen für einen Dateneingriff, da sie hierfür zu unbestimmt seien. Als Rechtsgrundlage komme allenfalls § 28 Abs. 1 Nr. 2 BDSG 1991[1533] in Betracht. Um danach rechtmäßig zu sein, müsste sich das Kontenmonitoring aber an bestimmte Grenzen halten. Transaktionen sollten nur bereichsspezifisch gerastert werden. Nur bei Banken, die insgesamt ein hohes Risiko für sich feststellen, wäre ein Monitoring sämtlicher Transaktionen möglich. Sobald Risiken bei Transaktionen erkannt würden, müssten diese entsprechend gekennzeichnet und separat gespeichert werden. Außerdem müssten die Bankkunden über die Anwendung von EDV-Systemen in den jeweiligen Instituten informiert werden.[1534] Im Übrigen müssten die verwendeten Parameter einer Plausibilitätskontrolle unterzogen werden, die sich am Ende am Ergebnis messen lassen muss. Nur ein effektives Monitoring, bei der die positiven Ergebnisse in einem angemessenen Verhältnis zu den einbezogenen Daten stünden, könne danach rechtmäßig sein.[1535]

d. Zusammenfassung und Stellungnahme

Das EDV-Monitoring wurde also nach der gesetzlichen Verankerung im Jahr 2002 stärker unter allgemein datenschutzrechtlichen und Aspekten der Wesentlichkeit diskutiert. Es findet sich zwar auch eine umfassende und sehr kritische Prüfung der verfassungsrechtlichen Verhältnismäßigkeit,[1536] besondere Aufmerksamkeit wurde dieser Frage aber nicht mehr gewidmet. Die Argumente lagen im Kern ja auch schon seit 1996 auf dem Tisch.[1537] Darüber hinaus war der ursprünglich angestellte Vergleich mit der strategi-

1531 *DSB Berlin,* Jahresbericht, 2000, S. 48 ff.
1532 *Ders.,* Jahresbericht, 2005, S. 50 ff.
1533 Idem, S. 51 f.
1534 Idem, S. 52 f.
1535 Idem, S. 53.
1536 *Degen,* Geldwäsche, 2009, S. 196 ff, zusammenfassend S. 270 ff.
1537 *Herzog*, WM 1996, 1753 (1757 ff.).

schen Fernmeldeaufklärung des BND[1538] kaum mehr fruchtbar zu machen, da das BVerfG in der Hauptsache die strategische Fernmeldeüberwachung für verfassungskonform befunden hatte.[1539]

Mit der Aufbewahrungspflicht setzten sich die Autoren größtenteils noch immer nicht vertieft auseinander. Immerhin *Herzog/Christmann* erkannten jedoch, dass die Pflicht zum EDV-Monitoring gemeinsam mit der Aufbewahrungspflicht zu einem Vorhalten der Daten für sicherheitsrechtsrechtliche Zwecke führen müsse und kritisierten, dass die neu geschaffene, beim BKA angesiedelte FIU auf diese Daten zugreifen könnte.[1540] Zwar hielt *Herzog* die Speicherung von Bankdaten grundsätzlich für kein Problem, sondern kanalisierte die Kritik auf die anschließende Monitoring-Pflicht.[1541] Das Problem, dass das Anti-Geldwäscherecht nicht nur eine Art strategische Rasterung vorsieht, sondern auch als Vorratsdatenspeicherung verstanden werden kann, war jedoch erstmals formuliert – und zwar, bevor die verfassungs- und europarechtliche Diskussion über eine Vorratsdatenspeicherung im Kontext der Telekommunikationsdaten überhaupt Fahrt aufnehmen konnte.[1542]

5. Kritik in Deutschland seit Einführung der Überwachungspflicht

In § 3 Abs. 1 Nr. 4 GwG 2008[1543] wurden die Verpflichteten des GwG in Umsetzung von Art. 8 Abs. 1 lit. d) der 3. GWRL bzw. Grundsatz 5 lit. d) der FATF-Empfehlungen[1544] zur *kontinuierlichen Überwachung ihrer Geschäftsbeziehungen einschließlich der in ihrem Verlauf durchgeführten Transaktionen* verpflichtet. Damit wurde die geldwäscherechtliche Überwachungspflicht, die in dieser Form noch heute besteht, als eine der allgemeinen Sorgfaltspflichten etabliert.

1538 *Dahm*, WM 1996, 1285 (1290) mit Verweis auf BVerfGE 93, 181

1539 BVerfGE 100, 313 – strategische Fernaufklärung.

1540 *Herzog/Christmann*, WM 2003, 6 (12).

1541 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (59 f.); *ders.*, WM 1996, 1753 (1757); *ders.*, WM 1999, 1905 (1916); ebenso *Degen,* Geldwäsche, 2009, S. 200.

1542 Übersicht der frühen Diskussion bei *Breyer,* Vorratsspeicherung, 2005, S. 29 ff.

1543 Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz - GwBekErgG) vom 13.08.2008 (BGBl. I, S. 1690).

1544 *FATF,* 40 Recommendations, 2003.

An diese Sorgfaltspflichten knüpft seitdem, wenngleich dies politisch durchaus kontrovers diskutiert wurde (s. o. Kap. D. III. 2. a. ff. (3)),[1545] die Aufzeichnungs- und Aufbewahrungspflicht des § 8 GwG 2008 an.

Auch die Verpflichtung zur Schaffung interner Sicherungsmaßnahmen war im GwBekErG neu gefasst worden. Nach § 25c Abs. 2 KWG 2008[1546] waren die Kreditinstitute nunmehr gehalten, *„angemessene Datenverarbeitungssysteme zu betreiben (…), mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen zu erkennen, die (…) als zweifelhaft oder ungewöhnlich anzusehen sind. (…). Die Institute dürfen personenbezogene Daten erheben, verarbeiten und benutzen, soweit dies zur Erfüllung dieser Pflicht erforderlich ist.*" Erstmals fand sich somit ausdrücklich eine unmittelbare Ermächtigung zur Datenverarbeitung für die systematische Erkennung von ungewöhnlichen Transaktionen.

Eine entsprechend ausdrückliche Verpflichtung bzw. Ermächtigung wurde im GwG hingegen nicht geschaffen. Hier war in § 9 Abs. 2 Nr. 2 GwG 2008 weiter nur von *angemessenen Sicherungssystemen* die Rede. Die bisher bestehende Regelung des § 14 Abs. 2 Nr. 2 GwG 2002 wurde lediglich verschoben. Damit war klargestellt, dass die Pflicht zum EDV-Monitoring ausschließlich Kreditinstitute (später alle Finanzinstitute sowie Finanzholding-Gesellschaften) betraf.

a. Akzeptanz des Monitorings in der deutschen Literatur

Von der Literatur wurde die Überwachungspflicht nach § 3 Abs. 1 Nr. 4 GwG 2008 im Kontext der bestehenden Debatte um das EDV-Monitoring besprochen. So stellten die Autoren meist fest, dass die Überwachungspflicht eine sachliche Nähe zu den internen Sicherungsmaßnahmen i. S. d. § 25c Abs. 2 KWG 2008 aufwiesen.[1547]

1545 BT-Drs. 16/9647, S. 3 f.

1546 Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz - GwBekErgG) vom 13.08.2008 (BGBl. I, S. 1690); zuvor § 25a Abs.1 Nr. 4 KWG 2002; § 25a Abs. 1 Satz 3 Nr. 6 KWG 2005; § 25a Abs. 1 Satz 6 Nr. 3 KWG 2007; zur Änderungsgeschichte *Achtelik* in Herzog GwG, 3. Aufl. 2018, KWG § 25h Rn. 1 f.

1547 *Warius* in Herzog GWG, 1. Aufl. 2010, § 3 Rn. 26, § 9 Rn. 55; *Ackermann/Reder*, WM 2009, 158 (164).

In der Praxis waren die Systeme mittlerweile flächendeckend etabliert.[1548] Die Diskussion um die Zulässigkeit des Monitorings stellte sich angesichts dieser neuen Faktenlage weitestgehend ein. Selbst in einem mitherausgegebenen Handbuch von *Herzog*, der sich bislang als beständigster Kritiker gezeigt hatte,[1549] wurde die Kritik am EDV-Monitoring von *Mülhausen* nunmehr als unberechtigt bezeichnet. Auffällige Transaktionen könnten faktisch und sicher nur durch EDV-Systeme erfasst werden. Zur Effektivität der Geldwäschebekämpfung seien die Systeme also obligatorisch.[1550]

Ähnlich äußerten sich die BaFin Mitarbeiter *Ackermann/Reder*.[1551] Diese fassten die kritischen Äußerungen der vorigen Jahre zusammen und kamen zu dem Schluss, dass zuletzt nur noch die Rechtsgrundlage des EDV-Monitorings ernsthaft diskutiert worden war.[1552] Mit der Neufassung des § 25c Abs. 2 KWG 2008 sei diese rein akademisch geführte Diskussion nunmehr obsolet, da die Vorschrift ausdrücklich zur Datenverarbeitung ermächtigte.[1553]

Verfassungsrechtliche Bedenken stellten sie nicht an. Das EDV-Monitoring müsse seiner Natur nach anlasslos sein, denn es ziele gerade nicht auf die Prüfung von anlassgebenden Fällen.[1554] Stattdessen verfolge es den Zweck, aus der großen Menge der irrelevanten Transaktionen typischerweise verdächtige Fälle zu identifizieren. Dies könne nur gelingen, wenn für alle Kunden ein Risiko- und Verhaltensprofil anhand ihrer Transaktionen erstellt würde, damit Abweichungen erkannt werden könnten.[1555] Eine anlasslose Rasterung aller Transkationen solle aber dennoch nicht erfolgen, da bestimmte Risikobereiche nach der institutsinternen Analyse aus dem Raster herausgenommen werden könnten.[1556]

1548 *BaFin,* Jahresbericht, 2006, S. 195.
1549 *Herzog*, WM 1996, 1753; *ders.*, WM 1999, 1905; *ders.*, FS Kohlmann, 2003, S. 427; *ders.* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47; *Herzog/Christmann*, WM 2003, 6.
1550 *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 53.
1551 *Ackermann/Reder*, WM 2009, 158 (164 f.).
1552 Idem, (164).
1553 Idem, (165).
1554 Ibid., so auch schon *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 52.
1555 *Ackermann/Reder*, WM 2009, 158 (165).
1556 Ibid.

Über die Auswirkungen der Überwachungspflicht auf die Aufbewahrungspflicht äußerten sich *Ackermann/Reder* nicht. Sie stellten lediglich fest, dass die Pflicht zur Aufbewahrung von Belegen über Geschäftsbeziehungen und Transaktionen neu in das Gesetz aufgenommen wurde.[1557] Dass eine solche Pflicht auch aus der Verknüpfung von sorgfaltspflichtiger Überwachung und entsprechender Aufzeichnung bzw. Aufbewahrung folgen könnte, bemerkten sie nicht. Sie erklärten allerdings, dass eine Kohärenz zur handelsrechtlichen Aufbewahrungspflicht wegen verschiedener Fristenläufe nicht hergestellt werden konnte.[1558] Offensichtlich gingen sie also davon aus, dass diese Regelungen zumindest inhaltlich identisch sein mussten. Dass eine sicherheitsrechtliche Pflicht zur Speicherung von Transaktionsbelegen verfassungsrechtlich problematisch sein könnte, kam den Autoren dabei nicht in den Sinn.

Weniger überzeugt zeigte sich der Rechtsanwalt *Kaetzler*. § 25c KWG 2008 sei zwar als Einführung einer datenschutzrechtlichen Grundlage hervorzuheben, die Norm schüfe aber nur einen groben Eingriffs- und Rechtfertigungstatbestand. Die datenschutzrechtliche Zulässigkeit von Rasterungen nach persönlichen Merkmalen, etwa der Staats- oder Religionsangehörigkeit im Rahmen der EDV-Systeme, seien durchaus zweifelhaft.[1559] Auch er meldete aber an der Verpflichtung der Banken zur elektronischen Rasterung ihrer Kundendaten keine grundsätzlichen verfassungsrechtlichen Bedenken mehr an.

Ein ähnliches Bild zeigte sich in der Kommentarliteratur. Laut *Achtelik* hätte sich der Streit um die datenschutzrechtliche Grundlage *„spürbar entschärft"*.[1560] Er wies jedoch darauf hin, dass die früher angemeldeten datenschutz- und verfassungsrechtlichen Bedenken durch die Schaffung einer rechtlichen Grundlage nicht ausgeräumt worden seien.[1561] Eine eigene Einschätzung gab er jedoch nur insofern ab, als dass er die Unbedenklichkeit der Monitoringsysteme zurückwies.[1562]

1557 *Ackermann/Reder*, WM 2009, 200 (207 f.).
1558 Idem, (208).
1559 *Kaetzler*, CCZ 2008, 174 (179 f.); zust. *Warius* in Herzog GWG, 1. Aufl. 2010, § 9 Rn. 63.
1560 *Achtelik* in Herzog GWG, 1. Aufl. 2010, KWG § 25c Rn. 25.
1561 Idem, KWG § 25c Rn. 26.
1562 Ibid.

b. Unzureichende Betrachtung der Aufzeichnungs- und Aufbewahrungspflicht unter dem Aspekt der Vorratsdatenspeicherung

Mit dem Abfallen der Kritik am Monitoring ging einher, dass eine kritische Betrachtung der ausgedehnten Aufbewahrungspflichten weitestgehend ausblieb. Dies vermag durchaus zu überraschen, denn die Neufassung des GwG im Jahr 2008 fiel in eine Zeit, in der kontrovers über das Thema Vorratsdatenspeicherung diskutiert wurde.[1563] Wie bereits dargestellt, war auch der Politik nicht verborgen geblieben, dass ein Anknüpfen der Aufbewahrungspflicht an die Überwachungspflicht zu einer umfassenden Speicherpflicht von Kontoinhaltsdaten aus sicherheitsrechtlichen Gründen führen könnte. Die FDP-Fraktion hatte diesen Umstand offen angesprochen und gefordert, dass die Aufbewahrungspflicht nicht an die Überwachungspflicht anknüpfte.[1564] Ohne Erfolg.

Man muss hier natürlich sehen, dass Art. 30 lit b.) der 3. GWRL ohnehin festlegte, dass *„bei Geschäftsbeziehungen und Transaktionen die Belege und Aufzeichnungen (…), für die Dauer von mindestens fünf Jahren nach Durchführung der Transaktion oder nach Beendigung der Geschäftsbeziehung"* aufbewahrt werden müssten. Die umfassende Speicherpflicht von Transaktionsbelegen konnte man daher auch unabhängig von der umfassenden Überwachungspflicht als obligatorisch ansehen. Wieso aber diese neue Pflicht in der GWRL grundsätzlich keine Kontroverse in Gang setzte, ist mit dieser Erkenntnis noch nicht beantwortet.

aa. Überblick der knappen Ansätze in der Literatur zum GwG

Völlig unbeachtet blieb der Komplex indes nicht. *Achtelik* etwa stellte in Bezug auf § 25c Abs. 2 KWG 2008 fest, dass das EDV-Monitoring, auch wenn der Gesetzgeber nach eigener Aussage datenschutzrechtliche Standards berücksichtigt haben wollte[1565], faktisch die Vorhaltung massenhafter Daten voraussetzt.[1566] Er stellte jedoch weder ausdrücklich die Frage, ob diese Datenvorhaltung verfassungs- oder europarechtswidrig sein könnte, noch ging er auf den Umstand ein, dass die Transaktionsdaten aufgrund von Vorschriften anderer Rechtsgebiete ohnehin gespeichert werden.

1563 Übersicht bei *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 164 ff.
1564 BT-Drs. 16/9647, S. 3.
1565 BR-Drs. 168/08, S.109.
1566 *Achtelik* in Herzog GWG, 1. Aufl. 2010, KWG § 25c Rn. 25.

Ähnlich knappe Betrachtungen finden sich in der jüngeren Literatur immer wieder hinsichtlich verschiedener Regelungen des Anti-Geldwäscherechts. Diese sind zwar sehr ausdrücklich, lassen aber eine tiefere Auseinandersetzung vermissen.

Von einer *„gesetzlich angeordneten anlasslosen Vorratsdatenspeicherung"* im aktuellen GwG spricht etwa *Heinson*[1567] und zwar in Bezug auf § 6 Abs. 6 GwG (Art. 42 der 4./5. GWRL), wonach die Verpflichteten Vorkehrungen treffen, *„um auf Anfrage der Zentralstelle für Finanztransaktionsuntersuchungen oder auf Anfrage anderer zuständiger Behörden Auskunft darüber zu geben, ob sie während eines Zeitraums von fünf Jahren vor der Anfrage mit bestimmten Personen eine Geschäftsbeziehung unterhalten haben und welcher Art diese Geschäftsbeziehung war. Sie haben sicherzustellen, dass die Informationen sicher und vertraulich an die anfragende Stelle übermittelt werden."*

Dabei übersieht *Heinson* die eigentlich sensiblen Regelungen. § 6 Abs. 6 GwG ist zwar auf den ersten Blick problematisch, da er die Einrichtung heimlicher Zugänge vorschreibt. Zu einer Vorratsdatenspeicherung kommt es aber zuvorderst durch eine umfassende Speicherpflicht bestimmter Daten und die spezifischen Ermächtigungen, auf diese Daten zuzugreifen. Dafür einzurichtende Kanäle ermöglichen dann zwar die Abfrage, sie sind aber nur als Teil eines Vorschriftenkomplexes bedenklich. Dieser Vorschriftenkomplex wird in der Besprechung von *Heinson* nicht ansatzweise ausführlich dargestellt. Darüber hinaus bezieht sich § 6 Abs. 6 GwG (Art. 42 der 4./5. GWRL) nur auf das Bestehen einer Geschäftsbeziehung und deren Eigenart. Es handelt sich also um eine Bestandsdatenabfrage. Diese ist in Deutschland ohnehin automatisiert möglich (s. o.). Ein Zugriffsrecht auf Finanztransaktionsdaten ergibt sich aus dem Wortlaut des § 6 Abs. 6 GwG nicht.

Eine ganz ähnliche Kritik findet sich bei *Krais*. Auch dieser erkannte eine europarechtlich zweifelhafte Vorratsdatenspeicherung[1568] in Art. 42 der 4. GWRL (umgesetzt durch § 6 Abs. 6 GwG). An der Aufbewahrungspflicht für Transaktionsbelege und andere Dokumente selbst aus § 8 GwG scheint er hingegen, wie auch *Heinson*, keine weiteren europa- oder verfassungsrechtlichen Bedenken zu hegen, wobei er aber diese Pflicht auch nicht umfassend für alle Transaktionsbelege, sondern nur für „*Erforderliche*" gelten

1567 *Heinson* in Specht/Mantz (Hrsg.), Hdb. Europ. & Deutsches Datenschutzrecht, 2019, § 14 Rn. 91.

1568 *Krais*, CCZ 2015, 251 (252).

lassen will.[1569] Diese Auslegung dürfte mit Art. 40 der 4./5. GWRL indes unvereinbar sein (s. o. Kap. D. III. 2. d. bb.).

Ausdrücklich bezeichnet auch *Spoerr* in einer aktuellen Kommentierung das allgemein in den Vorschriften, insbesondere aber in § 25h Abs. 2 KWG[1570], zum Ausdruck kommende *„Know-your-Transaction-Prinzip"* als *„umfassende Vorratsdatenspeicherung"*.[1571] Die Aufzeichnungs- und Aufbewahrungspflicht bzw. vergleichbare Vorschriften, auf denen die Anlegung des Datenbestandes für das EDV-Monitoring erst beruht, erwähnt er mit keinem Wort. Auch *Spoerr* stellt damit nur einen einzelnen Aspekt heraus, anstatt die Kombination aus Aufbewahrungs- und Überwachungspflicht als gemeinsamen Komplex zu beschreiben. Eine umfassende Prüfung der Rechtmäßigkeit dieses Komplexes vermisst man ohnehin.

bb. Erklärungsversuche der ausbleibenden Kritik

Darüber, weshalb das GwG seit der Neufassung im Jahr 2008 in Deutschland nicht in besonderer Weise unter dem Stichwort der Vorratsdatenspeicherung diskutiert bzw. überhaupt auf die Vereinbarkeit mit höherem Recht geprüft wurde, lassen sich natürlich nur Vermutungen anstellen. Einmal ist sicher zu beachten, dass § 8 Abs. 1 GwG 2008 eine Aufbewahrung von Transaktionsbelegen weiter von der Ausführung der Sorgfaltspflichten abhängig gemacht hatte. Welche Maßnahmen der Verpflichteten ganz konkret zu den Sorgfaltspflichten zählen, wurde von den Besprechungen aber nicht ausführlich genug betrachtet.

So wurde zwar schnell ein Zusammenhang der für die Banken geltenden Monitoring-Pflicht nach § 25c KWG 2008 und der Überwachungspflicht aus § 3 Abs. 1 Nr. 4 GwG 2008 hergestellt.[1572] Die konsequente Feststellung, dass damit das EDV-Monitoring sämtlicher Kundenbeziehung unter die Sorgfaltspflichten fällt, vermisst man aber in dieser Ausdrücklichkeit.

Mit dieser Erkenntnis hätte es keinen Zweifel mehr geben können, dass auch eine Aufbewahrungspflicht, die nur im Rahmen der Sorgfaltspflichten greift, sämtliche Transaktionsdaten erfasst. Dies musste schon damals unabhängig davon gelten, ob man die Aufbewahrung der Transaktionsdaten

1569 *Ders.*, Geldwäsche, 2018, Rn. 284.
1570 *Spoerr* in BeckOK Datenschutzrecht, Syst. J Rn. 226.
1571 Idem, Syst. J Rn. 153.
1572 Vgl. *Warius* in Herzog GWG, 1. Aufl. 2010, § 3 Rn. 26, § 9 Rn. 55; *Ackermann/Reder*, WM 2009, 158 (164).

als Folge oder Voraussetzung der Sorgfaltspflicht verstehen wollte, denn schon § 8 Abs. 1 GwG 2008 sprach von den „eingeholten" Informationen. Somit sind die Transaktionsdaten auch dann erfasst, wenn man sie nicht als Ergebnis der Überwachungspflicht, sondern als deren Grundlage versteht (s. o. Kap. D. III. 2. d. bb. (1)).

Auf diese Problematik wurde in der Literatur nicht eingegangen. Es bleibt damit im Unklaren, welche Vorstellungen sich die Autoren hinsichtlich des Umfangs der Aufbewahrungspflicht machten. Aber selbst wenn stillschweigend § 8 Abs. 1 GwG 2008 als umfassende Speicherpflicht betrachtet worden wäre, darf bei der Beurteilung der Diskussion nicht vergessen werden, dass es solche Pflichten in anderen Gesetzen schon gab. So wurde etwa bei der Fristenregelung durchaus erkannt, dass diese anfänglich nicht mit den Fristen aus § 257 HGB, § 147 Abs. 1, 3 AO gleichliefen.[1573] Da § 8 Abs. 3 GwG 2008 andere gesetzliche Bestimmungen für unbeschadet erklärte, wurde die geldwäscherechtliche Aufbewahrungspflicht, die jedenfalls hinter der zehnjährigen Frist aus dem Handelsrecht zurückblieb, schlicht für obsolet erklärt.[1574]

Es scheint, als ob die Kommentatoren des Anti-Geldwäscherechts aufgrund bestehender Aufbewahrungspflichten für Buchungsbelege kein Problem erkennen konnten. Schon früh wurde in der Literatur ja erkannt, dass zwar die Speicherung an sich in das Recht auf informationelle Selbstbestimmung eingreift[1575], kritisiert wurde aber von Beginn an nur die Verwendung der Daten, da man das Vorliegen des Datenbestands als gegeben betrachtete. Es wurde ignoriert, dass die geldwäscherechtliche Pflicht aufgrund ihrer Eigenart als Sicherheitsgesetz eine andere Qualität mit sich bringt. Außerdem wurde nicht geprüft, ob es bei der europa- oder verfassungsrechtlichen Bewertung eines Gesetzes überhaupt auf die Frage ankommen darf, ob das Gesetz auch faktische Auswirkungen auf die Menge der zu speichernden Daten mit sich bringt.

1573 *Ackermann/Reder*, WM 2009, 200 (208).

1574 *Warius* in Herzog GWG, 1. Aufl. 2010, § 8 Rn. 19; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438 jeweils zum GwG 2008, das sich aber hinsichtlich des Fristbeginns nicht vom aktuellen GwG unterscheidet,

1575 *Degen,* Geldwäsche, 2009, S. 200; *Herzog*, WM 1996, 1753 (1757); *ders.*, WM 1999, 1905 (1916).

Eine weitere Rolle dürfte gespielt haben, dass das GwG bis zur Schaffung des § 30 Abs. 3 GwG 2017[1576] noch keine Klausel enthielt, die es der FIU gestattet hätte, heimlich bei den Verpflichteten Informationen einzuholen. Die damals noch beim BKA angesiedelte FIU hatte nach § 10 Abs. 3 GwG 2008 lediglich die allgemeinen Datenerhebungsbefugnisse des BKA. Ein spezieller Zugriff auf den Datenschatz der Verpflichteten war also nicht vorgesehen. Jedenfalls bis zum Jahr 2017 hätte ein Vergleich mit der TK-Vorratsdatenspeicherung also mangels konkreter Zugriffsrechte nicht recht gepasst.

An der allgemeinen Befugnis des BKA zur prinzipiell offenen Datenerhebung gab es grundsätzlich wenig auszusetzen, war der Rückgriff auf Kontoinhaltsdaten durch Sicherheitsbehörden aufgrund bestehender Generalklauseln doch gängige Praxis[1577] und vom BVerfG selbst in einem Ausnahmefall[1578] abgesegnet worden (s. o. Kap. E. I. 1. c. bb.).

6. Kritische Stimmen aus Europa und Vergleich mit der TK-Vorratsdatenspeicherung

Deutlich konkretere Betrachtungen finden sich in der Literatur, die sich unmittelbar mit der europarechtlichen Grundlage des GWG, der GWRL, befasst. Spätestens mit der kommenden Vollharmonisierung durch die geplante EU-GWVO[1579] lassen sich diese Ausführungen unmittelbar auf die deutsche Rechtslage übertragen.

1576 Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017 (BGBl. I, S. 1822).

1577 Siehe nur *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 39 Rn. 40 *Kahler,* Kundendaten, 2017, 31 ff.; *F. Jansen,* Bankauskunftsersuchen, 2010, S. 30 ff.; *Reichling*, JR 2011, 12 (16).

1578 BVerfG, NJW 2009, 1405 (1407).

1579 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, 20. Juli 2021, COM(2021) 420 final, 2021/0239 (COD).

a. Kritik Europäischer Datenschutzbehörden

Dass die GWRL Fragen in Bezug auf den Datenschutz und Grundrechte aufwarf, war dem Europäischen Gesetzgeber selbst durchaus bekannt.[1580] Nach Erlass der 3. GWRL war er verstärkter Kritik der europäischen Datenschutzbehörden ausgesetzt.

aa. Stellungnahme der Article 29 Data Protection Working Party

Die *Article 29 Data Protection Working Party* (WP29), Vorläuferin des nach Art. 68 DSGVO eingerichteten Europäischen Datenschutzausschusses (EDPB), setzte sich im Jahr 2011 mit der 3. GWRL auseinander und erließ eine Stellungnahme. [1581] Um eine faire Balance von Datenschutz und Geldwäschebekämpfung zu gewährleisten, machte sie dem europäischen Gesetzgeber insgesamt 44 Vorschläge. Diese Vorschläge befassten sich u. a. auch mit dem Transaktionsmonitoring und den Aufbewahrungspflichten.

Die WP29 war der Meinung, dass sich die Reichweite des Monitorings nicht klar aus der Richtlinie ergeben würde. Insbesondere bei größeren Konzernen sei fraglich, welcher Datenaustausch hierfür notwendig und erlaubt sei. Die Richtlinie ließe sich so interpretieren, dass die vorgesehenen Compliance-Pflichten nur durch ein ausgeprägtes Outsourcing der gesamten Kundendaten eines Konzerns an Dritte mit adäquaten Data-Mining-Technologien erfüllt werden könnten. Genauso gut könnte man aber annehmen, dass in jedem Einzelfall eines Kunden eine individuelle Notwendigkeit vorliegen müsste, weshalb ein gruppenweites Transaktionsmonitoring gar nicht praktikabel wäre.[1582] Die Kritik der WP29 konkret am Transaktionsmonitoring scheint auf diese Problematik des Datenaustauschs innerhalb verschiedener Entitäten eines Konzerns begrenzt.[1583] Aus der Stellungnahme ergibt sich nicht, ob die WP29 an der rechtlichen Zulässigkeit eines umfassenden Transaktionsmonitorings selbst Zweifel hegte.

Konkreter wurde sie bei der Kontrolle der Aufbewahrungspflichten. Hier sei zunächst problematisch, dass die Richtlinie nur eine Minimal- und kei-

1580 *Europäische Kommission,* Commission Staff Working Paper, AML Compliance, SEC(2009) 030 final, 30.06.2009.

1581 *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011.

1582 Idem, Annex Nr. 25, S. 20 f.

1583 Ebenso *Europäische Kommission,* Commission Staff Working Paper, AML Compliance, SEC(2009) 030 final, 30.06.2009, Annex Nr. 7, S. 58 f.

ne Maximalfrist beinhaltete. Dieser Missstand wurde durch Art. 40 Abs. 1 UAbs. 2 der 4. GWRL allerdings behoben, nach der eine Speicherung maximal zehn Jahre lang zulässig ist.

Wichtiger war, dass die WP29 das Risiko einer „*evergreen data retention*" erkannte.[1584] Eine solche sei mit den Grundsätzen der Erforderlichkeit und Datenminimierung nicht zu vereinbaren. Art. 30 der 3. GWRL sei diesbezüglich unklar formuliert. Die Vorschrift gäbe nicht zu erkennen, ob und welche Grenzen für die Speicherung von Daten vorgesehen sei. Eine Auslegung dahingehend, dass Institute aufgrund der Identifikationsvorgänge oder Sorgfaltspflichten gespeicherten Daten ohne klaren Zweck der zukünftigen Verwendung vorhielten, dürfe aber nicht möglich sein. Andernfalls wäre die Vorschrift rechtswidrig. Deshalb sollten die Aufbewahrungspflichten verständlich normiert werden, wobei aber offenbar insbesondere der zeitliche Aspekt der Frist gemeint war. Grundsätzliche Einwände gegen das Vorhalten von Transaktionsdaten zu Zwecken der Geldwäschebekämpfung für eine gewisse Zeit brachten die Datenschützer in der Stellungnahme nicht vor.

Im Übrigen kritisierte die WP29, dass für sämtliche zu speichernde Daten dieselben Regeln galten, anstatt nach der Art der Daten zu differenzieren.[1585] Für die Transaktionsdaten sollte festgestellt werden, dass eine Speicherung zur Geldwäschebekämpfung prinzipiell nicht mehr erlaubt sein könne, wenn sich ein konkreter Verdacht als falsch herausgestellt hat oder die entsprechenden Ermittlungen eingestellt wurden. In diesen Fällen sollten die Daten nicht mehr von der Abteilung für Geldwäschebekämpfung eingesehen werden können, wozu sie entsprechend kodiert werden sollten.[1586]

1584 *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 27, S. 22.
1585 Idem, Annex Nr. 27-29, S. 21 ff.
1586 Idem, Annex Nr. 31, S. 24.

bb. Stellungnahmen des Europäischen Datenschutzbeauftragten

Auch der Europäische Datenschutzbeauftragte (EDPS) nahm mehrfach zur Entwicklung des Anti-Geldwäscherechts Stellung, erstmals ausführlich zum damals vorgeschlagenen[1587] Erlass der 4. GWRL im Jahr 2013.[1588]

Anders als viele Autoren aus der Rechtswissenschaft wies der EDPS zu Beginn seiner Stellungnahme auf den Umstand hin, dass die Erhebung von Personendaten zu Geldwäschezwecken gleichzeitig auch zu geschäftlichen Zwecken erfolgte.[1589] Auch deshalb würden die datenschutzrechtlichen Anforderungen des Europarechts auch für das Anti-Geldwäscherecht gelten, wenngleich die FATF-Standards auf den Datenschutz keine Rücksicht nähmen.[1590]

Als Schwierigkeiten des Anti-Geldwäscherechts in Bezug auf den Datenschutz erkannte der EDPS *„den Austausch von Informationen innerhalb der Unternehmensgruppe, die Zustimmung der betroffenen Personen, das Aufbewahren von Aufzeichnungen und die rechtlichen Unsicherheiten bezüglich der Verarbeitung von Daten betreffend die Bekämpfung der Geldwäsche/Terrorismusfinanzierung.“*[1591] Der EDPS verzichtete in seiner Stellungnahme zur damals geplanten 4. GWRL allerdings auf eine umfassende europarechtliche Kontrolle des Transaktionsmonitorings und der Aufbewahrung von Transaktionsdaten zu Zwecken der Geldwäschebekämpfung. Eine solche fand sich – jedenfalls ansatzweise – erst in der Stellungnahme[1592] zum Vorschlag[1593] zur 5. GWRL.

Dort erwähnte der EDPS schon zu Beginn die damals neue Rechtsprechung des EuGH zur TK-Vorratsdatenspeicherung im Fall *Digital Rights*

1587 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, 05. Februar 2013, COM(2013) 45 final, 2013/0025 (COD).

1588 *EDPS,* Stellungnahme 4. GeldwäscheRL, 04. Juli 2013.

1589 Idem, Nr. 12, S. 4.

1590 Idem, Nr. 15, S. 4.

1591 Idem, Nr. 19, S. 5.

1592 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017.

1593 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG, 05. Juli 2016, COM(2016) 450 final, 2016/0208 (COD).

Ireland.[1594] Es sei von der Rechtsprechung festgestellt worden, dass die Bekämpfung schwerer Kriminalität und Terrorismus zwar ein legitimes Ziel sei. Für diese Zwecke veranlasste Einschränkungen der Grundrechte auf Privatsphäre und Datenschutz müssten aber verhältnismäßig sein. Durch diese Einleitung zeigte der EDPS erstmals an, dass auch er die Vorschriften der Geldwäschebekämpfung nunmehr durchaus in dem Kontext der Diskussion um die Zulässigkeit einer Vorratsdatenspeicherung verstand. Konsequenterweise beschäftigte er sich dann auch in der Stellungnahme allgemeiner als zuvor mit der Frage, inwiefern das Vorhalten und Erforschen von Finanzdaten für staatliche Akteure verhältnismäßig sein kann.

So sei die Erweiterung der Pflichten etwa auf den Handel mit Kryptowährungen weniger beunruhigend als die vorgeschlagene allgemeine Erweiterung der Zwecke in der 5. GWRL. Diese nannte nicht mehr nur die Ahndung von Geldwäsche und die Terrorismusbekämpfung als Ziel, sondern – wenn auch weniger ausdrücklich – auch die Bekämpfung von Steuerbetrug und Steuerhinterziehung[1595], die bislang nur durch die Aufnahme von Steuerstraftaten als Vortat der Geldwäsche begünstigt werden sollte.[1596] Der Zweck der Richtlinie würde damit nach dem EDPS allgemein auf die Bekämpfung von Finanzkriminalität ausgedehnt.[1597] Dies sei kritisch zu betrachten, da die Verarbeitung von personenbezogenen Daten desto sensibler würde, je weiter der Zweck sei, dem sie diene.[1598]

Im Rahmen der Verhältnismäßigkeit sei sodann zu beachten, dass der EuGH für Eingriffe in das Recht auf Privatheit stets Anhaltspunkte gefordert hatte, die auf ein Verhalten im Zusammenhang mit einer Straftat schließen ließen. Pauschale Eingriffe seien danach unzulässig.[1599] Insofern sei problematisch, dass die Geldwäschebekämpfung nicht ausschließlich mehr einen risikoorientierten Ansatz verfolgte, sondern in Erwägungsgrund 19 auch die *methodische Überwachung einer Kategorie bestehender*

1594 Idem, Nr. 10, S. 6 f.
1595 Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016), S. 2 f.
1596 Vorschlag zur 4. EU-GWRL, 05. Februar 2013, COM(2013) 45 final, S. 5 f.; 4. EU-GWRL (EU) 2015/849, Erwägungsgründe 11, 44.
1597 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 27, S. 9 mit Verweis auf Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016), S. 3.
1598 Idem, Nr. 32, S. 10.
1599 Idem, Nr. 46, S. 13 mit Verweis auf EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 58 = NJW 2014, 2169.

Kunden[1600] forderte. Hierbei wird aber nicht ganz klar, welche Überwachung gemeint sein soll – und zwar weder unmittelbar in Erwägungsgrund 19 des Vorschlags zur 5. GWRL noch in der Stellungnahme des EDPS. Die pauschale Überwachung von Transaktionen war schließlich kein Novum der 5. GWRL, sondern schon seit der 3. GWRL aus 2005 vorgesehen. Offenbar hatte sich der EDPS nicht weiter mit der Frage auseinandergesetzt, wie weit das Transaktionsmonitoring reicht, und welche Daten dafür aufbewahrt werden müssen. Erneut blieb eine grundsätzliche Kritik an der Aufbewahrungspflicht in Verbindung mit der Überwachungspflicht also aus.

Was dem EDPS aber nicht verborgen blieb, war der Vorschlag, den FIUs einen umfassenden Zugang zu den von den Verpflichteten gespeicherten Daten unabhängig vom Vorliegen einer Verdachtsmeldung einzuräumen.[1601] Der Aufgabenbereich der FIUs würde nach Ansicht des Beauftragten damit keinen untersuchungsbezogenen Ansatz mehr verfolgen, sondern wäre schon bei bloßen *Erkenntnissen* eröffnet.[1602] Sie könnten damit „data mining"[1603] betreiben, nicht mehr nur gezielte Untersuchungen. Einen unmittelbaren Vergleich zur TK-Vorratsdatenspeicherung zog der EDPS an dieser Stelle aber nicht.

Stattdessen geriet seine Schlussfolgerung sehr allgemein und wiederholte letztlich nur allgemeine Ausführungen zur Verhältnismäßigkeit staatlicher Eingriffe in das Recht auf Privatsphäre und Datenschutz.[1604] So hätte in dem Vorschlag klargestellt werden sollen, dass alle Datenverarbeitungen und alle Grundrechtseingriffe stets einem genau festgelegten legitimen Zweck dienten, erforderlich und angemessen sind. Außerdem hätte geprüft werden sollen, ob die verfolgten politischen Ziele insgesamt mit dem Zweck zu vereinbaren sind.

Im Mai 2020 veröffentlichte die Europäische Kommission einen Aktionsplan zur Überarbeitung des Anti-Geldwäscherechts,[1605] der im Juli 2021 in

1600 Idem, Nr. 50, S. 13 mit Verweis auf Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016) Erwägungsgrund 19, S. 29.

1601 Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016), Nr. 11, S. 41, umgesetzt durch Art. 32 Abs. 9 der 5. EU-GWRL.

1602 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 52, S. 14.

1603 Ibid., in der deutschen Übersetzung fälschlich als „Datenminimierung" übersetzt.

1604 Idem, Nr. 66, S. 16 f.

1605 Mitteilung der Kommission zu einem Aktionsplan für eine umfassende Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, 07. Mai 2020, C(2020) 2800 final.

einem großen Gesetzgebungspaket mündete (s. o. Kap. D. III. 2. a. kk.)[1606]. Sowohl zum Aktionsplan[1607] als auch später zum Gesetzgebungspaket[1608] nahm der EDPS abermals Stellung, wobei nur letztere sich wirklich kritisch mit den Regelungen auseinandersetzte.

Die neuen Vorschriften über die Zugriffsrechte der FIUs seien danach insgesamt exzessiv, ihre Verhältnismäßigkeit fraglich.[1609] Art. 18 des Vorschlags für eine 6. GWRL enthält eine ausführliche Liste an Informationen und Datenbanken, auf die die FIUs Zugriff haben müssen. Hinzu tritt, dass die FIUs bei der einzurichtenden Europäischen Geldwäscheaufsichtsbehörde auch um Informationen aus deren zentralen Register ersuchen dürfen, Art. 11 Abs. 4 der vorgeschlagenen GWVO. Außerdem muss nach Art. 24 des Vorschlags für eine 6. GWRL der Datenaustausch zwischen den FIUs der Mitgliedstaaten gewährleistet werden. Die FIUs haben also einen Zugriff auf weitreichende Informationen, die nicht auf Finanzdaten limitiert sind. Diesen Umstand kritisiert der EDPS weiterhin als „intelligence-based", was angesichts seiner Natur als Verwaltungsbehörde nicht angemessen sein könnte.[1610] Die Zugriffsrechte sollten ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt und an die Notwendigkeit für operative Analysen der FIUs gebunden werden.[1611] Dabei kommentierte der EDPS den Zugriff der FIUs auf Informationen direkt bei den Verpflichteten gemäß der vorgeschlagenen Art. 50 Abs. 1 lit. b) GWVO[1612], Art. 18 Abs. 4 der 6. GWRL nicht mehr unmittelbar.[1613] Die Stellungnahme erwähnt nur die Art. 18 Abs. 1, 2 der 6. GWRL. Aus seinen Schilderungen ergibt sich jedoch, dass der EDPS die umfassenden Zugriffsrechte der FIUs insgesamt

1606 *Europäische Kommission,* Anti-money laundering and countering the financing of terrorism legislative package, https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en, zuletzt aufgerufen am 12.01.2025.

1607 *EDPS,* Stellungnahme Aktionsplan Geldwäsche 05/2020.

1608 *Ders.,* Opinion 12/2021 AML proposals, 22.09.2021.

1609 Idem, Nr. 20 ff, S. 11 .

1610 Idem, Nr. 37, S. 12; zuvor schon *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 53, S. 14; krit. zur Rolle der FIUs auch *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (249 f.).

1611 *EDPS,* Opinion 12/2021 AML proposals, 22.09.2021, Nr. 30, S. 11.

1612 Erwägungsgrund 79 der EU-GeldwäscheVO stellt klar, dass für Auskunftsersuchen der FIU keine vorherige Meldung erforderlich sein soll.

1613 So noch *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 52, S. 14.

kritisieren wollte, da die Möglichkeit zum Abgleich letztlich einem „data mining" gleichkomme.[1614]

Auch auf die Datenverarbeitung bei den Verpflichteten ging der EDPS ein. Wie bislang wurde aber weder die Rechtmäßigkeit der Aufbewahrungspflicht noch die Rechtmäßigkeit des Kontenmonitorings prinzipiell angezweifelt. Es wurde allerdings verlangt, dass in der Verordnung ausdrücklich bestimmt wird, welche Daten von den Verpflichteten für welche Zwecke bzw. an welcher Stelle der Geldwäschebekämpfung verarbeitet werden.[1615] Außerdem sollte die Verarbeitung persönlicher Daten, die in Verbindung zur sexuellen Orientierung oder ethnischer Abstammung stehen, verboten werden.[1616] Wie genau dies bei der Verarbeitung von Transaktionsdaten erfolgen soll, aus denen sich durchaus Rückschlüsse über diese Datenkategorien ergeben können, bespricht der EDPS allerdings nicht. Er scheint bei der Datenverarbeitung diesbezüglich allein die Identifizierungsmaßnahmen vor Augen gehabt zu haben.

b. Kritik in der Literatur

Ein solcher Ansatz, der die Parallelen des Anti-Geldwäscherechts und der TK-Vorratsdatenspeicherung in den Blick nimmt, wurde in der Europäischen Literatur zur GWRL in den letzten Jahren immer wieder vorgeschlagen. Im Folgenden sollen nur die Beiträge vorgestellt und kritisch kommentiert werden, die die Speicher- und Monitoring-Pflichten konkret anhand der Europäischen Rechtsprechung zur Vorratsdatenspeicherung bewerten. Allgemeine Betrachtungen der Kollision von Privatheit und Geldwäschebekämpfung, die auf eine spezifische Prüfung der einzelnen Pflichten anhand der Rechtsprechung verzichten, bleiben außen vor.[1617]

1614 *Ders.*, Opinion 12/2021 AML proposals, 22.09.2021, Nr. 37, S. 12.
1615 Idem, Nr. 16, S. 9; S. 16.
1616 Ibid.
1617 Etwa *Sciurba,* AML Regimes, 2019, S.88 ff.; *Ioannides,* Money Laundering, 2016, S. 135; *Mitsilegas/Vavoula*, Maastricht J. of EU and Comp. Law 23 (2016), 261 (279 ff.); *Gallant* in Rider (Hrsg.), Int. financial crime, 2015, S. 532.

aa. Böszörmenyi/Schweighofer

Im Jahr 2015, also bald nach Verkündung des wegweisenden EuGH-Urteils in der Sache *Digital Rights Ireland,* untersuchten *Böszörmenyi/Schweighofer*[1618] die Überwachungsmechanismen der sich damals im Gesetzgebungsverfahren befindenden 4. GWRL im Hinblick auf das Europäische Primär- und Menschenrecht. Zunächst stellten sie fest, dass der Vorschlag[1619] zur Richtlinie eine intensivierte Sammlung und Speicherung persönlicher Daten verlangte und nach der Rechtsprechung des EGMR schon dieser Speichervorgang in das Recht auf Privatsphäre aus Art. 8 EMRK eingreift.[1620] Die Nutzung dieser Daten für das laufende Monitoring mithilfe ausgefeilter Software könne man als „dataveillance" bezeichnen. Dieser von *Clarke* geprägte Begriff beschreibe die systematische Nutzung persönlicher Daten zur Ermittlung oder Überwachung bestimmter Handlungen oder Kommunikation einer oder mehrerer Personen[1621] – ein Vorgang, der gemeinhin intensiv und bedrohlich sei.[1622]

Zwischen dem Überwachungsregime der 4. GWRL und der vom EuGH in *Digital Rights Ireland* aufgehobenen Richtlinie über die TK-Vorratsdatenspeicherung[1623] erkannten *Böszörmenyi/Schweighofer* „offensichtliche

1618 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71); krit. zum Transaktionsmonitoring schon *dies.* in Schweighofer/Kummer/Hötzendorfer (Hrsg.), IRIS; Internationales Rechtsinformatik Symposium, Transparenz, 2014, S. 617 (621 f.).

1619 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, 05. Februar 2013, COM(2013) 45 final, 2013/0025 (COD).

1620 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71) mit Verweis auf EGMR, Factsheet – Personal Data Protection, aktuelle Version Januar 2022 https://www.echr.coe.int/Documents/FS_Data_ENG.pdf, zuletzt aufgerufen 12.01.2025; vgl. auch EGMR, Urt. vom 4. Dezember 2008, 350622/04 & 30566/04, Rn. 67 – Marper/Vereinigtes Königreich, EuGRZ 2009, 299; Urt. vom 16. Februar 2000, 27798/95, Rn. 69 – Amann/Schweiz, EMRK-E 2000-II, S. 201

1621 *Clarke* Communications of the ACM 31 (1988), 498 (499).

1622 Idem, (506).

1623 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates 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.

Gemeinsamkeiten".[1624] In der Entscheidung hätte der EuGH ebenfalls bemerkt, dass schon die Speicherung persönlicher Daten einen Eingriff in die Grundrechte auf Privatsphäre darstellte.[1625] Dies müsse auch für die geldwäscherechtlichen Aufbewahrungspflichten i. S. d. Art. 39-41[1626] des Vorschlags zur 4. GWRL gelten.[1627] Ebenso sehe die geplante 4. GWRL wie auch die VDS-RL vor, dass staatliche Sicherheitsbehörden auf die gespeicherten Daten zugreifen könnten. Dies geschehe einmal durch die Meldepflichten, würde aber auch durch den vorgeschlagenen Art. 40 der 4. GWRL[1628] gewährleistet. Dieser sah vor, dass die Verpflichteten Kommunikationswege bereitstellten, auf denen sie den Sicherheitsbehörden vertraulich mitteilen würden, ob und welche Geschäftsbeziehung zu einer gewissen Person besteht. Wie auch die Vorratsdatenspeicherung begründe das Anti-Geldwäscherecht in den beschriebenen Maßnahmen daher einen Eingriff in die Privatsphärenrechte aus Art. 7, 8 der EU-GRC, der gerechtfertigt werden müsse.[1629]

Einen eigenen Versuch solch einer Rechtfertigung bzw. Verhältnismäßigkeitsprüfung der Anti-Geldwäschemaßnahmen wagten die Autoren nicht. Sie bewerteten aber in ihrer Schlussfolgerung den Umstand positiv, dass die *„dataveillance"* nicht beim Staat stattfinde, sondern von Privaten ausgeführt werde. Der Staat habe daher nicht unmittelbaren und systematischen Zugriff auf sämtliche Finanzdaten.[1630]

Die Feinheiten der Speicherungspflichten und vor allem der staatlichen Zugriffsrechte wurden in den Ausführungen von *Böszörmenyi/Schweighofer* nicht sauber herausgearbeitet.

So bezeichnen die Autoren neben den Vorschriften über die Meldepflicht auch den späteren Art. 42. der 4. GWRL als Zugriffsvorschrift. Dieser aber sieht nur vor, dass die Verpflichteten bestimmte Kanäle einrichten müssen, um individuelle Bestandsdatenauskünfte vertraulich erteilen zu können.

1624 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71 f.).
1625 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 56 = NJW 2014, 2169.
1626 Art. 39-41 des Vorschlags, COM(2013) 45, wurden zu Art. 40-42 der 4. EU-GWRL.
1627 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (72).
1628 Entspricht Art. 42 der 4. EU-GWRL.
1629 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (72).
1630 Idem, (73).

Die Vorschrift entspricht damit eher dem Regelungsgehalt des § 44 KWG und ist vor dem Hintergrund, dass jedenfalls in Deutschland schon lange eine automatisierte Bestandsdatenauskunft möglich war, nicht weiter bemerkenswert. Art. 42. der 4. GWRL als Bestandteil eines Vorratsdatenspeicherungskomplex in Verbindung mit der Transaktionsüberwachung und -aufzeichnung zu begreifen, geht daher fehl. Dieser Fehler wurde allerdings auch in der deutschsprachigen Literatur begangen (s. o. II. 5. b. aa.).[1631]

Auch die vorgebrachten Meldepflichten eignen sich nicht für eine Gleichsetzung mit den Regeln über die TK-Vorratsdatenspeicherung. Zwar werden hier massenhaft Daten an die FIU geleitet, die dort je nach Praxis sehr lange gespeichert werden (zur deutschen Praxis siehe oben Kap. D. II. 2. c. dd.). Die Datenübermittlung erfolgt aber nicht anlasslos, sondern aufgrund der geldwäscherechtlichen Verdachtsschwelle. Außerdem ist der Staat hier auf das proaktive Mitwirken der Privaten angewiesen.

Die Schlussfolgerung von *Böszörmenyi/Schweighofer* zur 4. GWRL bzw. deren Vorschlag ist somit nur im Ergebnis nachvollziehbar. Aus heutiger Sicht ist die Arbeit relevant, da sie den Blick auf die Aufbewahrungspflichten als Teil einer Vorratsdatenspeicherung geworfen hat.

Dass noch keine kritische Zugriffsnorm genannt wurde, ist verständlich, da die Auseinandersetzung auf der 4. GWRL beruht. Erst später wurde mit Art. 32a Abs. 9 der 5. GWRL eine Norm geschaffen, deren Wortlaut ein Zugriffsrecht der FIUs offen vorsieht.

bb. Milaj/Kaiser

Ebenfalls mit der 4. GWRL beschäftigen sich ein Aufsatz von *Milaj/Kaiser*[1632] und die Dissertation von *Kaiser*[1633], die offenbar die Grundlage für den erstgenannten Beitrag darstellte. Die Arbeiten weisen allein schon aufgrund des unterschiedlichen Umfangs einige Unterschiede auf.

Die Autorinnen verglichen in ihrem Aufsatz wie auch *Böszörmenyi/Schweighofer* das Anti-Geldwäscherecht mit der EuGH-Rechtsprechung zur TK-Vorratsdatenspeicherung seit *Digital Rights Ireland*. Ihre Ausführungen, wie von einer Dissertationsschrift zu erwarten, sind aber

1631 *Heinson* in Specht/Mantz (Hrsg.), Hdb. Europ. & Deutsches Datenschutzrecht, 2019, § 14 Rn. 91; *Krais*, CCZ 2015, 251 (252).
1632 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115.
1633 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 122.

deutlich ausführlicher und wagen sich vor allem auch an eine eigene Prüfung der Verhältnismäßigkeit.

Die Vorschriften der 4. EU-Geldwäschebekämpfung verstehen *Milaj/Kaiser* als umfassende Pflicht zur Überwachung und Speicherung sämtlicher Kontotransaktionen.[1634] Dabei entstünden Sammlungen sensibelster Daten. Kaum ein Datenschatz sei so geeignet zum Erstellen von Persönlichkeitsprofilen wie Transaktionsdaten. Aus den Zahlungen ließen sich nicht nur Bewegungsprofile erstellen, sondern auch persönliche Vorlieben, Interessen, politische Einstellungen oder die Religionszugehörigkeit – etwa durch Spenden, Partei- oder Gewerkschaftsbeiträge.[1635]

Ausgangpunkt der Verhältnismäßigkeitsprüfung des Aufsatzes ist allein die Aufzeichnungs- und Aufbewahrungspflicht bzw. „data retention" aufgrund Art. 40 der 4. GWRL. Die Identifikationspflicht und das Monitoring sämtlicher Transaktionen werden zwar erwähnt, allerding nicht eigenständig auf ihre Vereinbarkeit mit höherrangigem Recht geprüft. Es ist zwar immer wieder von „surveillance" die Rede. Offenbar ist damit aber nicht der eigentliche EDV-Monitoring-Vorgang gemeint, bei dem Transkationen in Echtzeit, also unmittelbar bei der Ausführung, oder im Rahmen periodischer nachträglicher Kontrollen abgeglichen werden (s. o. Kap. D. II. 2. b. aa. (2)), sondern die Aufzeichnung und Aufbewahrung der Transaktionsdaten als solche.[1636] Im Rahmen der Verhältnismäßigkeit spielt deshalb vor allem die Sensibilität bzw. Privatheit der Daten und die Dauer der Aufbewahrung eine Rolle.[1637] Die Untersuchung der Finanzdaten durch die Geldwäscheverpflichteten wird jedoch im Rahmen der Verhältnismäßigkeit als Zweck der Speicherung relevant. So kommen *Milaj/Kaiser* zu dem Ergebnis, dass die überaus lange Aufbewahrung der Finanzdaten zur umfassenden Prüfung sämtlicher Transaktionen genau einen solchen Fall der *ständigen Überwachung*[1638] darstellt, die den EuGH zur Aufhebung der TK-Vorratsdatenspeicherungsrichtlinie veranlasst habe.[1639]

Im Ergebnis stellen sie fest, dass die ausnahmslose Speicherung zwangsweise dazu führt, dass Daten gespeichert werden, die für eine effektive

1634 Idem, S. 96 ff.; *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (122 f.).
1635 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 241 f., 430; *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (122).
1636 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (118, 122 ff.).
1637 Idem, (122 ff.).
1638 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 37 = NJW 2014, 2169.
1639 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (124).

Geldwäschebekämpfung mangels Verdachtsmoments völlig irrelevant sind. Die Speicherung sei somit nicht erforderlich und damit unverhältnismäßig.[1640] Auf die Frage, wie der Staat überhaupt auf die gespeicherten Daten zugreifen kann, und wie sich das auf die Frage der Verhältnismäßigkeit der Aufzeichnungs- und Aufbewahrungspflicht auswirkt, geht der Aufsatz nicht ein.

Differenzierter hinsichtlich der verschiedenen in der 4. GWRL angelegten Pflichten geht *Kaiser* in ihrer Dissertation vor. Dort werden zu Beginn der Verhältnismäßigkeitsprüfung die Identifikationspflicht, das EDV-Monitoring, die Meldepflicht, die Aufzeichnungs- und Aufbewahrungspflicht separat als eigenständige Grundrechtseingriffe vorgestellt.[1641] Im Rahmen der Verhältnismäßigkeit werden sie dann aber einheitlich als Komplex geprüft.[1642] Objekt der europarechtlichen Prüfung ist bei *Kaiser* offenbar die 4. GWRL in Gänze.

Dabei kommt sie insgesamt zum selben Ergebnis, das bereits in dem beschriebenen Aufsatz präsentiert wurde. Die Pflichten aus dem Anti-Geldwäscherecht begründeten eine Form der „Massenüberwachung"[1643], da ständig Informationen über den größten Teil der Bevölkerung verarbeitet und gespeichert würden. Das Zusammenspiel der einzelnen Maßnahmen führe im Ergebnis zur Unverhältnismäßigkeit der Richtlinie.

Die Meldepflichten etwa seien aufgrund der niedrigen Verdachtsschwelle extensiv und undurchsichtig.[1644] Ein Schutz besonderer Kategorien persönlicher Daten sei nirgends vorgesehen.[1645] Überhaupt fehle es an Transparenz und damit auch an der Möglichkeit, einen effektiven Rechtsschutz zu erhalten.[1646] Die Fristen der Speicherpflicht seien darüber hinaus deutlich überzogen.[1647]

Prominent werden auch die Zugriffsmöglichkeiten staatlicher Stellen auf die gespeicherten Daten als Aspekte der Verhältnismäßigkeit der Richtlinie besprochen, anstatt als Grundrechtseingriffe eigenständig geprüft zu wer-

1640 Ibid.
1641 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 432 ff.
1642 Idem, S. 451 ff.
1643 Idem, S. 452 ff.
1644 Idem, S. 465 ff.
1645 Idem, S. 467 ff.
1646 Idem, S. 486 ff.
1647 Idem, S. 493 ff.

den. Dabei ging *Kaiser* auf den damals vorliegenden Vorschlag[1648] zur 5. GWRL ein. In diesem war, neben der Einführung des Art. 32 Abs. 9, auch eine Änderung des Art. 33 Abs. 1 lit. b) der 4. GWRL vorgesehen.[1649] Nur letzterer wurde von der *Autorin* als Zugriffsnorm erkannt. Art. 32 Abs. 9 der 5. GWRL blieb unerwähnt.

Nach Art. 33 Abs. 1 lit. b) der 5. GWRL sollten die Verpflichteten „der zentralen Meldestelle auf Verlangen unmittelbar alle erforderlichen Auskünfte zur Verfügung stellen". Die Norm überschneidet sich inhaltlich mit Art. 32 Abs. 9 der 5. GWRL und Art. 32 Abs. 3 S. 4 der 4./5. GWRL, statuiert aber weniger ausdrücklich eine Zugriffsnorm als Art. 32 Abs. 9 der 5. GWRL.

Warum sich *Kaiser* in ihrer Bewertung der Zugriffsmöglichkeit nicht (auch) auf Art. 32 Abs. 9 der 5. GWRL stützte, bleibt unklar. Jedenfalls aber stellte sie fest, dass sich die Möglichkeit einer umfangreichen Ermächtigung der FIUs zu Auskunftsersuchen, unabhängig vom Vorliegen einer Meldepflicht, nachteilig auf die Verhältnismäßigkeit der geldwäscherechtlichen Verpflichtungen auswirkte.[1650] So sei es ein Hauptargument des EuGH in *Digital Rights Ireland* gewesen, dass im Rahmen der EU-VorratsdatenspeicherungsRL keine Voraussetzungen oder Hürden geregelt wurden, unter denen staatliche Sicherheitsbehörden die gespeicherten TK-Verkehrsadern abfragen durften.[1651] Diese Frage war durch Art. 4 der VDS-RL allein den Mitgliedstaaten überlassen worden. Auch die Zugriffrechte der FIUs auf die Informationen der Geldwäscheverpflichteten unterlägen nach der 4./5. GWRL keinen ausdrücklich geregelten Voraussetzungen. Die Aussagen des EuGH könnten also analog auf die Verhältnismäßigkeit der GWRL angewandt werden.[1652]

Kaiser kommt daher zu dem Ergebnis, dass die 4./5. GWRL nicht den Anforderungen des EuGH an die Verhältnismäßigkeit genügen könne.[1653] Durch die Massenüberwachung, die sich aus dem Zusammenwirken der geldwäscherechtlichen Verpflichtungen ergäbe, würden fast sämtliche Bür-

1648 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG, COM(2016) 450 final 2016/0208 (COD).

1649 Beide Vorschläge fanden unverändert Einzug in die Richtlinie.

1650 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 481 ff.

1651 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 61 = NJW 2014, 2169.

1652 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 483.

1653 Idem, S. 510 ff.

ger der EU unter Generalverdacht gestellt. Die Verhinderung von Geldwäsche und Terrorismusfinanzierung seien zwar sicher legitime Ziele. Sie könnten aber die Maßnahmen aufgrund deren extensiver Ausgestaltung nach den Grundsätzen des EuGH aus *Digital Rights Ireland* und *Tele2Sverige* nicht rechtfertigen.

Die Arbeiten von *Milaj/Kaiser* enthalten den bislang ausführlichsten Vergleich des Europäischen Anti-Geldwäscherechts und der TK-Vorratsdatenspeicherung bzw. der dazu ergangenen Rechtsprechung.

In beiden Schriften wird jedoch übersehen, dass in der GWRL – anders als bei der VDS-RL – verschiedene Pflichten für Private geregelt werden. Letztere enthielt lediglich eine Speicherpflicht bzgl. der TK-Verkehrsdaten sowie die Pflicht der Staaten, Zugriffe ihrer Sicherheitsbehörden auf die gespeicherten Daten zu ermöglichen. Daher konnte der EuGH sinnvollerweise nur eine einzelne Maßnahme prüfen, anhand derer die gesamte Richtlinie letztlich stand oder fiel.[1654]

Die Prüfung der GWRL scheint komplexer. Natürlich hängen die Überwachungs- bzw. Monitoring-Pflicht, die Meldepflicht und die Aufbewahrungspflicht inhaltlich zusammen. Sie wirken sich jedoch unterschiedlich aus und können separat voneinander geprüft werden, wobei sich die Intensität der einzelnen Maßnahmen synergetisch aus deren Wechselwirkung ergibt (s. dazu Kap. B. I. 1. c.).

Wie bereits dargelegt, führt allein das Monitoring noch nicht dazu, dass staatliche Sicherheitsbehörden ohne Weiteres auf anlasslos gespeicherte Daten zugreifen können. Erst durch die Meldung an die FIUs gelangen die Daten an den Staat, wenn die Verpflichteten im Rahmen des Monitorings einen Verdacht erkannt haben. Durch die proaktive Meldung erhalten die Sicherheitsbehörden somit nur einen selektierten Datenschatz (s. o. Kap. D. II. 2. c. ee.). Die Rechtsprechung des EuGH zur TK-Vorratsdatenspeicherung lässt sich auf diesen Teilkomplex der Pflichten also nicht so einfach übertragen, da es hier in sämtlichen Urteilen um den möglichen Zugriff auf anlasslos gespeicherte Daten ging.

Was die Arbeiten im Weiteren außer Acht lassen, sind die Auswirkungen der generellen Zwischenschaltung Privater. Es kann zwar kein Zweifel daran bestehen, dass die staatlich veranlassten Pflichten der Institute und anderer Personen mittelbar in die Rechte derer Kunden eingreifen,

1654 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 = NJW 2014, 2169.

es handelt sich also nicht um ein Problem der mittelbaren Drittwirkung (s. o.).[1655] Dennoch ist jedenfalls bei dem Komplex aus Überwachung und Meldung zu beachten, dass letztlich nur Private Daten verarbeiten, bei denen noch kein Verdachtsmoment vorliegt. Dabei handelt es sich um Daten, die den jeweils Verpflichteten aus verschiedenen rechtlichen und faktischen Gründen ohnehin vorliegen. Jedenfalls in dieser Hinsicht könnte man argumentieren, dass die Verpflichteten faktisch nicht zu einer eigenständigen Datensammlung, sondern nur zu einer spezifischen Verarbeitung der ihnen vorliegenden Daten gezwungen werden.

Ein unmittelbarer Vergleich der gesamten Richtlinien ist aufgrund der strukturellen Unterschiede, die die proaktive Einschaltung Privater bzgl. bestimmter Maßnahmen mit sich bringt, jedenfalls nicht angezeigt. Stattdessen sollten die verschiedenen Pflichten einzeln betrachtet und mit der vorhandenen Rechtsprechung abgeglichen werden (dazu unten Kap. G. III. 2.).

cc. Vogel

Der Abgleich der geldwäscherechtlichen Pflichten mit der Rechtsprechung des EuGH zur TK-Vorratsdatenspeicherung wird auch von *Vogel* in einer kritischen Gesamtschau der EU-Geldwäscherichtlinie und insbesondere des GwG bemüht.[1656] Da es in den Urteilen zu *Digital Rights Ireland* und *Tele2Sverige* um Kommunikationsdaten ging, könnten die Entscheidungen zwar nicht unmittelbar auf das Anti-Geldwäscherecht der EU angewandt werden. Aus deren Inhalt ließen sich jedoch die Grenzen der Verhältnismäßigkeit bei der Verarbeitung von Finanzdaten zu Sicherheitszwecken ableiten.[1657]

Hierzu müssten die TK-Verkehrsdaten und Finanzdaten zunächst hinsichtlich ihrer Grundrechtsrelevanz verglichen werden. Dabei könne man leicht annehmen, dass es schon aufgrund der Quantität beachtliche Unterschiede gäbe. Da die moderne Fernkommunikation fast ausschließlich

1655 So schon *Herzog*, WM 1996, 1753 (1757).

1656 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (897 ff.); zur deutschen Rechtslage *ders.* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (246 ff.).

1657 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (900 f.).

telekommunikativ erfolgt, entstehen zwangsläufig gewaltige Datenmengen. Wie der EuGH auch richtig bemerkt hätte, könne aus den TK-Verkehrsdaten allein aufgrund deren Massen präzise Rückschlüsse über das Privatleben der betroffenen Bürger gewonnen werden.[1658]

Persönliche Finanzdaten entstünden normalerweise in geringerem Umfang. Außerdem könnten Kunden nicht erwarten, dass die Daten so vertraulich behandelt würden wie ihre Telekommunikation, denn sie offenbaren sie in einem geschäftlichen und nicht in einem privaten Verhältnis. Transaktionen und andere wirtschaftliche Verhaltensweisen wären ohne ein gewisses Maß an Öffentlichkeit gar nicht möglich. (Analoge) Banküberweisungen etwa würden zwangsläufig dem verarbeitenden Mitarbeiter zuteilwerden.

Andererseits, meint *Vogel*, müsse beachtet werden, dass auch im laufenden Geschäftsverkehr elektronische Zahlungen immer stärker in den Vordergrund rücken, und zwar sowohl im Offline- als auch insbesondere im Onlinegeschäftsverkehr. Die so getätigten Transaktionen enthielten detaillierte Informationen über sämtliche Umstände des getätigten Geschäfts, aus denen nuanciert Bewegungsprofile, persönliche Verhaltensweisen oder Interessen und somit umfangreiche Persönlichkeitsbilder abgeleitet werden könnten. Da Transaktionsdaten alle Umstände des getätigten Geschäfts offenlegten, seien sie letztlich besser geeignet zur Erstellung von Persönlichkeitsprofilen als TK-Verkehrsdaten. Anders als diese könnten sie zusätzlich auch nicht verschlüsselt werden.[1659]

Mit Transaktionsdaten sei es aber auch noch nicht getan. Die Aufbewahrungspflichten des Anti-Geldwäscherechts wären nicht auf diese limitiert, sondern enthielten sämtliche Informationen, die die Verpflichteten im Rahmen der Sorgfaltspflichten einholten. Je nach Risiko könnten dies auch Social-Media-Analysen oder sonstige persönliche Hintergründe sein. Diese Informationen könnten in Verbindung mit den Transaktionsdaten „extensive Persönlichkeitsprofile" liefern. [1660]

Neben der Daten-Art müssten weiter auch die Umstände der Speicherpflicht untersucht werden, da nach dem EuGH bereits die Speicherpflicht zur späteren Verwendung an sich einen Eingriff in Art. 7, 8 EU-GRC darstellte.[1661] Auch hier aber zeige sich, dass sich das Anti-Geldwäscherecht

1658 Idem, (901).
1659 Idem, (901 f.).
1660 Idem, (902).
1661 Idem, (902 f.).

hinsichtlich der vom EuGH aufgestellten Voraussetzungen eher zulasten der Bürger von der VDS-RL unterscheide. Es würden nicht nur Transaktionsbelege aufbewahrt, sondern Transkationen mittels EDV-Systemen überwacht und auf Auffälligkeiten untersucht. Das Monitoring würde zwar primär zur Durchführung proaktiver Meldungen genutzt. Es bewirke aber dennoch, dass jeder Kunde möglicherweise zum Ziel staatlicher Ermittlung werden könnte, ohne tatsächlich eine Straftat begangen zu haben oder diese vorzubereiten. Die Speicherpflichten des europäischen Anti-Geldwäscherechts müssten daher nach den Standards des EuGH einen Grundrechtseingriff darstellen und könnten an die Voraussetzungen des EuGH an solch einen Eingriff gebunden sein.[1662]

Bei der Bewertung dieses Eingriffes spielten aber verschiedene Aspekte eine Rolle, die vor einer Eins-zu-Eins-Übertragung der Rechtsprechung geklärt werden müssten. Hier nennt *Vogel* zunächst die zuvor besprochene Unterschiedlichkeit von Transaktionsdaten und Telekommunikationsverkehrsdaten. Zwar lesen sich seine Ausführungen so, als ob er offenbar von einer erhöhten Sensibilität gegenüber den TK-Verkehrsdaten ausgeht. Eine ausdrückliche Festlegung erfolgt allerdings nicht. Er stellt lediglich fest, dass es am Ende auf die Möglichkeit der Profilbildung ankommen müsse.[1663] Weiter käme es bei der Bewertung der Speicherpflicht darauf an, welche Konsequenzen aus der Datenverarbeitung folgen – insbesondere, unter welchen Umständen die Daten an die FIUs gemeldet würden, und ob der Bürger gegen die Ausübung der Sorgfaltspflichten einen effektiven Rechtsschutz erlangen könnte.

Da nicht auszuschließen sei, dass die anti-geldwäscherechtliche Aufzeichnungs- und Aufbewahrungspflicht einen ähnlich intensiven Grundrechtseingriff wie die TK-Vorratsdatenspeicherung darstellt, sollten die Gesetzgeber dafür Sorge tragen, dass auf die gespeicherten Daten nur zur Ahndung und Verhinderung schwerer Straftaten zugegriffen werden dürfte.[1664] Ausdrücklich für europarechtswidrig werden die Vorschriften aber nicht erklärt.

Neben der Speicherpflicht untersucht *Vogel* weiter, wie die Datenverarbeitungsbefugnisse der FIUs rechtlich zu bewerten sind.[1665] Diese gingen mittlerweile weit über die Analyse eingehender Verdachtsmeldungen hi-

1662 Idem, (903 f.) .
1663 Idem, (904).
1664 Ibid.
1665 Idem, (904 ff.).

naus. Zwar hätten FIUs mit wenigen Ausnahmen, etwa den Kontobestandsdaten, keinen unmittelbaren Zugriff auf Finanzdaten. Ihnen stünden aber verschiedene Ermächtigungen zum Abfragen solcher Daten bei den Verpflichteten zur Verfügung.[1666]. Ferner könnten die Verpflichteten auf die Auskunftsersuchen hin eigene Untersuchungen vornehmen und so noch mehr Informationen erlangen, die sie dann den FIUs übergeben könnten.[1667]

Diese Umstände in Verbindung mit den verschiedenen Formen des Monitorings führten dazu, dass die Datenanfragen der FIUs letztlich keine bloßen Auskunftsersuchen bzw. Ermittlungen darstellten, sondern eine Überwachung der Kunden.[1668] Daher seien hier die Rechtsprechung des EGMR und des EuGH zu Überwachungsmaßnahmen zu beachten.[1669] Danach sollten insbesondere Ermächtigungsgrundlagen zu Eingriffen, die nicht vom Bestehen einer vorherigen Meldungen oder eines sonstigen Verdachts abhängig sind, von den Gesetzgebern unter spezifische Voraussetzungen gestellt werden.[1670]

Bei *Vogel* findet sich somit eine geteilte Besprechung der Speicherpflichten einerseits und der Ermächtigungsgrundlagen der FIUs andererseits, wobei letztere wiederum im Rahmen der Verhältnismäßigkeit der Speicherpflicht eine Rolle spielen, da die Bewertung der Speicherpflicht davon abhängig sein soll, wie die Daten in der Folge verarbeitet werden können.

Konkret stellt *Vogel* fest, dass es sich beim Anti-Geldwäscherecht letztlich um eine staatlich veranlasste Überwachung der Kunden handle, die zentral von den FIUs gesteuert werde. Auffällig an seiner Kritik ist, dass er es vermeidet, konkrete Normen als europa- oder menschenrechtswidrig zu bezeichnen. Vielmehr stellt er die Anwendbarkeit bestimmter Teile der Rechtsprechung von EuGH und EGMR lediglich in den Raum und macht sie von einer bestimmten Lesart der geldwäscherechtlichen Befugnisse abhängig, ohne sich dabei endgültig festzulegen, ob diese Lesart denn auch zutrifft.

1666 Zu § 30 Abs. 3 GwG: *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (242 ff.).

1667 *Ders.* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (905).

1668 Idem, (906 f.).

1669 Idem, (906 ff.).

1670 Idem, (909) mit Verweis auf EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717; EGMR, Urt. vom 29. Juni 2006, 54934/00, Rn. 97 – Weber and Saravia/Deutschland = NJW 2007, 1433; Urt. v. 27.10.2015, 62498/11, Rn. 134-146 – R.E./Vereinigtes Königreich = NJW 2016, 2013.

Jedenfalls bei der Speicherpflicht drängt sich dann aber doch der Eindruck auf, dass *Vogel* die umfangreichen Speicherpflichten angesichts der darauf aufbauenden Monitorsysteme, Meldepflichten und Zugangsberechtigungen für nicht vereinbar mit den Anforderungen des EuGH hält. Auch die Bewertung der Zugangsrechte der FIUs lässt erkennen, dass er angesichts der fehlenden ausdrücklichen Voraussetzungen eine Unvereinbarkeit der Normen (etwa § 30 Abs. 3 GwG) durchaus für möglich hält.

dd. Betrand/Maxwell/Vamparys

Der zuletzt hier vorzustellende Beitrag zu der Thematik stammt aus dem Jahr 2021 und kam von den Autoren *Betrand/Maxwell/Vamparys*.[1671] In dem Aufsatz wird die Anwendung künstlicher Intelligenz durch die geldwäscherechtlich Verpflichteten aus grundrechtlicher Perspektive untersucht. Dabei stoßen die Autoren auf die Frage, ob die Monitoring-Maßnahmen nach der GWRL, ausgehend von der EuGH Rechtsprechung zur Vorratsdatenspeicherung von TK-Verkehrsdaten[1672] und PNR-Daten[1673], mit den Europäischen Grundrechten auf Privatsphäre in Einklang gebracht werden können. Dies bestimmte sich nach dem Grundsatz der Verhältnismäßigkeit.

Zunächst stellen die Autoren daher den Rechtsrahmen der Verhältnismäßigkeitsprüfung vor. Für sicherheitsrechtliche Maßnahmen folge deren Notwendigkeit nicht nur aus Art. 52 Abs. 1 der EU-GRC und Art. 8 der EMRK, sondern auch aus Art. 11 der Konvention 108[1674] sowie Art. 23 DSGVO und Art. 4 der JI-Richtlinie. Zu unterschiedlichen Ergebnissen würden die verschiedenen Rechtsgrundlagen aber nicht führen, die Verhältnismäßigkeitsprüfung erfolge stattdessen immer nahezu identisch.[1675]

Auf die bisherigen Besprechungen der Verhältnismäßigkeit von Anti-Geldwäschemaßnahmen in der Literatur gehen die Autoren nur kurz ein.

1671 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276.

1672 berücksichtigt auch EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531.

1673 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 – PNR Canada = ZD 2018, 23; s.a. jüngst, GA EuGH (Pitruzzella), Schlussantrag v. 27.01.2022 – C-817/19.

1674 *Europarat*, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981, ETS Nr. 108, (BGBl. 1985 II S. 539).

1675 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (278 f.).

Insbesondere die Arbeit von *Milaj/Kaiser*[1676] (s. o.) weise eine große Ähnlichkeit zu ihrem Ansatz auf. Um sich davon abzugrenzen und eine Lücke zu schließen, legten *Betrand/Maxwell/Vamparys* den Fokus konkret auf die Verhältnismäßigkeit des Einsatzes künstlicher Intelligenz im Rahmen des Transaktionsmonitorings.[1677] Die Speicherpflichten der GWRL spielen in ihrem Aufsatz keine Rolle.

Deutlich intensiver als die Literatur besprechen die Autoren die vorhandene Rechtsprechung. Die Anforderungen an die Verhältnismäßigkeit werden Art. 52 Abs. 1 der EU-GRC entnommen und zunächst anhand der EuGH-Urteile *Digital Rights Ireland* und *Tele2Sverige* in Bezug auf sicherheitsrechtliche Datenverarbeitungen illustriert.[1678] In den Entscheidungen habe der EuGH geklärt, dass das anlasslose Speichern von TK-Verkehrsdaten zu sicherheitsrechtlichen Zwecken grundsätzlich unzulässig sei. Für bestimmte Bereiche oder Zeiträume könnten zwar hiervon Ausnahmen gemacht werden, aber nur, wenn enge Voraussetzungen gegeben seien.[1679] In einem weiteren Fall habe der EuGH allerdings klargestellt, dass nicht jede Form der Vorratsdatenspeicherung illegitim sei. Das universale Vorhalten von Kundendaten sei stattdessen nur dann exzessiv, wenn die entsprechenden Daten auch ein bestimmtes Maß an Sensibilität erreichen.

Besonders relevant für die Bewertung des Transaktionsmonitorings sei weiter das Gutachten des EuGH zum PNR-Abkommen[1680] der EU mit Kanada.[1681] Dieses sah vor, dass Airlines bestimmte Informationen über Passagiere von Flügen zwischen der EU und Kanada an eine kanadische Behörde übermittelten, die dort zur Bekämpfung von Terrorismus auf bestimmte Muster hin analysiert und sodann gespeichert wurden. Der EuGH erklärte in den Gutachten das Abkommen für ungültig, da es u. a. keine ausreichenden Voraussetzungen für den Zugriff auf die übertragenen Daten vorsah und die Speicherung der Daten über den Zeitraum des Aufenthalts in Kanada auch für solche Passagiere erlaubte, bei denen noch nicht fest-

1676 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115.
1677 Idem, (279 f.).
1678 Idem, (280 ff.)m
1679 Idem, (280) mit Verweis auf EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 9 = NJW 2017, 717.
1680 *Europäisches Parlament,* Agreement between Canada and the European Union on the Transfer and
Processing of Passenger Name Record, 23 June 2014, 2013/0250 (NLE), 12657/5/13 REV 5.
1681 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 – PNR Canada = ZD 2018, 23m

stand, ob von ihnen eine objektive Gefahr ausging. Auch zu der automatischen Analyse äußerte sich der EuGH. Diese sei nur dann verhältnismäßig, wenn, die verwendeten Datenbanken und Kriterien regelmäßig unter Berücksichtigung aktueller Forschung auf ihre Zuverlässigkeit, Aktualität und Diskriminierungsfreiheit untersucht würden.[1682] Hier sahen *Betrand/Maxwell/Vamparys* eine starke Parallele zum (EDV-)Transaktionsmonitoring (s. a. Kap. G. III 2. a. cc (1)).[1683]

Ebenfalls mit systematischer Analyse setzte sich der EuGH in *La Quadrature du Net* auseinander. Dort stellte er fest, dass das Echtzeitmonitoring von TK-Verkehrs- und Standortdaten durch die französische Polizei zur Erkennung von Mustern, die auf terroristische Bedrohungen schließen lassen könnten, einen erheblichen Grundrechtseingriff darstellte. Dieser könne nur legitim sein, wenn für den betreffenden Mitgliedstaat eine akute terroristische Bedrohungslage festgestellt werden könnte.[1684] Hieraus schlossen die Autoren, dass die Verwendung automatisierter Algorithmen zur Erkennung von Straftaten allgemein nicht ohne das Vorliegen bestimmter Voraussetzungen verhältnismäßig sein könne. Das ist wiederum eine Erkenntnis, die sich auf das Transaktionsmonitoring übertragen ließe.[1685]

Aus der Rechtsprechung zur EMRK identifizierten *Betrand/Maxwell/Vamparys* einen weiteren Fall zur Verwendung von Algorithmen im Bereich des Sicherheitsrechts. Im Rahmen des niederländischen SyRI-Programms wurden verschiedene Datenbanken der Sozialbehörden automatisiert auf Muster von Sozialleistungsbetrug hin durchleuchtet. Ein niederländisches Obergericht hielt das Programm mangels Transparenz für unverhältnismäßig i. S. d. Art. 8 Abs. 2 EMRK, obwohl sämtliche positive Treffer von Mitarbeitern händisch überprüft wurden.[1686] Auch dahingehend müsste die Verwendung von Algorithmen beim Transaktionsmonitoring also untersucht werden.[1687]

Ein regelbasiertes Monitoring sei aufgrund der steigenden Zahl von Transaktionen kaum mehr effektiv, da sie eine Vielzahl falschpositiver

1682 Idem, Rn. 174.
1683 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (281 f.).
1684 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 174 ff. = NJW 2021, 531.
1685 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (282).
1686 Rb. Den Haag - C/09/550982/HA ZA 18/388
1687 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (282 f.).

Meldungen und somit eine große Arbeitslast erzeuge.[1688] Daher setzten einige Institute vermehrt auf künstliche Intelligenz.[1689] Diese würde sehr viel effektiver als Menschen bestimmte Muster erkennen und sehr viel schneller lernen. Problematisch sei jedoch, dass die Systeme zum Lernen eine Grundlage benötigten. An dieser fehle es, da noch immer keine grundsätzlichen Muster bekannt seien, hinter denen regelmäßig tatsächlich kriminelles Verhalten steht.[1690] Das Transaktionsmonitoring beruhe daher überwiegend noch auf einem regelbasierten Ansatz ohne Verwendung maschinellen Lernens.[1691]

Im Rahmen der Verhältnismäßigkeitsprüfung wird das Transaktionsmonitoring dann grundsätzlich und nicht nur im Hinblick auf die Verwendung von Algorithmen untersucht. Zunächst stellen die Autoren fest, dass das Transaktionsmonitoring aufgrund seiner Anlasslosigkeit und Allgemeinheit eine erhebliche Intensität aufweise. Dabei berufen sie sich auf die EuGH-Rechtsprechung zur Vorratsdatenspeicherung von TK-Verkehrs- und PNR-Daten. Hinzu trete, dass bei der Erstellung von Persönlichkeitsprofilen teilweise auf Algorithmen zurückgegriffen würde, jedenfalls aber die Möglichkeit bestehe.[1692]

Der Frage, ob diesem Eingriff ein proportionaler Zweck entgegensteht, wird die Klärung der gesetzlichen Grundlage und deren Bestimmtheit i. S. d. Art. 52 Abs. 1 S. 1 EU-GRC vorangestellt. Insbesondere an der Bestimmtheit haben *Betrand/Maxwell/Vamparys* erhebliche Zweifel, da das Transaktionsmonitoring in der GWRL nicht näher beschrieben werde.[1693]

1688 Idem, (284) mit Verweis auf *IBM,* financial crime AI, 2019, https://web.archive.org/web/20220208195208/https://www.ibm.com/downloads/cas/WKLQKD3W , zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im April 2022); M. *Weber et al.,* AML (preprint), 2018, https://arxiv.org/pdf/1812.00076, zuletzt aufgerufen am 12.01.2025.

1689 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (284 f.) mit Verweis u.a. auf *Canhoto* J. of Business Research 131 (2020), 441; *Accenture,* AML Machine Learning, 2017, https://web.archive.org/web/20220303015059/https://www.accenture.com/_acnmedia/pdf-61/accenture-leveraging-machine-learning-anti-money-laundering-transaction-monitoring.pdf, zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im April 2022).

1690 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (285).

1691 Idem, (286) mit Verweis auf *Verhage*, J. of Money Laundering Control 2009, 371; s.a. *Canhoto*, J. of Business Research 131 (2020), 441 (442 mwN.).

1692 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (286).

1693 Idem, (287 f.)

Auch von der Erforderlichkeit der Maßnahme i. S. d. Art. 52 Abs, 1 S. 2 EU-GRC sind die Autoren nicht überzeugt. Schon die finanziellen Kosten des Transaktionsmonitorings würden den Wert der aufgrund gemeldeter Transaktionen konfiszierten Gelder überschreiten.[1694] Ob alternative Systeme weniger einschneidend, aber gleich effektiv sein könnten, müsse besser evaluiert werden.

Zuletzt wird die Angemessenheit nach Art. 52 Abs. 1 S. 2 EU-GRC geprüft. Entscheidend hierfür seien die Maßstäbe des EuGH zur TK-Verkehrs- und Bestandsdatenabfrage. In diesen Entscheidungen zur Verhältnismäßigkeit einer Vorratsdatenspeicherung sei es insbesondere auf die Zugriffsmöglichkeiten der Sicherheitsbehörden angekommen. Aus *Ministerio Fiscal* ergebe sich, dass ein Zugriff auf – im sicherheitsrechtlichen Sinne – anlasslos vorgehaltene Daten nicht grundsätzlich auf schwere Straftaten reduziert werden muss.[1695] Vielmehr ergebe sich aus der EuGH-Rechtsprechung ein Dreistufenkonzept, das zwischen ernsten Gefahren für die nationale Sicherheit, schweren Straftaten und einfachen Straftaten unterscheide (s. dazu oben Kap. C. II. 3.).[1696]

Bei sensiblen Daten wie den Transaktionsdaten wäre eine allgemeine Datenverarbeitung nach den Grundsätzen des EuGH eigentlich nicht möglich. Das führe jedoch zu einem Dilemma. Die Geldwäschebekämpfung basiere auf der Idee, dass sich Risiken nur aus Ungewöhnlichkeiten ableiten ließen. Um Ungewöhnlichkeiten zu erkennen, müsse man aber zwangsläufig alle Transaktionen überwachen, da man sonst ja den Maßstab nicht kenne, aus dem heraus sich Abweichungen erst ergeben.[1697] Dieses Dilemma könne man nur lösen, wenn das Monitoring streng in einen automatisierten Teil und die händische Kontrolle aufgeteilt würde, sodass die allgemeine Überwachung auf den EDV-Prozess beschränkt bleibt. Dieser Prozess müsse von *angemessenen Schutzmaßnahmen* begleitet werden. Einmal müssten die Betroffenen in Kenntnis gesetzt werden, wenn bei ihnen ein „Treffer" erzielt oder gar eine Meldung bei den FIUs vorgelegt wird. Außerdem müssten die Verpflichteten stets erklären können, wie es zu dem Treffer gekommen ist. Zuletzt müsste das System auf seine Rechtskonformität bzw. Effektivität von zuständigen Behörden oder Gerichten kontrolliert

1694 Idem, (288) mit Verweis auf *Sciurba,* AML Regimes, 2019, S. 99.
1695 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 54 ff. = NJW 2019, 655.
1696 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (289 f.).
1697 Idem, (290).

werden.[1698] Da es derzeit noch an solchen Schutzmaßnahmen fehle, schließen die Autoren damit, dass sich das aktuelle Anti-Geldwäscherecht auch im Rahmen der Angemessenheit als durchaus problematisch darstelle.

Diese Überlegungen zur Verhältnismäßigkeit kranken daran, dass zwischen der allgemeinen Datenverarbeitung durch Vorratsdatenspeicherung und der automatisierten Massenanalyse nicht genau unterschieden wird. Die Vorratsdatenspeicherung zeichnet sich durch zwei Grundrechtseingriffe aus: Speicherung und Zugriff. In *Ministerio Fiscal* etwa betrachtet der EuGH allein das Zugriffsrecht. Zur anlasslosen Speicherung von Bestandsdaten äußert er sich – anders als das BVerfG[1699] – nicht. Zwar ist es richtig, dass der EuGH in den Entscheidungen zur Vorratsdatenspeicherung eigentlich schon die massenhafte Anlegung der Daten und damit die Verarbeitung bei Privaten, die hinter der Massenanalyse zurückbleibt, an Voraussetzungen knüpfen wollte. Die Verhältnismäßigkeit steht aber stets unter der Erkenntnis, dass durch das Vorhalten der Daten letztlich ein staatlicher Zugriff ermöglicht wird. Dieser Umstand ist für das Transaktionsmonitoring nicht unmittelbar zu erkennen, da es allein der proaktiven Meldung von Verdachtsfällen dient. Der staatliche Zugriff ergibt sich erst aus den Aufbewahrungspflichten und den Zugriffsrechten der FIU. Diese Vorschriften werden in dem Beitrag aber an keiner Stelle erwähnt.

Wohl deshalb stellen die Autoren auch nicht nur auf die Rechtsprechung zu den Speicherpflichten ab. Der EuGH hatte sowohl in seinem Gutachten zum PNR-Abkommen[1700] als auch in *La Quadrature du Net*[1701] die automatisierte Datenanalyse und das Vorhalten der verarbeiteten Daten für einen späteren Zugriff als separate Eingriffe behandelt. Lediglich im Rahmen der Verhältnismäßigkeit kommt es dabei zur Interaktion zwischen den einzelnen Maßnahmen. *Betrand/Maxwell/Vamparys* weisen somit auf die passenden Vergleichsobjekte hin, sie beziehen ihre Argumente gegen das Monitoring dann aber primär aus dem allgemeinen Vorbringen gegen anlasslose Speicherpflichten. Die Rechtsprechung des EuGH aus verschieden gelagerten Fällen wird insofern zu pauschal wiedergegeben.

1698 Idem, (290 ff.).

1699 BVerfGE 118, 168 – Kontostammdaten; E 130, 151– Bestandsdatenauskunft I; E 155, 119 – Bestandsdatenauskunft II.

1700 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 – PNR Canada, Analyse ab Rn. 168 ff.; Speicherung ab Rn. 190 ff. = ZD 2018, 23.

1701 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Speicherung ab Rn. 134 ff; Analyse ab Rn. 172 ff. = NJW 2021, 531.

Im Grunde bleibt es bei der Aussage, dass die Voraussetzungen der Vorratsdatenspeicherung zur Unverhältnismäßigkeit des Monitorings führen. Der Unterschied zwischen diesen beiden Maßnahmen wird auf diese Weise verwischt.

c. Zusammenfassung und Stellungnahme

Insbesondere in der europäischen Literatur wird also stark argumentiert, dass die Aufbewahrungspflichten, die Überwachungspflicht samt Transaktionsmonitoring und die Zugriffsrechte der FIU letztlich einen Überwachungskomplex darstellen, der sich an den Voraussetzungen des EuGH zur Vorratsdatenspeicherung messen lassen müsste.[1702]

Übergreifend zeigen sich bei den Besprechungen aber Probleme bei der Übertragung dieser Grundsätze. Anders als die Vorratsdatenspeicherung von TK-Verkehrsdaten besteht das Anti-Geldwäscherecht nicht nur aus einer sicherheitsrechtlichen Speicherpflicht und entsprechenden Zugriffsrechten. Das System basiert primär auf proaktivem Tätigwerden der Verpflichteten zur Überwachung und Meldung. Zwar ist das Monitoring sämtlicher Transaktionen eine intensivere Verarbeitung als das bloße Speichern all dieser Informationen, die automatisierte Analyse mit anschließender Prüfung ist aber auf die Verdachtsmeldung fokussiert. Eine Vorratsdatenspeicherung kann sich erst aus der Pflicht ergeben, die analysierten Daten aufzubewahren – verbunden mit dem Recht der FIUs, anlasslos und geheim darauf zuzugreifen.

Zusammenfassend lässt sich somit sagen, dass die Literatur die Probleme, die sich aus der EuGH-Rechtsprechung zur Vorratsdatenspeicherung für das Anti-Geldwäscherecht ergeben, erkannt und besprochen hat. Die Betrachtungen sind aber in großen Teilen zu undifferenziert geblieben und reflektieren insbesondere nicht die dogmatischen Entwicklungen der Rechtsprechung zum Sicherheitsverfassungsrecht.

Vor deren Hintergrund ist es nicht mehr möglich, die GWRL pauschal für unverhältnismäßig zu erklären, wie es der EuGH mit der VDS-Rl in *Digital Rights Ireland* getan hat (s. o. Kap. C. II. 1. a. aa.). Vielmehr muss

1702 *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.

die konkrete gesetzliche Ausgestaltung der jeweiligen Datenverarbeitungsschritte untersucht werden, wobei die Intensität dieser Einzeleingriffe nicht im Rahmen einer isolierten Betrachtung erfolgen kann, sondern in Anbetracht der Wechselwirkungen mit den übrigen Informationseingriffen des Antigeldwäschekomplexes (vgl. Kap. B. I. 1. c.).

7. Ansätze in der Rechtsprechung des BVerfG, EuGH und EGMR

Die Rechtsprechung hat sich bislang nur rudimentär mit der Vereinbarkeit von Anti-Geldwäscherecht und höherrangigem Recht beschäftigt. Eine Verfassungsbeschwerde gegen die verschiedenen Pflichten des Geldwäschegesetzes von mehreren Verpflichteten wies das BVerfG in einem Kammerbeschluss als unzulässig ab. Sie genüge nicht dem Grundsatz der Subsidiarität.[1703] Gegen die geldwäscherechtlichen Pflichten könnten sie mithilfe verwaltungsgerichtlicher negativer Feststellungsklagen vorgehen. Die Voraussetzungen für eine ausnahmsweise mögliche Verfassungsbeschwerde ohne vorherigen fachgerichtlichen Rechtsschutz lägen daher nicht vor, denn über den Verwaltungsrechtsweg könnten die Verpflichteten Rechtsschutz erlangen, ohne zunächst gegen Regeln verstoßen zu müssen, um sodann ein Ordnungswidrigkeiten- oder Strafverfahren zu führen.[1704]

Der fachgerichtliche Rechtsschutz sei den Verpflichteten auch zumutbar. Es stellten sich nicht nur verfassungsrechtliche Fragen, sondern auch ein erheblicher Klärungsbedarf bzgl. den gesetzlichen Vorschriften selbst. So enthalte das GwG eine große Zahl unbestimmter Rechtsbegriffe, deren Bedeutung erst fachgerichtlich geklärt werden müsse.[1705] Außerdem seien etliche Fragen unionsrechtlicher Natur. Auch diese müssten von den Fachgerichten geklärt und eventuell dem EuGH vorgelegt werden.[1706] Eine Vorabentscheidung nach § 90 Abs. 2 BVerfGG käme wegen dieses erheblichen Klärungsbedarfs nicht in Betracht.[1707]

Auf die inhaltlichen Fragen ging das BVerfG quasi nicht ein. Die Überlegung, dass durch die Verpflichtungen auch das Recht der informationellen Selbstbestimmung betroffener Kunden tangiert wird, findet sich in dem Beschluss an keiner Stelle.

1703 BVerfG, NJW 2019, 659.
1704 Iden, (569).
1705 Idem, (660).
1706 Ibid mit Verweis auf BVerfGE 129, 186 (202).
1707 Ibid mit Verweis auf BVerfGE 86, 382 (388).

Auch in der Rechtsprechung des EuGH spielt dieser Aspekt bislang noch eine untergeordnete Rolle. Die bisherigen Urteile zur GWRL befassen sich vorrangig mit Harmonisierungsfragen bzw., inwiefern die Mitgliedstaaten zulasten der Verpflichteten strengere Vorschriften erlassen durften. Die weitergehenden Regeln der nationalen Gesetzgeber wurden aber nicht aufgrund einer etwaigen stärkeren Beeinträchtigung der Kundengrundrechte überprüft, sondern nur als möglicher Verstoß entweder gegen die GWRL selbst oder die europäischen Grundfreiheiten der Verpflichteten.[1708]

Ob die Verpflichtungen nach Maßgabe der Richtlinie selbst gegen höherrangiges Recht verstoßen, wurde vom EuGH bislang nur für Rechtsanwälte geprüft, und zwar in Bezug auf das Recht auf ein faires Verfahren nach Art. 6 Abs 2 EUV und Art, 6 EMRK. Dieses sei allerdings nicht verletzt, da für die Meldepflichten der Rechtsanwälte ausreichende Ausnahmen – etwa für Informationen in Zusammenhang mit rechtlichen Streitigkeiten – geschaffen worden waren.[1709] An der Rechtmäßigkeit der geldwäscherechtlichen Meldepflicht an sich ließ der EuGH keine Bedenken erkennen. Auf die informationelle Selbstbestimmung der betroffenen Mandanten ging der EuGH erst gar nicht ein. Mangels einer vertieften Beschäftigung mit den im Rahmen dieser Arbeit aufgeworfenen Fragen, lassen sich aus den Entscheidungen des EuGH keine entscheidenden Erkenntnisse ziehen.

Der Entscheidung des EuGH zu den Meldepflichten der Rechtsanwälte schloss sich der EGMR im Ergebnis an, stützte seinen Befund aber auf das Recht der Anwälte auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK.[1710] Auf die Rechte der Mandanten stellte der EGMR nicht unmittelbar ab, auch wenn er offenbar von einer Beeinträchtigung dieser ausging.[1711] Mit der Rechtmäßigkeit der geldwäscherechtlichen Aufbewahrungs- und Meldepflichten setzte sich der EGMR ebenfalls nicht auseinander. Auch aus seiner Rechtsprechung lässt sich daher bislang nicht viel mehr schließen, als dass er keine Zweifel an der Vereinbarkeit einer Meldepflicht bzgl. bestimmten Geschäften zur Bekämpfung der Geldwäsche mit der EMRK hegt.

1708 Vgl. EuGH, Urt. v. 10.03.2016, C-235/14 = ZD 2016, 404 (Ls.); Urt. v. 25.4.2013, C-212/11 (Bank Gibraltar) = ZD 2013, 398.
1709 EuGH Urt. v. 26. 6. 2007, C-305/05 (Ordre des barreaux) = NJW 2007, 2387.
1710 EGMR, Urt. v. 6. 12. 2012, 12323/11 – Michaud/Frankreich = NJW 2013, 3423.
1711 Idem, Rn. 114, 123.

8. Zusammenfassung und Stellungnahme

In diesem Kapitel wurde die Entwicklung der Diskussion um das Geldwäscherecht chronologisch dargestellt. Es zeigte sich, dass die Vorschriften des Anti-Geldwäscherechts von Anfang an kritisch begleitet wurden und noch heute die Frage offen gestellt wird, ob sie mit den Grundrechten auf Privatsphäre und Datenschutz in Einklang zu bringen sind.

Der grundsätzliche Ansatz, Private zur Überwachung des Finanzverkehrs und Meldung bestimmter Vorgänge zu verpflichten, um Geldwäsche und Terrorismusfinanzierung zu bekämpfen, wurde zwar von der deutschen Literatur anfangs als illegitime Delegation einer staatlichen Aufgabe kritisiert[1712], ist heute aber weitgehend als eine klassische Compliance-Struktur anerkannt. Jedenfalls an der Legitimität der Meldepflichten können kaum noch Zweifel bestehen, nachdem die Rechtsprechung die Meldepflicht der Rechtsanwälte aufrechterhalten hat.[1713] Diese wurde früher als besonders problematisch bezeichnet.[1714] Man muss also davon ausgehen, dass sich der EuGH und der EGMR auch an den Meldepflichten der Banken und Finanzdienstleister nicht prinzipiell stören.

Schon in den 1990ern wurde aber erkannt, dass die Geldwäschebekämpfung nach Vorstellung des Gesetzgebers und der mit ihr betrauten staatlichen Institutionen letztlich auf eine verfassungsfeindliche Massenüberwachung insb. der Bankkunden herausläuft, da sie nur durch ein umfassendes Monitoring sämtlicher Kundentransaktionen auskommen könne. Hiergegen wurden erhebliche datenschutz- und verfassungsrechtliche Bedenken geäußert. [1715] Diese Kritik wurde im Laufe der 2000er Jahre weiter aufgegriffen – insbesondere, nachdem das Kontenmonitoring auch gesetzlich festgelegt wurde.[1716] Diese Diskussion drang auch zu den Datenschutzbe-

1712 *Löwe-Krahl*, wistra 1994, 121 (125 f.); Oswald Eur. J. of Crime, Criminal Law & Justice 5 (1997), 196 (198).

1713 EuGH Urt. v. 26. 6. 2007, C-305/05 (Ordre des barreaux) = NJW 2007, 2387; EGMR, Urt. v. 6. 12. 2012, 12323/11 – Michaud/Frankreich = NJW 2013, 3423.

1714 Vgl. *Wegner*, NJW 2002, 794 (795 f.) *Wägenbaur*, EuZW 2002, 293 (296); *Hellwig* AnwBl 2002, 144 (146); *Zuck*, NJW 2002, 1397; *Shaugnessy*, Law & Policy in Int. Business 34 (2002), 25 (29 f., 36 f.).

1715 *Dahm*, WM 1996, 1285 (1289 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.; dagegen *Findeisen*, wistra 1997, 121 (127).

1716 Etwa *Jahn*, ZRP 2002, 109 (110 f.) *Herzog/Christmann*, WM 2003, 6 (11 f.); *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (72 f.); *Degen,* Geldwäsche, 2009, S. 196 ff.; dagegen *Scherp*, WM 2003, 1254

auftragten vor.[1717] Zweifel wurden aber zunächst nur an der Verpflichtung zum Kontenmonitoring geäußert. Die Aufbewahrungspflichten für Informationen im Zusammenhang mit den Sorgfaltspflichten spielten in der rechtswissenschaftlichen Betrachtung kaum eine Rolle. Zwar hatte *Herzog* früh darauf aufmerksam gemacht, dass schon die Speicherung der Transaktionsdaten in die Rechte der Kunden eingriff. Prinzipielle Zweifel an der Rechtmäßigkeit der Aufbewahrungspflicht ließ er aber nicht erkennen.[1718]

Die europäischen und deutschen Gesetzgeber ließen sich von der Diskussion um das Kontenmonitoring nicht weiter beeindrucken und schrieben die Überwachungspflicht letztlich sogar ausdrücklich in Art. 8 Abs.1 lit. d) der 3. GWRL bzw. in § 3 Abs. 1 Nr. 4 GwG 2008 fest. Da die datenschutzrechtliche Bestimmtheitsproblematik aufgelöst schien, ebbte die deutsche Kritik am Transaktionsmonitoring in den folgenden Jahren ab.[1719]

Dass das Geldwäscherecht bestimmte Parallelen zur Vorratsdatenspeicherung von TK-Verkehrsdaten aufweist, blieb von der deutschen Rechtswissenschaft nicht völlig unbeachtet. Sie verpasste es jedoch, die problematischen Normen des GwG konkret zu identifizieren. So wurden zwar die Zusammenarbeitspflichten von Banken und FIUs und das Transaktionsüberwachungskonzept nebulös mit dem Prinzip der Vorratsdatenspeicherung in Verbindung gebracht.[1720] Eine explizite verfassungs- oder europarechtliche Prüfung der Aufbewahrungspflichten suchte man jedoch vergebens.

Auch vom Europäischen Datenschutzbeauftragten ist offenbar erkannt worden, dass das Anti-Geldwäscherecht an verschiedenen Stellen Parallelen zur Problematik der Vorratsdatenspeicherung aufweist. In den Stellung-

(1257 f.); *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95.

1717 Krit. der *DSB Berlin,* Jahresbericht, 2000, S. 48 ff.; *ders.,* Jahresbericht, 2005, S. 50 ff.; weniger krit. *DSB Bund,* 19. Tätigkeitsbericht, 2001-2002, S. 67.

1718 *Herzog*, WM 1996, 1753 (1757); s.a. *Degen,* Geldwäsche, 2009, S. 200.

1719 Vgl. *Ackermann/Reder*, WM 2009, 158 (164); *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 53; *Achtelik* in Herzog GWG, 1. Aufl. 2010, KWG § 25c Rn. 25; krit noch *Kaetzler*, CCZ 2008, 174 (179 f.) und *Warius* in Herzog GWG, 1. Aufl. 2010, § 9 Rn. 63 aber nur In Bezug auf bestimmte Datenkategorien.

1720 *Heinson* in Specht/Mantz (Hrsg.), Hdb. Europ. & Deutsches Datenschutzrecht, 2019, § 14 Rn. 91; *Spoerr* in BeckOK Datenschutzrecht, Syst. J Rn. 226; *Krais*, CCZ 2015, 251 (252); *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 117 (117, Fn 1) erwähnt ebenfalls die Existenz einer Vorratsdatenspeicherung von Finanzdaten und verweist auf *C. Kaiser,* Privacy in Financial Transactions, 2018.

nahmen zur EU-Geldwäschebekämpfung wird unmittelbar auf die Rechtsprechung aus *Digital Rights Ireland*[1721] Bezug genommen.[1722] Weder die Aufbewahrungspflichten noch das Transaktionsmonitoring wurden vom EDPS aber bislang als unverhältnismäßiger Eingriff in die Grundrechte eingestuft.[1723] Er hat allenfalls die Zugriffsrechte der FIUs kritisiert und angemahnt, dass der Ansatz der FIUs nicht mehr auf konkreten Ermittlungen beruhe, sondern letztlich ein „data mining" darstelle.[1724]

Deutlich offensivere Kritik äußerte die rechtswissenschaftliche Literatur auf europäischer Ebene. Wie auch der EDPS knüpfen einige Autoren an der Rechtsprechung zur Vorratsdatenspeicherung an, gehen aber weiter, indem sie grundlegende Pflichten, Maßnahmen und Rechte der GWRL auf ihre Vereinbarkeit mit Art. 7, 8 der EU-GRC überprüfen.[1725]

Die Beiträge differenzieren aber teilweise nicht sauber zwischen den einzelnen Maßnahmen und offenbaren ein kaum ausreichendes Verständnis des Sicherheitsverfassungsrechts, da sie zu sehr auf eine Rationalitätskontrolle mit absolutem Ausgang drängen, anstatt den Weg der Rechtsprechung einer Prozeduralisierung[1726] konsequent zu Ende zu gehen.

Durch das PNR-Urteil wurden die (unions-)grundrechtlichen Anforderungen an Maßnahmen der Massenüberwachung noch weiter differenziert. Eine umfangreiche Übertragung dieser Prinzipien auf das Anti-Geldwäscherecht hat bislang noch nicht stattgefunden.

1721 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

1722 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 10, S. 6 f.

1723 Vgl. *ders.,* Stellungnahme 4. GeldwäscheRL, 04. Juli 2013; *ders.,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017; *ders.,* Stellungnahme Aktionsplan Geldwäsche 05/2020; *ders.,* Opinion 12/2021 AML proposals, 22.09.2021.

1724 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 52, S. 14.

1725 *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.

1726 Vgl. *Tzanou/Karyda*, European Public Law 28 (2022), 123 (153 f.).

Kapitel G: Das Anti-Geldwäscherecht in der Sicherheitsverfassung

In den vorherigen Kapiteln wurde gezeigt, dass sich in den letzten Jahrzehnten neben dem klassischen Sicherheitsrecht ein spezielles Rechtsregime entwickelt hat, das der Versorgung von Sicherheitsbehörden mit Finanzdaten dient: das (Anti-)Geldwäscherecht. Dieses beinhaltet an verschiedenen Stellen Aspekte einer Massenüberwachung und wurde insofern von verschiedenen Stellen kritisch untersucht.

In diesem Kapitel soll nunmehr eine eigene Untersuchung unternommen werden, die das geltende Rechtsregime der Geldwäschebekämpfung aus dem Blickwinkel des aktuellen europäischen und deutschen Sicherheitsverfassungsrechts betrachten soll. Insbesondere das Urteil zur PNR-Überwachung soll insoweit wegweisend sein.

Die Bestandsdatenabfrage (dazu Kap. F. II. 1., zur Diskussion Kap. G. I.) soll insofern keine Rolle mehr spielen. Ihr Rahmen wird heute auch durch die EU-Finanzinformationsrichtlinie (FinanzinformationsRL) europarechtlich umfänglich geregelt.[1727] Spätestens mit der Entscheidung *Ministerio Fiscal*[1728] dürfte die Verhältnismäßigkeit des Zugriffs auf gespeicherte Bestandsdaten allgemein festgestellt sein.

I. Übersicht: Finanzdatenüberwachung im Sicherheitsrecht

Obwohl, wie gesehen, durchaus über die Rechtmäßigkeit sicherheitsrechtlicher Verwendung von Finanzdaten auf Grundlage des Anti-Geldwäscherechts diskutiert wird, führen insbesondere die Transaktionsdaten im Vergleich zu den Telekommunikationsdaten ein Nischendasein. Während insbesondere das BVerfG und der EuGH in den letzten Dekaden immer strenge Anforderungen an verschiedene Überwachungsmaßnahmen aufge-

1727 Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates, ABl. 2019, L 186/122.

1728 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal) = NJW 2019, 655.

stellt und dabei letztlich ein selbstreferentielles[1729], rechtsfortbildendes[1730] Regime geschaffen haben, hat sich das System der GWRL konsolidiert.

Weder das BVerfG noch der EGMR oder der EuGH haben sich umfassend mit dem geldwäscherechtlichen Überwachungskomplex befasst.[1731] Da die Geldwäschebekämpfung eine Schnittstelle von Bankenaufsichts-, Strafprozess- und Gefahrenabwehrrecht darstellt, überrascht es nicht, dass das Rechtsregime aus sicherheitsverfassungsrechtlicher Perspektive noch nicht ausreichend untersucht wurde.[1732]

I. Kontodatenabfrage als strafprozessuale Praxis

Dass die Geldwäschebekämpfung im Sicherheitsverfassungsrecht weniger Aufmerksam erhalten hat als die Vorratsdatenspeicherung und Analyse von Telekommunikations- und Fluggastdaten dürfte zunächst daran liegen, dass die Nutzung von Finanzdaten schon seit Langem im praktisch relevanten[1733] Strafprozessrecht sehr etabliert ist. Die Anforderungen an den Abruf solcher Daten bei Kreditinstituten ist niederschwellig. Der zweite Senat des BVerfG hat die (Massen-)Abfrage von Kontoinhaltsdaten, gestützt auf die Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 Alt. 2 StPO, gebilligt[1734] und

1729 *Rusteberg*, KritV 2017, 24 (26 f.).

1730 Vgl. nur BVerfGE 141, 220 (267 ff.) – BKA-Gesetz; aus der Lit. v.a. *Poscher* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 3 Rn. 82; *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (253 ff.); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 84; *Volkmann*, NVwZ 2022, 1408 (1410 f.).

1731 s. insofern nur BVerfG, NJW 2019, 659; EuGH, Urt. v. 10.03.2016, C-235/14 = ZD 2016, 404 (Ls.); Urt. v. 25.4.2013, C-212/11 (Bank Gibraltar) = ZD 2013, 398; EGMR, Urt. v. 6. 12. 2012, Nr. 12323/11 –(Michaud/Frankreich) = NJW 2013, 3423.

1732 Hier v.a. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881.

1733 Transaktionsdaten fallen meist erst an, wenn mindestens ein Straftatenverdacht vorliegt, vgl. insf. *Barreto da Rosa* in Herzog GwG, § 30 Rn. 13; *Degen,* Geldwäsche, 2009, S. 152 ff.

1734 BVerfG, NJW 2009, 1405; krit. *Kahler,* Kundendaten, 2017, S. 123 ff., 182; *Petri*, StV 2007, 266 (268 f.); *Singelnstein*, NStZ 2012, 593 (603); *ders.* in Barton/Kölbel/Lindemann (Hrsg.), Ermittlungsverfahren, 2015, S. 251 (254 ff.).

somit die staatsanwaltschaftliche Praxis der *Abwendungsauskünfte*[1735] bei Vorliegen eines Anfangsverdachts abgesichert.

Dies sagt mehr über das Strafprozessrecht aus als über die Verfassungsmäßigkeit der sicherheitsrechtlichen Verwendung von Finanzdaten. Ein Vergleich mit den nachrichtendienstlichen Auskunftsersuchen gegenüber Kreditinstituten und anderen Wirtschaftsunternehmen, mit denen sich der erste Senat des BVerfG bereits beschäftigt hat,[1736] macht deutlich, dass die StPO sich noch an einigen Stellen nicht konsistent in das Regime der *Sicherheitsverfassung*[1737] einfügt.[1738]

Anders als im Recht der Nachrichtendienste (etwa § 8a BVerfSchG) ist das Auskunftsrecht der Strafverfolgungsbehörden gegenüber Privaten nur in einigen Teilbereichen – insbesondere für Telekommunikation und Telemedien – konkret geregelt und mit spezifischen Eingriffsschwellen etc. ausgestaltet. Darin besteht ein grundlegendes Problem.[1739] Es gilt gewissermaßen der Grundsatz, dass alle privaten Daten den Strafverfolgungsbehörden zugänglich sein müssen.[1740] Soll auf Daten zugegriffen werden, die in anderen (Wirtschafts-)Bereichen anfallen, kommt primär die Ermittlungsgeneralklausel zum Einsatz.[1741]

Zwar geht mit den Auskunftsersuchen der Strafverfolgungsbehörden nach § 161 Abs. 1 S. 1 Alt. 2 StPO – anders als bei den Nachrichtendiensten (vgl. § 8b Abs. 6 BVerfSchG) – keine Auskunftspflicht einher,[1742] die fehlen-

1735 *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 39 Rn. 40; *Reichling*, JR 2011, 12 (16); ausf. dazu *F. Jansen,* Bankauskunftsersuchen, 2010, S. 189 ff.

1736 BVerfGE 120, 274 (346 ff.) – Online-Durchsuchung.

1737 Zum Begriff vgl. *Tanneberger,* Sicherheitsverfassung, 2014; *Dietrich/Gärditz* (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245; *Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 192.

1738 Vgl. Insofern auch *Zöller*, ZStW 2012, 411; *Singelnstein*, NStZ 2012, 593 (606); angedeutet bei *Masing*, NJW 2012, 2305 (2309).

1739 *Kölbel* in MüKo StPO, § 161 Rn. 26; *Singelnstein*, NStZ 2012, 593 (602 f.); in Bezug auf Bankdaten *Kahler,* Kundendaten, 2017, S. 111 ff.

1740 *Masing*, NJW 2012, 2305 (2309).

1741 *Singelnstein*, NStZ 2012, 593 (602 f.).

1742 LG Hof, NJW 1968, 65 (65); *Köhler* in Meyer-Goßner/Schmitt StPO, § 161 Rn. 4 *Kahler,* Kundendaten, 2017, S. 42 *Jansen,* Bankauskunftsersuchen, 2010, S. 42 f.

de Pflicht kann aber in der Praxis durch sogenannte Abwendungsauskünfte umgangen werden.[1743]

Die Datenabfrage bei Privaten auf Grundlage der StPO wirft also noch einige Fragen auf.[1744] Sie lässt sich aktuell kaum mit den sicherheitsverfassungsrechtlichen Prinzipien vereinbaren. Die Praxis der Staatsanwaltschaft, Kontoinhalte auf Grundlage der allgemeinen Generalklausel abzufragen, ist mehr als fragwürdig[1745] – insbesondere, wenn die Abfrage nicht auf eine Person konkretisiert wird, sondern eine Massenabfrage anhand bestimmter Transaktionsumstände vorgenommen wird (dazu oben Kap E I. 1. d. cc.).[1746] Einer Bewertung der Maßnahmen nach dem Geldwäscherecht anhand der Rechtsprechung zu Massenüberwachungskomplexen kann also nicht entgegengehalten werden, dass der Zugriff auf Finanzdaten schon im Rahmen klassischer Ermittlungsmaßnahmen umfassend stattfindet.

2. „Klassische" Ermittlung als Lücke der Sicherheitsverfassung?

Vielmehr offenbart die Betrachtung der Finanzdaten insofern, dass die vom BVerfG eingerichtete Sicherheitsverfassung noch einige Fragen hinsichtlich klassischer Ermittlungsmaßnahmen offenlässt. Dies lässt sich an den Finanzdaten exemplifizieren.

Dass die Konsolidation noch nicht abgeschlossen ist, zeigt sich schon daran, dass sich die Rechtsprechung nicht intensiver mit dem Begriff der Überwachung auseinandersetzt (oben Kap. B. I. 2.), wenngleich sowohl das BVerfG als auch die europäischen Gerichte offensichtlich ein System etablieren wollten, dass staatliche (Massen-)*Überwachung prozeduralisiert*.[1747]

Nach dem dieser Arbeit zugrunde liegenden Verständnis liegt eine (grundrechtlich) beachtliche *Überwachung* immer dann vor, wenn ver-

1743 *Reichling*, JR 2011, 12 (15 ff.); *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 8 Rn. 40; ausf. *F. Jansen,* Bankauskunftsersuchen, 2010, S. 189 ff.

1744 Problematisch ist auch die „heimliche Durchsuchung" nach § 95a StPO vgl. dazu *Burhoff*, StRR (9) 2021, 6 (6); *Vassilaki*, MMR 2022, 103; *Gallus/Zeyher*, NStZ 2022, 462.

1745 EGMR, Urt. v. 27.4.2017, 73607/13 – Sommer/Deutschland, Rn. 58 ff. = NJOZ 2019, 455; *Singelnstein*, NStZ 2012, 593 (603); *ders.* in Barton/Kölbel/Lindemann (Hrsg.), Ermittlungsverfahren, 2015, S. 251 (254 ff.); *Brodowski*, JR 2010, 543.

1746 *Kahler,* Kundendaten, 2017, S. 123 ff., 182; *Petri*, StV 2007, 266 (268 f.).

1747 "proceduralisation" bei *Tzanou/Karyda*, European Public Law 28 (2022), 123 (153 f.).

schiedene Datenverarbeitungsschritte im sicherheitsrechtlichen Kontext kombiniert werden. Dieses Verständnis befreit nicht davon, jeden einzelnen Datenverarbeitungsschritt als eigenständigen Eingriff zu verstehen, er öffnet aber die Tür zu einer Eingriffsbestimmung, die nicht allein auf den jeweiligen Verarbeitungsschritt blickt, sondern die Intensität aus der entsprechenden Kombination ableitet (oben Kap B. I. 1. c. und III 2. a. aa.).[1748]

Mit diesem Überwachungsbegriff kann insbesondere die Grundrechtssensibilität von Massenüberwachungsmaßnahmen dargestellt werden, etwa der Vorratsdatenspeicherung. Bei dieser wird die Speicherung mit einer etwaigen zukünftigen Weitergabe der Daten verbunden. Aufgrund dieser Verknüpfung stellt schon die Speicherung einen (intensiven) Grundrechtseingriff dar.[1749] Dieses Ergebnis ließe sich mit einer völlig isolierten Betrachtung der Datenverarbeitungsschritte kaum begründen.

Wie aber verhält es sich, wenn auf Daten zugegriffen wird, deren Speicherung ohnehin anfällt? Wieso unterscheiden sich die Vorratsdatenspeicherungskomplexe von Zugriffen, etwa auf Wirtschaftsdaten, die aufgrund allgemeiner Aufbewahrungspflichten gespeichert werden? Nach der typischen Vorstellung der Privatheitsgrundrechte dürfte es schließlich allein darauf ankommen, inwieweit die Datenherrschaft[1750] einer Person verlorengeht.

Kontostammdatenabfragen wurde beispielsweise bereits vor Einführung der § 24c KWG und §§ 93b, 93 Abs. 7, 8 AO auf Grundlage der allgemeinen Ermittlungs- bzw. Datenerhebungsklauseln direkt gegenüber einzelnen Banken praktiziert.[1751] Schließlich lagen die Vertragsdaten aller Konteninhaber bei den jeweiligen Instituten schon immer vor. Erst als ein automatisiertes System eingerichtet wurde, mit dem die BaFin als Mittler eigenstän-

1748 Vgl. BVerfGE 125, 260 (327 ff.) – Vorratsdatenspeicherung; EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 = NJW 2014, 2169; dazu *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.); s.a. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 97 ff. = EuZW 2022, 706; dazu auch VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI, Rn. 73 „funktionale Einheit".

1749 BVerfGE 125, 260 (319 f.) – Vorratsdatenspeicherung; jüngst wieder EuGH, Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 88 = NJW 2022, 3135.

1750 BVerfGE 155, 119 (166) – Bestandsdatenauskunft II; E 156, 11 (39) – Antiterrordatei II.; „Eigentumsanalogie" vgl. *Vogelgesang,* Informationelle Selbstbestimmung, 1987, S. 139 ff. *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (132 f.); *Trute*, JZ 1998, 822 (825).

1751 Vgl. *ZKA,* Stellungnahme zum 4. Finanzmarktförderungsgesetz, AZ: 413-FPLD, 13. Februar 2002, S. 8 f.

dig auf speziell geschaffene Dateisysteme der einzelnen Institute zugreifen konnte, entbrannte eine Grundrechtsdiskussion.

Man wird dies kaum allein mit der Heimlichkeit eines solchen Systems erklären können, denn trotz Waffengleichheit würde der Betroffene auch im klassischen Strafverfahren praktisch erst einmal nichts von der Kontenabfrage oder einer ähnlichen Ermittlung erfahren.[1752] Sicher macht die Heimlichkeit den Eingriff intensiver, aber es überrascht doch, dass erst mit der Einführung des neuen Dateisystems überhaupt erst eine Diskussion entbrannte.

Dasselbe gilt für das Geldwäscherecht, das praktisch weder einen Datenbestand noch eine Zugriffsmöglichkeiten schafft, die der Staatsanwaltschaft nicht ohnehin zustünden. Dennoch wird in den (verhältnismäßig wenigen) Beiträgen so getan, als ermöglichte erst die Geldwäschebekämpfung einen universalen Zugriff auf Kontoinhaltsdaten.

„Klassische" Ermittlungsmaßnahmen, die in Verbindung mit allgemeinen Aufbewahrungspflichten – etwa nach § 257 HGB – stehen, stellen insofern eine „Lücke" der Sicherheitsverfassung dar. Sie werden nicht unter dem Topos der *Überwachung* behandelt und erfahren in der Folge eine entsprechend oberflächliche Behandlung durch Rechtswissenschaften und Rechtsprechung.

Es kam beispielsweise auch noch niemand auf die Idee, über die Intensität einer Zeugenvernehmung zu debattieren, obwohl auch hier in Abhängigkeit vom Straftatenverdacht bestimmte Datenerhebungen (in Form spezifischer Fragen) unverhältnismäßig sein könnten, denn die Zeugenvernehmung stellt quasi *a priori* keine heimliche Überwachungsmaßnahme dar. Sie wird nicht aus der Perspektive des Gesamtkonzeptes der Sicherheitsverfassung betrachtet, da insbesondere das Strafprozessrecht noch immer eigene Wege geht.[1753]

3. Umgehung tradierter Prinzipien des Sicherheitsrechts durch (Massen-) *Überwachung*

Diese Lücke, die die klassischen Ermittlungsmaßnahmen, also etwa das staatsanwaltschaftliche Auskunftsersuchen, in der Sicherheitsverfassung scheinbar hinterlassen, existiert nicht ohne Grund. In der Untersuchung

1752 *Bäcker,* Kriminalpräventionsrecht, 2015, S. 303.
1753 Vgl. *Zöller*, ZStW 2012, 411; *Singelnstein*, NStZ 2012, 593 (606).

der Rechtsprechung des BVerfG wurde aufgezeigt, dass die Intensitätskriterien der (Massen)-Überwachungsmaßnahmen schwerlich mit der individuellen Schutzrichtung der Grundrechte begriffen werden können. Die verschiedenen Privatheitsgrundrechte dienen primär der Herrschaft über persönliche Daten und spezifisch der Integrität bestimmter Medien und Räume, in denen diese Daten offenbar werden. Der Grad der Beeinträchtigung dieser Integrität wird weder durch die Streubreite noch durch die Heimlichkeit einer Maßnahme unmittelbar beeinträchtigt. Es bedurfte insofern vertiefender Erklärungsansätze, wieso die Intensität u. a. von diesen Umständen bestimmt wird. Solche wurden von der Rechtsprechung nur unzureichend geliefert, weshalb man sich in der Literatur um ergänzende Erklärungsversuche bemüht hat (vgl. oben Kap B. III. b. bb.).

Diese Erklärungsversuche der Intensitätsbestimmung überzeugen jedenfalls an einigen Stellen nicht. Es ist erkennbar, dass sich die Problematik der Überwachungsmaßnahmen weniger aus einer traditionellen Grundrechtsperspektive ergibt, sondern aus rechtsstaatlichen Fragestellungen, mit denen die Grundrechtsprüfung letztlich aufgeladen wird.

Vor diesem Hintergrund lässt sich auch die Inkonsequenz der Sicherheitsverfassung in Bezug auf traditionelle Ermittlungsmaßnahmen erklären. Das immer detailliertere Sicherheitsverfassungsrecht ist gerade nicht als Gesamtkonzept sämtlicher hoheitlicher Eingriffe in die Privatheitsgrundrechte zu begreifen, sondern als Reaktion auf die Verwerfungen[1754], denen die sicherheitsrechtliche Ermittlungstätigkeit in den letzten Jahren ausgesetzt war. Gerade weil sich die Sicherheitsgesetze von der tradierten Vorstellung einer reaktiven, klar zwischen präventivem und repressivem Tätigwerden trennenden Sicherheitsgewährleistung verabschiedet haben,[1755] wurde ein Konzept der Rechtsprechung erforderlich, das diese Entwicklungen einhegt.

1754 Dazu *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 391 ff.; *Albers,* Determination, 2001, S. 112 ff., 215 ff., 252 ff.; *Zöller,* Informationssysteme, 2002, S. 319 ff.; *Thiel,* Entgrenzung, 2012, S. 81 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 194 ff; 205 ff.; *Hoppe,* Vorfeldermittlungen, 1999; *Denninger* in Huster/Rudolph (Hrsg.), Präventionsstaat, 2008, S. 85 (88 ff.); *Poscher*, Die Verwaltung 2008, 345 (348 ff.); *ders.* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245; *Volkmann*, NVwZ 2022, 1408 (1410 f.).; *M. Baldus*, Die Verwaltung 47 (2014), 1.

1755 Jüngst ausf. *Danne,* Prävention und Repression, 2022.

Es ist mitnichten zufällig, dass die klassische Ermittlungstätigkeit unseren rechtsstaatlichen Prinzipien, insbesondere der Reaktivität[1756], entspricht. Vielmehr hat das (ältere) Strafprozessrecht insofern die Vorstellungen über eine rechtsstaatliche Sicherheitsgewährleistung wesentlich geprägt.[1757]

Wenn also die Übertragung der Rechtsprechung zu staatlichen Überwachungsmaßnahmen auf bestimmte Vorschriften im Raum steht, kommt es nicht darauf an, ob diese Vorschriften praktisch über die Möglichkeiten hinausgehen, die den Sicherheitsbehörden traditionell zustehen, sondern, ob diese Vorschriften eine sicherheitsrechtliche Datenverarbeitung ermöglichen, deren Charakter sich von den tradierten Prinzipien der Sicherheitsgewährleistung löst.

Typischerweise ist dies der Fall, wenn sich die Überwachungsmaßnahme nicht reaktiv verhält, sondern im Vorfeld ansetzt und entsprechend – zumindest hinsichtlich bestimmter Verarbeitungsschritte – massenhaft und anlasslos ausgestaltet ist, denn die vorfeldmäßige Massenüberwachung zur vorläufigen Beweissicherung oder zur Verdachtsgewinnung ist dem ursprünglichen Sicherheitsrecht, insbesondere dem Strafprozessrecht,[1758] fremd.[1759] Auch die Einbeziehung Privater kann insofern ein Hinweis sein[1760], wenngleich die Ausgliederung bestimmter Maßnahmen an Private sich für die Intensitätsbewertung neutral verhält.[1761]

Das (Anti-)Geldwäscherecht zeigt sich vor diesem Hintergrund als typischer Fall einer Abkehr vom klassischen Sicherheitsmodell, da es strukturell auf eine massenhafte Datenanalyse zur Vorbereitung von Strafverfah-

1756 Dazu *Bäcker,* Kriminalpräventionsrecht, 2015, S. 51 ff., 122 ff.; *Gärditz* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. II, 2. Aufl. 2022, § 22 Rn. 60 ff.; entspr. krit. zu anlasslosen Maßnahmen *Puschke/Singelnstein*, NJW 2008, 113 (118); *Lisken*, ZRP 1990, 15 (17 ff.); *ders*., ZRP 1994, 264 (267 f.); *Hund*, NJW 1992, 2118 (2119).

1757 Vgl. *Schünemann*, FS 25 Jahre DAV, 2009, S. 827 (829 ff.).

1758 *Kölbel* in MüKo StPO, § 160 Rn. 13 ff. zu Vorfeldermittlungen mwN.

1759 TK-Vorratsdatenspeicherung insofern als „Dammbruch" *Breyer*, StV 2007, 214 (219 f.); s.a. *Puschke/Singelnstein*, NJW 2008, 113 (118 f.); krit. auch *Baur* ZIS 2020, 275 (277) mwN. insb. zur strafrechtlichen Literatur.

1760 Zur Privatisierung als Trend der neuen Sicherheitsarchitektur *Engelhart* in Engelhart/Roksandić Vidlička (Hrsg.), Terrorism, 2019, S. 287 (290 f.).

1761 BVerfGE 125, 260 (321) – Vorratsdatenspeicherung; *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff.; aA. *Szuba,* Vorratsdatenspeicherung, 2011, S. 194 ff.; *Grafe,* Verkehrsdaten, 2008, S. 18 f.; *Herzog*, WM 1996, 1753 (1762); keinen Eingriff durch die Speicherung bei Privaten erkennt *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 2 Rn. 30.

ren ausgelegt ist (Kap. E. II. 2. c. bb. (2)).[1762] Es verpflichtet Private zu verschiedenen Datenverarbeitungsmaßnahmen, die letztlich allesamt der Aufklärung sicherheitsrelevanter Umstände und der Aufklärung staatlicher Behörden hierüber dienen. Das System verhält sich graduell, wobei die frühen Maßnahmen anlasslos und spätere, zielgerichtete Verarbeitungen heimlich erfolgen. Es dient also gerade dazu, die Defizite klassischer Ermittlungstätigkeit im Bereich der Geldwäsche und der Terrorismusfinanzierung zu beseitigen.[1763] Deshalb bedarf es einer verfassungsrechtlichen Überprüfung nach den besonderen Maßstäben des Sicherheitsverfassungsrechts.

II. Das Überwachungssystem des Geldwäscherechts als Untersuchungsgegenstand

Im Folgenden sollen die einzelnen Grundrechtseingriffe im Rahmen der Geldwäschebekämpfung vor dem Hintergrund des Sicherheitsverfassungsrechts übersichtlich dargestellt, aber noch nicht abschließend bewertet werden (dies sogleich unter G. III.)

Die Grundstruktur der Geldwäschebekämpfung sieht eine Reihe von Informationseingriffen vor, die hinsichtlich der individuellen Betroffenheit graduell bzw. trichterförmig verlaufen, also zunächst viele Personen nur wenig intensiv betreffen und mit Abnehmen der Zahl der Betroffenen immer invasiver werden. Insofern handelt es sich grundsätzlich um eine strategische Überwachungsmaßnahme.[1764]

Da sämtliche Daten, die in diesem Prozess anfallen, für eine spätere Verwendung aufbewahrt werden müssen, sieht der Normkomplex aber auch eine Vorratsdatenspeicherung vor[1765], verbindet also verschiedene Formen der Massenüberwachung.

1762 ausf. *Degen,* Geldwäsche, 2009, S. 148 ff.; *Barreto da Rosa* in Herzog GwG, § 30 Rn. 13 ff.; *Baur* ZIS 2020, 275 (277); aA., bzw. Verweis auf administrativ-gefahrenabwehrrechtlichen Charakter der FIU: BT-Drs. 18/11555, S. 136; zust. etwa *Krais,* Geldwäsche, 2018, Rn. 475; *Bülte*, NVwZ-Extra 4b/2022, 1 (14 ff.).

1763 Vgl. die Erwägunggründe 1, 2, 37 der 4. EU-GeldwäscheRL.

1764 Vgl. zur Gradualität EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 325. = NVwZ-Beil. 2021, 11.

1765 S. nur *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71 f.); *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (897 ff.); zur deutschen Rechtslage *ders.* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (246 ff.); undifferenziert *Spoerr* in BeckOK Datenschutzrecht, Grundl. Syst. J Rn. 226.

1. Transaktionsmonitoring

§ 10 Abs. 1 Nr. 5 GwG i. V. m. § 25h Abs. 2 KWG schreibt (insbesondere) den Kreditinstituten vor, die Transaktionen ihrer Kunden mit Datenverarbeitungssystem zu überwachen.[1766]

a. *Kontinuierliche Überwachung* nach §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG

Diese kontinuierliche Überwachung wurde oben umfassend beschrieben (Kap D. III. 2. b. (2)). Sie geht u. a. nach § 10 Abs. 3 Nr. 1 GwG mit der Begründung einer Geschäftsbeziehung einher – damit muss der Vertragsschluss gemeint sein[1767] – und gilt ab dann fortlaufend bzw. *kontinuierlich*.[1768]

Wie üblich wird der Begriff der *Überwachung* § 10 Abs. 1 Nr. 5 GwG vom Gesetz nicht definiert. Es lässt sich jedoch aus der Norm und den hierzu ergangenen Leitlinien durchaus erschließen, dass mehrere Datenverarbeitungsschritte i. S. v. Art. 4 Nr. 2 DSGVO darunterfallen.

In den Auslegungshinweisen der BaFin für Kreditinstitute wird heute zwischen Screening und Monitoring unterschieden.[1769] Screening stellt die Echtzeitüberwachung[1770] besonders auffälliger Transaktionen vor deren Durchführung dar. Es handelt sich um eine manuelle Kontrolle, die etwa aufgrund eines Embargos notwendig werden kann. Auch in diesem Fall geht aber meist eine digitale bzw. automatisierte Kontrolle voraus, die auf-

1766 Vgl. BT-Drs. 17/9038, S. 49 f.; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 343; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Ackermann/Reder*, WM 2009, 158 (164); *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (456).

1767 *Sotiriadis,* Gewinnabschöpfung und Geldwäsche, 2010, S. 451 f.

1768 BT-Drs. 16/9038, S. 34; *Ackermann/Reder*, WM 2009, 158 (166); vgl. auch *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Z. 9, S. 10.

1769 *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14.

1770 Vgl. dazu auch *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), S. 49, lfd. Nr. 4.74 lit. a).

grund bestimmter Umstände die Transaktion anhält und zur menschlichen Überprüfung markiert.[1771]

Unter dem Monitoring hingegen wird die Ex-Post-Kontrolle einer Vielzahl von Transaktionen verstanden.[1772] Sie erfolgt turnusmäßig und umfasst etwa bei Girokonten prinzipiell sämtliche Transaktionen. Dabei wird geprüft, ob die Transaktionen dem Risikoprofil des Kunden entsprechen, und ob einzelne Transaktionen *auffällig* sind bzw. waren.

Stellt sich heraus, dass bei der Transaktion (auch im Einzelfall) ein höheres Risiko i. S. d. § 15 Abs. 3 GwG vorliegt, sind die erhöhten Sorgfaltspflichten des § 15 GwG zu beachten. Ein höheres Risiko liegt nach § 15 Abs. 3 Nr. 3 lit. a) GwG etwa vor, wenn eine Transaktion *im Vergleich zu ähnlichen Fällen besonders komplex oder ungewöhnlich groß* ist, *einem ungewöhnlichen Muster folgt* (lit. b)) oder *keinen offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck hat* (lit. c)). Entsprechend sieht § 25h Abs. 2 KWG vor, dass *die Datenverarbeitungssysteme einzelne Transaktionen im Zahlungsverkehr erkennen, (…) die im Verhältnis zu vergleichbaren Fällen besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen.*[1773] Schon aufgrund dieser relativen Bestimmung ist es notwendig, dass die Monitoringsysteme sämtliche Transaktionen eines jeden Kunden in die Analyse miteinbeziehen.[1774]

Dass in vielen Fällen, insbesondere bei Kunden mit niedrigem Risikoprofil, grundsätzlich nur vereinfachte Sorgfaltspflichten nach § 14 GwG gelten, ändert nichts an der Universalität der Monitoringsysteme, denn *die Verpflichteten müssen in jedem Fall die Überprüfung von Transaktionen und die Überwachung von Geschäftsbeziehungen in einem Umfang sicherstellen, der es ihnen ermöglicht, ungewöhnliche oder verdächtige Transaktionen zu erkennen und zu melden*§ 14 Abs. 2 S. 2 GwG. Da der risikobasierte Ansatz am Einzelfall orientiert ist, kann er sich logischerweise auf den Umfang

1771 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 57 ff.

1772 *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14;

1773 Zum Zusammenhang von § 15 Abs. 3 GwG und 25h Abs. 2 KWG: *Vollmuth,* Geldwäscheprävention, 2020, S. 171 ff.

1774 Vgl. *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 15 *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Z. 86d; *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 11 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462 f.).

der (elektronischen) Erstüberprüfung bzw. der Datenerhebung auch nicht auswirken, da sich erst aufgrund der Daten im Einzelfall ableiten lässt, ob denn bei der individuellen Transaktion ein (erwartbar) geringes Risiko besteht oder nicht.

Es wurde bereits dargestellt, dass man nun diskutieren könnte, ob die Pflicht zum Monitoring eine Rechtsgrundlage zur *Erhebung* der Daten beinhaltet, oder ob sie davon ausgeht, dass diese Daten ohnehin bestehen und nur noch entsprechend *verarbeitet* werden sollen. Zwar drängt sich ersteres Verständnis auf[1775], denn sonst wäre das Screening kaum sinnvoll möglich. Es spielt im Ergebnis aber keine Rolle, da jedenfalls nach § 8 Abs. 1 GwG sämtliche Informationen, die zur Erfüllung der Sorgfaltspflichten eingeholt werden, aufgezeichnet und aufbewahrt werden müssen.

b. Transaktionsmonitoring als *strategische Datenanalyse*

Jede Kontobewegung, etwa im Rahmen eines Girokontos oder eines Kreditkartenvertrags, wird (auch) aufgrund der geldwäscherechtlichen Verpflichtungen erhoben und analysiert.[1776] Diese Analyse stellt den ersten Schritt einer längeren Verarbeitungskette dar, die im Ergebnis der Verfolgung und Verhinderung bestimmter Straftaten dient, die in § 1 Abs. 1, 2 GwG genannt werden. Entscheidend ist dabei, dass im Moment der Datenverarbeitung durch den automatisierten Abgleich kein sicherheitsrechtlicher Anlass für die jeweilige Transaktion vorliegt. Vielmehr werden schlicht sämtliche Transaktionen verarbeitet und analysiert, wodurch Anlassfälle erst entdeckt werden sollen.[1777]

Die kontinuierliche Überwachung sämtlicher Kunden dient in mittelbarer Konsequenz der Vorbereitung von Verdachtsmeldungen i. S. d. § 43 Abs. 1 GwG (Art. 33 GWRL). Danach müssen u. a. Sachverhalte der FIU gemeldet werden, bei denen Tatsachen darauf hindeuten, dass *ein Vermö-*

1775 So wohl auch *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d) S. 69 f.

1776 Vgl. *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 101 ff; 493 ff.; *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (123); *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 28. 29, S. 22 ff.; *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462); offen gelassen bei *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (990); aA. *Krais,* Geldwäsche, 2018, Rn. 284.

1777 *Böse*, ZStW 2007, 848 (866 ff.); auch schon *Dahm*, WM 1996, 1285 (1290); *Herzog*, WM 1996, 1753 (1761).

gensgegenstand, der mit einer Geschäftsbeziehung, einem Maklergeschäft oder einer Transaktion im Zusammenhang steht, aus einer strafbaren Handlung stammt, die eine Vortat der Geldwäsche darstellen könnte, oder *ein Geschäftsvorfall, eine Transaktion oder ein Vermögensgegenstand im Zusammenhang mit Terrorismusfinanzierung steht*, § 43 Abs. 1 Nr. 1, 2 GwG.

Die nach dem GwG Verpflichteten sind also berufen, proaktiv geldwäscherechtliche *Verdachtsfälle* aufzuspüren. Über den Verdachtsgrad der geldwäscherechtlichen Meldungen wurde und wird viel diskutiert. Früher wurde über den Vergleich zur Strafanzeige i. S. d. § 152 Abs. 1 StPO versucht, die Notwendigkeit eines strafprozessualen Anfangsverdachts abzuleiten.[1778] Diese Analogie ergibt schon deshalb keinen Sinn, weil der Anfangsverdacht nicht für den Anzeigenden gilt, sondern nur für die Staatsanwaltschaft bzw. deren Reaktion auf die Anzeige. Sie allein prüft, ob der angezeigte Sachverhalt einen Anfangsverdacht etabliert, was der Fall ist, wenn „konkrete Anhaltspunkte"[1779] für die Begehung einer Straftat vorliegen.

Heute ist man sich einig, dass bei den geldwäscherechtlich Verpflichteten kein Anfangsverdacht vorliegen muss. Die Verdachtsschwelle des § 43 Abs. 1 GwG ist also – zumindest in der Theorie – genuin.[1780] Ob man sie sinnvoll vom denkbar niedrigschwelligen Anfangsverdacht der StPO abgrenzen kann,[1781] sei dahingestellt.

Auch sagt der Verdachtsgrad nichts darüber aus, ob die Meldung dem *Strafverfahren* in einem materiellen bzw. verfassungsrechtlichen Sinne[1782] zuzuordnen ist oder nicht.[1783]

Funktional betrachtet steht die Verdachtsmeldung als erstes Glied einer Kette von Maßnahmen, die ganz primär auf die Aufdeckung von Straftaten gerichtet sind.

1778 *Krais,* Geldwäsche, 2018, Rn. 510; *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (68); *ders.* in Herzog GWG, 1. Aufl. 2010, § 11 Rn. 18 ff.; *Klugmann*, NJW 2012, 641 (644); *Carl/Klos*, wistra 1994, 161 (162); *Bülte*, NZWiSt 2017, 276 (280 f.); *Degen,* Geldwäsche, 2009, S. 127 f.

1779 *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 152 Rn. 4; *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 15 mwN.

1780 BT-Drs. 17/6804, S. 21, 35.; BT-Drs. 18/11928, S. 26; BVerfG, NJW 2020, 1351 (1353, Rn. 43); OLG Frankfurt, NStZ 2020, 173 (175).

1781 Insofern krit. *Höche/Rößler*, WM 2012, 1505 (1509); *Bülte*, NZWiSt 2017, 276 (280 f.).

1782 Vgl. BVerfGE 113, 348 (371); allg. zum Begriff der Strafverfolgung *Greco,* Strafprozesstheorie, 2015, S. 119 ff.

1783 *Barreto da Rosa* in Herzog GwG, § 30 Rn. 13; *N. Lange*, DRiZ 2002, 264 (266); vgl. auch *Schenke*, FS Paeffgen, 2015, S. 393 (396 ff.); verkannt bei *Bülte*, NVwZ-Extra 4b/2022, 1 (17).

Für die Einordnung des Transaktionsmonitorings als Maßnahme des Sicherheitsrechts (zum Begriff (Kap. B. I. 2. c.) spielt es letztlich aber ohnehin keine Rolle, ob die Überwachung der Gefahrenabwehr, der Strafverfolgung oder der nachrichtendienstlichen Vorfeldaufklärung zugeordnet werden soll. Dies wird nur bei der Datenübermittlung zwischen den Behörden relevant (dazu unten III. 3.). Entscheidend ist, dass überhaupt ein sicherheitsrechtlicher Zusammenhang bereits beim Handeln der Privaten besteht.

Die Einordnung einer informationellen Maßnahme in das Sicherheitsrecht ist für die grundrechtliche Bewertung essenziell. Allen Privatheitsgrundrechten ist gemein, dass ihr Schutzgut mit sekundären Wirkungen erklärt werden muss.[1784] Die Autonomie über private Daten ist faktisch kein Interesse an sich, anders als bspw. die Berufswahlfreiheit, denn eine „Herrschaft" über Informationen wäre illusorisch. Erst aus den spezifischen Gefahren, die mit einer fremden Verfügung über die Daten einhergehen können, ergibt sich die Notwendigkeit eines grundrechtlichen Schutzes.[1785] Stets ist also bei der jeweiligen Datenverarbeitung entscheidend, welche Gefahren bzw. potenziell tatsächlich negative Konsequenzen mit ihr einhergehen. Sicherheitsrechtliche Informationseingriffe sind danach insofern grundrechtssensibel, als dass sie zu weiteren Repressionsmaßnahmen führen können, die dann tatsächlich die Freiheiten des Betroffenen einschränken. Damit unterscheiden sie sich fundamental von der privaten Informationserlangung.

Vor diesem Hintergrund möchte der Gesetzgeber mit der Bezeichnung des Monitorings als „gewerberechtlicher Pflicht"[1786] wohl den Eindruck erwecken, dass es sich bei den Maßnahmen der Geldwäschebekämpfung nicht um eine sicherheitsrechtliche Indienstnahme wie bei der TK-Vorratsdatenspeicherung handelt.

Dies überzeugt nicht.[1787] Zwar lässt sich durchaus ein Eigeninteresse der Verpflichteten an der Bekämpfung von Geldwäsche erkennen, die staatliche Motivation ist allerdings ganz offensichtlich in der Sicherheitsgewährleis-

1784 vgl. *Poscher* in Gander/Perron/Poscher ua. (Hrsg.), Resilienz, 2012, S. 167; *ders.* in Miller (Hrsg.), Privacy and Power, 2017, S. 129der insofern anders als die Rspr. keinen eigenständigen Schutzbereich anerkennt.

1785 In diesem Sinne schon BVerfGE 65, 1 (45) – Volkszählung; dazu *Pfisterer*, JöR 2017, 393 (413)

1786 BT-Drs. 18/11928, S. 26; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 75.

1787 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 7 f.

tung zu erkennen.[1788] Durch die Privatisierung und die damit einhergehende massenhafte Gewinnung von Verdachtsmomenten wird das reaktive Korrektiv, der Anfangsverdacht, unterlaufen.[1789] Sämtliche Maßnahmen, die die Verpflichteten zur Vorbereitung ihrer Meldepflichten ausführen, sind insofern als primär strafprozessuale, im Zweifel jedenfalls doppelfunktionale, Vorermittlungen zu bewerten.[1790] Für die Analysetätigkeit der FIU gilt dies erst recht. Hier ergibt sich jedoch das Folgeproblem, dass die Tätigkeit der FIU insgesamt eher dem eines Nachrichtendienstes entspricht.[1791] Mit der FIU wurde eine primär im Rahmen des Strafverfahrens vorermittelnde Behörde geschaffen, die nachrichtendienstliche Fähigkeiten aufweist. Das ist ein Novum in der deutschen Sicherheitsarchitektur (unten III. 3. b. (6)).

Das Transaktionsmonitoring lässt sich in dieser Konsequenz also durchaus mit anderen Formen der strategischen Datenanalyse vergleichen. Stets erfolgen die grundlegende Datenerhebung und der darauffolgende erste Abgleich, ohne dass in diesem Moment ein sicherheitsrechtlicher Anlass besteht. Vielmehr sollen solche Anlassfälle erst gefunden werden.[1792]

Graduell wird also zunächst eine riesige Datenmenge mittels EDV analysiert, die dann durch eine weitere manuelle Kontrolle zur Gewinnung von Verdachtssituationen führt. Ähnliches geschieht bei der strategischen Fernmeldekontrolle[1793] oder der automatisierten Kontrolle von KFZ-Kennzeichen[1794], wenngleich hier immerhin ein Abgleich mit externen Daten stattfindet, die von sich aus anlassbezogen sind und entsprechend ausgestaltet werden können. Allerdings wird auch bei diesen Maßnahmen faktisch in den meisten Situationen im Falle eines „Treffers" nicht wirklich eine Situation vorliegen, die Anlass für (weitere) sicherheitsrechtliche Maßnahmen liefert.[1795]

1788 *Herzog*, FS Kohlmann, 2003, S. 427 (449); vgl. auch BVerfG, NJW 2020, 1351 (1353, Rn. 44)

1789 *Krais,* Geldwäsche, 2018, Rn. 510; *Lenk*, JR 2020, 103 (107 f., insb, Fn 51); *Böse*, ZStW 2007, 848 (861, 866 ff.).

1790 *Barreto da Rosa* in Herzog GwG, § 43 Rn. 7 f.; vgl. auch BVerfG, NJW 2020, 1351 (1353, Rn. 44).

1791 *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21; ausf. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.).

1792 Vgl. zu dieser Typisierung strategischer Überwachungsmaßnahmen *Bäcker,* Kriminalpräventionsrecht, 2015, S. 53 ff.

1793 BVerfGE 154, 152 (245 ff.) – Ausland-Ausland-Fernmeldeaufklärung.

1794 dazu *Roggan*, NStZ 2022, 19 (20).

1795 Vgl. zur Kennzeichenkontrolle BW-LT-Drs. 16/5009, S. 5; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 53 ff.; *Engert* – Wie die Polizei Millionen Auto-

Beim Geldwäschemonitoring findet nicht nur ein Abgleich mit externen Datenbanken und bestimmten Suchbegriffen statt.[1796] Vielmehr werden innerhalb des Datensatzes selbst Auffälligkeiten bzw. ungewöhnliche Muster gesucht. Das Monitoring kann schon dann einen Treffer anzeigen, wenn innerhalb der Kontobewegungen eines Kunden eine Transaktion „aus dem Rahmen fällt" und nicht mehr dem bisherigen Kundenprofil entspricht.

Insofern ist das Kundenmonitoring strukturell eng mit der Fluggastdatenüberwachung[1797] verwandt.[1798] Auch hier werden nicht nur Abgleiche mit verdachtsbegründenden, externen Datensätzen, z. B. Fahndungsdateien, vorgenommen, sondern die erhobenen Daten werden auf Muster untersucht, die sich allein aus den jeweils untersuchten Fluggastdaten ergeben und regelmäßig neu erstellt werden, § 4 Abs. 2 Nr. 2, Abs. 3, 4 FluGDaG. Der Anwendungsbereich der Flugdatenüberwachung fällt allerdings gegenüber dem Transaktionsmonitoring deutlich geringer aus. Die Flugdatenüberwachung betrifft die meisten Menschen wohl nur ein paar wenige male im Jahr. Ganz anders verhält es sich bei der geldwäscherechtlichen Überwachung. Diese berührt einen Jeden, der am digitalen Zahlungsverkehr teilnimmt, täglich.

2. Aufzeichnungs- und Aufbewahrungspflicht

Nicht nur im Hinblick auf das Monitoring kommt eine Überprüfung des Anti-Geldwäscherechts anhand der sicherheitsrechtlichen Maßstäbe des BVerfG und des EuGH in Betracht. Auch die Aufbewahrungspflichten der GWRL bzw. des GwG stehen zur Debatte.[1799]

---

fahrer mit einem System überwacht, das nicht funktioniert Buzzfeed.com vom 15.10.2018, https://www.buzzfeed.com/de/marcusengert/kennzeichenerfassung-der-polizei-funktioniert-nicht, zuletzt aufgerufen am 12.01.2025.

1796 Bspe. bei *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (468).

1797 Vgl. *Arzt*, DÖV 2017, 1023 (1025); *ders.* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap G Rn. 1330.

1798 zur Analyse von Telekommunikationsverkehrs und -Standortdaten auch schon EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 ff. = NJW 2021, 531.

1799 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 101 ff, 493 ff.; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (897 ff.); *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (72); *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (118, 122 ff.).

Der Umfang der Aufbewahrungspflicht nach Art. 40 Abs. 1 GWRL und § 8 Abs. 1 GwG wurde bereits erläutert. Auffällig an der deutschen Umsetzung ist, dass – anders als bei Art. 40 Abs. 1 Nr. 1, 2 GWRL – nicht zwischen den Dokumenten, *die bei den Sorgfaltspflichten anfallen*, und den Transaktionsbelegen getrennt wird, sondern alle aufgezählten und aufzubewahrenden Dokumente unter dem Vorbehalt stehen, dass sie *im Rahmen der Erfüllung der Sorgfaltspflichten erhoben oder eingeholt* wurden.

Aufgrund des Vorrangs der Richtlinie, die ausdrücklich eine uneingeschränkte Aufbewahrung von Transaktionsbelegen fordert, ist § 8 Abs. 1 GwG aber schlicht i. V. m. der Überwachungspflicht dahingehend zu verstehen, dass sämtliche Transaktionsbelege ohnehin aufgrund des obligatorischen Monitorings anfallen, jedenfalls aber für dieses *eingeholt* und damit auch aufbewahrt werden müssen.[1800] Im Ergebnis sehen also sowohl Art. 40 Abs. 1 GWRL als auch § 8 Abs. 1 GwG eine umfangreiche Pflicht zur Aufbewahrung sämtlicher Transaktionsdaten vor.[1801]

Die Daten sind nach § 8 Abs. 4 S. 1, 2 GwG mindestens fünf und maximal zehn Jahre zu speichern. Die Frist beginnt bei Transaktionsbelegen nach § 8 Abs. 4 S. 4 GwG erst ab dem Ende des Jahres zu laufen, in dem die Transaktion stattfand. Da die §§ 257 Abs. 5 HGB, 147 Abs. 4 AO[1802] eine Speicherfrist von zehn Jahren ab Ende des Kalenderjahres, in dem der Beleg anfiel, vorsehen, dürfte nach § 8 Abs. 4 S. 1 HS. 2 GwG aber stets eine Speicherung von zehn Jahren stattfinden. § 8 Abs. 4 S. 4 GwG hat für Transaktionsbelege hinsichtlich der Frist neben den §§ 257 Abs. 5 HGB, 147 Abs. 4 AO also keine eigenständige Bedeutung.[1803]

§§ 257 Abs. 5 HGB und 147 Abs. 4 AO sind nicht nur für die Fristbestimmung relevant, sondern statuieren ein besonderes Problem für die

1800 Vgl. *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (462).

1801 So schon BT-Drs. 16/9647, S. 3.; s.a. *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 5.1; *FATF,* Recommendations 2012, konsolidierte Fassung März 2022, lfd. Nr. 11; . *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 101 ff; 493 ff.; *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (123); *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 28. 29, S. 22 ff.; offen gelassen bei *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (990); aA. *Krais,* Geldwäsche, 2018, Rn. 284.

1802 Vgl. *Schober*, BC 2013, 528 (532).

1803 *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438; vgl. auch BT-Drs. 19/13827, S. 76; *Brian/Krais* in BeckOK GwG, § 8 Rn. 45.

grundrechtliche Behandlung der Aufbewahrungspflicht. Neben anderen Vorschriften (siehe Kap. D. II) regeln sie eine umfangreiche Pflicht bestimmter Wirtschaftsteilnehmer zur Speicherung von Transaktionsdaten bzw. von Buchungsbelegen (Kontoauszüge).

Nun ist aus der sicherheitsrechtlichen Rechtsprechung des BVerfG[1804], des EuGH[1805] und des EGMR[1806] bekannt, dass Speicherpflichten per se in die Privatheitsgrundrechte der Betroffenen eingreifen. Die zugrunde liegenden Fälle waren jedoch stets so gelagert, dass ohne den jeweiligen sicherheitsrechtlichen Zweck nicht von einer Speicherung auszugehen war. Es ist gerade die Absicht von *Vorratsdatenspeicherungen*, dass den Daten eine inhärente Potentialität für sicherheitsrechtliche Ermittlungen zugesprochen wird (s. o. Kap. B II. 2. B. (1)) und deswegen eine Speicherung spezifisch angeordnet wird. Daten, die aufgrund verschiedener (nicht sicherheitsrechtlicher) Normen und Vorgänge im Wirtschaftsleben ohnehin anfallen, bedürfen einer solchen Bevorratung gerade nicht. Sie sind im Wege der klassischen Ermittlung zugänglich.

§ 8 Abs. 1 GwG bzw. Art. 40 Abs. 1 GWRL stellen insofern ein Novum dar. Sie etablieren eine sicherheitsrechtliche Speicherpflicht, die sich faktisch kaum auswirken dürfte, da die entsprechenden Daten ohnehin aufgrund verschiedener wirtschaftsrechtlicher Normen gespeichert werden.

Diese Komplexität lässt sich nur auflösen, wenn die Wechselwirkung der einzelnen Datenverarbeitungsschritte der Vorratsdatenspeicherung in den Vordergrund gestellt wird.[1807] Die Vorratsdatenspeicherung ist gewissermaßen intensiver als die Summe ihrer Teile. Die Zusammenschau von § 8

1804 BVerfGE 125, 260 (310 f.) – Vorratsdatenspeicherung; krit.; *Schluckebier* abw. Meinung BVerfGE 125, 260 (366); Betonung der separaten Betrachtung auch bei *Eichberger* abw. Meinung BVerfGE 125, 360 (380 ff.); zust. *Bull,* Informationelle Selbstbestimmung, 2. Aufl. 2011, S. 96 ff.; *Gersdorf* in BeckOK Informations-/MedienR, GG Art. 10 Rn. 30.

1805 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; zuletzt Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 60 = NJW 2022, 3135.

1806 EGMR, Urt. v. 26.03.1987, Nr. 9248/81 (Leander/Schweden), Rn. 84; Urt. v. 16.2.2000, Nr. 27798/95 (Amann/Schweiz), Rn. 69.; Urt. v. 04.12.2008, Nr. 30562/04, 30566/04 (Marper/Vereinigtes Königreich), Rn. 59 ff. = EuGRZ 2009, 299.

1807 BVerfGE 125, 260 (327 ff.) – Vorratsdatenspeicherung; dazu *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 159; EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 = NJW 2014, 2169; s.a. Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 97 ff. = EuZW 2022, 706; VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI, Rn. 73 „funktionale Einheit".

Abs. 1 GwG bzw. Art. 40 Abs. 1 GWRL und etwa §§ 257 Abs. 5 HGB, 147 Abs. 4 AO führt vor Augen, dass nur die Speicheranordnung allein nicht ausreichend ist, um den grundrechtlichen Charakter der Maßnahme zu verstehen. Nur in Kombination mit den Zugriffen, die auf der jeweiligen Regelung aufbauen, lässt sich der tatsächliche Nutzen der Speichernorm und damit ihr Eingriffscharakter erschließen.

Während bei der Bevorratung von TK-Verkehrsdaten im Vordergrund steht, dass die Daten erst aufgrund der Speicheranordnung überhaupt längerfristig existieren und deswegen unabhängig von der Zugriffsausgestaltung problematisch bleiben[1808], muss bei Normen, die der Speicherung letztlich nur einen sicherheitsrechtlichen Zweck hinzufügen, etwas anderes gelten. Für die Bewertung kann hier nur ausschlaggebend sein, inwiefern die spezifische Speicherpflicht zur Umgehung klassischer Ermittlung führen soll, die einen retrograden Zugriff eigentlich nur unter bestimmten Umständen ermöglichen würden.

Durch die Ergänzung um einen sicherheitsrechtlichen Zweck werden die Daten ab dem Beginn der Speicherung als potenziell relevant eingestuft, obwohl der Betroffene keinerlei Anlass dazu gab. In dieser Vorsorge liegt eine Abkehr von der tradierten Reaktivität des Sicherheitsrechts, die jedenfalls rechtsstaatlich bedenklich ist, und der kritischen Betrachtung von Massenüberwachung zugrunde liegt (s. Kap. B. III 2. a. aa. & c.). Die Speicherung ist also in noch engerem Zusammenhang mit den entsprechenden Zugriffsrechten zu betrachten. Nur wenn die sicherheitsrechtliche Speicherung auch mit einer Zugangsvereinfachung einhergeht, kann von einer grundrechtssensitiven *(Massen-)Überwachung* die Rede sein.

Gerade hier zeigt sich also, dass ein definiertes Verständnis des Überwachungsbegriffes durchaus dabei helfen kann, die grundrechtliche Problematik konkreter Datenverarbeitungen, die auf den ersten Blick harmlos wirken, grundrechtlich korrekt zu erfassen. Die mit der Speicherpflicht einhergehende Zweckerweiterung und darauf aufbauende Zugriffsmöglichkeiten führen zu einer relevanten Beeinträchtigung der Privatheit.

1808 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169; zuletzt Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135; s.a. *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.).

3. Zugriffsrechte der FIU

Eine mit den Aufbewahrungspflichten verbundene Zugriffsmöglichkeit sieht das Anti-Geldwäscherecht ebenfalls vor. Nach Art. 32 Abs. 9 GWRL (9) kann *jede zentrale Meldestelle im Rahmen ihrer Aufgaben unbeschadet des Artikels 34 Absatz 2 von jedem Verpflichteten Informationen für (sic) den in Absatz 1 genannten Zweck anfordern, einholen und nutzen, selbst wenn keine vorherige Meldung gemäß Artikel 33 Absatz 1 Buchstabe a oder Artikel 34 Absatz 1 erstattet wurde.*

Art. 32 Abs. 9 wurde erst durch die 5. GWRL eingeführt. In Deutschland bedurfte es insofern aber keiner Änderung, da § 30 Abs. 3 GwG bereits mit der Umsetzung der 4. GWRL erlassen wurde und eine ausreichende Ermächtigung vorsieht. Nach § 30 Abs. 3 GwG kann die FIU *unabhängig vom Vorliegen einer Meldung Informationen von Verpflichteten einholen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.*

Die Auskunftsersuchen der FIU dürfen sich im Bereich der Aufgaben der FIU auf umfassende Informationen beziehen. Der Begriff der Informationen in § 30 Abs. 3 GwG ist mangels einschränkender Umschreibungen weit zu verstehen und bezieht sich auf sämtliche Kontobestands- und Inhaltsdaten.[1809]

Die Aufgaben der FIU sind in § 28 GwG genannt und werden durch die §§ 29 ff. GwG ausgestaltet. Aus diesen ergibt sich die Funktion der FIU, die nicht nur in der Analyse von Verdachtsmeldungen i. S. d. § 43 GwG zu sehen ist, sondern ganz primär auch in der Weitergabe relevanter Finanzinformationen an bestimmte Sicherheitsbehörden, § 28 Abs. 1 Nr. 6 i. V. m. § 32 Abs. 2, 3 GwG.

Besonders bemerkt werden muss dabei, dass nach § 32 Abs. 3 Nr. 2 GwG auf Ersuchen (insb. der Staatsanwaltschaft) auch Finanzinformationen zur Verhinderung und Aufklärung *sonstiger Gefahren und Straftaten* übermittelt werden dürfen, die nicht im Zusammenhang mit der Bekämpfung von Geldwäsche und Terrorismusfinanzierung stehen.

Die FIU selbst kann also auf sämtliche gespeicherten Finanzdaten bei den Verpflichteten zugreifen. Angesichts der umfangreichen Speicherpflicht nach § 8 Abs. 1 GwG bzw. Art. 40 Abs. 1 GWRL ist ihr eine Abfrage von Kontoauszügen mit einem Alter von bis zu zehn Jahren ermöglicht. § 30 Abs. 3 GwG eröffnet der FIU damit denselben Zugriff, der nach § 8a Abs. 1 Nr. 2 BVerfSchG den Nachrichtendiensten offen steht.

1809 *Barreto da Rosa* in Herzog GwG, § 30 Rn. 19.

Anders als diese Norm sieht § 30 Abs. 3 GwG allerdings keinerlei spezifische Voraussetzungen oder Verfahrensvorschriften vor. Lediglich die *Erforderlichkeit* zur Aufgabenwahrnehmung muss gewahrt sein.

III. Geldwäscherechtliche Überwachung von Finanzdaten am Maßstab deutscher und europäischer Grundrechte

Für die grundrechtliche Bewertung der einzelnen Maßnahmen nach dem Anti-Geldwäscherecht – die einzelnen Datenverarbeitungsschritte sind einzeln zu betrachten, ihre Intensität leitet sich aber aus der Wechselwirkung mit den kombinierten Maßnahmen ab (Kap. B. I. 1. c.) – muss jeweils zunächst geklärt werden, welche Normen im Einzelnen einschlägig sind. Dabei ist weniger die inhaltliche Festlegung problematisch als die Festlegung des einschlägigen Normenregimes innerhalb des grundrechtlichen Mehrebenensystems.

Das Anti-Geldwäscherecht wird vom Europarecht dominiert, aber nicht abschließend geregelt. Die Mitgliedstaaten können nach Art. 5 GWRL *zur Verhinderung von Geldwäsche und Terrorismusfinanzierung in den Grenzen des Unionsrechts strengere Vorschriften auf dem unter diese Richtlinie fallenden Gebiet erlassen oder beibehalten*. Folglich muss bei jeder Maßnahme bestimmt werden, ob nur die europäischen Grundrechte und entsprechend die Rechtsprechung des EuGH einschlägig sind oder auch die Grundrechte des Grundgesetzes bzw. die Rechtsprechung des BVerfG herangezogen werden können. In beiden Fällen wäre sodann zu beachten, inwiefern die einschlägige Rechtsprechung des EGMR sich auswirkt.

1. Anwendungsvorrang des Unionsrechts: Åkerberg Fransson & Recht auf Vergessen I

Wenn von einem solchen Verhältnis europäischer und nationaler Grundrechte die Rede ist, muss zunächst zwischen der Rechtsgeltung[1810] und der -anwendung unterschieden werden. Beansprucht nur ein Rechtsregime Geltung (deutsche Grundrechte *gelten* für Unionsrechtsakte nicht unmittel-

1810 Kurze Übersicht zum Geltungsbegriff bei *Auer,* RW 2017, 45 (49 ff.)

bar, da Art. 1 Abs. 3 GG nur die deutsche Staatsgewalt adressiert[1811]), stellt sich auch die Anwendungsfrage nicht.

Teilweise wird vertreten, dass in Kollisionsfällen nur das unionsrechtliche Grundrechtsregime *gelten* soll.[1812] Vom BVerfG[1813] und selbst vom EuGH wird aber kein solcher Geltungs-, sondern nur ein Anwendungsvorrang anerkannt.[1814] Dem ist zuzustimmen, denn für hoheitliche Akte deutscher Staatsorgane gelten die Grundrechte unabhängig davon, ob auch andere Rechtsregime Geltung beanspruchen, Art. 1 Abs. 3 GG.

Bei der folgenden Darstellung wird also nicht das Geltungsverhältnis von europäischen Grundrechten und jenen des Grundgesetzes besprochen, sondern nur die Anwendungsfrage, und zwar für den Fall, dass nationale Gesetze das Unionsrecht umsetzen. Es soll dargestellt werden, welche Grundrechte ein (nationales) Gericht bei der Prüfung geldwäscherechtlicher Normen heranziehen würde bzw. ob es überhaupt eine eigenständige Prüfung vornehmen würde. Dieses Anwendungsverhältnis wurde in den jüngsten Entscheidungen *Recht auf Vergessen* I und II vom BVerfG konsolidiert.

a. Europäische (Grund-)Rechte und nationales Recht

Die arbeitsgegenständlichen Überwachungsmaßnahmen mit Bezug auf Finanzdaten basieren nur zu einem geringen Teil auf unmittelbar anwendbarem Unionsrecht, namentlich der GeldtransferVO.[1815] Das Gros der Re-

1811 *Kunig/Kotzur*, von Münch/Kunig GG, Art. 1 Rn. 74; soweit das BVerfG europäische Rechtsakte i. R. d. Identitätskontrolle prüft, adressiert es nur die deutsche Staatsgewalt und verbietet die Mitwirkung an den „Ultra-Vires"-Akten, vgl. BVerfGE 154, 17 (84 ff.) – PSPP.

1812 Dafür etwa *Hwang*, EuR 2016, 355.

1813 BVerfGE 152, 216 (235) – Recht auf Vergessen II mwN; hM vgl. *Streinz* in Streinz EUV/AEUV, EUV Art. 4 Rn. 37.

1814 EuGH, Urt. v. 22. 10. 1998, C-10–97, C-22–97 (IN.CO.GE.'9 / Ministero delle Finanze), Rn. 21 = NJW 1999, 200.

1815 Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006, Abl. 2015, L 141/1.

gelungen findet sich im Geldwäschegesetz (GwG)[1816], das die EU-GeldwäscheRL[1817] umsetzt – also in einer nationalen Gesetzesnorm.

Das Anwendungsverhältnis von deutschen und europäischen (Grund-)Rechten[1818] bei der Prüfung nationaler Rechtsnormen ist von einer längeren Rechtsprechungshistorie geprägt[1819], auf deren umfangreiche Darstellung hier verzichtet werden kann. Ihre Kernaussage ist der bereits angesprochene Anwendungsvorrang europäischer Grundrechte bei der Prüfung nationalen Rechts im Geltungsbereich des Unionsrechts.

Grundsätzlich gilt die EU-GRC nur für nationale Rechtsakte, insb. Normen, wenn diese das Recht der EU *durchführen*, Art. 51 Abs. 1 EU-GRC. Diesen Geltungsbereich legt der EuGH mittlerweile allerdings sehr weit aus. Er lässt seit der Entscheidung *Åkerberg Fransson* im Grunde jeden Zusammenhang genügen und fordert einschränkend nur, dass dem jeweiligen nationalen und Unionsrecht der gleiche Regelungszweck zugrunde liegt.[1820] Insbesondere bei staatlichen Überwachungsmaßnahmen würden EU- und nationale Grundrechte danach stets nebeneinanderstehen[1821], da das Sekundärrecht der EU staatliche Datenverarbeitungen umfangreich regelt. Bei der Überprüfung von Überwachungsgesetzen müsste wegen des Vorrangs des Unionsrechts also regelmäßig die EU-GRC zur Anwendung kommen.

Auf diese *Expansion*[1822] der EU-Grundrechte musste das BVerfG reagieren. In der Entscheidung *Recht auf Vergessen I* stellte das BVerfG deshalb einen eigenen Ansatz vor, nachdem der Anwendungsvorrang der Unions-

1816 Geldwäschegesetz vom 23. Juni 2017 (BGBl. I S. 1822), zuletzt geändert durch Artikel 4 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2606).

1817 Zuletzt Richtlinie (EU) 2018/843 des Europäischen Parlaments und des Rates vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl. 2018, L 156/43.

1818 Siehe nur *Kingreen/Poscher,* Grundrechte, 37. Aufl. 2021, § 3 Rn. 79 ff.; vgl. auch die Tabelle bei *Honer*, JA 2021, 219 (224).

1819 Ausf. *Calliess* in Dürig/Herzog/Scholz GG, Art. 24 Rn. 76 ff.; Übersichtlich *Lehner*, JA 2022, 177 (178 ff.).

1820 EuGH Urt. v. 26.2.2013, C-617/10 (Åkerberg Fransson), Rn. 17 ff. =NVwZ 2013, 561; Urt. v. 10.7.2014, C-198/13 (Hernández), Rn. 41 = EuZW 2014, 795; dazu *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 51 Rn. 8 ff.; *Hancox*, Common Market Law Rev. 50 (2013), 1411.

1821 *Johannes/Weinhold,* Datenschutzrecht Polizei, 2018, § 1 Rn. 29; *Pfeffer*, NVwZ 2022, 294 (297); *M. W. Müller/Schwabenbauer*, NJW 2021, 2079 (2084); *Safferling/Rückert*, NJW 2021, 287 (288).

1822 *Lehner*, JA 2022, 177 (181).

grundrechte vom Grad der Harmonisierung des dem jeweiligen Fall zugrunde liegenden EU-Rechts abhängig sein soll.[1823] Mit dieser Antwort versuchte das Gericht, sein föderatives Grundrechtsverständnis zu festigen.[1824]

Liegt nur eine Teilharmonisierung vor, will das BVerfG primär die Grundrechte des GG zur Prüfung heranziehen, auch wenn der Prüfgegenstand nach der Rechtsprechung des EuGH grundsätzlich dem Art. 51 Abs. 1 EU-GRC unterfällt. Damit drängt das BVerfG den Anwendungsvorrang der EU-GRC zurück, will aber deren Geltungsanspruch unberührt lassen, da es vermutet, das Schutzniveau der EU-GRC durch die Anwendung der Grundrechte des Grundgesetzes abzudecken.[1825] So löst es den offenkundigen Widerspruch zur Linie des EuGH seit *Åkerberg Fransson* auf.[1826]

Ob eine Regelung unionsrechtlich vollständig determiniert ist, richtet sich nach dem BVerfG *nach einer Auslegung des jeweils anzuwendenden unionsrechtlichen Fachrechts.* „*Die Frage der Gestaltungsoffenheit ist dabei jeweils in Bezug auf die konkret auf den Fall anzuwendenden Vorschriften in ihrem Kontext zu beurteilen, nicht aber aufgrund einer allgemeinen Betrachtung des Regelungsbereichs.*“[1827]

Im informationellen Sicherheitsrecht stellt sich die Frage der Gestaltungsoffenheit etwa, wenn das Unionsrecht den Datenzugriff nur für bestimmte Behördengruppen vorschreibt und die Mitgliedstaaten noch für weitere Behörden einen Zugriff ermöglichen. Wollte der europäische Gesetzgeber einen solchen Zugriff ausschließen, also einen abschließenden Berechtigtenkreis festlegen, stünde die nationale Regelung der Richtlinie entgegen und wäre schon deshalb unzulässig.[1828]

Lässt eine unionsrechtliche Regelung ausdrücklich einen Anwendungsspielraum[1829] für den Gesetzgeber – etwa, indem nur Mindest- oder Maxi-

1823 BVerfGE 152, 152 (169 ff.) – Recht auf Vergessen I.

1824 *Masing* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 2 Rn. 144 ff.

1825 BVerfGE 152, 152 (169 ff.) – Recht auf Vergessen I; *Masing* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 2 Rn. 144 ff.

1826 *Hoffmann*, NVwZ 2020, 33 (35 f.).

1827 BVerfGE 152, 216 (246 f.) – Recht auf Vergessen II ; s.a., GA *Bobek*, Schlussanträge v. 25.7.2018, C-310/16 (Bulgarien/Dzivev) Rn. 70 ff.; *Wendel*, EuR 2022, 327 (346 ff.).

1828 Vgl. EuGH, Urt. v. 25.04.2002, C-52/00, Rn. 13 ff. (Kommission/Frankreich); *Schröder* in Streinz EUV/AEUV, AEUV Art. 114 Rn. 46 mwN.; *Habersack/Mayer* in Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, § 14 Rn. 17.

1829 EuGH Urt. v. 19.11.2019, C-609/17, C-610/17 (TSN & AKT), Rn. 51 ff. = NJW 2020, 35; dazu *Richard Král/ Petr Mádr*, Eur. Law Rev. 2021, 81 (84 ff.).

malvorgaben für eine Regelung gemacht werden oder deren Umsetzung gar nicht erst obligatorisch formuliert wird, handelt es sich um eine Teilharmonisierung.

Da der Unionsgesetzgeber jedenfalls bei Richtlinien nicht immer abschließend sämtliche mit einer Materie zusammenhängende Fragen regeln kann, sind nationale Regelungen, die von der Richtlinie nicht verlangt werden, fast immer denkbar. Das bedeutet aber nicht, dass jede Richtlinie als Teilharmonisierung verstanden werden muss. Allein der Wille des europäischen Gesetzgebers ist für diese Einteilung entscheidend.[1830]

Ob eine Richtlinienregelung abschließend sein soll, ergibt sich also im Zweifel durch Auslegung. Relevant sind besonders die Fälle, in denen der Richtlinientext abschließend gefasst ist, also nicht ausdrücklich darauf eingeht, dass die Mitgliedstaaten weitere Regeln treffen können und dürfen. Schafft der nationale Gesetzgeber in diesem Fall weitere Regelungen, die zwar das Ziel der entsprechenden Unionsnorm verfolgen, aber nicht von dieser vorgeschrieben wurden, handelt es sich um Fälle der *überschießenden* oder *übererfüllenden Regelung*.[1831]

Als solche Übererfüllung gilt, wenn ein Mitgliedstaat versucht, eine Richtliniennorm noch zweckmäßiger umzusetzen, als dies durch eine Eins-zu-Eins-Übernahme des Richtlinientexts möglich schien, und wird deshalb auch als „gold-plating" bezeichnet.[1832] Kommt eine Auslegung in diesen Fällen zu dem Ergebnis, dass die Richtlinie abschließend sein sollte, verstößt die nationale Norm gegen die Richtlinie und ist schon deshalb unanwendbar. Lässt sich indes argumentieren, dass die Richtlinie eine Übererfüllung zulässt, beurteilt sich die nationale Norm im Rahmen der Übererfüllung grundsätzlich nach nationalem Recht.

Mit der überschießenden Umsetzung wird eine Übertragung von Regelungen der Richtlinie auf andere Sachverhalte bezeichnet. Eine solche Übertragung verstößt grundsätzlich nicht gegen das Unionsrecht. Mangels Geltungsanspruch können sich aus einer Richtlinie keine Rechtsfolgen für

1830 EuGH, Urt. v. 25.04.2002, C-52/00, Rn. 13 ff. (Kommission/Frankreich); BVerfGE 152, 216 (230 ff.) – Recht auf Vergessen II;); *Schröder* in Streinz EUV/AEUV, AEUV Art. 114 Rn. 46 mwN.

1831 Vgl. *Brandner,* Richtlinien, 2003, S. 10 ff.; Abgrenzung von *überschießender* und *überfüllender* Umsetzung bei *Habersack/Mayer* in Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, § 14 Rn. 11; *Leidenmühler*, EuR 2019, 383; „echtes/unechtes gold-plating" bei *Payrhuber/Stelkens*, EuR 2019, 190 (195).

1832 Vgl. *Habersack/Mayer* in Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, § 14 Rn. 10 ff.; *Leidenmühler*, EuR 2019, 383.

solche Gebiete folgern lassen, die diese nicht betrifft. Das gilt erst recht, wenn die überschießende Anwendung einen rechtlichen Bereich betrifft, der nicht der Kompetenz der Union unterstellt ist. [1833] In diesen Fällen ist nach den oben aufgeführten Grundsätzen wiederum das nationale Verfassungsrecht ausschlaggebend.

Für die Anwendung des nationalen höherrangigen Rechts ist die Unterscheidung von Übererfüllung und überschießender Regelung also nicht relevant. Es kommt allein auf die konkrete Determination durch die Richtlinie an. Wird die nationalstaatliche Regelung nicht von der zugrunde liegenden Unionsvorschrift verlangt, ist sie in jedem Fall an den jeweiligen nationalen Grundrechten zu bemessen, denn solche Regeln unterfallen auch bei engem Sachzusammenhang nicht dem Art. 51 Abs. 1 EU-GRC.[1834]

b. Gerichtliche Prüfungskompetenz: *Recht auf Vergessen II*

Von der Frage der Anwendung ist die Frage zu trennen, welches Gericht die Prüfung der Vereinbarkeit einer nationalen Rechtsnorm mit Unionsgrundrechten vornimmt.

Herrscht nach den beschriebenen Grundsätzen aufs *Recht auf Vergessen I* kein Anwendungsvorrang des Unionsrechts, sondern eine primäre Anwendung der Grundrechte des Grundgesetzes, besteht selbstredend eine Prüfungskompetenz des BVerfG.

Existiert hingegen ein Anwendungsvorrang, wollte das BVerfG ursprünglich keine eigenständige Prüfung (anhand der Unionsgrundrechte) vornehmen, sondern die fraglichen Rechtsakte stets dem EuGH vorlegen, soweit sich dieser im Rahmen seiner Kompetenz bewegt und die Verfassungsidentität der Bundesrepublik unberührt lässt.[1835]

In *Recht auf Vergessen II* ist das BVerfG von dieser Rechtsprechung aber abgekehrt und hat entschieden, dass es fortan selbstständig die Umsetzung vollharmonisierter Regelungen auf deren Vereinbarkeit mit den

1833 *Nettesheim* in Grabitz/Hilf/Nettesheim Recht der EU, AEUV Art. 288 Rn. 131; Vorlagefragen zum EuGH sind jedoch möglich, wenngleich diese keine Bindung beanspruchen, vgl. EuGH, Urt. v. 18.10.1990, C-297/88, C-197/89 (Dzodzi/Belgien).

1834 Vgl. EuGH Urt. v. 19.11.2019, C-609/17, C-610/17 (TSN & AKT), Rn. 51 ff. = NJW 2020, 35; dazu *Richard Král/ Petr Mádr*, Eur. Law Rev. 2021, 81 (84 ff.); *Wendel*, EuR 2022, 327 (353 ff.).

1835 Zur Identitäts- / *Ultra-vires* Kontrolle: BVerfGE 126, 286 (302 ff.) – Honeywell; E 154, 17 (84 ff.) – PSPP; *Calliess* in Dürig/Herzog/Scholz GG, Art. 24 Rn. 136 ff.

Unionsgrundrechten hin überprüft.[1836] Eine Vorlage zum EuGH ist danach nur noch notwendig, wenn die Auslegung der betroffenen Grundrechte vom Gerichtshof noch nicht geklärt wurde und die anzuwendenden Auslegungsgrundsätze *aus sich heraus nicht offenkundig sind*.[1837]

Auch diese Rechtsprechung kann als Reaktion auf die Expansion der Unionsgrundrechte verstanden werden. Die bisherige Rechtsprechung des BVerfG, die zwar einen Anwendungsvorrang des Unionsrechts anerkennt, aber keine Anwendung dessen vorsieht, hätte konsequent zu einem Rückzug des BVerfG führen müssen, wenn der Geltungsbereich der Unionsgrundrechte immer umfangreicher wird. Daher ist es zu begrüßen, dass das BVerfG sich nicht nur die Anwendung der Grundrechte des Grundgesetzes bei nicht vollständig determiniertem Unionsrecht vorbehält, sondern darüber hinaus bei endgültiger Auslegung der Unionsgrundrechte diese eigenständig anwendet.

c. Anwendung auf das Geldwäscherecht, Beachtung des Art. 5 GWRL

Bei den einzelnen Datenverarbeitungsschritten im Rahmen des geldwäscherechtlichen Überwachungssystems muss ausgehend von diesen Grundsätzen also zunächst im Einzelnen geprüft werden, ob durch die GWRL im Einzelnen eine vollständige Determinierung vorgenommen wurde. Wo dies der Fall ist, muss nur die Primärrechtskonformität der GWRL festgestellt werden. Die Bestimmungen des GwG können sich dann unmittelbar an der Richtlinie messen lassen.

Insofern besteht beim Geldwäscherecht eine Besonderheit in Form des Art. 5 GWRL. Danach können die Mitgliedstaaten *zur Verhinderung von Geldwäsche und Terrorismusfinanzierung* (nur) *in den Grenzen des Unionsrechts strengere Vorschriften auf dem unter diese Richtlinie fallenden Gebiet erlassen oder beibehalten*.

Abweichungen im nationalen Recht stellen demnach grundsätzlich einen Verstoß gegen die Richtlinie dar, es sei denn, die Abweichung fällt unter diese Öffnungsklausel des Art. 5 GWRL.

1836 BVerfGE 152, 216 (236 ff.) – Recht auf Vergessen II; dazu *Britz*, NJW 2021, 1489; *Hoffmann*, NVwZ 2020, 33; übersichtlich zur Kritik *Schmahl* in Stern/Sodan/Möstl (Hrsg.), Staatsrecht, Bd. III, 2. Aufl. 2022, § 99 Rn. 33 f.

1837 BVerfGE 152, 216 (244) – Recht auf Vergessen II.

Die GWRL erlaubt also die *übererfüllende* Umsetzung bzw. das „gold-plating"[1838] nur eingeschränkt. Die Untererfüllung ist hingegen grundsätzlich ausgeschlossen. Daraus folgt, dass zwar nicht per se eine Vollharmonisierung vorliegt, faktisch aber stets die Unionsgrundrechte zu prüfen sind, da Abweichungen im nationalen Recht nach Art. 5 GWRL nur dann zulässig sind, wenn diese Änderungen nicht gegen Unionsrecht verstoßen.

Daher müssen sämtliche Abweichungen zulasten der Betroffenen auf ihre Vereinbarkeit mit der EU-GRC geprüft werden, da andernfalls ein Verstoß gegen die GWRL vorliegt. Art. 5 GWRL führt insofern zu einer mittelbaren Anwendung der EU-GRC auf übererfüllende Regelungen in den mitgliedstaatlichen Geldwäschegesetzen. Die eigentlich auf Abweichungen primär anzuwendenden nationalen Grundrechte rücken dadurch in den Hintergrund.

Für Informationseingriffe der GWRL bzw. des GwG ergibt sich somit folgendes Prüfungsschema:

Maßnahmen, die identisch umgesetzt wurden, sind nur anhand der EU-GRC zu überprüfen. Die Richtlinie und die nationale Umsetzung können in diesem Fall sinnvollerweise gemeinsam geprüft werden, da sie beide der EU-GRC unterfallen.

Maßnahmen des GwG, die nicht unmittelbar von der Richtlinie vorausgesetzt werden, müssen zunächst daraufhin überprüft werden, ob sie eine Abweichung i. S. d. Art. 5 GWRL darstellen. Eine solche Abweichung ist dann anzunehmen, wenn die GWRL einen Umstand grundsätzlich regelt – etwa durch Mindeststandards –, aber keine abschließende Vorgabe macht. In diesem Fall muss sich die nationale Umsetzung wegen Art. 5 GWRL an der EU-GRC messen lassen. Nur bei nationalen Regelungen, für die die GWRL den Nationalstaaten einen umfangreichen Spielraum einräumt, wo also mangels Regelung gar keine *Abweichung* i. S. d. Art. 5 GWRK vorliegen kann, kommen allein die nationalen Grundrechte zur Anwendung.

2. Bewertung der einzelnen Anti-Geldwäschemaßnahmen

Die einzelnen Maßnahmen des Anti-Geldwäscherechts, die als funktional einheitliches Überwachungsregime gesehen werden können, sollen nach

1838 Vgl. *Habersack/Mayer* in Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, § 14 Rn. 10 ff.; *Leidenmühler*, EuR 2019, 383.

diesem Maßstab aus dem Blickwinkel der deutschen und europäischen Sicherheitsverfassung[1839] betrachtet werden.

a. Transaktionsmonitoring nach §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG, Art. 13 Abs. 1 lit. d) der GWRL

Dabei ist zunächst das Transaktionsmonitoring zu betrachten. Die Notwendigkeit des Monitorings mitsamt der Option eines manuellen *Screenings* in Echtzeit, d. h. vor Abschluss der Transaktion, legt nahe, dass das automatisierte Monitoring eine Datenerhebung logisch miteinschließt. Das Monitoring kann deshalb chronologisch als erste Maßnahme im Überwachungskontext verstanden werden, wenngleich die Speicherung der Daten naturgemäß zuerst anfallen wird.

Ähnlich wie bei der Fluggastdatenspeicherung lässt sich das geldwäscherechtliche Überwachungssystem demnach gedanklich so illustrieren, dass die Transaktionsdaten erhoben und analysiert und sodann für eine später eventuell eintretende Notwendigkeit bevorratet werden.

aa. Maßstab: Prüfung anhand des Unionsrechts

Das automatisierte Transaktionsmonitoring findet seine Rechtslage in den (im Zusammenhang zu lesenden[1840]) §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG. Danach müssen die nach dem GwG Verpflichteten ihre Geschäftsbeziehungen bzw. die innerhalb dieser durchgeführten Transaktionen *kontinuierlich überwachen*, § 10 Abs. 1 Nr. 5 GwG, wobei die Kreditinstitute nach § 25h Abs. 2 KWG verpflichtet sind, *Datenverarbeitungssysteme zu*

1839 Zum Begriff vgl. *Tanneberger,* Sicherheitsverfassung, 2014; *Dietrich/Gärditz* (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, 2019; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245; *Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 192; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 1 ff.

1840 Vgl. BT-Drs. 17/9038, S. 49 f.; BT-Drs. 18/11555, S. 176; *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86d; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 343; *Achtelik* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 25h Rn. 18; *Vollmuth,* Geldwäscheprävention, 2020, 168 f; 171 ff.; *Ackermann/Reder*, WM 2009, 158 (164); *Buggel* in Bakaus/Kruse/Schwerdtner (Hrsg.), Die "Zentrale Stelle", 2019, S. 455 (456).

betreiben und zu aktualisieren, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr zu erkennen, die (…) im Verhältnis zu vergleichbaren Fällen besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck erfolgen.

Bei den §§ 10 Abs. 1 Nr. 5 GwG und 25h Abs. 2 KWG handelt es sich um unionsrechtlich vollständig determiniertes Recht. Eine Überprüfung der Vorschriften muss daher anhand der EU-GRC erfolgen und gilt demnach unmittelbar auch für das zugrunde liegende Unionsrecht, Art. 13 Abs. 1 lit. d) GWRL. Dies ergibt sich aus folgenden Überlegungen:

Die Pflicht zur *kontinuierlichen Überwachung* i. S. d. § 10 Abs. 1 Nr. 5 GwG setzt Art. 13 Abs. 1 lit. d) der GWRL um. Dort heißt es: „*Die Sorgfaltspflichten gegenüber Kunden umfassen die: (…) d) kontinuierliche Überwachung der Geschäftsbeziehung, einschließlich einer Überprüfung der im Verlauf der Geschäftsbeziehung ausgeführten Transaktionen, um sicherzustellen, dass diese mit den Kenntnissen der Verpflichteten über den Kunden, seine Geschäftstätigkeit und sein Risikoprofil, einschließlich erforderlichenfalls der Herkunft der Mittel, übereinstimmen, und Gewährleistung, dass die betreffenden Dokumente, Daten oder Informationen auf aktuellem Stand gehalten werden.*“

Für die Einführung des § 10 Abs. 1 Nr. 5 GwG ist insofern kein Umsetzungsspielraum erkennbar. Bei Art. 13 Abs. 1 lit. d) der GWRL handelt es sich um eine vollständig determinierende Rechtsnorm. Für die Überwachungspflicht an sich können deutsche Grundrechte daher nicht zur Anwendung kommen.

Von einer Notwendigkeit automatisierter Datenverarbeitungssysteme, wie § 25h Abs. 2 KWG sie vorsieht, ist in Art. 13 Abs. 1 lit. d) der GWRL hingegen keine Rede.

Ob es sich auch bei der Regelung von § 25h Abs. 2 KWG um unionsrechtlich determiniertes Recht handelt, ist aber nicht allein vom Wortlaut der GWRL abhängig, sondern vom Willen des europäischen Gesetzgebers, der eine effektive Umsetzung erwartet.[1841] Um den gesetzgeberischen Willen zu ermitteln, können insofern die Leitlinien der Europäischen Banken-

1841 Zum „effet utile“ vgl. nur EuGH, Urt. v. 15. 9. 2011, C-53/10, Rn. 22 ff. – Mücksch = EuZW 2011 (873); *Streinz* in Streinz EUV/AEUV, EUV Art. 4 Rn. 33; *Potacs*, EuR 2009, 465; *Seyr,* effet utile, 2010, S. 94 ff., jeweils mwN aus der Rechtsprechung des EuGH.

aufsicht[1842] herangezogen werden. Zum Erlass dieser Leitlinien berechtigen bzw. verpflichten die Art. 17, 18 Abs. 4 GWRL. Danach sollen in den Leitlinien zwar nur die vereinfachten und verstärkten Sorgfaltspflichten näher umschrieben werden, doch enthalten diese auch Bestimmungen zu den allgemeinen Sorgfaltspflichten.

Zur kontinuierlichen Überwachungspflicht i. S. d. Art. 13 Abs.1 lit. d) GWRL verhalten sich näher die lfd. Nr. 4.72 ff.[1843]

Nach lfd. Nr. 4.72 *sollten Unternehmen dafür Sorge tragen, dass ihr Ansatz für die Transaktionsüberwachung wirksam und angemessen ist.* Weiter heißt es in lfd. Nr. 4.74: *Was angemessen ist, hängt von der Art, Umfang und Komplexität der Geschäftstätigkeit des Unternehmens sowie vom Risiko ab, (…) b) ob sie Transaktionen manuell überwachen oder ein automatisiertes System für die Transaktionsüberwachung einsetzen. Unternehmen, die ein hohes Transaktionsvolumen verarbeiten, sollten in Erwägung ziehen, ein automatisiertes System für die Transaktionsüberwachung einzurichten.*

Automatisierte Systeme sind nach der europäischen Rechtslage, also jedenfalls nach Ansicht der EBA, die in Art. 17, 18 Abs. 4 GWRL zum Erlass von (nicht verbindlichen[1844]) Leitlinien ermächtigt wurde, nicht zwingend vorgesehen. Sie stellen vielmehr eine faktische Notwendigkeit dar, denn in jedem Fall sieht die GWRL vor, dass im Rahmen der kontinuierlichen Überwachung jede Transaktion von den Verpflichteten berücksichtigt wird, da sich Auffälligkeiten gerade erst aus der Gesamtheit der Transaktionen ergeben. Bei großen Kreditinstituten ist in Zeiten von Online-Banking[1845] eine kontinuierliche Überwachung ohne automatisierte Systeme schlicht nicht mehr vorstellbar.

Insofern muss argumentiert werden, dass eine effektive Umsetzung der geldwäscherechtlichen Sorgfaltspflichten, jedenfalls für größere Kreditinstitute mit Privatkundengeschäft, ohne automatisierte Systeme gar nicht möglich wäre. Ein Wahlrecht zur Einführung dieser Systeme, so wie es in lfd. Nr. 4.74 lit. b) der EBA-Leitlinien anklingt, dürfte real also nicht existieren.

Auch der deutsche Gesetzgeber scheint von einer unionsrechtlichen Notwendigkeit des § 25h Abs. 2 KWG ausgegangen zu sein. Zur Umsetzung der

1842 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung).

1843 Idem, S. 48 ff.

1844 Vgl. EuGH, Urt. v. 15.07.2021, C-911/19 (Conseil d'État), Rn. 45 = BKR 2021, 650.

1845 zur praktischen Bedeutung *Deutsche Bundesbank,* Zahlungsverhalten in Deutschland, 2017, S. 8 ff.; *Borges* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 11 Rn. 6.

4. GWRL wurde die Vorschrift in Bezug auf die geldwäscherechtlichen Auffälligkeiten angepasst. Zuvor sollten die Datenverarbeitungssysteme gem. § 25a Abs. 1 Nr. 4 KWG 2002 solche Transaktionen erkennen, die *zweifelhaft oder ungewöhnlich* waren.[1846] Da die Überwachungspflicht nach Art. 13 Abs.1 lit. d) GWRL dem Auffinden solcher Transaktionen dient, bei denen verschärfte Sorgfaltspflichten durchgeführt werden müssen, übernahm der deutsche Gesetzgeber die unionsrechtliche Definition (*„im Verhältnis zu vergleichbaren Fällen besonders komplex oder groß sind, ungewöhnlich ablaufen oder ohne offensichtlichen wirtschaftlichen oder rechtmäßigen Zweck")* in § 25h Abs. 2 KWG.[1847]

Offensichtlich dient also auch § 25 h Abs. 2 KWG einer unter Effektivitätsaspekten notwendigen Umsetzung der Pflicht aus Art. 13 Abs.1 lit. d) GWRL. Die Vorschrift muss deshalb als Durchführung einer vollharmonisierten Regelung betrachtet werden, ohne dass dem Gesetzgeber ein erkennbarer Spielraum (bzgl. Kreditinstituten) eröffnet wäre. § 25h Abs. 2 KWG ist danach ebenfalls nicht an den deutschen Grundrechten zu messen.

Vielmehr sind §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG, als faktische Eins-zu-Eins-Umsetzung des Art. 13 Abs.1 lit. d) GWRL zu werten. §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG und Art. 13 Abs.1 lit. d) GWRL stehen und fallen daher zusammen im Rahmen einer Prüfung anhand der Unionsgrundrechte.

bb. Art. 7, 8 EU-GRC und DSGVO

Das Transaktionsmonitoring stellt aufgrund der staatlichen Anordnung einen Grundrechtseingriff in die Privatheitsrechte der Betroffenen aus Art. 7, 8 EU-GRC dar.

Da in den Kontoinhaltsdaten Informationen preisgegeben werden, die das Privatleben betreffen, können Art. 7, 8 EU-GRC als Verbund geprüft werden.[1848] Zwar geht die jüngere Rechtsprechung des EuGH dahin, zwi-

1846 Zur Änderungsgeschichte *Achtelik* in Herzog GWG, 1. Aufl. 2010, § 25c KWG Rn. 15; *ders.* in Herzog GwG, 3. Aufl. 2018, KWG § 25h Rn. 1 f.

1847 BT-Drs. 18/11555, S. 176

1848 So noch EuGH, Urteil v. 17.10.2013, C-291/12 (Schwarz/Bochum), Rn. 24 ff. = NVwZ 2014, 435; Urteil v. 09.11. 2010, C 92/09, C 93/09 (Schecke u Eifert/Hessen), Rn. 52; Urteil v. 09.01.2008, C–275/06 (Promusicae/Telefónica), Rn. 64; *González Fuster,* Data Protection, 2013, S. 234 ff.; dazu *Nettesheim* in Grabenwar-

schen den einzelnen Gewährleistungen jedenfalls auf Schutzbereichsebene zu trennen[1849], d. h. eine *parallele*[1850] Prüfung vorzunehmen, im Rahmen der Eingriffsbewertung bzw. der Rechtfertigung spielt diese Trennung aber keine weitere Rolle (s. o. Kap. C. I. 1.).

Dass die Maßnahmen unmittelbar von Privaten ausgeführt werden, ist dabei irrelevant. Von Privaten im Auftrag des Staates durchgeführte Verarbeitungen privater Daten i. R. d. Sicherheitsgewährleistung sind bei verpflichtender Anordnung dem Staat als eigene Grundrechtseingriffe zuzurechnen.[1851]

Neben der Grundrechtsebene wäre grundsätzlich das europäische Sekundärrecht zu beachten. Nach Art. 41 Abs. 1 GWRL gilt für die Verarbeitung personenbezogener Daten i. R. d. Richtlinie die DSGVO. Die Verarbeitung personenbezogener Daten zu Zwecken der Verhinderung von Geldwäsche und Terrorismusfinanzierung ist insofern als Angelegenheit von öffentlichem Interesse i. S. d. Art. 6 Abs. 1 lit. e) DSGVO anzusehen, Art. 43 GWRL.

Diese gesetzliche Anordnung entspricht der Rechtsprechung des EuGH, die private Datenverarbeitungen streng dem Regime der DSGVO zuordnet, auch wenn die Verarbeitung unmittelbar der Sicherheitsgewährleistung dient – etwa in Form einer Übermittlung von Daten an Sicherheitsbehörden.[1852] Umstritten ist dabei nur noch, ob auch die Handlungen der FIU

---

ter/Breuer/Bungenberg ua. (Hrsg.), Europ. Grundrechtsschutz, 2. Auflage 2022, § 10 Rn. 52; *J.-P. Schneider* in BeckOK Datenschutzrecht, Syst. B Rn. 23, 31 f.; *Streinz* in Streinz EUV/AEUV, EU-GRC Art. 8 Rn. 7; *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 2; zu den Vorteilen dieser Rspr. *Marsch,* Datenschutzgrundrecht, 2018, S. 217 ff.; ähnlich *W. Michl*, DuD 2017, 349 (353).

1849 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 96 ff. = EuZW 2022, 706.

1850 *Kühling*, NVwZ 2014, 681 (682); *Jarass* in Jarass EU-GRC, Art. 8 Rn. 4; *Johlen* in Stern/Sachs EU-GRC, Art. 28 Rn. 24, Fn 51.

1851 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 ff. = NJW 2014, 2169; ebenso BVerfGE 125, 260 (321) – Vorratsdatenspeicherung; dazu *Durner* in Dürig/Herzog/Scholz GG, Art. 2 Rn. 154 ff. mwN.; für das Transaktionsmonitoring: *Herzog*, WM 1996, 1753 (1762).

1852 S.a. EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 102 = NJW 2021, 531; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 63 ff. = EuZW 2022, 706.

aufgrund der Anweisung in Art. 41 Abs. 1 GWRL der DSGVO unterstellt sind.[1853]

Die Geltung der DSGVO wirkt sich auf die Ausübung des Transaktionsmonitorings nicht aus. Da aus der DSVGO lediglich ein gesetzlicher Vorbehalt folgt, vgl. Art. 6 Abs. 1 lit. c), e) DSGVO, ergibt sich aus ihr grundsätzlich keine Grenze für die Verpflichtung Privater zu Datenverarbeitungen i. R. d. Sicherheitsrechts (s. o. Kap C. I. 3. a.). Vielmehr komplimentiert sie diese nur, indem sie allgemein geltende Verfahrensvorschriften implementiert. Von diesen kann allerdings wiederum per Gesetz abgewichen werden, etwa durch Art. 41 Abs. 4 lit. a), b) GWRL bzw. § 11a Abs. 2 GwG, nach denen die Informationspflicht i. S. d. Art. 13 Abs. 3 DSGVO und der Auskunftsanspruch nach Art. 15 DSGVO bei Übermittlungen der Verpflichteten auf Grundlage des Anti-Geldwäscherechts nicht bestehen.

Die Rechtmäßigkeit des Transaktionsmonitorings an sich ist also von der DSGVO unabhängig und richtet sich allein nach dem Primärrecht. Bei der Bewertung sind allerdings die geltenden Vorschriften der DSGVO zu berücksichtigen, die im Rahmen der Geldwäschebekämpfung Anwendung finden.

cc. Bewertung anhand der Rechtsprechung des EuGH

Ob die Verpflichtung zur kontinuierlichen Überwachung von Finanztransaktionen zum Zwecke der Filterung von geldwäscherechtlichen Auffälligkeiten, die sinnvoll bzw. effektiv nur durch automatisierte Datenverarbeitungssysteme ausgeführt werden kann, einen nicht zu rechtfertigenden Grundrechtseingriff darstellt, lässt sich nur mit Blick auf die bestehende Rechtsprechung zu den europäischen Grundrechten klären. Es soll daher an dieser Stelle untersucht werden, welche Feststellungen der Rechtsprechung des EuGH auf das Transaktionsmonitoring angewandt werden können.

1853 *Quintel*, ERA Forum 2022, 53 (61 ff.); *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (11 ff.).

(1) Das PNR-Urteil als aktueller Maßstab automatisierter Datenanalysen

Insofern wurde bereits festgestellt, dass es sich beim Monitoring um eine strategische Datenanalyse handelt, die durch einen anlasslosen Universalvergleich sämtlicher Transaktionen charakterisiert wird.

Solche Rasterungen großer Datenmengen kennt man von der strategischen Fernmeldeaufklärung, zu der auf europäischer Ebene allerdings nur Urteile des EGMR[1854] vorliegen[1855], von der Analyse von TK-Verkehrsdaten[1856] und der Fluggastdatenüberwachung.

Bei der strategischen Fernmeldekontrolle und der Kennzeichenüberwachung kommen die Informationen, auf denen die Rasterung aufbaut, allerdings stets von außen. Es handelt sich um vorgefertigte Listen mit formalen und inhaltlichen Suchbegriffen und anderen Umständen, den sogenannten *Selektoren*.[1857]

Zwar werden auch beim Transaktionsmonitoring bestimmte Umstände vorgefiltert, etwa Transaktionen in Staaten auf der *black list*[1858] oder der Inhalt des Verwendungszwecks, der auf Suchbegriffe gefiltert werden kann. Ein wichtiges Augenmerk liegt aber auf der Erkennung *interner* Abweichungen. Die Auffälligkeit einer konkreten Transaktion ergibt sich daraus, dass das entsprechende Verhalten nicht zum jeweiligen Kunden bzw. dessen vorliegender Transaktionshistorie passt und diese Abweichung nicht unmittelbar aus der Transaktion heraus erklärt werden kann.

Solche Abweichungen von der Regelmäßigkeit innerhalb des überwachten Datensatzes sind nicht Gegenstand der strategischen Fernmeldekontrolle oder gar der Kennzeichenüberwachung. Dort kann ein „Treffer"

1854 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich) = NVwZ-Beil. 2021, 11; Urt. v. 25.5.2021, Nr. 35252/08 (Centrum för Rättvisa / Schweden) = NVwZ-Beil. 2021, 30.

1855 Auch in EuGH, Urteil v. 6.10.2020, C-623/17 (Privacy International) = GSZ 2021, 36 wurden nur *Metadaten* besprochen.

1856 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 ff. = NJW 2021, 531.

1857 Bspe. zur strategischen Fernmeldeaufklärung bei *B. Huber*, NJW 2013, 2572 (2573); umfassend zu den formalen Selektoren aus der Zusammenarbeit BND-NSA *Graulich*, (1. UA des 18. Deutschen Bundestags), Fernmeldeaufklärung mit Selektoren, MAT A SV-11/2, zu A-Drs. 404, 23.10.2015, S. 23 ff., 98 ff.

1858 Delegierte Verordnung (EU) 2016/1675 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates durch Ermittlung von Drittländern mit hohem Risiko, die strategische Mängel aufweisen, ABl. 2016, L 254/1; konsolidierte Fassung vom 07.02.2021: Document 02016R1675-20210207.

immer nur durch Anwendung eines Abgleichdatensatzes erzielt werden. Das Transaktionsmonitoring geht in dieser Hinsicht also über diese Maßnahmen hinaus, da es sowohl einen Abgleich mit Suchbegriffen vornimmt als auch reine Unregelmäßigkeiten untersucht.

Eine ähnliche Regelung findet sich nur im Rahmen der Fluggastüberwachung. Nach Art. 6 Abs. 2 lit. a) i. V. m. Abs. 3 lit. a), b) PNR-RL können die PNR-Daten von Passagieren vor deren Ankunft nicht nur mit polizeilichen (Fahndungs-)Datenbanken (Abs. 3 lit. a.)), sondern auch mit *im Voraus festgelegten Kriterien abgeglichen werden* (lit b.)). Außerdem werden nach Art. 6 Abs. 2 lit. c) PNR-RL die PNR-Daten von der Zentralstelle auch analysiert, zur *„Aktualisierung der Kriterien oder Aufstellung neuer Kriterien zur Verwendung in gemäß Absatz 3 Buchstabe b durchgeführten Überprüfungen, die der Ermittlung von Personen gelten, die möglicherweise an einer terroristischen Straftat oder an schwerer Kriminalität beteiligt sind".*

Die Fluggastdaten werden also ebenfalls auf Muster untersucht, die sich allein aus den gegenständlichen Daten – etwa den Flugrouten – ergeben, wobei diese Muster wiederum auf zuvor analysierten Massen von PNR-Daten aufbauen.

Die Funktionsweise entspricht insofern dem Geldwäschesystem, als dass sich aus der Kategorie der Flugdaten selbst ergibt, welche (in Zukunft anfallenden) Flugdaten einen Verdacht begründen könnten. Aufgrund dieser Entsprechung kann das PNR-Urteil des EuGH als erster Ansatzpunkt zur Bewertung des Transaktionsmonitorings herangezogen werden.[1859]

Die Aussagen des EuGH zur Analyse von TK-Verkehrs- und Standortdaten[1860] gelten ebenfalls, sind jedoch älter und weniger detailliert als die Feststellungen im PNR-Urteil. Sie gehen in diesem auf.

(2) Intensität des Transaktionsmonitorings

Zunächst ist für diese Bewertung die Intensität des Transaktionsmonitorings zu bestimmen. Wie auch das BVerfG prüft der EuGH die Verhältnismäßigkeit von Eingriffen in Art. 7,8 EU-GRC mittels einer Art Je-des-

1859 Vgl. auch *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (281 f.).

1860 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 172 ff. = NJW 2021, 531.

to-Formel[1861], bei der erst die Eingriffsintensität anhand bestimmter Merkmale festgestellt wird und sodann geprüft wird, ob die einschränkenden Vorschriften (Anlass, Formvorschriften etc.) dieser Intensität entsprechen. Überwachung wird nicht verboten, sondern prozeduralisiert.[1862] Die Aufgabe des Gesetzgebers besteht also darin, die Überwachungsmaßnahme so effektiv auszugestalten, dass Maßnahme und Zweck stets angemessen verlinkt sind.[1863]

Die Anforderungen des EuGH sind dabei weniger nuanciert als jene des BVerfG. Eine schematische Ordnung hat der Gerichtshof nur insofern herausgestellt, als dass die Schwere des Anlasses der Intensität entsprechen muss. Besonders intensive Eingriffe sind danach nur zur Bekämpfung schwerer Kriminalität zulässig.[1864]

Die Intensität bestimmt sich danach, welche Aussagen sich mit den Daten über eine Person treffen lassen,[1865] und der Streubreite der Maßnahme, also das Ausmaß der Betroffenen.[1866] Die Heimlichkeit betont der EuGH in seinen Urteilen nicht ausdrücklich. Sie spielt bei Massenanalysen aber auch nur eine untergeordnete Rolle, da sich schon aus dem Gesetz ergibt, dass die Analysen universell stattfinden. Die Heimlichkeit spielt deshalb

1861 Dazu nur BVerfGE 141, 220 (269) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 395 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 220 ff.; *Starck* in v. Mangoldt/Klein/Starck GG, Art. 2 Rn. 116;

1862 *Tzanou/Karyda*, European Public Law 28 (2022), 123 (153 f.); s.a. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (104 ff.).

1863 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 80 = NJW 2021, 531; dazu *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (148); zum Effektivitätsaspekt bei der Verhältnismäßigkeit von Überwachungsmaßnahmen *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 242 ff.; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 82 f., 14 ff.; *Stern,* StaatsR Bd. III/2, 1994, S. 836; aus der Rspr etwa BVerfGE 115, 166 (197 f.); insb. aber BVerfGE 141, 220 (268 ff.) – BKA-Gesetz.

1864 Vgl. EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 54 ff. = NJW 2019, 655.

1865 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 100 = EuZW 2022, 706; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 = NJW 2017, 717; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 77 = NJW 2022, 3135; s. dazu *Brkan*, German Law Journal 20 (2019), 864 (872 f.)

1866 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), 98 f. = EuZW 2022, 706; Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 56 = NJW 2014, 2169; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 83 = NJW 2022, 3135.

sinnlogisch nur bei den (individuell ausgerichteten) Folgemaßnahmen eine Rolle.

Nach diesen Grundsätzen handelt es sich beim automatisierten Transaktionsmonitoring um einen schweren Grundrechtseingriff.[1867] Beim Monitoring alltäglicher Bank- und Kreditkartengeschäfte werden Daten von der gesamten Bevölkerung verarbeitet, da fast jeder Bürger am (digitalen) Zahlungsverkehr der Kreditwirtschaft teilnimmt.

Dabei ergeben sich aus den einzelnen Transaktionsdaten tiefe Einblicke in die Persönlichkeit und den Alltag der Betroffenen,[1868] denn die analysierten Transaktionsbelege müssen ausreichend sein, um die geldwäscherechtlichen Pflichten zu erfüllen.[1869] Sie enthalten dazu mindestens den Kundennamen, die Kontonummer, Empfangs- und Versendungsinstitut, Empfangs- und Versendungsland, das Transaktionsdatum, den Betrag und die Währung sowie den Verwendungszweck.[1870] Aufgrund der weitverbreiteten Möglichkeit bargeldloser Zahlungen können mit Transaktionsbelegen, aus denen sich anhand des Empfängernamens oft auch der Ort der Zahlung ableiten lässt, nicht nur Persönlichkeits- sondern auch Bewegungsprofile erstellt werden. Regelmäßige Lastschriftverfahren und Überweisungen können ferner den Familienstand oder die Gewerkschaftszugehörigkeit, die unter Art. 9 Abs. 1 DSGVO fällt, offenlegen.

Dass aus dem Monitoring allein unmittelbar keine Nachteile für die Betroffenen folgen, ist aus Sicht des EuGH irrelevant.[1871] Wie auch die universelle Speicherung, die allein der Bevorratung dient und somit die jeweiligen Daten mit einem allgemeinen Nützlichkeitsverdikt für Sicherheitsinteressen belegt, stellt der dauernde automatisierte Abgleich der Daten eine Persönlichkeitsbeeinträchtigung dar.

1867 Vgl. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 102 ff., 111 = EuZW 2022, 706.

1868 BVerfGE 120, 274 (347 f.) – Online-Durchsuchung; *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

1869 Vgl. *DK,* Auslegungs- & Anwendungshinweise Geldwäsche, Februar 2014, lfd. Nr. 86 lit. d) S. 71.

1870 *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 53; *Fiedler/Krumma/Zanconato ua.,* Geldwäscherisiko Glücksspiel, 2017, S. 38.

1871 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 96 = EuZW 2022, 706.

Auch das BVerfG verlangt keinen *Treffer*, sondern erkennt in der Erstverarbeitung einen Eingriff. Es sei denn, dieser dient allein einer Vorsortierung, weil sich das behördliche Interesse noch nicht *verdichtet* hat.[1872]

(3) Wahrung der Verhältnismäßigkeit durch effektive Ausgestaltung?

Es ist also nur fraglich, ob das Transaktionsmonitoring angesichts der Eingriffsschwere gerechtfertigt werden kann. Da ein Eingriff sowohl in Art. 7 als auch 8 EU-GRC vorliegt, muss die Rechtfertigung sowohl Art. 8 Abs. 2 EU-GRC, der allerdings nur einen qualifizierten Gesetzesvorbehalt vorsieht[1873], als auch Art. 52 Abs. 1 EU-GRC entsprechen.

(a) Angemessenheit als primäre Prüffrage

Nach Art. 52 Abs. 1 S. 1 EU-GRC darf zunächst der Wesensgehalt der Grundrechte nicht beeinträchtigt werden. Dies wäre indes nur bei einer umfangreichen und unmittelbar durch den Staat vorgenommenen Totalüberwachung ohne Zweckbegrenzung der Fall[1874] und wurde bislang bei einzelnen Massenüberwachungsphänomenen nie angenommen. Aufgrund der Zweckbegrenzung in Art. 41 Abs. 2 GWRL, *nach dem personenbezogene Daten von Verpflichteten auf der Grundlage dieser Richtlinie ausschließlich für die Zwecke der Verhinderung von Geldwäsche und Terrorismusfinanzierung verarbeitet werden dürfen,* ist unwahrscheinlich, dass der EuGH im Transaktionsmonitoring eine Verletzung des Wesensgehalts von Art. 7, 8 EU-GRC in Erwägung ziehen würde. Von größerer Relevanz ist der nach Art. 52 Abs. 1 S. 2 EU-GRC geltende Verhältnismäßigkeitsgrundsatz, aus dem die Verfassungsgerichte ganz primär die Grenzen sicherheitsrechtlicher Überwachungstätigkeit abgeleitet haben.

Auf Ebene der Geeignetheit bestehen bei Massenüberwachungsmaßnahmen prinzipiell keine Probleme, da diese aufgrund ihrer universalen Aus-

1872 BVerfGE 150, 244 (266 ff.) – Autom. Kennzeichenkontrolle II; E 154, 152 (230) – Ausland-Ausland-Fernmeldeaufklärung; krit. *Schnieders*, NVwZ 2019, 381 (397); *Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 43.

1873 Zum Verhältnis zu Art. 16 Abs. 1 AEUV bzw. Art. 52 Abs. 2 EU-GRC siehe *Kingreen* in Callies/Ruffert EUV/AEUV, EU-GRC Art. 8 Rn. 4.

1874 Vgl. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), 120 = EuZW 2022, 706; Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), 39 = NJW 2014, 2169.

richtung immer den sicherheitsrechtlichen Zweck fördern. Das Verhältnis von (im Nachhinein betrachtet) unnötigen Datenverarbeitungen zu den echten *Treffern* spielt hier noch keine Rolle. Allein die Tatsache, dass die verarbeiteten Daten grundsätzlich für spätere Ermittlungen oder die Verdachtsgenerierung verwendet werden können, macht die Maßnahmen der Massenüberwachung geeignet.

Die eigentliche Prüfung wird daher im Bereich der Angemessenheit bzw. im Falle des EuGH auch der Erforderlichkeit vorgenommen, wobei es in beiden Fällen auf eine Prüfung der durch die Bestimmtheit erzwungenen Effektivität ankommt – also darauf, ob der gesetzliche Zuschnitt der Maßnahme die Handlungsmöglichkeiten der Behörden so einengt, dass (wiederum im Nachhinein betrachtet) unnütze und sinnvolle Datenverarbeitungen in einem akzeptablen Verhältnis zueinanderstehen.

(b) Geldwäsche als schwere Kriminalität?

Die erste Begrenzung, die der EuGH insofern fordert, ist eine Einschränkung des Zwecks in Anbetracht der Schwere des jeweiligen Grundrechtseingriffs. *Ein schwerer Eingriff im Bereich der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten kann nämlich nur durch einen Zweck der Bekämpfung einer ebenfalls als „schwer" einzustufenden Kriminalität gerechtfertigt sein*,[1875] oder zur Terrorismusbekämpfung in nationalen Gefährdungssituationen, wenn eine solche Situation gerichtlich festgestellt wurde.[1876] Außerdem müssen die vom jeweiligen Überwachungssystem adressierten Kriminalitätsformen mit dem jeweils überwachten Bereich in einem Sinnzusammenhang stehen. Die PNR-Überwachung darf deshalb nur zur Bekämpfung solcher schweren Straftaten genutzt werden, die *in einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen* stehen.[1877]

Die entscheidende allgemeine Rechtfertigungsanforderung des EuGH ist also, dass schwere Grundrechtseingriffe, wozu jedenfalls bei sensiblen

1875 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 148 = EuZW 2022, 706; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

1876 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 175 ff. = NJW 2021, 531

1877 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 157 = EuZW 2022, 706.

Daten auch die massenhafte Datenanalyse zählt,[1878] nur zur Bekämpfung schwerer Kriminalität und Terrorismus durchgeführt werden dürfen. Insofern ist jedenfalls der Bezug in Art. 41 Abs. 2 GWRL auf die Terrorismusfinanzierung ausreichend, da eine effektive Terrorismusbekämpfung sicher auch eine Unterbindung fördernder Finanzströme beinhalten muss.

Schwieriger ist die Bewertung des Geldwäschetatbestandes. Zwar zählte Art. 3 Nr. 9 i. V. m. Anhang II, Nr. 8 PNR-RL die *Wäsche von Erträgen aus Straftaten und Geldfälschung, einschließlich Euro-Fälschung* als Form der schweren Kriminalität auf, der EuGH legte diese Vorschrift aber dahingehend aus, dass nicht eine konkrete Straftat gemeint sein soll, sondern nur eine Kategorie, und sich erst aus dem nationalen Recht ergeben solle, ob die jeweiligen Delikte eine schwere Straftat darstellen.[1879]

Der EuGH überlässt es traditionell den Mitgliedstaaten festzulegen, was eine *schwere Straftat* darstellen soll. Auch im PNR-Urteil konnte er diese Frage umgehen. Nach Art. 3 Nr. 9 PNR-RL müssen die zweckbindenden Straftaten – wenn sie unter eine in Anhang II genannte Kategorie fallen – mit einer Höchststrafe von mindestens drei Jahren bedroht werden. Eine Schwelle für die Mindeststrafe wird aber nicht genannt. Der EuGH wies deshalb darauf hin, dass eine Straftat, die grundsätzlich eine ausreichende Schwere aufweist, nach dem mitgliedstaatlichen Recht weiterhin auch nur eine allgemeine Straftat darstellen kann.[1880] Die PNR-RL definiert also nicht, was aus europarechtlicher Sicht eine schwere Straftat darstellen soll.

Bei der Geldwäsche handelt es sich ferner um einen *besonders schweren Kriminalitätsbereich* i. S. d. Art. 83 Abs. 1 UAbs. 2 AEUV.[1881] Ob damit aber jedes Geldwäschedelikt eine Form schwerer Kriminalität im Sinne der EuGH-Rechtsprechung darstellt, deren Verfolgung und Verhütung schwere Grundrechtseingriffe rechtfertigt, ist weiterhin fraglich[1882], denn Art. 83 Abs. 1 UAbs. 2 AEUV regelt nur eine Kompetenz der EU zur Harmonisierung von Kriminalitäts*bereichen* mit einer grenzüberschreitenden Dimension. Die EU kann danach Mindestregeln der Strafbarkeit erlassen. Entsprechende (nationale) Strafnormen können aber jedenfalls dann nicht

1878 Idem, Rn. 102 ff., 111.
1879 Idem, Rn. 147
1880 Idem, Rn. 148 ff.
1881 Zu Art. 3 Nr. 9 i. V. m. Anhang II, Nr. 8 PNR-RL insofern Idem, Rn. 149; GA *Pitruzzella*, Schlussantrag v. 27.01.2022, C-817/19 (Ligue des droit humains (PNR)), Rn. 121, Fn 123.
1882 Vgl. *Hochmayr* in Frankfurter Kommentar, AEUV Art. 83 Rn. 12; s.a. *Böse/S. Jansen*, JZ 2019, 591 (594).

automatisch als besonders schwer im europarechtlichen Sinne gelten, wenn diese zwar die Mindeststandards erfüllen, aber auch Delikte umschreiben, die keinen grenzüberschreitenden Bezug aufweisen. Für Geldwäschedelikte ohne solche Dimension lässt sich aus der Kompetenznorm Art. 83 Abs. 1 UAbs. 2 AEUV schon deshalb nichts schließen.

Einen weiteren Anhaltspunkt im Unionsrecht bietet Art. 85 Abs. 1 AEUV, nach dem die Behörde Eurojust nationale Behörden koordiniert, *die für die Ermittlung und Verfolgung von schwerer Kriminalität zuständig sind*. In Art. 3 Abs. 1 i. V. m. Anhang I der Eurojust-VO[1883] werden *Formen* solcher schwerer Kriminalität aufgelistet u. a. *Geldwäschehandlungen*.

Die Eurojust-VO als Akt des Sekundärrechts kann allerdings nicht den unionsprimärrechtlich verwandten Begriff der schweren Kriminalität in Bezug auf die Verhältnismäßigkeit staatlicher Überwachungsmaßnahmen ausfüllen. Vielmehr ist andersherum zu fragen, ob die Zuständigkeitsbestimmung in Art. 3 Abs. 1 i. V. m. Anhang I Eurojust-VO dem Unionsprimärrecht nicht entgegensteht. Es bedarf deshalb auch für die Zuständigkeit von Eurojust einer einzelfallgerechten Auslegung, ob ihr Tätigwerden bei der jeweiligen Maßnahme auf eine Straftat von besonderer Schwere ausgerichtet ist. Art. 3 Abs. 1 i. V. m. Anhang I Eurojust-VO ist insofern restriktiv auszulegen.[1884]

Einer solchen einzelfallgerechten – also mindestens auf den konkreten Straftatbestand bezogenen – Betrachtung bedarf es auch zur Bestimmung der schweren Kriminalität im Rahmen der Verhältnismäßigkeitsprüfung von Überwachungsmaßnahmen. Die Tatbestandsmerkmale der Geldwäschestrafbarkeit wurden in den vergangenen Jahren derart aufgeweicht, dass nunmehr jede Verwertung illegitimer Vermögenswertung darunterfällt[1885] („all-crimes-approach"[1886]). Auch die typische Alltagskriminalität ist betroffen.

Alltägliche Vermögensdelikte, etwa Diebstahl oder Betrug, ziehen in den meisten Fällen eine Verwertung nach sich und mithin eine Geldwäsche.

1883 Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates vom 14. November 2018 betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und zur Ersetzung und Aufhebung des Beschlusses 2002/187/JI des Rates, ABl. 2018, L 295/138.

1884 *B. Vogel/Eisele* in Grabitz/Hilf/Nettesheim Recht der EU, AEUV Art. 85, Rn. 9a; *Böse* in Schwarze/Becker/Hatje/Schoo, EU-Recht, AEUV Art. 85 Rn. 4.

1885 Übersichtlich *El-Ghazi* in Herzog GwG, StGB § 261 Rn. 144.

1886 *Pelz* in BeckOK GwG, § 43 Rn. 28.

Der Unrechtsgehalt[1887] des Geschehens wird hierdurch jedoch kaum erweitert, geht er doch meist in der Vortat voll auf.[1888] Bei der Geldwäsche von Erträgen aus Alltagskriminalität kann es sich also nicht grundsätzlich um schwere Kriminalität handeln. Der Selektionsanspruch der Einordnung von Straftaten in Schweregrade würde unterlaufen, wenn bei Delikten, die eine Vortat voraussetzen, der Schweregrad jener Vortat nicht berücksichtigt würde.

Auch der EuGH scheint im PNR-Urteil nicht davon überzeugt, dass jedes Verhalten im Bereich der Geldwäsche eine schwere Straftat darstellt, sondern nennt die *Wäsche von Erträgen aus Straftaten* in einem Atemzug mit den anderen in Art. 3 Nr. 9 i. V. m. Anhang II, Nr. 8 PNR-RL aufgeführten allgemeinen Kriminalitätsbereichen wie *Betrugsdelikten, Geldfälschung, Umweltkriminalität und illegaler Handel mit Kulturgütern*. Bei diesen soll es eben auf die konkrete Ausgestaltung im nationalen Recht ankommen.[1889]

Entsprechend den Aussagen im PNR-Urteil müssten die Nationalstaaten das Transaktionsmonitoring also auf bestimmte Unterfälle ihrer Geldwäschedelikte begrenzen, wenn sie nicht von vornherein den Tatbestand so kreiert haben, dass er stets als besonders schwer angesehen werden muss. Dies aber ist nach dem unmittelbaren Wortlaut des Unionsrechts nicht möglich, da Art. 1 Abs. 3 GWRL und Art. 3 Geldwäschestrafbarkeits-RL zwingend den *All-crimes-Approach* vorgeben.

Es bedürfte insofern also einer Auslegung bzw. einer teleologischen Reduktion der Geldwäschemaßnahmen dahingehend, dass sie nicht zur Verfolgung und Verhinderung sämtlicher Geldwäschehandlungen eingesetzt werden dürfen, sondern nur zu solchen, die konkret auch eine schwere Straftat darstellen. In Deutschland wurde entsprechend § 100a Abs. 2 Nr. 1 lit. m) StPO dahingehend eingegrenzt, dass die TKÜ nur zur Aufklärung von Geldwäschedelikten erfolgen darf, deren Vortat ebenfalls eine schwere Straftat darstellt.[1890]

1887 Zum geschützten Rechtsgut des § 261 Abs. 1 StGB: BT-Dr 12/3533, S. 11; BGHSt 53, 205; *Hecker* in Schönke/Schröder StGB, § 261 Rn. 2 mwN.; bei § 261 Abs. 2 StGB ist auch das Rechtsgut der Vortat mitumfasst, BGHSt 63, 228 (241); ausf. *Neuheuser* in MüKo StGB, § 261 Rn. 8 ff.; *El-Ghazi* in Herzog GwG, StGB § 261 Rn. 28 ff. jeweils mwN.

1888 BT-Drs. 18/6389, S. 11 ff.; *Böse/S. Jansen*, JZ 2019, 591 (593 f.); *El-Ghazi* in Herzog GwG, StGB § 261 Rn. 28 ff., 144.

1889 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 147 = EuZW 2022, 706

1890 dazu BT-Drucks. 18/6389, S. 15 f., *Böse/Janzen*, JZ 2019, 591 (594).

Nach den Maßstäben des PNR-Urteils, das an verschiedenen Stellen nichts weniger als eine Contra-Lege-Auslegung vornimmt,[1891] ist aktuell nicht ausgeschlossen, dass der EuGH eine solche Auslegung trotz der eindeutigen Begriffsbestimmung des Art. 1 Abs. 3 GWRL, Art. 3 Geldwäschestrafbarkeits-RL für denkbar halten könnte und die Geldwäschemaßnahmen insofern nicht für unverhältnismäßig hält.

Kommt eine solche Auslegung nicht in Betracht, müsste die Ermächtigung zum Transaktionsmonitoring angepasst und dahingehend beschränkt werden, dass nur die schweren Fälle der Geldwäsche mit dieser Maßnahme bekämpft werden dürfen.

(c) Anforderungen an den automatisierten Datenabgleich im PNR-Urteil

Neben der grundsätzlichen Anforderung, intensive Überwachungsmaßnahmen auf schwerwiegende Kriminalitätsbekämpfung zu begrenzen, hat der EuGH auch spezifische Voraussetzungen für die konkreten Überwachungsmaßnahmen etabliert. Für das Transaktionsmonitoring sind insbesondere die Verhältnismäßigkeitserwägungen des EuGH[1892] zu Art. 6 Abs. 2 lit. a), Abs. 3 lit. b) PNR-RL bzgl. des automatisierten (Vorab-)Datenabgleichs bedeutsam, da dieser Abgleich insofern eine Analogie darstellt (s. o.).

Der EuGH forderte für Analysen von PNR-Daten allgemein zunächst formelle Verfahrens- bzw. datenschutzrechtliche Sicherungsschritte. So sollen die in der PNR-RL benannten nationalen Kontrollstellen, der Datenschutzbeauftragte und die PNR-Zentralstelle *mit den nötigen materiellen und personellen Mitteln für die Ausübung der ihnen nach der PNR-Richtlinie obliegenden Kontrolle ausgestattet werden*. In den nationalen Umsetzungsgesetzen müssten weiter *klare und präzise Vorschriften für die Bestimmung der Datenbanken sowie der herangezogenen Analysekriterien aufgestellt werden*.[1893]

Damit die Rechtmäßigkeit der Vorabüberprüfung effektiv kontrolliert werden kann, müssen sowohl ausreichende Transparenznormen für die

1891 *Thönnes*, Die Verwaltung 2022, 527 (539); *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025

1892 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 176 ff, 193 ff., 202 ff. = EuZW 2022, 706.

1893 Idem, Rn. 179 f.

aufgrund der Vorabprüfung getroffenen Maßnahmen als auch eine regelmäßige Kontrolle der Kriterien durch die Aufsicht etabliert werden.[1894]

In materieller Hinsicht sei allgemein bedeutsam, dass die Menge der *false positives* auf ein Minimum reduziert bliebe.[1895] Im Übrigen legte der EuGH großen Wert auf die in der PNR-Richtlinie vorgesehene, menschliche Letztentscheidung. Alle Treffer müssten vor einer Weiterleitung an Sicherheitsbehörden menschlich geprüft werden, bevor nachteilige Maßnahmen gegen die Betroffenen eingeleitet würden.[1896] Eine Übermittlung an Sicherheitsbehörden könne nur stattfinden, wenn Anhaltspunkte vorliegen, *aus denen sich in rechtlich hinreichender Weise der begründete Verdacht einer Beteiligung der mittels der automatisierten Verarbeitungen identifizierten Personen an terroristischen Straftaten oder schwerer Kriminalität ergibt.*[1897] Die Mitgliedstaaten müssten insofern *klare und präzise Regeln vorsehen, die Leitlinien und einen Rahmen für vorzunehmende Analysen vorgeben, um für die uneingeschränkte Achtung der in den Art. 7, 8 und 21 der Charta verankerten Grundrechte zu sorgen.*[1898]

Der EuGH stellte noch konkretere Anforderungen getrennt danach auf, ob sich die Analyse auf externe Datenbanken, insb. Fahndungsdateien, bezieht oder anhand *im Voraus festgelegter Kriterien* durchgeführt wird.

Bei dem (Fahndungs-)Datenbankabgleich sah der EuGH die Gefahr der Erstellung von Persönlichkeitsprofilen, die bei den Betroffenen das Gefühl der Überwachung hervorrufen könnten, wenn die verwandten Dateien nicht auf ganz konkrete Fälle reduziert würden. Art. 6 Abs. 3 lit. a) PNR-RL erlaubt den Einsatz von *Datenbanken, die zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität maßgeblich sind, einschließlich Datenbanken betreffend Personen oder Gegenstände, nach denen gefahndet wird oder die Gegenstand einer Ausschreibung sind.*

Die Begrenzung durch den Terminus „maßgeblich" sei für eine verhältnismäßige bzw. ausreichend bestimmte – der EuGH betrachtet die Bestimmtheit als Unterpunkt der Verhältnismäßigkeit (s. o. Kap. C. II. 1. a. aa. (2) (b)) – Eingrenzung nicht ausreichend. Die Norm müsse daher da-

1894 Idem, Rn. 210 ff.
1895 Idem, Rn. 203.
1896 Idem, Rn. 206.
1897 Idem, Rn. 204.
1898 Idem, Rn. 205.

hingehend ausgelegt werden, dass nur die *personenbezogenen* Datenbanken i. S. d. Art. 6 Abs. 3 lit. a) 2. HS PNR-RL eingesetzt werden dürften.[1899]

Im Falle des Abgleichs mit diesen Datenbanken müsse sodann sichergestellt sein, dass es bei einem absolut notwendigen Grundrechtseingriff bliebe. Dazu müsste zunächst Art. 6 Abs. 4 PNR-RL auf Art. 6 Abs. 3 lit. a) analog angewandt werden. Die verwandten Datenbanken müssten demnach diskriminierungsfrei und verhältnismäßig sein und von den PNR-Zentralstellen in Zusammenarbeit mit den Aufsichtsbehörden regelmäßig überprüft werden.[1900]

Verhältnismäßig sei insofern nur der Einsatz von Datenbanken, *die im Zusammenhang mit der Bekämpfung terroristischer Straftaten und schwerer Kriminalität mit einem – zumindest mittelbaren – objektiven Zusammenhang mit der Beförderung von Fluggästen betrieben werden,* was wiederum voraussetze, dass diese Datenbanken von den Behörden verwaltet würden, die auf die Daten der PNR-Zentralstelle auch zugreifen dürften. [1901]

Bei der Analyse mit *im Voraus festgelegten Kriterien* legte der EuGH Wert auf eine stringente Anwendung der Diskriminierungsfreiheit. Die Kriterien dürften auf keinen Fall dazu führen, dass Betroffene wegen ihrer rassischen oder ethnischen Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, Mitgliedschaft in einer Gewerkschaft, ihres Gesundheitszustands, ihres Sexuallebens oder ihrer sexuellen Orientierung benachteiligt würden.[1902]

Die bei der Vorabüberprüfung herangezogenen Kriterien seien weiter so festzulegen, dass sie speziell auf Personen abzielen, bei denen der begründete Verdacht einer Beteiligung an terroristischen Straftaten oder schwerer Kriminalität bestand. Deshalb müssten sowohl „belastende" als auch „entlastende" Gesichtspunkte berücksichtigt werden.[1903]

Künstliche Intelligenz, *die – ohne menschliche Einwirkung und Kontrolle – den Bewertungsprozess und insbesondere die Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern könnte*, dürfe nicht eingesetzt werden.[1904]

1899 Idem, Rn. 187 f.
1900 Idem, Rn. 189 ff.
1901 Idem, Rn. 191 f.; dazu *Thönnes*, Die Verwaltung 2022, 527 (552 ff.).
1902 Idem, Rn. 196 f.
1903 Idem, Rn. 198 ff.
1904 Idem, Rn. 194; s.a, *Orrù, Information Polity* 27 (2022), 131.

(4) Anwendung auf das Transaktionsmonitoring

Bei dem Versuch einer Übertragung des PNR-Urteils auf das Transaktionsmonitoring muss zunächst beachtet werden, dass das auf Verdachtsmeldungen ausgerichtete Monitoring in einem dreistufigen, nicht in einem zweistufigen Verfahren abläuft. Anders als beim PNR-System rastern die geldwäscherechtlich Verpflichteten selbst und übermitteln nur dann Daten, wenn sie eine Auffälligkeit erkannt haben wollen.

(a) Ausgestaltung der Folgeübermittlungspflichten

Typischerweise steigt mit jedem Schritt die individuelle Intensität des Überwachungskomplexes, da sich mit jeder Datenverarbeitung der Verdacht weiter erhärtet und deswegen eine tiefergehende Betrachtung der jeweiligen Daten erforderlich wird. Das ist auch bei der Geldwäschebekämpfung der Fall. Je breiter die Maßnahmen, desto weniger stark werden die Betroffenen beeinträchtigt. Daher muss mit jeder weiteren Datenverwendung immer auch eine strengere Prozeduralisierung einhergehen.

Aufgrund der Wechselwirkung bzw. Synergie der einzelnen Überwachungsmaßnahmen müssen die Schwellen der Übermittlungspflichten bzw. -rechte bereits bei der Bewertung des ersten Überwachungsschrittes beachtet werden. Sind die letzten Schritte des Überwachungskomplexes, die eine hohe individuelle Betroffenheit aufweisen, nicht ausreichend prozeduralisiert, sind auch die anfänglichen Datenverarbeitungen unverhältnismäßig.

Für das Transaktionsmonitoring bedeutet das, dass die Meldepflichten von den Verpflichteten an die FIU und der FIU an die Sicherheitsbehörden rechtskonform gestaltet werden müssen. Andernfalls verstößt das Monitoring, das die Meldungen vorbereiten bzw. ermöglichen soll, gegen Art. 8 Abs. 1 EU-GRC.

Die Anforderung, dass nur bei konkretem Verdacht einer schweren Straftat eine Übermittlung der PNR-Zentralstelle an (operative) Sicherheitsbehörden stattfinden soll[1905], kann allerdings nicht für das Transaktionsmonitoring durch Private gelten, sondern muss auf den Prozess insgesamt bezogen werden.

1905 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), 204 = EuZW 2022, 706.

Da im PNR-Urteil eine unfiltrierte (Massen-)Übermittlung von Daten durch Private an eine zentrale Analysestelle im Grundsatz für rechtskonform erachtet wurde[1906], begegnen das geldwäscherechtliche Meldesystem bzw. die niedrigen Verdachtsschwellen der privaten Verpflichteten nach § 43 Abs. 1 GwG keinen prinzipiellen Bedenken.[1907] Entscheidend ist, dass die jeweilige Filterstelle – als letzte Hürde vor den operativen Sicherheitsbehörden – nur unter bestimmten Umständen an diese übermittelt. Da es sich bei der Prüfung, ob ein bestimmter Sachverhalt sicherheitsrechtlich relevant ist, um eine originär staatliche Aufgabe handelt, sind die Anforderungen an Private in diesem Bereich mit guten Gründen gering zu halten.

Nur die abgestuften Verdachtsschwellen des § 32 Abs. 2 GwG, die für die Übermittlung der FIU an Strafverfolgungsbehörden gelten sollen, sind demnach problematisch. Die FIU ist nach der Auffassung des GwG-Gesetzgebers nicht erst bei einem konkreten Straftatverdacht, sondern unter dieser Schwelle zur proaktiven Weiterleitung verpflichtet, wenn sie feststellt, dass ein Vermögensgegenstand mit Geldwäsche, mit Terrorismusfinanzierung oder mit einer sonstigen Straftat im Zusammenhang steht.[1908] Zum gefahrenabwehrrechtlichen Verdachtsgrad äußert § 32 Abs. 2 GwG sich nicht, da keine proaktive Übermittlungspflicht an Gefahrenabwehrbehörden vorgesehen ist.

Eine Übermittlungspflicht an den Verfassungsschutz nach § 32 Abs. 1 oder an den BND nach § 32 Abs. 2 S. 2 GwG besteht immer dann, *wenn diese Übermittlung für deren Aufgabenerfüllung erforderlich ist.* Auch hierbei gilt kein strenger Verdachtsgrad. *Anhaltspunkte* sollen reichen.[1909] Die Übermittlung an den BND nach 32 Abs. 2 S. 2 GwG ist dabei aber abhängig von einer Übermittlung an die Strafverfolgungsbehörden nach § 32 Abs. 2 S. 1 GwG, findet also nie separat statt.

Die Verdachtsgrade der Übermittlungspflichten im GwG dürften enger auszulegen sein, als es der Gesetzgeber vorsieht. Art. 32 Abs. 3 S. 3 der GWRL fordert für proaktive Meldungen der FIU, dass die FIUs bei *begründetem Verdacht auf Geldwäsche damit zusammenhängende Vortaten oder Terrorismusfinanzierung* übermitteln. Der begründete Verdacht kann

1906 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 248 ff. = EuZW 2022, 706.

1907 S.a. EuGH Urt. v. 26. 6. 2007, C-305/05 (Ordre des barreaux) = NJW 2007, 2387; EGMR, Urt. v. 6. 12. 2012, 12323/11 – Michaud/Frankreich = NJW 2013, 3423.

1908 BT-Drs. 18/11555, S. 144; 18/11928, S. 26; krit. *Barreto da Rosa* in Herzog GwG, § 43 Rn. 16 ff.; *Höche/Rößler*, WM 2012, 1505 (1509); *Bülte*, NZWiSt 2017, 276 (280 f.).

1909 BT-Drs. 18/11555, S. 144.

problemlos dahingehend ausgelegt werden, dass *konkrete Anhaltspunkte* vorliegen müssen.

Die Anforderungen an die Übermittlungspflicht der FIU sind also nicht nur eine grundrechtliche Problematik, sondern eine der Richtlinienkonformität des GwG. Entgegen den Ausführungen des Gesetzgebers[1910] müsste jedenfalls § 32 Abs. 2 GwG richtlinienkonform dahingehend ausgelegt werden, dass die FIU erst dann Informationen aus ihrer Analyse proaktiv übermitteln darf, wenn sich aus dieser Anhaltspunkte einer konkreten Gefahr oder ein strafprozessualer Anfangsverdacht hinsichtlich Geldwäsche oder Terrorismusfinanzierung ergeben haben. Diese Schwellen des deutschen Sicherheitsverfassungsrechts dürften sich mit den vom EuGH als Mindestschwelle geforderten *konkreten Anhaltspunkten* decken.

Würde das GwG eine Übermittlungspraxis unterhalb dieser Schwellen vorsehen, wäre schon das Transaktionsmonitoring nicht mehr mit den Anforderungen des EuGH an eine mit Art. 7, 8 EU-GRC konforme Ausgestaltung von Massenüberwachungsmaßnahmen vereinbar. Auf eine separate Darstellung der Anforderungen an die proaktive Übermittlung wird hier im Sinne der Wechselwirkung verzichtet.

(b) Ausgestaltung des massenhaften Datenabgleichs

Weiter müsste das Transaktionsmonitoring mit den Ausführungen des EuGH zur Gestaltung, Kontrolle und Transparenz des Datenabgleichs zu vereinbaren sein.

Soweit mit bestehenden Datenbanken abgeglichen wird, ist entscheidend, dass diese in konkretem Zusammenhang mit den Delikten stehen, deren Bekämpfung das Überwachungssystem dient. Dies wird insbesondere bei Embargo-Listen und PEP-Listen durchaus der Fall sein.[1911] Es bedarf jedoch insofern einer regelmäßigen Kontrolle durch die Aufsichtsbehörden, die nach Art. 48 GWRL ermächtigt wurden, etwa zur Erstellung von Leitlinien und Auslegungshinweisen nach Art. 48 Abs. 10 GWRL[1912] (in Deutschland siehe § 51 Abs. 8 GwG, § 25h Abs. 5 KWG.)

Außerdem forderte der EuGH, dass die herangezogenen Datenbanken von der abgleichenden Stelle geführt werden. Letzteres lässt sich auf das

1910 BT-Drs. 18/11555, S. 144; 18/11928, S. 26.
1911 Vgl. *Achtelik* in Herzog GwG, KWG § 25h Rn. 12.
1912 Etwa *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung).

Anti-Geldwäscherecht kaum übertragen, da der ursprüngliche Abgleich nicht von den Zentralstellen, sondern den privaten Verpflichteten vorgenommen wird. Dass in der Praxis solche Listen von Privatanbietern erstellt werden,[1913] ist insofern zwar nicht unproblematisch, sollte sich jedoch ebenfalls aufsichtsrechtlich einfangen lassen.[1914]

Überhaupt dürfte der Fokus einer Prozeduralisierung des Transaktionsmonitorings weniger auf dem Abgleich mit externen Datenbanken als der Recherche nach Auffälligkeiten in den Transaktionsmustern liegen. Hierbei kommt der Aufsicht eine entscheidende Rolle zu, da die Rasterung an Private ausgelagert wird. Die Prüfkriterien müssen so festgelegt sein, *dass die Zahl unschuldiger Personen, die fälschlicherweise mit dem durch die Richtlinie geschaffenen System identifiziert werden, auf ein Minimum beschränkt wird.*[1915] Ferner müssen *klare und in präziser Weise festgelegte Kriterien für die objektive Überprüfung aufstellt werden*, *die es* (der FIU) *ermöglichen, zum einen zu prüfen, ob und inwieweit ein Treffer tatsächlich eine Person betrifft*, *die möglicherweise* (an Geldwäsche oder Terrorismusfinanzierung) *beteiligt ist und deshalb einer weiteren Überprüfung unterzogen werden muss.*[1916] Dabei gilt zu beachten, dass die Prüfkriterien nicht zu einer (auch mittelbaren) Diskriminierung bestimmter Personengruppen führen dürfen,[1917] weshalb insbesondere geografische Parameter mit mittelbarem Diskriminierungspotential streng geprüft werden sollten.

Bedenklich sind auch die Bestrebungen zum Einsatz künstlicher Intelligenz im Rahmen der Monitoringsysteme.[1918] Der EuGH hielt die Anwendung solcher Systeme im Rahmen der PNR-Überwachung für unzulässig, *wenn sie Bewertungskriterien, auf denen das Ergebnis der Anwendung dieses Prozesses beruht, sowie die Gewichtung der Kriterien ändern können*, da die Kriterien der Rasterung nach Art. 6 Abs. 3 lit. b) PNR-RL „im Voraus festge-

1913 Vgl. *SEON,* Top 14 Anti Money Laundering (AML) Software & Tools 2023, https://seon.io/resources/comparisons/aml-software-tools/, zuletzt aufgerufen am 12.01.2025

1914 *BaFin,* Leitlinien und Q&As der ESA, S. 16 f., https://www.bafin.de/DE/RechtRegelungen/Leitlinien_und_Q_and_A_der_ESAs/Leitlinien_und_Q_and_A_der_ESAs_node.html, zuletzt aufgerufen am 12.01.2025.

1915 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 203 ff. = EuZW 2022, 706.

1916 Idem, Rn. 206.

1917 Idem, Rn. 197.

1918 Dazu *EBA,* JC 2017, 81, Innovative Solutions, 23.01.2018; *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276.

legt" worden sein mussten.[1919] Darüber hinaus stünde der Einsatz solcher Systeme einer effektiven bzw. wirksamen Rechtskontrolle im Wege.[1920]

Ob der Einsatz künstlicher Intelligenz bzw. selbstlernender Systeme in der Geldwäschebekämpfung stattfinden darf,[1921] ist demnach noch offen, da der EuGH im PNR-Urteil sein Verbot primär einfachrechtlich begründet hatte. Naheliegend wird jedenfalls eine aus den Grundrechten folgende Begrenzung des KI-Einsatzes sein. Soweit die vom EuGH entwickelten Anforderungen an Massenraster eingehalten werden und es stets zu einer menschlichen Letztkontrolle vor der Weiterleitung an operative Sicherheitsbehörden kommt, spricht wohl nichts prinzipiell gegen den Einsatz von KI-Systemen im Rahmen der Sicherheitsgewährleistung[1922], insbesondere dann nicht, wenn diese Systeme zu besseren Ergebnissen als die ordinären automatisierten Datenanalysen führen.

Ob die GWRL eine effektive Rechtskontrolle ermöglicht, ist überdies fraglich, da es ihr an Benachrichtigungspflichten und Auskunftsverfahren mangelt. Nach Art. 39 Abs. 1 GWRL (umgesetzt in § 47 GwG) ist den Verpflichteten eine Information ihrer Kunden über Mitteilungen an die Meldestellen untersagt. Die Auskunftspflichten der DSGVO dürfen nach Art. 41 Abs. 4, der auf Art. 39 Abs. 1 GWRL verweist, von den Mitgliedstaaten abbedungen werden.

Es besteht also keine Möglichkeit der Kunden, die Rechtmäßigkeit einer sie betreffenden Meldung, etwa nach Art. 77 DSGVO, effektiv überprüfen zu lassen.[1923] Angesichts der Intensität des Transaktionsmonitorings ist die Grundrechtskonformität dieser Ausgestaltung mehr als fraglich.

Keine Auswirkungen dürfte hingegen die Notwendigkeit menschlicher Entscheidung auf das Transaktionsmonitoring haben. Dieses sieht nur in allererster Phase eine rein automatisierte Verarbeitung vor. Sowohl die Meldungen durch die Privaten an die FIU nach Art. 33 Abs. 2 GWRL, als auch die Meldungen der FIU an die Sicherheitsbehörden erfolgen erst nach menschlicher Prüfung.

1919 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 194 ff. = EuZW 2022, 706; dazu *Thönnes*, Die Verwaltung 2022, 527 (547 ff.).

1920 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 195 = EuZW 2022, 706.

1921 Dazu *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276.

1922 Dazu *Billis/Knust/Rui,* FS Sieber Bd. II, 2022, 693 (705 ff.).

1923 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (244).

dd. Ergänzung durch die EGMR-Rechtsprechung (*Big Brother* & *Rättvisa*)

Bei der Bewertung der unionsprimärrechtlichen Konformität des Transaktionsmonitorings könnte in Zweifelsfragen die Rechtsprechung des EGMR herangezogen werden, Art. 52 Abs. 3 EU-GRC.

Der EuGH hält zwar die Eigenständigkeit der Charta hoch und hat die EMRK bzw. die Rechtsprechung des EGMR bislang nur zur Bestimmung des Schutzbereiches herangezogen, während er bei der Bestimmung der Schranken und insb. Schranken-Schranken allein auf die Normen der EU-GRC abstellen will. Dabei verweist er jedoch im Einzelfall auf Entsprechungen in der Rechtsprechung des EGMR, die er als Mindeststandard und Ergänzung zur Erklärung seiner Rechtsprechung heranzieht.[1924]

Die Rechtsprechung des EuGH zur automatisierten Datenanalyse im PNR-Urteil könnte insofern von den Urteilen des EGMR zur Massenüberwachung von Telekommunikation ergänzt werden.[1925] Auch bei dieser findet eine schrittweise, trichterartige Überwachung privater Daten statt, wobei Anlassmomente für weitere Befugnisse extrahiert werden sollen. Ein wichtiger Unterschied besteht jedoch darin, dass der Fokus bei der Telekommunikationsüberwachung auf extern erstellten Selektoren basiert, während beim PNR- und Transaktionsmonitoring (insbesondere) Auffälligkeiten angesichts der Datenhistorie des Betroffenen untersucht werden sollen, der Anlass sich also aus den überwachten Daten selbst ergibt.

Auf der Ebene der Massenüberwachung, also der universellen (Erst-)Erhebung der Daten mit sich unmittelbar anschließender automatisierter Analyse, fordert der EGMR zunächst eine strikte Aufsicht über die Auswahl der Selektoren.[1926] Dies deckt sich mit der Forderung des EuGH, dass die Kriterien der Datenanalyse von der Aufsicht angemessen zu gestalten sind.[1927]

Des Weiteren fordert der EGMR konkrete Sicherungsvorkehrungen bei der Massenüberwachung von Telekommunikationsdaten. Danach haben die jeweiligen Sicherheitsgesetzgeber bestimmte Regeln zu erlassen über „*I.)*

1924 Vgl. EuGH, Urt. v. 15.3.2017, C-528/15 (Al Chodor), Rn. 37 = NVwZ 2017, 777; zu Art 7 EU-GRC/ Art. 8 EMRK: Urt. v. 17.12.2015, C-419/14 (WebMindLicenses kft), Rn. 70 ff.; *Streinz/W. Michl* in Streinz EUV/AEUV, EU-GRC Art. 52 Rn. 29 f. mwN.

1925 Vgl. dazu *Boehm/Andrees*, CR 2016, 146 (150 ff.).

1926 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/ Vereinigtes Königreich), Rn. 350. = NVwZ-Beil. 2021, 11.

1927 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 203 = EuZW 2022, 706.

die Gründe, aus denen die Massenüberwachung genehmigt werden kann, 2.) die Umstände, unter denen die Kommunikationen eines Einzelnen überwacht werden können, 3.) das Verfahren, das bei der Genehmigung einzuhalten ist, 4.) das Verfahren bei der Auswahl, Auswertung, und Verwendung abgefangenen Materials, 5.) die Vorsichtsmaßnahmen, die bei Weitergabe des Materials an andere zu treffen sind, 6.) die zeitliche Begrenzung der Überwachung und Speicherung des erhobenen Materials sowie die Umstände, unter denen dieses Material gelöscht und vernichtet werden muss, 7.) das Verfahren und die Einzelheiten der Überwachung durch eine unabhängige Stelle, ob die genannten Garantien beachtetet wurden, und die Befugnis dieser Stelle, bei Verstößen zu entscheiden und 8.) das Verfahren für eine unabhängige nachträgliche Kontrolle der Einhaltung dieser Garantien und die Befugnis der zuständigen Stelle, zu entscheiden, wenn das nicht der Fall war."[1928]

Insbesondere die Forderung des EGMR nach einer möglichen nachträglichen Kontrolle ist insofern relevant, da der EuGH diese bislang einfachgesetzlich vorgefunden hatte und nur eine strenge Beachtung anmahnen konnte. Der EGMR leitet das Erfordernis hingegen unmittelbar aus den Konventionsgrundrechten her.

Bei der Prüfung, ob die geldwäscherechtliche Verschwiegenheitspflicht der Verpflichteten nach Art. 41 Abs. 4, Art. 39 Abs. 1 GWRL mangels effektiver Rechtsschutzmöglichkeit einen Verstoß gegen Unionsgrundrechte darstellt, könnte ergänzend die Rechtsprechung des EGMR angeführt werden. Auch nach dieser ist sehr zweifelhaft, ob das Fehlen einer Benachrichtigungspflicht über Maßnahmen im Anschluss an das Transaktionsmonitoring nicht zu dessen Unverhältnismäßigkeit führen muss.

ee. Zwischenergebnis

Das Transaktionsmonitoring stellt eine Form der Massenüberwachung in Form einer automatisierten Datenanalyse dar. Es wirkt universell, es betrifft sensible persönliche Daten und muss schon deshalb als intensiver Eingriff in Privatheitsgrundrechte erachtet werden.[1929]

1928 EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 361 = NVwZ-Beil. 2021, 11;

1929 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), 98 ff. = EuZW 2022, 706; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 76 ff. = NJW 2022, 3135.

Bei der Einführung der §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG hatte der deutsche Gesetzgeber keinen Spielraum, sondern hat sich strikt an den effektiven Willen des EU-Gesetzgebers gehalten, wofür insbesondere spricht, dass er in 25h Abs. 2 KWG die Definition der *Auffälligkeit* aus dem Unionsrecht übernommen hat.[1930] Das Geldwäscherecht ist in dieser Hinsicht vollharmonisiert, weshalb der europäische Grundrechtsschutz einschlägig ist.[1931] Maßstab der Bewertung sind daher die Art. 7, 8 EU-GRC und bewertet werden können §§ 10 Abs. 1 Nr. 5 GwG, 25h Abs. 2 KWG nur einheitlich mit Art. 13 Abs. 1 lit. d) der GWRL.

Beim Transaktionsmonitoring werden Finanztransaktionen von privaten Verpflichteten nicht nur mit externen Selektoren (etwa Staaten auf der *black list*[1932]) zur Einleitung von Sofortmaßnahmen abgeglichen. Es findet auch ein *interner* Abgleich statt, bei dem allein aus der verarbeiteten Datenmenge *Auffälligkeiten* extrahiert werden. Ähnliches findet bei der Vorabprüfung von Fluggästen nach Art. 6 Abs. 2 lit. a) i. V. m. Abs. 3 lit. a), b) PNR-RL statt, weshalb das hierzu ergangene PNR-Urteil als Vorlage für die grundrechtliche Bewertung herangezogen werden kann.

Der EuGH hat in dieser Entscheidung die Vorabprüfung von Fluggästen mit automatisierten Systemen zur Terrorismusbekämpfung und schwerer Kriminalität nicht für grundsätzlich unzulässig erachtet, sondern nur bestimmte Anforderungen aufgestellt. Die wichtigste Anforderung an massenhafte Datenanalysen ist danach, dass solche Systeme auf die Bekämpfung solcher schweren Straftaten im unionsrechtlichen Sinne begrenzt werden, die im Zusammenhang mit der überwachten Datenkategorie stehen.[1933]

Außerdem muss das System so ausgestaltet werden, dass möglichst wenige falsche Treffer erzielt werden, keine Diskriminierung bestimmter Personengruppen etabliert wird und nachteilige weitere Maßnahmen gegenüber dem Betroffenen nur nach menschlicher Entscheidung getroffen werden. *Treffer* des Systems müssen also überprüft werden. Finden aufgrund eines

1930 BT-Drs. 18/11555, S. 176.

1931 BVerfGE 152, 216 (236 ff.) – Recht auf Vergessen II.

1932 Delegierte Verordnung (EU) 2016/1675 der Kommission vom 14. Juli 2016 zur Ergänzung der Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates durch Ermittlung von Drittländern mit hohem Risiko, die strategische Mängel aufweisen, ABl. 2016, L 254/1; konsolidierte Fassung vom 07.02.2021: Document 02016R1675-20210207.

1933 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 153 ff. = EuZW 2022, 706.

Treffers Datenverarbeitungen statt, müssen die Betroffenen benachrichtigt werden.[1934]

Auf das Transaktionsmonitoring lässt sich diese Rechtsprechung, ergänzt nach Art. 52 Abs. 3 EU-GRC durch die Rechtsprechung des EGMR zur (nicht ganz so) ähnlich gelagerten Massenüberwachung von Telekommunikationsleitungen, übertragen, wobei die Unterschiede in den Überwachungssystemen berücksichtigt werden müssen.

Die wohl drängendste Frage dürfte insofern darin liegen, ob das Transaktionsmonitoring nur zur Bekämpfung schwerer Kriminalität eingesetzt wird. Als Massenüberwachungsmaßahme ist sie als besonders intensiver Eingriff zu sehen, der nur insofern gerechtfertigt werden kann.[1935]

Die Terrorismusfinanzierung dürfte zwar unproblematisch als schwere Kriminalität zu fassen sein, bei der Geldwäsche ist dies allerdings fraglich, da der Unrechtsgehalt hier von der Vortat abhängt.[1936] Es bedürfte einer einschränkenden Auslegung dahingehend, dass das Monitoring nur zur Bekämpfung besonders schwerer Fälle von Geldwäsche genutzt werden darf.

Weiter problematisch ist, dass das Anti-Geldwäscherecht eine strikte Geheimhaltung der Verdachtsmeldungen vorsieht, die, immerhin nach menschlicher Prüfung[1937], eine primäre Folge des Transaktionsmonitorings darstellt. Eine effektive gerichtliche oder anders organisierte unabhängige Kontrolle[1938] ist so nicht möglich, was angesichts der Intensität des Monitorings nicht mit den Forderungen von EuGH und EGMR zu vereinbaren sein dürfte.[1939]

1934 Idem, Rn. 210 ff.; EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 357 f. = NVwZ-Beil. 2021, 11.; dazu *B. Huber*, NVwZ-Beilage 2021, 3 (6 f.).

1935 Vgl. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 148 = EuZW 2022, 706; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

1936 BT-Drs. 18/6389, S. 11 ff.; *Böse/S. Jansen*, JZ 2019, 591 (593 f.); *El-Ghazi* in Herzog GwG, StGB § 261 Rn. 28 ff., 144.

1937 Zum Prozess *O. Pauly/Hefter* in Gehra/Gittfried/Lienke ua. (Hrsg.), Prävention Geldwäsche, 2. Aufl. 2020, Kap. 6 Rn. 24 ff.

1938 Vgl. EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 359 ff.

1939 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 210 ff. = EuZW 2022, 706; EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 359 ff. = NVwZ-Beil. 2021, 11.

Die konkreten Anforderungen an die Ausgestaltung des Monitoringprozesses dürften hingegen einer unionsprimärrechtskonformen Auslegung, bei der der EuGH mittlerweile enorm weitgehende Spielräume zulässt,[1940] zugänglich sein. Hier wird es Aufgabe der Aufsichtsbehörden sein, eine grundrechtsschonende Praxis, die möglichst wenige falsche Treffer generiert, insb. durch Richtlinien und Auslegungshinweise, zu etablieren. Eine besondere Rolle spielen insofern die Maßgaben in den Leitlinien der Europäischen Bankenaufsicht i. S. d. Art. 17, 18 GWRL [1941]

b. Aufzeichnung- und Aufbewahrungspflicht nach § 8 GwG, Art. 40 Abs. 1 GWRL

Mit dem Transaktionsmonitoring eng verbunden ist die Obligation der Verpflichteten, alle Informationen, die im Rahmen der Erfüllung der Sorgfaltspflichten erhoben werden oder anfallen, insbesondere Transaktionsbelege, für mindestens fünf Jahre aufzubewahren, § 8 GwG, Art. 40 Abs. 1 GWRL. Da ein effektives Transaktionsmonitoring die Rasterung sämtlicher Transaktionen voraussetzt, bedeutet die geldwäscherechtliche Aufbewahrungspflicht nichts weniger als eine vollständige Bevorratung sämtlicher Kontoauszüge der Kunden von Kreditinstituten und anderen Finanzunternehmen. Diese Aufbewahrungspflicht ist im Kontext mit der Ermächtigung der FIUs zum Zugriff auf sämtliche Finanzdaten bei den Verpflichteten zu lesen, Art. 32 Abs. 9 GWRL, § 30 Abs. 3 GwG.

Speicherpflichten für Wirtschaftsteilnehmer oder Verwaltungsstellen sind nicht automatisch sicherheitsrechtlich relevant, sondern in etlichen Bereichen alltägliche Praxis. Ebenso wenig wird die Tatsache als verfassungsrechtliches Problem behandelt, dass jedenfalls die Staatsanwaltschaft, aber auch die Nachrichtendienste unter strengeren Voraussetzungen, etwa § 8a BVerfSchG, auf existierende Daten bei Privaten grundsätzlich zugreifen dürfen.[1942]

Allein problematisch ist die *Vorrats*datenspeicherung, wenn bestimmte personenbezogene Daten kategorisch – unabhängig davon, auf wen sie sich beziehen und woher sie stammen – als potenziell relevant für die Sicher-

1940 *Thönnes*, Die Verwaltung 2022, 527 (539); *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

1941 *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung).

1942 *Masing*, NJW 2012, 2305 (2309).

heitsgewährleistung eingestuft werden und deshalb verpflichtend vorgehalten werden müssen. In diesen Fällen entzieht sich der Staat im Rahmen der Sicherheitsgewährleistung dem natürlichen Risiko, das ansonsten bei Datensammlungen besteht, und belegt eine bestimmte Datenkategorie mit dem Verdikt einer stetigen Potentialität für die Sicherheitsgewährleistung.

Verfassungsrechtlich sensible Vorratsdatenspeicherungskomplexe zeichnen sich also dadurch aus, dass bestimmten Daten eine kategorische Relevanz zugesprochen wird und deshalb ein Rechtsregime etabliert wird, nach dem diese Daten für Sicherheitsbehörden verfügbar gehalten werden müssen. Aus dieser Kombination folgt denn aber auch, dass die Bewertung von Speicherpflicht und (notwendigen) Zugriffrechten nur in Anbetracht deren Wechselwirkung bzw. Synergie erfolgen kann. Die Intensität und damit Verhältnismäßigkeit der Speicherung hängt mithin von der Ausgestaltung des Zugriffes ab.[1943]

Da im Geldwäscherecht sowohl eine Speicherpflicht als auch ein darauf gemünzter Zugriff geregelt ist, handelt es sich um eine kritische Vorratsdatenspeicherung, auf die die Rechtsprechung von BVerfG und EuGH zur Vorratsdatenspeicherung von TK-Verkehrsdaten übertragen werden muss.[1944]

aa. Maßstab: Europäische Grundrechte und Rechtsprechung des EuGH

Sowohl die fünfjährige Aufbewahrungspflicht bei den Verpflichteten, § 8 GwG (Art. 40 Abs. 1 GWRL), als auch das Zugriffsrecht der FIU nach § 30 Abs. 3 GwG (Art. 32 Abs. 9 GWRL), sind europarechtlich determiniert. Die Mitgliedstaaten dürfen die Aufbewahrungsfrist um fünf Jahre verlängern, wenn sie dies für die Verhinderung, Aufdeckung oder Ermittlung von Geld-

1943 BVerfGE 125, 260 (327 ff.) – Vorratsdatenspeicherung; dazu *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 159; EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 = NJW 2014, 2169; dazu *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.); s.a. EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 97 ff. = EuZW 2022, 706; dazu auch VG Wiesbaden, Urteil v. 06.12.2022 - 6 K 805/19.WI, Rn. 73: „funktionale Einheit".

1944 Dieser Ansatz bei *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.

wäsche oder Terrorismusfinanzierung für erforderlich halten. Art. 40 Abs. 1 UAbs. 2 S. 2, 3 GWRL.

Die Umstände der Übermittlung durch die FIU an andere nationale Sicherheitsbehörden werden von der GWRL hingegen nur grob vorgeschrieben. In Art. 32 Abs. 3 GWRL heißt es nur, dass es der FIU *obliegt, bei begründetem Verdacht auf Geldwäsche, damit zusammenhängende Vortaten oder Terrorismusfinanzierung die Ergebnisse ihrer Analysen und alle zusätzlichen relevanten Informationen an die zuständigen Behörden weiterzugeben.*

Das Anti-Geldwäscherecht schaltet die FIU als Mittler zwischen die privaten Verpflichteten und die Sicherheitsbehörden. Hier besteht ein Unterschied zur Vorratsdatenspeicherung von TK-Verkehrsdaten, da die Daten unmittelbar von den verpflichteten privaten Providern an die verschiedenen *zuständigen Behörden* übermittelt werden sollen, vgl. etwa §§ 176, 177 TKG.

Damit entspricht die GWRL mehr dem Vorratsdatenspeicherungsregime der Flugastüberwachung nach Art. 12 Abs. 1,2, Art. 6 Abs. 2 lit. b) PNR-RL. Auch dort werden den einzelnen operativen Sicherheitsbehörden keine Daten unmittelbar von den Privaten übermittelt. Die Airlines übermitteln nur an die Meldestelle.

Von der Fluggastdatenüberwachung unterscheidet sich das Anti-Geldwäschesystem wiederum dahingehend, dass die Privaten nach der PNR-RL nicht selbst die Speicherung vornehmen. Sämtliche Daten werden bei der PNR-Zentralstelle bevorratet, Art. 12 Abs. 1 PNR-RL.

Für die Frage des grundrechtlichen Maßstabes spielt die Gestaltung des Zugriffswegs in der GWRL allerdings keine Rolle, soweit sie lediglich bestimmt, welche Personen in den Übermittlungsvorgang involviert sind. Entscheidend sind die Voraussetzungen, unter denen die Sicherheitsbehörden schließlich zum Zugriff auf die Daten berechtigt sein sollen. Das lässt die GWRL offen.

Das BVerfG nahm die fehlende Determinierung des Zugriffs auf europarechtlicher Ebene im Urteil zur Vorratsdatenspeicherung von TK-Verkehrsdaten zum Anlass, nicht nur die Zugriffsrechte, sondern auch die Ausgestaltung der Speicherpflicht an den Grundrechten des Grundgesetzes zu überprüfen,[1945] obwohl die VDS-RL schon eine Mindestfrist vorsah und damit keinen Gestaltungsspielraum mehr eröffnete. Das ist nicht überzeugend.

1945 BVerfGE 125, 260 (308 ff.) – Vorratsdatenspeicherung.

Diese Rechtsprechung wurde zu Recht als mit der ständigen „Solange II"-Rechtsprechungslinie inkohärent kritisiert[1946] und kann auch mit der jüngeren Rechtsprechung des BVerfG zum Verhältnis deutscher und europäischer Grundrechte[1947] nicht vereinbar werden.

Soweit die Speicherpflicht geprüft werden soll, müssen vorrangig europäische Grundrechte angewandt werden, da die Speicherung der Transaktionsdaten in Form von Buchungsbelegen bzw. Kontoauszügen, digital oder analog, strikt von Art. 40 Abs. 1 lit. b) GWRL vollumfänglich vorgegeben wird.

Dem BVerfG ist zwar darin zuzustimmen, dass sich die Bewertung der Speicherpflichten nur anhand der Zugriffsregeln bestimmen lässt. Dies kann aber nicht dazu führen, dass für die Speicherpflichten eine Teilharmonisierung angenommen wird. Vielmehr wirkt sich die Unbestimmtheit der Zugriffsregelung in der Richtlinie auf die Verhältnismäßigkeit der auf dieser Ebene angesiedelten Speicherpflicht aus. Andernfalls läge es an den Mitgliedstaaten, durch eine grundrechtskonforme Ausgestaltung die Grundrechtskonformität der Richtlinie sicherzustellen. Eine solche Entlastung des europäischen Gesetzgebers ist in der EU-GRC nicht angelegt. Wenn der europäische Gesetzgeber Massenüberwachungsmaßnahmen einführt, bei denen die Verhältnismäßigkeit der einzelnen Eingriffe sich aus der Wechselwirkung bzw. Synergie der einzelnen Verarbeitungsschritte ergibt, ist er gehalten, bereits auf Richtlinienebene dafür zu sorgen, dass die Verhältnismäßigkeit sämtlicher Verarbeitungsschritte gewahrt bleibt.

Entgegen dem Vorratsdatenspeicherungsurteil des BVerfG ist also von einer Vollharmonisierung der Speicherpflichten auszugehen, obwohl die Zugriffsregeln in der Richtlinie nicht umfangreich formuliert werden.

bb. Bewertung: Analogie zur Vorratsdatenspeicherung von Verkehrs- und PNR-Daten

Zur Verhältnismäßigkeit einer universellen Vorratsdatenspeicherung nach den Unionsgrundrechten hat sich der EuGH in einer ganzen Reihe von

1946 *Westphal*, EuZW 2010, 494 (497 f.); *Szuba,* Vorratsdatenspeicherung, 2011, S. 239 ff.; *Wolff*, NVwZ 2010, 751 (751).

1947 BVerfGE 152, 152 – Recht auf Vergessen I; BVerfGE 152, 216 – Recht auf Vergessen II; dazu *Lehner*, JA 2022, 177.

Urteilen geäußert. Ausgehend von der Aufhebung der VDS-RL[1948] prüfte der Gerichtshof eine ganze Reihe nationaler Speicherpflichten von TK-Verkehrsdaten.[1949]

(1) Grundsätzliche Unzulässigkeit universeller Vorratsdatenspeicherung

Kernanspruch dieser Rechtsprechung ist es zu verhindern, dass Daten zu Sicherheitszwecken vorratsmäßig gespeichert werden, ohne dass im Moment der Speicherung ein Zusammenhang zwischen den Daten und den verfolgten Zwecken besteht.[1950] Das ursprüngliche, grundsätzliche Verbot der Vorratsdatenspeicherung wurde mittlerweile mit zahlreichen Ausnahmen so ausgestaltet, dass ebenfalls nicht mehr von einem absoluten Verbot, sondern von einer Prozeduralisierung gesprochen werden muss.[1951]

Eine universelle Speicherung von TK-Verkehrsdaten ist danach zulässig, wenn diese der nationalen Sicherheit dient und nur in Zeiträumen eingesetzt wird, in denen die nationale Sicherheit aufgrund einer besonderen Lage akut bedroht wird.[1952] Zur Bekämpfung (allgemeiner) schwerer Kriminalität ist eine universelle Speicherung nicht zulässig. Hier kommt nur eine *targeted retention*[1953] in Betracht, also eine Speicherung, die auf bestimmte Orte oder Personenkreise begrenzt wird, von denen ein Zusam-

1948 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

1949 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.) = NJW 2017, 717; Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531; Urteil v. 6.10.2020, C-623/17 (Privacy International) = GSZ 2021, 36; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom) = NJW 2022, 3135.

1950 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 118 = EuZW 2022, 706; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 70 = NJW 2022, 3135.

1951 Vgl. *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143; übersichtlich die Tabelle bei *Mitsilegas/Guild/Kuskonmaz ua.*, European Law Journal 2022 (online preprint), 1 (7).

1952 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 137 = NJW 2021, 531.

1953 Vgl. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (101); *Cameron*, Common Market Law Rev. 58 (2021), 1433 (1449); *Eskens*, Europ. Data Protection Law Rev. 8 (2022), 143 (149).

menhang mit schwerer Kriminalität zu erwarten ist.[1954] Auch kommt das anlassbezogene „Quick-freeze"-Verfahren[1955] in Betracht, bei dem die Provider auf Anordnung zukunftsgerichtet Verkehrsdaten einer verdächtigen Person oder deren Umfeld speichern.[1956]

Noch weniger streng verhält es sich mit der Speicherung (dynamischer) IP-Adressen[1957] und PNR-Daten.[1958] Bei diesen kommt eine universelle Vorratsdatenspeicherung grundsätzlich in Betracht, wenn sie (zeitlich) auf das Notwendige beschränkt werden, und *sofern diese Möglichkeit von der strikten Einhaltung der materiellen und prozeduralen Voraussetzungen abhängig gemacht wird, die die Nutzung dieser Daten regeln müssen.*[1959]

Welche Speicherdauer dabei das maximal absolut Notwendige darstellt, legte der EuGH nur für die PNR-RL fest. Hier entschied er, dass eine anlasslose Speicherung maximal für sechs Monate in Betracht kommt.[1960] Nur solche Daten, die im Rahmen der Vorabprüfung auffällig wurden und daher im Verdacht stehen durften, eventuell für die Bekämpfung schwerer Kriminalität oder Terrorismus relevant zu werden, könnten länger gespeichert werden. Auch für solche Daten gilt aber die Pflicht zur Depersonalisierung nach sechs Monaten gem. Art. 12 Abs. 2 PNR-RL.

Übertragen auf das Transaktionsmonitoring bzw. die sich anschließende Speicherung zu Sicherheitszwecken bedeutet dies, dass eine sicherheitsrechtliche Speicherung bei den Verpflichteten eigentlich nur für sechs Mo-

1954 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 140 ff. = NJW 2021, 531; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 105 ff. = NJW 2022, 3135;

1955 Dazu *Juszczak/Sason*, eucrim 2021, 238 (247); zur Rechtslage in der StPO: *Rückert* in MüKo StPO, § 100g Rn. 116; mittlerweile liegt allerdings ein Referentenentwurf des *BMJ* vor https://kripoz.de/wp-content/uploads/2022/10/refE-quick-freeze.pdf, zuletzt aufgerufen am 12.01.2025.

1956 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 163 ff. = NJW 2021, 531; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 95 ff. = NJW 2022, 3135.

1957 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 152 ff. = NJW 2021, 531; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), Rn. 95 ff. = NJW 2022, 3135.

1958 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 248 ff. = EuZW 2022, 706;

1959 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), 155 = NJW 2021, 531; Urteil v. 20.9.2022, C-793/19, C-794/19 (SpaceNet AG/Telekom), 101 = NJW 2022, 3135; s.a. Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 253 i. V. m. Rn. 214 ff. = EuZW 2022, 706.

1960 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 255 = EuZW 2022, 706.

nate ab Erhebung zulässig sein dürfte. Da aber eine Löschung aufgrund anderer Speicherpflichten nicht in Betracht kommt, ist die Frist so zu verstehen, dass nur in dieser Zeit eine Verwendung der Daten zur Bekämpfung von Geldwäsche oder Terrorismusfinanzierung zulässig ist (dazu sogleich (3)). Es besteht also die Pflicht, möglichst bald nach Erhebung mit dem Monitoring zu verfahren. Dies hat zur Folge, dass der Turnus des Monitorings in möglichst geringen Zeitabständen stattzufinden hat.

(2) Keine universelle Speicherung von Finanzdaten bei der FIU länger als sechs Monate

Dies gilt gleichermaßen für die Speicherung von Verdachtsmeldungen bei der FIU (s. Kap. D. III. 2. c. dd.)). Diese müssen prinzipiell gelöscht werden, wenn sich i. R. d. Analyse herausgestellt hat, dass es sich nicht um geldwäscheauffällige bzw. verdächtige Transaktionen handelt. Die entsprechende Analyse muss also möglichst bald stattfinden und entsprechend schnell geprüft werden, ob sicherheitsrechtlich erkennbar irrelevante Daten gespeichert sind.[1961]

Eine Speicherung bei der FIU darf also maximal für sechs Monate erfolgen, es sei denn, es stellt sich innerhalb dieser Zeit heraus, dass die Daten für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung relevant sein könnten.

Eine entsprechende Auslegung des Geldwäscherechts ist durchaus möglich. Im nationalen Recht kann die Begrenzung in § 37 Abs. 2 GwG hineininterpretiert werden, wonach die FIU gespeicherte personenbezogene Daten löscht, *wenn die Speicherung dieser Daten unzulässig ist oder die Kenntnis dieser Daten für die Aufgabenerfüllung nicht mehr erforderlich ist*. In der GWRL findet sich eine entsprechende Regel zwar nicht, lässt sich aber aus dem sekundärrechtlichen Datenschutzrecht konstruieren. Insofern bedarf es auch keiner Festlegung, ob für die FIU die JI-RL oder die DSGVO gilt,[1962] da sowohl Art. 5 JI-RL als auch Art. 17 Abs. 1 DSGVO eine Löschpflicht vorsehen, wenn der Grund einer Datenspeicherung entfällt.

1961 Krit. zu BT-Drs. 19/2263, S. 8 f. insofern *Barreto da Rosa* in Herzog GwG, § 37 Rn. 10.

1962 dazu *Quintel*, ERA Forum 2022, 53 (61 ff.); *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (11 ff.).

(3) Keine Unzulässigkeit einer universellen Speicherpflicht von Finanzdaten bei Verpflichteten

Die fünfjährige Aufbewahrungspflicht der Verpflichteten (Kreditinstitute, Zahlungsdienstleister etc.) nach Art. 40 Abs. 1 GWRL, die auch Finanzdaten umfasst, die i. R. d. Monitoring unauffällig blieben, ist also eigentlich nicht mit Art. 7,8 EU-GRC zu vereinbaren.

Die Speicherung von Finanztransaktionsdaten unterscheidet sich gegenüber den bekannten Vorratsdatenspeicherung jedoch darin, dass es sich nicht um eine originäre Anordnung der Speicherung handelt, sondern diese neben einer Vielzahl bestehender Pflichten im Wirtschaftsrecht tritt, § 675d BGB, Art. 248 EGBGB, §§ 25a KWG, 257 HGB, 22 UStG, 147 AO, Art. 5 SEPA-VO (dazu Kap. D. II.).[1963] Die Transaktionsdaten müssen auch nicht separat gespeichert werden. Eine Löschpflicht der Verpflichteten nach sechs Monaten käme insofern also praktisch kaum in Betracht. Darauf nimmt auch Art. 40 Abs. 1 UAbs. 2 S. 1 GWRL Rücksicht, der die Löschpflicht entfallen lässt, wenn die Daten nach anderen nationalen Regeln gespeichert werden müssen. Aufgrund dieses speziellen Umstands erlangt abermals die Kombination von Speicherung und Zugriff Bedeutung.

Wie sich an § 675d BGB, Art. 248 EGBGB, §§ 25a KWG, 257 HGB, 22 UStG, 147 AO, Art. 5 SEPA-VO exemplifizieren lässt, ist die Speicherung der Transaktionsdaten an sich noch nicht von grundrechtlicher Sensibilität. Die Aufbewahrung von Kontodaten ist geübte Alltagspraxis und entspricht dem Wissen und meist sogar dem Willen der Betroffenen, die ihre Ausgaben auch nach einiger Zeit noch nachvollziehen wollen.

Dass Kontodaten somit theoretisch stets von den Sicherheitsbehörden erlangt werden können,[1964] ist also nicht das Problem, dem sich die sicherheitsverfassungsrechtlichen Grundsätze widmen sollen. Diese sind vielmehr als Reaktion auf eine Entwicklung zu verstehen, die von der traditionellen Ermittlung immer weiter Abstand nimmt.[1965]

Da die grundrechtliche Sensibilität insofern nicht aus der Speicherung (bei den Privaten) als solcher, sondern aus der spezifischen Bevorratung für konkrete Zugriffe herrührt, müssen sicherheitsrechtliche Speicherpflichten,

1963 Zum Gleichlauf der Fristen *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438.

1964 *Masing*, NJW 2012, 2305 (2309).

1965 Vgl. *Albers,* Determination, 2001, S. 111 ff.; *Bäcker,* Kriminalpräventionsrecht, 2015, S. 35 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (S. 253 ff.); *ders.*, Die Verwaltung 2008, 345 (345 ff.).

die nicht originär zur Speicherung führen, sondern letztlich nur einen Zweck ergänzen, allein auf der Zugriffsebene eingehegt werden.

Das Verbot einer universellen Speicherung von TK-Verkehrsdaten kann also nicht einfach auf Finanz- bzw. Kontotransaktionsdaten angewandt werden. Diesen Punkt übersehen die bislang erschienenen Ausführungen zur grundrechtlichen Bewertung der Geldwäschebekämpfung.

Die Rechtsprechung des EuGH kann nicht formalistisch auf sämtliche Datenspeicherungen übertragen werden, sondern muss entsprechend ihrer Zielsetzung Anwendung finden. Dabei darf man das Verbot der universellen Vorratsdatenspeicherung nicht als Versuch begreifen, den sogenannten digitalen Fußabdruck einer Person in jeder Hinsicht zu verwaschen. Es gibt kein allgemeines Datenspeicherungsverbot. Ein solches kann es auch nicht geben. Die Vorstellung, dass Informationen über eine Person generell nur für einen Zeitraum über maximal wenige Monate verkörpert werden dürfen, ist geradezu absurd. Das offenbaren schon die verschiedenen Speicherpflichten des Wirtschaftsrechts. Die Urteile zur Vorratsdatenspeicherung sind deshalb nur in ihrem konkreten sicherheitsrechtlichen Kontext zu verstehen.

Indem sich der Staat eine bestimmte Datenkategorie aussucht, für die es im Übrigen (meistens ausnahmsweise) keine Gründe zur Aufbewahrung gibt, und für diese nur deswegen eine Speicherpflicht anordnet, weil er davon ausgeht, dass diese Daten grundsätzlich sicherheitsrechtlich relevant werden können, verdreht er den Grundsatz des Vertrauens in die Rechtstreue seiner Bürger ins Gegenteil. Die Betroffenen werden unter Generalverdacht gestellt.[1966] Dieser Umstand lag der grundrechtlichen Sensibilität der sicherheitsrechtlichen Verkehrsdatenspeicherung zugrunde und nicht die bloße Tatsache, dass bestimmte Daten längerfristig gespeichert werden. Die TK-Vorratsdatenspeicherung war im eigentlichen Sinne also gar kein Datenschutzproblem, sondern eine fulminante Abkehr von sicher geglaubten Grundsätzen des Rechtsstaats (Kap. B. III. 2. c.).[1967]

Daraus folgt, dass nicht jeder Anordnung von Speicherpflichten im Sicherheitsrecht nach den Maßstäben der Urteile zur Vorratsdatenspeiche-

1966 Zur Verkehrsdatenspeicherung *Orantek* NJ 2010, 193 (195); *Breyer,* StV 2007, 214 (217); allg. *Barczak,* Der nervöse Staat, 2. Aufl. 2021, S. 493 ff.; *Lepsius* in Schuppert/Merkel/Nolte ua. (Hrsg.), Rechtsstaat, 2010, S. 23 (31 f.); vgl. auch *B. Hirsch* in Huster/Rudolph (Hrsg.), Präventionsstaat, 2008, S. 164 (166 ff.).

1967 *Puschke/Singelnstein,* NJW 2008, 113 (118); *Szuba,* Vorratsdatenspeicherung, 2011, S. 196 ff. in diese Richtung auch *Lisken, ZRP* 1990, 15 (17 ff.); *ders., ZRP* 1994, 264 (267 f.); übersichtlich *K. Weber,* Polizeirecht, 2011, S. 79 ff.

rung begegnet werden muss, sondern nur, wenn dies zur Einhaltung einer rechtsstaatlichen Sicherheitsgewährleistung notwendig ist.

Das Ziel der Rechtsprechung von EuGH, BVerfG und EGMR muss darin gesehen werden, einer Unterwanderung rechtsstaatlicher Anforderungen an das Sicherheitsrecht durch Massenüberwachungsmaßnahmen entgegenzuwirken. Es geht längst nicht mehr darum, die anlasslose Massenüberwachung grundsätzlich zu verbieten,[1968] sondern dieser einen Rahmen zu geben.[1969] Ein solcher Rahmen kann aber nicht durch das Aufstellen möglichst formalistischer Aussagen über die Zulässigkeit von Datenverarbeitungen geschaffen werden, sondern verlangt eine spezifische Prozeduralisierung der jeweiligen Massenüberwachungsmaßnahme.

Eine Aufhebung der geldwäscherechtlichen Speicherpflichten der Verpflichteten würde sich auf die Verfügbarkeit der Daten nicht auswirken. Diese Eigenheit führt dazu, dass es keiner unmittelbaren Übertragung der Grundsätze der Rechtsprechung zur TK-Verkehrsdatenspeicherung bedarf, sondern einer im konkreten Fall angemessenen Gestaltung.

Nur soweit durch die GWRL ein Zugriff zu sicherheitsrechtlichen Zwecken geschaffen wird, der die Anforderungen und faktischen Schwierigkeiten klassischer Maßnahmen umgeht, müssen die Grundrechte einhegend wirken.

c. Zugriffsrechte der FIU, Art. 32 Abs. 9 GWRL; § 30 Abs. 3 GwG

Da bei den Verpflichteten eine Speicherung unabhängig von den Vorschriften des Geldwäscherechts erfolgt, muss die Verhältnismäßigkeit der Speicherpflicht durch eine grundrechtskonforme Gestaltung des Zugriffs gewährleistet werden. Andernfalls würden die klassischen Ermittlungsanforderungen durch die geldwäscherechtlichen Zugriffe weiterhin ausgehöhlt werden. Die Wechselwirkung von Speicherpflicht und Zugriff erstreckt sich dabei auch auf die weitere Übermittlung, da von deren Gestaltung die Verhältnismäßigkeit des Zugriffs abhängt.

1968 BVerfGE 141, 220 (272) – BKA-Gesetz.

1969 *Tzanou/Karyda,* European Public Law 28 (2022), 123 (153 f.); s.a. *Albers* in Albers/Sarlet (Hrsg.), Data Protection, 2022, S. 69 (104 ff.).

aa. Maßstab: Grundrechtsparallelität mit primärer Anwendung der EU-GRC

Die Ausgestaltung der Zugriffsrechte wurde in den von der Rechtsprechung schon behandelten Modellen nur teilweise vom EU-Recht determiniert, was den Abgleich mit der GWRL erschwert.

Art. 4 VDS-RL verlangte lediglich, dass die Mitgliedstaaten den Zugang zu den Verkehrsdaten auf *Einzelfälle* beschränkten und das *Verfahren und die Bedingungen für den Zugang zu auf Vorrat gespeicherten Daten* so festlegten, *dass sie den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit* entsprachen. Eine Beschränkung des Zugangs schon auf europäischer Ebene auf die Übermittlung etwa nur zu bestimmten Zwecken oder nur bei Überschreiten bestimmter Prognoseschwellen, enthielt die Richtlinie nicht und wurde (auch) deshalb insgesamt für unverhältnismäßig befunden und aufgehoben.[1970]

Konsequenterweise sieht die jüngere PNR-RL deshalb konkrete Anforderungen an die Verwendung der gespeicherten PNR-Daten durch die national zuständigen Behörden vor. Nach Art. 6 Abs. 2 lit. b) PNR-RL dürfen PNR-Daten nur *im Einzelfall* übermittelt werden, zur Beantwortung, *auf einer hinreichenden Grundlage gebührend begründeten Anfragen in besonderen Fällen zum Zwecke der Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten oder schwerer Kriminalität.* Der EuGH hat diese notwendige Zugangsbeschränkung im Wege der Auslegung noch weiter dahingehend eingeschränkt, dass die zu verhütenden oder verfolgenden Delikte im Zusammenhang mit der Beförderung von Fluggästen stehen müssen.[1971]

Der EuGH betrachtete den Zugriff auf gespeicherte PNR-Daten aber nicht nur als Bestandteil der PNR-Vorratsdatenspeicherung, sondern als Teil des gesamten PNR-Überwachungskonzepts und leitete daraus weitere Einschränkungen ab. Da die gespeicherten Daten bereits im Rahmen der automatisierten Analyse zum Gegenstand einer Überwachungsmaßnahme wurden und die Frage eines Zusammenhangs der jeweiligen Daten mit sicherheitsrechtlichen Zwecken schon geprüft wurde, steht eine spätere Zur-

1970 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 ff. = NJW 2014, 2169.

1971 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 217 = EuZW 2022, 706.

verfügungstellung unter der weiteren Einschränkung, dass *neue* Umstände vorliegen, die eine Übermittlung notwendig machen.[1972]

Für die Ausgestaltung von Zugangsregeln im Rahmen von Vorratsdatenspeicherungskomplexen besteht also eine doppellagige Grundrechtsprüfung. Zunächst müssen schon auf der EU-rechtlichen Ebene bestimmte Standards gewahrt werden, die sich aus einer Operationalisierung des Verhältnismäßigkeitsgrundsatzes ergeben. Darüber hinaus muss die Ausgestaltung der Zugriffsregeln durch Mitgliedstaaten den nationalen- und Unionsgrundrechten entsprechen, wenn sie über die Mindestanforderungen der Richtlinie hinausgehen.

bb. Bewertung des Zugriffsrechts der FIU unter Berücksichtigung der Übermittlungspflicht auf Richtlinienebene

Vorliegend bestehen erhebliche Zweifel, ob die Zugangseinschränkungen der GWRL den Anforderungen der Rechtsprechung genügen.

Zunächst muss untersucht werden, ob die Gestaltung des Zugriffs der FIU auf Kontoinhaltsdaten in der GWRL überhaupt mit Art. 7, 8 EU-GRC vereinbart werden kann. Dabei ist zunächst zu beachten, dass es sich um einen Zugriff auf vorratsmäßig gespeicherte Daten handelt und deshalb mit der umfassenden Speicherpflicht eine Wechselwirkung besteht. Darüber hinaus dient der Zugriff der FIU final der Weiterleitung an operative Sicherheitsbehörden.

Die Verhältnismäßigkeitsanforderungen von Speicherung, Zugriff und Weiterleitung ergeben sich aus einer komplexen Betrachtung sämtlicher dieser Verarbeitungsschritte der FIU. Die Intensität eines jeden Verarbeitungsschrittes lässt sich nur begreifen, wenn die Verarbeitungsschritte als Teil eines zusammenhängenden Überwachungskomplexes betrachtet werden (Kap. B. I. 1. c.).

Eine Datenzugriffsermächtigung im Rahmen eines sicherheitsrechtlichen Gesetzes, das eigenständig auch eine Speicherpflicht der jeweiligen Daten anordnet, kann demnach einen intensiveren Grundrechtseingriff darstellen als eine vergleichbare Zugriffsermächtigung in einem Gesetz, das eine solche Speicherpflicht nicht vorsieht. (etwa ein staatsanwaltliches Herausgabeverlangen nach § 95 Abs.1 StPO). Obwohl die Zugriffe jeweils separat

1972 Idem, Rn. 218; EuGH, Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 200. – PNR Canada = ZD 2018, 23.

betrachtet denselben Informationseingriff darstellen, unterscheiden sich die jeweiligen Ermächtigungen fundamental.

Es ist hier stets der Einzelfall zu betrachten, da unterschiedliche Umstände die Intensität eines Informationseingriffs beeinflussen. Insbesondere kommt es auf den Charakter und die übrigen Befugnisse der Behörde an, die zum Zugriff ermächtigt wird.[1973]

(1) Umfangreiche Auskunftsrechte und Weiterleitungspflichten der FIU

Nach Art. 32 Abs. 9 GWRL kann jede zentrale Meldestelle *im Rahmen ihrer Aufgaben von jedem Verpflichteten Informationen für den in Absatz 1 genannten Zweck anfordern, einholen und nutzen, selbst wenn keine vorherige Meldung erstattet wurde.*

Nach Art. 32 Abs. 4 S. 2 GWRL muss sie in der Lage sein, *Auskunftsersuchen der zuständigen Behörden ihres jeweiligen Mitgliedstaats zu beantworten, sofern die Auskunftsersuchen auf Belangen im Zusammenhang mit Geldwäsche, damit im Zusammenhang stehenden Vortaten oder Terrorismusfinanzierung beruhen.*

Außerdem hat die FIU gem. Art. 32 Abs. 3 S. 3 GWRL *bei begründetem Verdacht auf Geldwäsche oder damit zusammenhängende Vortaten oder Terrorismusfinanzierung die Ergebnisse ihrer Analysen und alle zusätzlichen relevanten Informationen an die zuständigen Behörden weiterzugeben.*

Die GWRL sieht also, unabhängig davon, dass der FIU von den Verpflichteten massenweise Daten im Rahmen der Meldepflichten geliefert werden, ein umfassendes Zugriffsrecht der FIU vor und verpflichtet diese sowohl zur proaktiven Weiterleitung als auch zur Beantwortung von Auskunftsersuchen, ohne dafür besondere Einschränkungen zu statuieren.

Die proaktive Weiterleitung wird sich allerdings auf Daten beschränken, die der FIU von den Verpflichteten gemeldet und von der FIU weiter analysiert und für verdächtig befunden wurden. Insofern besteht also kein mittelbarer Datenzugriff von Sicherheitsbehörden auf (anlasslos gespeicherte) Vorratsdaten, sondern ein Zugang von Daten von außen. Diese Übermittlungsrichtung muss zwar ebenfalls bestimmte Gestaltungsanforderungen erfüllen, da von den Meldepflichten der Privaten und Weiterleitungspflichten der FIU aufgrund der Wechselwirkung die Rechtmäßigkeit des Monito-

1973 Vgl. BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.) – Antiterrordatei II; NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; *Gusy*, GA 1999, 319 (327); *Gärditz*, JZ 2013, 633 (634); näher dazu unten (III.3.a).

rings abhängt (III. 2. a. cc. (4). (a)). An dieser Stelle spielt er aber keine Rolle.

Die Rechtmäßigkeit des Zugriffsrechts der FIU ist hier vielmehr als Teil eines Vorratsdatenspeicherungskomplexes zu untersuchen und hängt demnach von der Frage ab, inwiefern über dieses Zugriffsrecht den operativen Sicherheitsbehörden ein mittelbarer, aber eigens veranlasster Zugriff zu (nicht gemeldeten) Daten bei Privaten eingeräumt wird.

(a) Zugriffsrecht der FIU, Art. 32 Abs. 9 GWRL

Bis zum Erlass der 5. GWRL war nicht klar, unter welchen Voraussetzungen ein solcher Zugang bestehen sollte. Die einzige Norm in der 4. GWRL, die einen Zugriff der FIU auf Informationen der Verpflichteten vorsah, war Art. 31 Abs. 3 S. 4 der 4. GWRL. Dieser verlangt, dass die FIUs in der Lage *sind, von den Verpflichteten zusätzliche Informationen einzuholen.*

Der deutsche Gesetzgeber verstand diese Norm als Auftrag zur Schöpfung einer allgemeinen Zugriffermächtigung der FIU auf Finanzinformationen der Verpflichteten und setzte sie durch Einführung des § 30 Abs. 3 GwG[1974] um[1975]. Nach § 30 Abs. 3 S. 1 GwG kann die FIU unabhängig *vom Vorliegen einer Meldung Informationen von Verpflichteten einholen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.* Tatsächlich dürfte es sich um eine übererfüllende Umsetzung gehandelt haben, da Art. 32 Abs. 3 S. 4 der 4. GWRL im Zusammenhang mit Verdachtsmeldungen stand und daher eher als Erlaubnis zu Rückfragen bzgl. ergangener Verdachtsmeldungen zu verstehen ist.[1976]

Diese Streitfrage wurde mit der 5. GWRL entschärft, in der der klarstellende Art. 32 Abs. 9 GWRL eingeführt wurde. Danach kann jede FIU *unbeschadet des Artikels 34 Abs. 2 im Rahmen ihrer Aufgaben von jedem Verpflichteten Informationen für den in Art. 32 Abs.1 genannten Zweck anfordern, einholen und nutzen, selbst wenn keine vorherige Meldung erstattet wurde.* Damit korrespondiert Art. 33 Abs. 1 lit. b) GWRL, wonach *die Verpflichteten der zentralen Meldestelle auf Verlangen unmittelbar oder mittelbar alle erforderlichen Auskünfte gemäß den im geltenden Recht festgeleg-*

1974 Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017 (BGBl. I, S. 1822).

1975 BT-Drs. 18/11555, S. 141.

1976 *Barreto da Rosa* in Herzog GwG, § 30 Rn. 17.

ten Verfahren zur Verfügung stellen. Über solche Auskünfte müssen die Verpflichteten unter Androhung von Bußgeldern Stillschweigen bewahren, Art. 39 Abs. 1, 59 Abs. 1 lit. b) GWRL. Es handelt sich also um eine Ermächtigung der FIU zu heimlichen Auskünften.

Art. 32 Abs. 9 GWRL sieht demnach eine umfangreiche Zugriffsnorm der FIU auf Finanzinformationen vor,[1977] während Art. 32 Abs. 3 S. 4 auf Rückfragen zu eingegangenen Verdachtsmeldungen beschränkt bleibt. Systematisch regelt Art. 32 Abs. S. 3, 4 GWRL damit den proaktiven Übermittlungsweg der FIU an die Sicherheitsbehörden, während Auskunftsersuchen der Sicherheitsbehörden, die auf deren eigener Ermittlungen basieren, in Art. 32 Abs. 4 GWRL geregelt sind.

(b) Übermittlungspflicht der FIU, Art. 32 Abs. 4 S. 2 GWRL

Die FIUs müssen nach Art. 32 Abs. 4 S. 2 GWRL in der Lage sein, *Auskunftsersuchen der zuständigen Behörden ihres jeweiligen Mitgliedstaats zu beantworten, sofern die Auskunftsersuchen auf Belangen im Zusammenhang mit Geldwäsche, damit im Zusammenhang stehenden Vortaten oder Terrorismusfinanzierung beruhen.*

Ergänzt wird diese Regelung durch Art. 6 FinanzinformationsRL, wonach ein Austausch von *Finanzinformationen* auch zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung schwerer Straftaten erfolgen soll. Dabei werden Finanzinformationen definiert als *alle Arten von Informationen oder Daten, wie Daten über finanzielle Vermögenswerte, Geldbewegungen oder finanzgeschäftliche Beziehungen, die bereits bei zentralen Meldestellen vorhanden sind, um Geldwäsche und Terrorismusfinanzierung zu verhüten, aufzudecken und wirksam zu bekämpfen*, Art. 2 Nr. 5 FinanzinformationsRL.

Unter welchen konkreten Bedingungen eine Auskunft an die Sicherheitsbehörden erfolgt, schreiben die Richtlinien aber nicht vor. Sie überlassen den Mitgliedstaaten einen weiten Spielraum.

(c) Mittelbarer Zugriff operativer Sicherheitsbehörden

Betrachtet man die Übermittlungspflichten und die Auskunftsrechte der FIU hiernach in einer Gesamtschau, ergibt sich ein Bild, das zahlreiche

1977 Zu § 30 Abs. 3 GwG siehe *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (242 ff.).

Mängel des geldwäscherechtlichen Vorratsdatenspeicherungssystems offenlegt.

Über Art. 32 Abs. 9 GWRL ist der FIU ein umfangreicher Zugriff auf Finanzinformationen bei den Verpflichteten eingeräumt, der nur dadurch begrenzt ist, dass die Informationen den Aufgaben der FIU dienen sollen. Zu den Aufgaben der FIU gehört insbesondere der Informationsaustausch mit staatlichen Sicherheitsbehörden, wenn dieser Austausch der Bekämpfung von Geldwäsche und Terrorismusfinanzierung dient, Art. 32 Abs. 4 S. 2 GWRL. Dies bedeutet, dass, unabhängig von etwaigen Verdachtsmeldungen, die FIU auf Auskunftsersuchen von Sicherheitsbehörden hin, heimlich entsprechende Informationen bei den Verpflichteten abrufen könnte, da sie nur so ihrer Aufgabe der Informationsversorgung nachkommt.[1978] Über diesen Umweg erhielten also Sicherheitsbehörden die Möglichkeit, heimlich auf vorratsmäßig gespeicherte Finanzdaten zuzugreifen, ohne dass hierbei irgendwelche materiellen Einschränkungen oder formelle Absicherungen vorgesehen wären.

An dieser Stelle muss die Finanzinformations-RL beachtet werden. Diese regelt die Übermittlung von Finanzinformationen zur Bekämpfung schwerer Kriminalität, die nicht in Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung stehen.

Die Möglichkeit solcher Übermittlungen durch die FIU ist nach Art. 7 Abs. 1 Finanzinformations-RL nur an eine spezielle Behörde erlaubt, die nach Art. 3 Abs. 2 Finanzinformations-RL von jedem Mitgliedstaat eigens benannt werden muss. Im GwG wurde das BKA nach § 32 Abs. 3a GwG als Behörde nach Art. 3 Abs. 2 Finanzinformations-RL benannt. Die FIU kann Finanzinformationen zur Bekämpfung schwerer Kriminalität, die nicht in Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung stehen, nach § 32 Abs. 3a GwG an das BKA übermitteln.

Nach Art. 2 Nr. 5 Finanzinformations-RL gelten dabei nur solche Daten als (übermittelbare) Finanzinformationen, die bei der FIU schon vorliegen. Es ist der FIU also verwehrt, bei Ersuchen der nach Art. 3 Abs. 2 Finanzinformations-RL benannten Stelle, die auf die Bekämpfung allgemeiner schwerer Kriminalität gerichtet ist, aktiv tätig zu werden und die angefragten Informationen zu beschaffen. In diesem Rahmen ist den Sicherheitsbehörden also kein Zugriff auf die vorratsmäßig bei den Privaten gespeicherten Daten eingeräumt, sondern nur auf die Daten der FIU, die immerhin aufgrund der Verdachtsmeldeschwelle und der Analysetätigkeit in gewissem

1978 Vgl. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157.

Maße begrenzt sind. Art. 7 Abs. 1 Finanzinformations-RL, bzw. § 32 Abs. 3a GwG soll daher bei der folgenden Prüfung außen vor bleiben.

(2) Vereinbarkeit von Art. 32 Abs. 9, Abs. 4 S. 2 GWRL mit Art. 7, 8 EU-GRC durch Auslegung?

Ob die Ausgestaltung der Zugriffsrechte und Übermittlungspflichten der FIU auf unionsrechtlicher Ebene, Art. 32 Abs. 9 i. V. m. Abs. 4. S. 2 GWR, mit Art. 7, 8 EU-GRC vereinbart werden kann, ergibt sich aus der Rechtsprechung des EuGH zur TK- und PNR-Vorratsdatenspeicherung.

Zugriffsrechte und Übermittlungspflichten sind dabei im Komplex zu prüfen, da die Verhältnismäßigkeit des Zugriffs von der Gestaltung der Übermittlungspflicht abhängt (Kap. B. I. 1. c.). Zwar hat der EuGH im PNR-Urteil die massenhafte Übermittlung von Daten durch Private an eine zentrale Stelle nicht grundsätzlich beanstandet.[1979] Daraus folgt aber noch nicht, dass die zentrale Stelle auf Anruf der operativen Sicherheitsbehörden ohne weitere Voraussetzungen als deren Datenvermittlerin tätig werden kann. Vielmehr ist die Verhältnismäßigkeit der massenhaften Sammlung von PNR-Daten bei einer zentralen Stelle davon abhängig gemacht worden, dass die Daten von dort aus nur unter engen Voraussetzungen weitergeleitet werden können.[1980]

Wenn das Unionsrecht einen Vorratsdatenspeicherungskomplex per Richtlinie anordnet, fordert der EuGH, dass bereits in der Richtlinie die Bedingungen und Verfahrensschritte eines Zugriffs auf vorratsmäßige Daten geregelt werden. Andernfalls wäre schon die Speicherung unverhältnismäßig.[1981] Für das Geldwäscherecht ist diese Anforderung von besonderer Bedeutung, da die Speicherpflicht hier – anders als bei der Vorratsdatenspeicherung von TK-Verkehrsdaten[1982] – nicht losgelöst von der Ausgestaltung der Zugriffsrechte als Verletzung der Art. 7, 8 EU-GRC betrachtet werden kann (s. o. III. 2. b. bb.(3)).

1979 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 248 ff. = EuZW 2022, 706.

1980 Idem, Rn. 218 ff.

1981 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 ff. = NJW 2014, 2169; s.a. BVerfGE 125, 260 (347 ff.) – Vorratsdatenspeicherung.

1982 Vgl. EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 100 ff. = NJW 2017, 717; zur Diskussion s. *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139 f.).

Mit dieser Rechtsprechung ist die aktuelle Ausgestaltung des Datenflusses durch die FIU ohne einschränkende Ausgestaltung der GWRL nicht zu vereinbaren. Aufgrund der Formulierungen, die allein auf die Aufgaben und den Zweck der FIU abstellen, ist nämlich eine Interpretation möglich, nach der die FIU heimlich Finanzdaten bei den Verpflichteten im Auftrag der Sicherheitsbehörden ermitteln kann, Art. 32 Abs. 9 i. V. m. Art. 32 Abs. 4 S. 2 GWRL, ohne dass hierbei irgendwelche Anforderungen zu beachten wären.

Angesichts der Sensibilität[1983] von Finanzdaten, insbesondere der Kontoinhaltsdaten, kommt ein solcher Zugriff nicht infrage. Es handelt sich um einen schweren Grundrechtseingriff, der nur zur Bekämpfung schwerer Kriminalität gerechtfertigt werden könnte. Schon dieser Umstand ist fraglich, wenn ein Ersuchen bei der FIU nach privat gespeicherten Daten eingeht, das im Zusammenhang mit der Bekämpfung von Geldwäsche steht (s. o.). Der all-crimes-approach[1984] hat zur Folge, dass dem Tatbestand der Geldwäsche ein äußerst variabler Unrechtsgehalt zukommt.[1985] Eine pauschale Einstufung von Geldwäsche als schwere Kriminalität im europarechtlichen Sinne ist daher überaus zweifelhaft (s. o. III. 2. a. cc. (3) (b)).[1986] Noch schwerer wirkt jedoch das völlige Fehlen konkreter materieller Eingriffsschwellen und verfahrensrechtlicher Sicherungen. Ein (mittelbarer) Zugriff operativer Sicherheitsbehörden auf vorratsmäßig gespeicherte Finanzdaten dürfte in jedem Fall einen Richtvorbehalt oder eine vergleichbare Kontrolle notwendig machen.[1987] Solche Einschränkungen sucht man in Art. 32 GWRL allerdings vergeblich.

Es stellt sich angesichts der jüngeren EuGH-Rechtsprechung die Frage, ob und inwiefern die Mängel der Zugriffsregeln im Wege der Auslegung behoben werden könnten.

1983 BVerfGE 120, 274 (347 f.) – Online-Durchsuchung; *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.

1984 *Pelz* in BeckOK GwG, § 43 Rn. 28.

1985 Vgl. BT-Drs. 18/6389, S. 11 ff.; *Böse/S. Jansen*, JZ 2019, 591 (593 f.); *El-Ghazi* in Herzog GwG, StGB § 261 Rn. 28 ff., 144.

1986 Vgl. *Hochmayr* in Frankfurter Kommentar, AEUV Art. 83 Rn. 12; s.a. *Böse/S. Jansen*, JZ 2019, 591 (594).

1987 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 62 = NJW 2014, 2169; Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 51 ff. = NJW 2021, 2103; ; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

(a) Zeitliche Begrenzung des Zugriffsrechts

Da Art. 32 Abs. 9 GWRL in Verbindung mit den Speicherpflichten zum Vorliegen einer Vorratsdatenspeicherung führt, müsste der Zugriff auf die grundrechtlich maximal mögliche Speicherdauer, also sechs Monate, begrenzt werden. Ältere anlasslos gespeicherte Daten darf die FIU nach der Rechtsprechung des EuGH[1988] nicht eigenständig abrufen. An einer solchen Einschränkung fehlt es i. R. d. Art. 32 Abs. 9 GWRL. Unberührt hiervon bleiben Ersuchen nach Art. 32 Abs. 3 S. 4 GWRL, die zeitlich keine Grenze beachten müssen, allerdings auf Rückfragen zu eingegangenen Verdachtsmeldungen zu beschränken sind.

Diese Eingrenzung gilt ungeachtet dessen, dass der EuGH der PNR-Zentralstelle den Zugriff grundsätzlich auf sämtliche Flugdaten einräumt und erst nach erstmaliger Übermittlung durch die Fluggesellschaften eine Löschfrist beginnt.

Wie im PNR-System steht die FIU zwar als *zentrale Stelle* zwischen den geldwäscherechtlich verpflichteten Privaten und den nationalen Sicherheitsbehörden und nimmt auch selbst operative Aufgaben wahr. Ihre primäre[1989] Arbeit liegt aber in der Entgegennahme und Analyse von Verdachtsmeldungen (zum Rechtscharakter unten III. 2. c. bb. (2)). Sie ist also weniger Sammel- als Analysestelle. Die wesentliche Speicherung findet bei den Verpflichteten statt.

Vergleicht man die FIU mit der PNR-Zentralstelle, erscheint der Umfang der von der FIU entgegengenommenen Daten zwar gering, sammelt letztere doch sämtliche Fluggastdaten und verwaltet diese eigenständig, wohingegen die FIU lediglich Verdachtsmeldungen entgegennimmt. Die Daten, die die FIU verwaltet, sind jedoch deutlich invasiver. Aus den einzelnen Transaktionsdaten ergeben sich tiefe Einblicke in die Persönlichkeit und den Alltag der Betroffenen.[1990] Darüber hinaus können die Betroffenen kaum verhindern, dass Finanzdaten anfallen, da die Wahrnehmung von Zahlungsdiensten, anders als Flugreisen, kaum noch verzichtbar erscheint.

1988 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 218 ff. = EuZW 2022, 706

1989 BT-Drs. 18/11928, S. 26.

1990 BVerfGE 120, 274 (347 f.) – Online-Durchsuchung; *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

Ein Push-System wie jenes der PNR-RL, bei dem die Privaten universell alle bei ihnen anfallenden Daten zur Analyse an eine staatliche Stelle ausleiten, wäre im Geldwäscherecht also schon deswegen kaum denkbar. Ferner machen die Kosten, die die Monitoringsysteme verursachen[1991], deutlich, dass eine effektive Überwachung von Finanztransaktionen wohl faktisch nur über eine Aufgabenauslagerung an den Privatsektor möglich ist.

Der Umstand, dass grundsätzlich auch eine Universalübermittlung an staatliche Stellen im EU-Recht vorkommt und im Grundsatz vom EuGH nicht beanstandet wurde, solange die Speicherung bei der Sammelstelle zeitlich befristet wird,[1992] kann auf das Geldwäscherecht also nur insofern übertragen werden, als dass der FIU ein umfängliches Zugriffsrecht nur für Finanzdaten zusteht, deren Entstehung nicht länger als sechs Monate zurückliegt (zur anschließenden Löschpflicht dieser Daten s. III. 2. b. bb. (2)).

Eine solche zeitliche Grenze sieht Art. 32 Abs. 9 GWRL nicht vor. Sie müsste also per Auslegung erst entwickelt werden. Nach den Maßstäben des PNR-Urteils, das an verschiedenen Stellen nichts weniger als eine Contra-Lege Auslegung vornimmt,[1993] ist aktuell nicht ausgeschlossen, dass der EuGH eine solche Auslegung der Unvereinbarkeitserklärung von Art. 32 Abs. 9 GWRL vorziehen würde. Eine Gesetzesanpassung wäre jedoch angebracht.

(b) Übermittlung nur bereits vorhandener Daten unter Richtervorbehalt

Neben dieser zeitlichen Eingrenzung des Zugriffsrechts der FIU gegenüber den Privaten nach Art. 32 Abs. 9 GWRL bedarf es auch verschiedener Einschränkungen der Übermittlungspflicht i. S. d. § 32 Abs. 4 S. 2 GWRL.

Hier kommt Art. 2 Nr. 5 Finanzinformations-RL wieder ins Spiel, wonach unter Finanzinformationen (i. S. d. Finanzinformations-RL) nur solche Informationen zu verstehen sind, die bei der FIU bereits vorhanden sind. Eine Übermittlung von erst abzurufenden Informationen ist damit jedenfalls dann verwehrt, wenn das Auskunftsersuchen bei der FIU nicht in

1991 Vgl. *Saperstein/Sant/Ng*, Notre Dame Law Rev. Online 91 (2015), 1 (2 ff.).

1992 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)) = EuZW 2022, 706.

1993 *Thönnes*, Die Verwaltung 2022, 527 (539); *ders.,* directive beyond recognition, 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt aufgerufen am 12.01.2025.

Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung, sondern allgemein schwerer Kriminalität steht. Zwar soll die GWRL nach Art. 1 Abs. 2 lit. a) Finanzinformations-RL von dieser unberührt bleiben. Es ließe sich dennoch argumentieren, dass diese enge Definition auch i. R. d. Art. 32 Abs. 4 S. 2 GWRL gilt bzw. gelten muss. Art. 2 Nr. 5 Finanzinformations-RL ließe sich also *mutatis mutandis* auch für Übermittlungshandlungen i. R. d. Bekämpfung von Geldwäsche oder Terrorismusfinanzierung anwenden.

Damit wäre es der FIU untersagt, bei den Privaten vorratsmäßig gespeicherte Informationen abzufragen, um damit ein Auskunftsersuchen einer Sicherheitsbehörde zu beantworten.

Eine Übermittlung käme danach nur noch hinsichtlich solcher Informationen in Betracht, die bei der FIU etwa aufgrund von Verdachtsmeldungen bereits vorliegen. Ein mit den PNR-Daten oder TK-Verkehrsdaten vergleichbarer Vorratsdatenspeicherungskomplex ließe sich in der GWRL dann nur noch insofern ausmachen, als dass aufgrund der niedrigen Verdachtsmeldeschwelle auch bei der FIU sicherheitsrechtlich unbedenkliche Daten vorratsmäßig gespeichert werden. Hier würde sich aber mildernd auswirken, dass für die FIU strenge Löschpflichten gelten (s. o. Kap. D. III. 2. c. dd.).

Die Übermittlung solch sensibler Daten durch die FIU stellt allerdings – auch, wenn es sich um *auffällige* Daten handelt, – weiter einen schweren Grundrechtseingriff dar. Zwar müssen die Betroffenen nicht grundsätzlich damit rechnen, dass auf die bei ihren Banken gespeicherten Daten zugegriffen werden kann. Die niedrigschwellige Pflicht zur heimlichen Meldung aufgrund des zuvor ausgeübten Monitorings stellt insgesamt dennoch einen undurchschaubaren Überwachungstatbestand dar.

Die Übermittlung von aus diesem System gewonnenen, sensiblen Daten an Sicherheitsbehörden ist mit der Übermittlung gespeicherter TK-Verkehrsdaten oder PNR-Daten durchaus vergleichbar und lastet schwer auf den Grundrechten der Betroffenen aus Art. 7, 8 EU-GRC.

Daher ist grundsätzlich ein Richtervorbehalt notwendig.[1994] Auch wenn Art. 32 Abs. 9 i. V. m. Abs. 4 S. 2, GWRL nicht als mittelbare Zugriffsmöglichkeit der Sicherheitsbehörden auf private Vorratsdaten gelesen werden kann, sondern nur als Ermächtigung zum Zugriff auf Daten, die der FIU

1994 EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 51 ff. = NJW 2021, 2103; ; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

bereits vorliegen, dürfte insofern ein Ausgestaltungsmangel vorliegen, der zur Unverhältnismäßigkeit des Zugriffs führt.

(c) Übermittlung nur bei Verdacht eines *schweren* Falles der Geldwäsche

Darüber hinaus dürfte eine Übermittlung von Daten, die der FIU vorliegen, an operative Sicherheitsbehörden unter dem Vorbehalt stehen, dass dies zur Bekämpfung schwerer Kriminalität notwendig ist.[1995] Eine solche Einschränkung enthält aber Art. 32 Abs. 4 S. 2 GWRL, der die Pflicht der FIU auf Ersuchen hin zu übermitteln vorsieht, nicht. Nach dieser Vorschrift ist vielmehr ein Verdacht auf Geldwäsche oder Terrorismusfinanzierung ausreichend.

Damit stellt sich erneut das Problem ein, dass nicht jeder Geldwäscheverdacht eine *schwere Kriminalität* darstellen wird. [1996] Der Unrechtsgehalt der Geldwäsche hängt von der Vortat ab.[1997] Art. 32 Abs. 4 S. 2 GWRL müsste also teleologisch reduziert und eine Übermittlung auf Ersuchen beschränkt werden, denen ein Verdacht auf Geldwäschedelikte mit einem besonderen Schweregrad zugrunde liegt.

Einer solchen Auslegung dürfte die unionsrechtliche Definition der Geldwäsche, die keine unterschiedlichen Schweregrade vorsieht, Art. 1 Abs. 3 GWRL und Art. 3 Geldwäschestrafbarkeits-RL, nicht zwingend entgegenstehen. In Deutschland wurde beispielsweise § 100a Abs. 2 Nr. 1 lit. m) StPO dahingehend eingegrenzt, dass die TKÜ nur zur Aufklärung von Geldwäschedelikten erfolgen darf, deren Vortat ebenfalls eine schwere Straftat darstellt.[1998]

Nach den Maßstäben des PNR-Urteils ist wiederum nicht ausgeschlossen, dass der EuGH eine solche Auslegung trotz der eindeutigen Begriffsbestimmung des Art. 1 Abs. 3 GWRL und Art. 3 Geldwäschestrafbarkeits-RL für denkbar halten könnte und die Übermittlungspflicht der FIU nach Art.32 Abs. 4 S. 2 GWRL grundsätzlich als auf schwere Fälle der Geldwäschekriminalität begrenzt und mithin als verhältnismäßig ansieht.

1995 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 218 ff. = EuZW 2022, 706.

1996 *Hochmayr* in Frankfurter Kommentar, AEUV Art. 83 Rn. 12; s.a. *Böse/S. Jansen*, JZ 2019, 591 (594).

1997 *Böse/S. Jansen*, JZ 2019, 591 (593 f.); *El-Ghazi* in Herzog GwG, StGB § 261 Rn. 28 ff., 144.

1998 dazu BT-Drucks. 18/6389, S. 15 f., *Böse/Janzen*, JZ 2019, 591 (594).

Zu klären ist dann noch, welcher Verdachtsgrad vorliegen muss. Zur Bekämpfung schwerer Kriminalität ist eine Übermittlung nach dem EuGH nur *erforderlich* – was letztlich *angemessen* bedeutet (Kap. C. II. 1. a. aa. (b) –[1999], wenn damit eine effektive Kriminalitätsbekämpfung einhergeht.[2000] Deshalb müssen je nach Grundrechtsintensität der Datenübermittlung bestimmte Verdachtsgrade vorliegen.

Durch die Einschränkung der Übermittlung auf bei der FIU vorliegende Daten durch analoge Anwendung des Art. 2 Nr. 5 Finanzinformations-RL wird bereits gewährleistet, dass es nicht zu einem Zugriff auf private Daten kommt, die ohne sicherheitsrechtlichen Anlass gespeichert sind. Außerdem ergeben sich zeitliche Grenzen durch die Einschränkung des Zugriffsrechts der FIU auf nicht länger als sechs Monate bei den Privaten gespeicherten Daten und daran anschließend eine Begrenzung der Speicherpflicht bei der FIU selbst.

Der Übermittlung liegen also bei Beachtung der bislang aufgestellten Einschränkungen nur begrenzt Daten zugrunde, die immer eine privat veranlasste Kontrolle im Rahmen der Verdachtsmeldung durchlaufen haben. Daher dürfte es verhältnismäßig sein, die Übermittlung trotz der Heimlichkeit und trotz der Zurechnung der Daten zu einem umfassenden Überwachungssystem von einem niederschwelligen Verdachtsgrad abhängig zu machen, solange dieser auf objektiven Anhaltspunkten beruht.

(d) Einschränkung der Übermittlungspflicht bei bereits analysierten Daten

Der Zugriff auf bei der FIU vorhandenen Daten, die aufgrund einer Analyse bekanntermaßen nicht im Zusammenhang mit Geldwäsche und Terrorismus stehen und deshalb nur maximal sechs Monate gespeichert werden dürfen (II. 2. B. bb. (2)), kommt darüber hinaus aufgrund der Anlasslosigkeit der Speicherung einem Zugriff im Rahmen einer Vorratsdatenspeicherung gleich. Es muss daher die zusätzliche Maßgabe gelten, dass

1999 Kingreen in Callies/Ruffert EUV/AEUV, EU-GRC Art. 52 Rn 69.

2000 Vgl. *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.).

eine Übermittlung von bereits analysierten Daten auf neuen Umständen beruht.[2001]

Art. 32 Abs. 9 und Art. 32 Abs. 4 S. 2 GWRL dürften danach zunächst unverhältnismäßig sein. Die Normen unterscheiden nicht danach, ob es sich bei den bei der FIU vorliegenden Daten um anlasslos bzw. bereits analysierte Vorgänge handelt. Eine grundrechtskonforme Auslegung dürfte aber nach den Maßstäben des EuGH nicht ausgeschlossen sein.

(3) Zwischenergebnis

Mangels materieller und formeller Anforderungen wäre ein heimlicher Zugriff auf privat gespeicherte Kontoinhaltsdaten durch Sicherheitsbehörden mittels Beauftragung der FIU über Art. 32 Abs. 9 i. V. m. Abs. 4. S. 2 GWRL nach der etablierten Rechtsprechung zur Vorratsdatenspeicherung unverhältnismäßig und somit primärrechtswidrig.[2002]

Die Normen müssen also analog Art. 2 Nr. 5 Finanzinformations-RL zunächst dahingehend ausgelegt werden, dass die FIU auf Ersuchen nur Informationen an Sicherheitsbehörden weiterleiten darf, die sich im Moment der Anfrage schon bei der FIU befanden.

Der Zugriff der FIU auf vorratsmäßig gespeicherte Finanzdaten bei den Verpflichteten dürfte aufgrund ihrer Funktion als Zentralstelle im europarechtlichen Sinne grundsätzlich unproblematisch sein, da der EuGH im PNR-Urteil ein System gebilligt hat[2003], bei dem die Zentralstelle selbst alle Daten speichert,

Notwendige Einschränkungen für Ersuchen der FIU bei den Verpflichteten ergeben sich aber hinsichtlich der Dauer des retrograden Zugriffs und der Übermittlungsrechte der FIU. Ein Zugriff auf Daten, die länger als sechs Monate bei den Privaten vorliegen, und die in dieser Zeit nicht sicherheitsrechtlich relevant wurden, ist auszuschließen, da andernfalls eine Speicherung anlassloser Daten für insgesamt länger als sechs Monate vorgesehen

2001 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 218 = EuZW 2022, 706.

2002 In diesem Sinne auch *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.

2003 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)) = EuZW 2022, 706.

wäre. Art. 32 Abs. 9 GWRL weist insofern einen Mangel auf und müsste teleologisch reduziert, besser aber gesetzlich verändert werden. Dazu sollte die geldwäscherechtliche Speicherpflicht in Art. 40 Abs. 1 GWRL auf sechs Monate begrenzt und der Zugriff der FIU an diese Speicherpflicht gekoppelt werden.

Die Weiterleitung von Kontoinhaltsdaten auf Anfrage stellt aufgrund der Sensibilität dieser Daten und der niedrigen Meldeschwelle der Privaten einen schwerwiegenden Grundrechtseingriff dar, was nur mit der Bekämpfung schwerer Kriminalität gerechtfertigt werden kann. Insofern bedarf es einer teleologischen Reduktion des Geldwäscheverdachts, wobei § 100a Abs. 2 Nr. 1 lit. m) StPO als Vorbild dienen könnte. Ein besonderer Verdachtsgrad dürfte insofern allerdings nicht notwendig sein. In jedem Fall aber sind solche Übermittlungen nur unter Richtervorbehalt zulässig.[2004]

Soweit die FIU auch solche Daten speichert, bei denen sich im Rahmen der Analyse kein Zusammenhang mit Geldwäsche und Terrorismusfinanzierung herausgestellt hat, handelt es sich um eine anlasslose Vorratsspeicherung. Diese ist wiederum auf sechs Monate zu begrenzen. Eine Übermittlung solcher Daten an Sicherheitsbehörden darf nur stattfinden, wenn *neue* Umstände eine solche Übermittlung notwendig erscheinen lassen.[2005]

cc. Bewertung des Zugriffsrechts der FIU unter Berücksichtigung der Übermittlungspflicht auf nationaler Ebene

Von der primärrechtskonformen Auslegung des Art. 32 Abs. 9 i. V. m. Art. 32 Abs. 4 S. 2 GWRL abhängig ist die Bewertung der mitgliedstaatlichen Ausgestaltung der Zugriffs- und Übermittlungspflichten der FIU.

In Deutschland sieht § 30 Abs. 3 GwG vor, dass die FIU *unabhängig vom Vorliegen einer Meldung Informationen von Verpflichteten einholen kann, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.* Damit entspricht § 30 Abs. 3 GwG wortlautgetreu dem Art. 32 Abs. 9 GWRL. Letztere Norm muss aber unionsgrundrechtskonform einschränkend ausgelegt werden. Soweit § 30 Abs. 3 GwG dieser Auslegung nicht entspricht und eine *strengere Regelung* darstellt, gelten nach Art. 5 GWRL die Unionsgrundrechte jedenfalls

2004 EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 51 ff. = NJW 2021, 2103; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

2005 Idem, Rn. 218; EuGH, s.a. Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 200. – PNR Canada = ZD 2018, 23

mittelbar, da andernfalls ein Verstoß gegen die GWRL vorliegt, der von den deutschen Fachgerichten geprüft werden könnte.[2006]

Da es sich bei § 30 Abs. 3 GwG um die Umsetzung determinierten Unionsrechts handelt, gelten die Unionsgrundrechte allerdings auch unmittelbar mit derselben Maßgabe wie für die Richtlinie[2007] und könnten vom BVerfG geprüft werden.[2008] Insofern kann an dieser Stelle auf die Ausführungen zu Art. 32 Abs. 9 GWRL verwiesen werden (s. o. III. 2. c. bb. (2)).

§ 30 Abs. 3 GwG wäre danach jedenfalls dann unionsrechtswidrig, wenn er einen Zugriff auf vorratsmäßig gespeicherte Daten bei den Verpflichteten auch zur Beantwortung von Auskunftsersuchen zuließe, die nicht mit bei der FIU vorhandenen Daten beantwortet werden können. Anderenfalls bestünde ein mittelbarer Zugriff der Sicherheitsbehörden, der nicht mit ausreichenden materiellen und formellen Anforderungen ausgestaltet wurde. Außerdem ist der Zugriff der FIU auf Daten zu reduzieren, die weniger als sechs Monate anlasslos von den Privaten gespeichert wurden.

(1) Überschießende oder übererfüllende Umsetzung durch § 32 Abs. 3 Nr. 2 GwG

§ 30 Abs. 3 GwG ist im Zusammenhang mit § 32 Abs. 3, 3 a GwG zu lesen, in denen die FIU zur Beantwortung von Ersuchen bestimmter Sicherheitsbehörden verpflichtet wird, die sich auf *Daten aus Finanzinformationen und Finanzanalysen, auch soweit sie personenbezogene Daten enthalten,* beziehen. Als entsprechende Behörden benannt werden die Strafverfolgungsbehörden, das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst und der Militärische Abschirmdienst.

Die Pflicht, auf diese Ersuchen zu antworten, besteht, wenn dies erforderlich ist für *die Aufklärung von Geldwäsche und Terrorismusfinanzierung oder die Durchführung von diesbezüglichen Strafverfahren*, § 32 Abs. 3 Nr. 1, *oder die Aufklärung sonstiger Gefahren und die Durchführung von anderen, nicht von Nummer 1 erfassten Strafverfahren*, § 32 Abs. 3 Nr. 2 GwG.

2006 BVerfGE 129, 186 (202).

2007 Vgl. zur Umsetzung des PNR-Urteils: VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI; *Wissenschaftliche Dienste des Bundestags,* PNR-Urteil, 2022, S. 4 ff.; zur deutschen Vorratsdatenspeicherung von TK-Verkehrsdaten OVG Münster, NVwZ-RR 2018, 43; VG Köln, ZD 2019, 187.

2008 BVerfGE 152, 216 (236 ff.) – Recht auf Vergessen II.

Nach § 32 Abs. 3 Nr. 2 GwG besteht also auch eine Übermittlungspflicht, wenn das Ersuchen nicht im Zusammenhang mit Terrorismusfinanzierung oder Geldwäsche steht. Insofern ließe sich zunächst andenken, dass § 32 Abs. 3 Nr. 2 GwG den Art. 7 Abs. 1 Finanzinformations-RL umsetzt, der auf einen solchen Zusammenhang ja gerade verzichtet. Dies ist aber nicht der Fall. Art. 7 Abs. 1 Finanzinformations-RL sieht nur eine Übermittlung zur Verhinderung oder Verfolgung und Ahndung *schwerer* Straftaten vor. Diese Übermittlung muss darüber hinaus an eine speziell benannte Behörde erfolgen, Art. 3 Abs. 2 Finanzinformations-RL.

Eine Umsetzung dieser Norm ist (allein) durch Einführung des § 32 Abs. 3a GwG erfolgt.[2009] Als insofern zuständige Behörde wurde das BKA benannt, § 3 Abs. 2a S. 2 BKAG. Soweit Art. 7 Abs. 1 Finanzinformations-RL Einschränkungen formuliert, wollte sich der Gesetzgeber diesen bei § 32 Abs. 3 GwG also gerade nicht unterwerfen.

Bei § 32 Abs. 3 Nr. 2 GwG handelt es sich also, da Art. 32 Abs. 4 S. 2 GWRL eine Übermittlung nur bei Zusammenhang mit Geldwäsche oder Terrorismusfinanzierung vorsieht, um eine Regelung, die nicht vom Text des entsprechenden Unionsrechts gefordert wird.

Es könnte sich insofern um eine überschießende oder übererfüllende Umsetzung handeln.[2010] Bei der überschießenden Umsetzung wird ein Rechtssatz der Richtlinie auf einen Sachverhalt außerhalb des Regelungsbereichs übertragen, bei der übererfüllenden Umsetzung innerhalb des Regelungsbereich höhere Standards eingeführt als von der Richtlinie gefordert (auch „gold-plating").[2011]

§ 32 Abs. 3 Nr. 2 GwG fällt in letztere Kategorie. Zwar werden die zu übermittelnden Daten der FIU aus dem Zusammenhang mit Geldwäsche und Terrorismusfinanzierung gelöst, weshalb die Norm den Regelungsbereich der Geldwäschebekämpfung verlässt. Es handelt sich jedoch weiterhin um eine Pflicht, die erst durch ihre Anknüpfung an die Fähigkeiten und Aufgaben der FIU als zentrale Anti-Geldwäschebehörde Wirkung erzielt. Außerdem ergibt sich aus Art. 7 Finanzinformations-RL, dass der EU-Gesetzgeber sämtliche Weiterleitungspflichten der FIU determinieren wollte. Der Regelungsbereich des Geldwäscherechts kann insofern als erweitert

2009 BT-Drs. 19/28164, S. 54.

2010 *Habersack/Mayer* in Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, § 14 Rn. 11; „echtes/unechtes gold-plating" bei *Payrhuber/Stelkens*, EuR 2019, 190 (195); gegen eine Abgrenzung *Brandner,* Richtlinien, 2003, S. 10 ff.

2011 Vgl. *Habersack/Mayer* in Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, § 14 Rn. 10 ff.; *Leidenmühler*, EuR 2019, 383.

verstanden werden. jedenfalls aber bewegen sich sämtliche Weiterleitungsmaßnahmen der FIU in einem unionsrechtlich determinierten Bereich.

Handelt es sich um eine übererfüllende bzw. determinierte Vorschrift, steht neben der unmittelbaren Anwendung des Unionsprimärrechts[2012] allgemein ein Verstoß gegen die Richtlinie selbst im Raum, wenn die Umsetzung dem Richtlinienzweck entgegensteht.[2013] Im Anti-Geldwäscherecht folgt dies im Übrigen schon von Gesetzes wegen nach Art. 5 GWRL. Der Richtlinienzweck muss dabei durch grundrechtskonforme Auslegung ermittelt werden.

(2) Auswirkungen der primärrechtskonformen Auslegung von Art. 32 Abs. 3, 9 GWRL

Nicht nur bei § 32 Abs. 3 Nr. 2 GwG, sondern auch bei jenen Normen des GwG, die zunächst eine Eins-zu-Eins-Umsetzung verfolgen, kommt in Betracht, dass es sich ebenfalls um von der Richtlinie abweichende Umsetzungen handelt, wenn man die primärrechtskonforme Auslegung der entsprechenden Richtliniennormen zugrunde legt.

Ergeben sich aus den Unionsgrundrechten Grenzen für die Auslegung einer Richtlinie, gelten diese Grenzen auch für das mitgliedstaatliche Recht.[2014] Es kommt hierbei allerdings immer noch darauf an, ob das entsprechende Recht unionsrechtlich determiniert ist oder nicht. In letzterem Fall sind primär die Grundrechte des Grundgesetzes anzuwenden.[2015]

Von einer solchen Determinierung ist bei Art. 32 Abs. 4, 9 GWRL im Rahmen einer grundrechtskonformen Auslegung auszugehen. Da schwere Eingriffe in die Art. 7, 8 EU-GRC nur zur Bekämpfung schwerer Kriminalität möglich sind, muss Art. 32 Abs. 4, 9 GWRL dahingehend verstanden werden, dass der EU-Gesetzgeber eine Übermittlungspflicht der FIU auf Ersuchen operativer Sicherheitsbehörden ausschließlich bei einem Zusam-

2012 BVerfGE 152, 216 (236 ff.) – Recht auf Vergessen II.

2013 s.a. unabhängig von Art. 5 GWRL: *Habersack/Mayer* in Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, § 14 Rn. 17; *Leidenmühler*, EuR 2019, 383; Für eine prinzipielles Verbot des „gold-plating" *Burmeister/Staebe*, EuR 2009, 444.

2014 Vgl. zur Umsetzung des PNR-Urteils: VG Wiesbaden, Urteil vom 06.12.2022 - 6 K 805/19.WI; *Wissenschaftliche Dienste des Bundestags,* PNR-Urteil, 2022, S. 4 ff.; zur deutschen Vorratsdatenspeicherung von TK-Verkehrsdaten OVG Münster, NVwZ-RR 2018, 43; VG Köln, ZD 2019, 187.

2015 BVerfGE 152, 152 (170 ff.) – Recht auf Vergessen I.

menhang des Ersuchens mit Geldwäsche oder Terrorismusfinanzierung, die er offenbar als schwere Kriminalität betrachtet, vorsehen wollte.

(a) § 32 Abs. 3 Nr. 2 GwG

Die Erweiterung auf die *Aufklärung sonstiger Gefahren und die Durchführung von anderen, nicht von Nummer 1 erfassten Strafverfahren* in § 32 Abs. 3 Nr. 2 GwG fällt damit in einen unionsrechtlich determinierten Regelungsbereich innerhalb der Geldwäsche-RL.

§ 32 Abs. 3 Nr. 2 GwG dürfte daher bereits nach den Grundsätzen des BVerfG nicht gegen Art. 7, 8 EU-GRC verstoßen. Vorliegend gelten die Art. 7, 8 EU-GRC allerdings in jedem Fall mittelbar nach der eingeschränkten Öffnungsklausel des Art. 5 GWRL.

Schon zur zugrunde liegenden Richtliniennorm, dem Art. 32 Abs. 4 S. 2 GWRL, wurde insofern festgestellt, dass er weder konkrete materielle Eingriffsschwellen noch formelle Absicherungen vorsieht. Die Norm wäre bei reiner Wortlautbetrachtung nach der ständigen EuGH-Rechtsprechung auf jeden Fall ungeeignet, einen Zugriff auf vorratsmäßig gespeicherte Daten zu ermöglichen.[2016] Analog Art. 2 Nr. 5 Finanzinformations-RL ist sie daher einschränkend dahingehend auszulegen, dass die Ersuchen auf Daten begrenzt sein müssen, die bei der FIU bereits vorliegen. Dies ist auf § 32 Abs. 3 GwG zu übertragen.

Da die Übermittlung nach § 32 Abs. 3 GwG Teil eines auf sensible Daten ausgerichteten Überwachungssystems ist, stellt sie trotz der Beschränkung auf bei der FIU vorhandene Daten einen schweren Grundrechtseingriff dar (s. o.). Das gilt insbesondere, soweit bei der FIU anlasslos gespeicherte Daten vorliegen, was etwa der Fall ist, wenn diese Daten gem. § 30 Abs. 2 GwG analysiert wurden.

Eine Übermittlung nach § 32 Abs. 3 GwG kommt daher nach der Rechtsprechung des EuGH nur zur Bekämpfung schwerer Kriminalität in Betracht.[2017] § 32 Abs. 3 Nr. 2 GwG, der eine Übertragung zu sämtlichen Kriminalitätsformen zulässt, ist danach ein unverhältnismäßiger Eingriff in die Art. 7, 8 EU-GRC.

2016 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 ff. = NJW 2014, 2169.

2017 EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 51 ff. = NJW 2021, 2103; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

Darüber hinaus dürfte ein Verstoß gegen die Privatheitsgrundrechte des Grundgesetzes vorliegen, da auch hier Übermittlungen, die als schwerer Grundrechtseingriff zu werten sind, nur zur Verfolgung schwerer Straftaten oder zur Verhütung von Gefahren für besonderes geschützte Rechtsgüter zulässig sind.[2018]

Neben diesem grundrechtlichen Aspekt ist unmittelbar die Regelung der Finanzinformations-RL zu beachten. Diese legt fest, dass ein Austausch der FIU nur mit national benannten (zuständigen) Behörden, Art. 3 Abs. 2 und nur zur Bekämpfung schwerer Kriminalität, Art. 4 Abs. 1 erfolgen darf. Die Norm ist ausgehend von Art. 7, 8 EU-GRC so zu interpretieren, dass sie einer Übermittlung außerhalb dieses Regelungsbereichs entgegensteht.

§ 32 Abs. 3 Nr. 2 GwG verstößt damit unmittelbar (und mittelbar nach Art. 5 GWRL) gegen Art. 7, 8 EU-GRC, soweit er über Art. 32 Abs. 4 S. 2 GWRL hinausgehend eine Übermittlung zu anderen Zwecken als der Bekämpfung von Terrorismusfinanzierung und *schwerer* Fälle der Geldwäsche vorsieht. Er verstößt ferner auch gegen Art. 3, 4, 7 Finanzinformations-RL (analog), da er den Zweck dieser Richtlinie, die Eingrenzung der Übermittlung zu anderen als GWRL-relevanten Zwecken, konterkariert.

(b) § 32 Abs. 3 Nr. 1 GwG

Für § 32 Abs. 3 Nr. 1 GwG, der die Übermittlung von Daten an die Sicherheitsbehörden zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung vorsieht, gelten die Ausführungen zu Art. 32 Abs. 4 S. 2 GWRL entsprechend (III. 2. c. bb. (2)). Grundsätzlich problematisch ist also, dass es sich kaum bei allen Formen der Geldwäsche um schwere Kriminalität handeln wird. Insofern wäre eine Einschränkung notwendig, die nur durch teleologische Reduktion zu erzielen ist. Hierbei könnte § 100a Abs. 2 Nr. 1 lit. m) StPO als Vorbild dienen. Einen besonderen Verdachtsgrad bedürfte es hingegen wohl nicht.

Der Zugriff auf bei der FIU gespeicherte Daten, die mit Geldwäsche oder Terrorismusfinanzierung in Zusammenhang stehen, dürfte bei einer Begrenzung auf schwere Kriminalität nicht grundsätzlich unzulässig sein, sondern müsste prozeduralisiert werden.

2018 jüngst BVerfG, NVwZ-RR 2023, 1 (9 ff.) – Nachrichtendienstliche Informationsübermittlung.

Es muss insbesondere differenziert werden, ob die angefragten Daten bereits von der FIU analysiert wurden und sich dabei als verdächtig erwiesen haben. Wurden die Daten bereits analysiert und es hat sich kein Verdacht auf Geldwäsche oder Terrorismusfinanzierung ergeben, gilt, dass eine Übermittlung gegenüber der Ersterhebung auf neuen Umständen beruhen muss.[2019] Außerdem erfordert die Übermittlung eine vorherige Kontrolle durch einen Richter oder eine andere unabhängige Stelle.[2020]

Diese Ergänzungen sollten gesetzlich verankert werden. Sie überreizen die Möglichkeiten grundrechtskonformer Auslegung. Die Maßstäbe des EuGH sind für bundesdeutsche Gesetze nicht heranzuziehen.

(3) Zwischenergebnis

Aufgrund der europarechtlichen Determination sind § 30 Abs. 3 GwG und § 32 Abs. 3 GwG auf ihre Konformität mit der GWRL und der Finanzinformations-RL in unionsgrundrechtlich konform ausgelegter Gestalt zu prüfen, also letztlich daraufhin, ob sie mit Art. 7, 8 EU-GRC zu vereinbaren sind. Dies folgt ferner bereits aus Art. 5 GWRL, der nationale Regelungen nur im Rahmen des Unionsrechts zulässt.

Hinsichtlich § 30 Abs. 3 GwG kann auf die Ausführungen zu Art. 32 Abs. 9 GWRL verwiesen werden. Ein universeller Zugang einer Zentralstelle auf private Vorratsdaten ist danach nicht problematisch, wenn der Zugang zweckgebunden ausgestaltet ist und die Weiterleitungspflichten grundrechtskonform ausgestaltet sind.

Dabei ist zunächst auf die analoge Geltung des Art. 2 Nr. 5 EU-Finanzinformations-RL zu verweisen. Zwar wurde Art. 7 Abs. 1 EU-Finanzinformations-RL eigens durch die Einführung des § 32 Abs. 3a GwG umgesetzt, auch für die Übermittlung nach § 32 Abs. 3 GwG muss jedoch gelten, dass nur Daten aus dem Bestand der FIU übermittelt werden können. Bei den Daten der FIU ist sodann danach zu differenzieren, ob es sich um auffällige oder anlasslos gespeicherte Daten handelt, was sich aus der Analysetätigkeit der FIU, § 30 Abs. 1 GwG, ergeben wird. Anlasslose Daten, die länger als sechs

2019 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 218 = EuZW 2022, 706; s.a. Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 200. – PNR Canada = ZD 2018, 23

2020 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 62 = NJW 2014, 2169.

Monate gespeichert wurden, dürfen nicht übermittelt werden, sondern sind dringend zu löschen, § 37 Abs. 2 GwG.

Die Übermittlung der von der FIU gespeicherten Daten ist nur zur Bekämpfung schwerer Kriminalität möglich und nur an die benannte Behörde i. S. d. Art. 3 Abs. 1 Finanzinformations-RL. Jedenfalls § 32 Abs. 3 Nr. 2 GwG ist schon deshalb nicht mehr mit dem Unionssekundär- und vor allem Primärrecht zu vereinbaren.

Bei § 32 Abs. 3 Nr. 1 GwG dürfte wiederum eine teleologische Reduktion auf besonders schwere Fälle der Geldwäsche notwendig sein, da nicht jedes Geldwäschedelikt eine Form *schwerer Kriminalität* darstellt. [2021] Hierbei könnte § 100a Abs. 2 Nr. 1 lit. m) StPO als Vorbild dienen. Einen besonderen Verdachtsgrad bedürfte es hingegen wohl nicht.

Überdies fehlt es in § 32 Abs. 3 Nr. 1, 2 GwG an konkreten materiellen und formellen Einschränkungen. Jedenfalls, soweit anlasslos gespeicherte Daten übermittelt werden, müsste die Übermittlung gegenüber der Ersterhebung auf neuen Umständen beruhen[2022] und eine vorherige Kontrolle durch einen Richter oder eine andere unabhängige Stelle erfolgen.[2023]

3. Das informationelle Trennungsprinzip und die FIU

Neben diesen Problemen der Informationseingriffe durch die FIU, die sich primär aus der Anwendung der grundrechtlichen EuGH-Rechtsprechung ergeben, muss die FIU auch strukturell untersucht werden. In der deutschen Sicherheitsarchitektur stellt sie nämlich ein Novum dar.

Anders als Staatsanwaltschaften und Polizei können Nachrichtendienste und die FIU mittels heimlicher Auskunftsersuchen auf Kontoinhaltsdaten zugreifen. Dass die FIU diese Daten zumindest an Staatsanwaltschaften weiterleiten kann, wurde bereits aufgezeigt. Vergleichbare Vorschriften finden sich aber auch im Recht der Nachrichtendienste, etwa § 19 Abs. 1 BVerfSchG. Durch solche Normen soll die Limitierung der Mittel von Gefahrenabwehr und Staatsanwaltschaften aber nicht unterlaufen werden.

2021 Krit. insofern *Hochmayr* in Frankfurter Kommentar, AEUV Art. 83 Rn. 12; s.a. *Böse/S. Jansen*, JZ 2019, 591 (594).

2022 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 218 = EuZW 2022, 706; s.a. Gutachten v. 26.07.2017, Gutachten 1/15, Rn. 200. – PNR Canada = ZD 2018, 23

2023 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 62 = NJW 2014, 2169.

Der Status der FIUs ist insofern unklar. Der Gesetzgeber möchte die FIU als *administrativ präventiv handelnde* Behörde ansehen, deren Rolle vor allem in der Analyse liegt.[2024] Es wird jedoch von wissenschaftlicher Seite vorgetragen, dass das Aufgabenprofil der FIU eher dem eines Nachrichtendienstes entspreche, da sie in heimlicher Vorgehensweise auch aktiv Informationen einholen, vergleichen und weiterleiten kann.[2025]

Das denkbare Zusammenspiel von § 30 Abs. 3 GwG und § 32 Abs. 3 GwG (s.o.) hätte eine noch größere Bedeutung, wenn man die FIU tatsächlich als Nachrichtendienst begreifen und anderen Nachrichtendiensten eine vergleichbare Zusammenarbeit mit den Strafverfolgungsbehörden nicht zustehen würde. Es stellte sich dann nicht nur die Frage, ob die Möglichkeiten und Pflichten der FIU in einem Widersprich zur Rechtsprechung zu Art. 7, 8 Abs. 1 EU-GRC stehen. Man müsste auch klären, ob das GwG mit der traditionellen Vorstellung von der Zusammenarbeit zwischen Nachrichtendiensten und anderen Sicherheitsbehörden bricht und ob dieser Umstand rechtliche Konsequenzen nach sich zieht. Dies wiederum hängt davon ab, inwieweit die Anwendung des deutschen Trennungsprinzips angesichts des europarechtlichen Hintergrunds des GwG bzw. der anstehenden Vollharmonisierung überhaupt eröffnet ist.

a. „Klassische" Nachrichtendienste: Trennungsprinzip und hypothetische Datenneuerhebung

Das Recht der deutschen Nachrichtendienste ist von der Idee geprägt, dass die Dienste weder Gefahrenabwehr noch Strafverfolgung im engeren Sinne betreiben, sondern die sogenannte politische Vorfeldaufklärung.[2026] So stehen etwa dem Bundesamt für Verfassungsschutz ausdrücklich keine polizeilichen Befugnisse zu, § 8 Abs. 3 BVerfSchG. Man spricht insofern

2024 BT-Drs. 18/11555, S. 136 dazu *Bülte*, NVwZ-Extra 4b/2022, 1 (9).

2025 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.); von „einer Art Finanz-Nachrichtendienst" sprechen die *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21.

2026 BVerfGE 133, 277 (325 f.) – Antiterrordatei I; *Poscher/Rusteberg* KJ 2014, 57 (59); schon *Evers,* Privatsphäre, 1960, S. 96 ff.

vom Prinzip (oder Gebot)[2027] der Trennung von Nachrichtendiensten und anderen Sicherheitsbehörden.[2028]

Anerkannt ist insofern seit den Entscheidungen des BVerfG zur Antiterrordatei, dass jedenfalls zwischen den Informationen der Nachrichtendienste und Informationen operativer Sicherheitsbehörden grundsätzlich zu trennen ist.[2029] Dies bedeutet nun aber nicht, dass zwischen den Behörden gar kein Informationsaustausch stattfindet, sondern nur, dass „*Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendiensten ermöglichen, gesteigerten verfassungsrechtlichen Anforderungen unterliegen*."[2030] Diese Regelungen sind notwendig, da den Nachrichtendiensten vom Gesetzgeber intensivere Überwachungsrechte eingeräumt wurden. Diese Befugnisse sind nur berechtigt, da den Diensten im Gegenzug keine bzw. kaum operative Möglichkeiten eingeräumt wurden. Eine omnipotente Sicherheitsbehörde, die *alles wissen darf und alles tun kann*,[2031] wäre mit den Grundrechten nicht zu vereinbaren.[2032] Dieser Grundsatz würde unterlaufen, wenn die Behörden, die *alles wissen*, ihre Erkenntnisse frei mit denen Behörden tauschen könnten, *die alles tun können*.[2033]

Im Aufgabenbereich von Nachrichtendiensten und anderen Sicherheitsbehörden kommt es allerdings zwangsläufig zu Überschneidungen, die nur durch Kooperation gelöst werden können.[2034] Die Möglichkeit einer

2027 Zu den Begriffen *Gusy*, GSZ 2021, 141 (144 f.).

2028 Dazu nur *Brandt,* Verfassungsschutz, 2015, S. 254 ff.; *Arzt* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, ATDG § 1 Rn. 29 ff.; *ders.*, NVwZ 2013, 1328; *Gusy*, GSZ 2021, 141 (144 ff.); *Ibler* in Dürig/Herzog/Scholz GG, Rn. 143; *Bergemann* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht,Rn. 9 mwN, der den Streit um Inhalt und Natur des Trennungsgebots durch die ATDG Urteile für geklärt erachtet.

2029 „Informationelles Trennungsgebot" vgl. BVerfGE 133, 277 – Antiterrordatei I; E 156, 11 – Antiterrordatei II; *Bergemann* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. H Rn. 9; *Unterreitmeier*, DÖV 2021, 659.

2030 BVerfGE 133, 277 (329) – Antiterrordatei I; E 156, 11 (50) – Antiterrordatei II.

2031 *Gusy*, GA 1999, 319 (327).

2032 Vgl. BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.) – Antiterrordatei II; NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Gärditz*, JZ 2013, 633 (634);

2033 vgl. BVerfG, NVwZ-RR 2023, 1 (8) – Nachrichtendienstliche Informationsübermittlung *Gärditz*, JZ 2013, 633 (634); *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (191).

2034 *Dietrich* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, III § 3 Rn. 8; ebd. *Gusy* IV § 2 Rn. 46, 55; ebd. *Warg* V § 1 Rn. 8; *J. Franz Lindner/Unterreitmeier*, DÖV 2019, 165 (168) *Zöller,* Informationssysteme, 2002, S. 322 ff.; *ders.* in

Kooperation steht der Annahme einer informationellen Trennung nicht entgegen, sondern wird durch diese gedanklich erst notwendig.[2035] Zwar besteht die Aufgabe der Nachrichtendienste *primär* in der Information der Politik.[2036] Von diesem Prinzip darf aber abgewichen werden, wenn legitime Gründe die Informationsversorgung von Sicherheitsbehörden erfordern und bestimmte Übermittlungsschwellen eingehalten werden, damit keine sicherheitsrechtlichen Voraussetzungen unterlaufen werden.[2037] Letzteres wird primär durch den Grundsatz der hypothetischen Datenneuerhebung sichergestellt.[2038]

Die Kooperation von Nachrichtendiensten und anderen Sicherheitsbehörden ist also nicht Regel, sondern Ausnahme und deshalb rechtfertigungsbedürftig.

Die informationelle Trennung ist nach diesem Regel-Ausnahme-Konzept der Rechtsprechung des BVerfG als Verhältnismäßigkeitsauftrag von Datenübermittlungen zwischen Nachrichtendiensten und anderen Sicherheitsbehörden zu verstehen.[2039] Da bei der Übermittlung zwischen Diensten und Sicherheitsbehörden der Grundsatz der informationellen Trennung durchbrochen und somit Grundrechte beeinträchtigt werden, muss der Austausch von Gesetzen reglementiert werden. Dabei sind verfassungsrecht-

---

Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (190 f.); *Thiel,* Entgrenzung, 2012, S. 387 ff.

2035 Zu diesem Aspekt *Gusy*, GSZ 2021, 141 (146 ff.); *ders.* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, IV § 2 Rn. 44 ff.; *Thiel,* Entgrenzung, 2012, S. 387 ff.; *Poscher* in Korioth/Vesting (Hrsg.), Verfassungsrecht, 2011, S. 245 (250).

2036 BVerfGE 156, 11 (51 f.) – Antiterrordatei II; strenger noch E 133, 277 (325 f.) – Antiterrordatei I, so auch *Poscher/Rusteberg* KJ 2014, 57 (62 f.).

2037 BVerfGE 133, 277 (29) – Antiterrordatei I E 156, 11 (51 f.) – Antiterrordatei II; zum Umgehungsgedanken: BVerfG, NVwZ-RR 2023, 1 (8) – Nachrichtendienstliche Informationsübermittlung *Gärditz*, JZ 2013, 633 (634); *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (191).

2038 BVerfGE 156, 11 (49 f.) – Antiterrordatei II; E 141, 229 (327 f.) –BKA-Gesetz; BVerfG, NJW 2022, 1583 (1588 Rn. 173 ff., 1596 Rn. 231 ff.) – Bayerisches Verfassungsschutzgesetz; dazu *F. Schneider*, GSZ 2022, 1; *Löffelmann*, GSZ 2019, 16; zum Verhältnis der hypothetischen Neuergebung und Trennungsprinzip in der Rechtsprechung: *Unterreitmeier*, DÖV 2021, 659 (662 f.); s.a. *Gusy*, GSZ 2021, 141 (143).

2039 *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (191); *Unterreitmeier*, DÖV 2021, 659 (660 ff.); *Poscher/Rusteberg* KJ 2014, 57 (68 f.); *dies.* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Reform der Nachrichtendienste, 2020, S. 145 (S. 152 ff.).

liche Grundsätze zu beachten.[2040] Das informationelle Trennungsprinzip wurde von *Bäcker* insofern ganz treffend als „grundrechtliche Reflexwirkung" bezeichnet.[2041]

Regeln über den Datenaustausch mit operativen Sicherheitsbehörden finden sich in allen Gesetzen über die Nachrichtendienste. Danach sind die Dienste unter bestimmten Voraussetzungen berechtigt, andere proaktiv mit Informationen zu versorgen (sog. Spontanübermittlung), § 20 Abs. 1 BVerfSchG, § 11 Abs. 1, 3 BNDG, 10 Abs. 1, § 11 Abs. 2 MADG, § 2 BWVSG, oder um Auskünfte bei anderen Behörden zu ersuchen, § 18 Abs. 3 BVerfSchG, § 10 Abs. 3 BNDG, § 10 Abs. 2 MADG.

Die Sicherheitsbehörden dürfen ihrerseits den Nachrichtendiensten proaktiv Informationen übermitteln, wenn bestimmte Umstände vorliegen, § 18 Abs. 1 BVerfSchG, § 10 Abs. 1 BNDG, § 10 Abs.1 MADG, § 9 Abs. 1 BWVSG. Die Spontanübermittlung unterliegt allerdings grundsätzlich sehr strengen Voraussetzungen.[2042] Neben dieser Möglichkeit der proaktiven Spontanübermittlung können auch die Sicherheitsbehörden, gestützt auf ihr Recht, etwa nach § 161 Abs. 1 S. 1 Alt. 2 StPO, bei den Nachrichtendiensten um Auskunft ersuchen.[2043] Ein Recht für Auskunftsersuchen der Landespolizeien müssen die jeweiligen Landesgesetze separat vorsehen, vgl. etwa Art. 60 Abs. 3 BayPAG. Ob all diese Vorschriften derzeit den Anforderungen des BVerfG zur informationellen Trennung entsprechen, ist durchaus zweifelhaft.[2044]

Die Pflicht der Nachrichtendienste, auf Auskunftsersuchen unter Beachtung ihres Rechts zu antworten, ist aber auf vorhandene Informationen be-

2040 *Gusy*, GSZ 2021, 141 (146); *Bäcker et al.*, (Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland), Sicherheitsgesetzgebung, 2013, S. 200 ff. vgl. zu § 19 BVerfSchG *W. Bock* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BVerfSchG § 19 Rn. 1.

2041 *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 245 ff.

2042 Dazu jüngst BVerfG, NVwZ-RR 2023, 1 – Nachrichtendienstliche Informationsübermittlung

2043 *Krauß/ Matthias* in BeckOK StPO, RiStBV 205, Rn. 40; *Gazeas,* Nachrichtendienstliche Erkenntnisse, 2014, S. 494 mwN; für die nachrichtendienstlichen Vorschriften als spezielle Ermächtigungen *König,* Trennung und Zusammenarbeit, 2005, S. 285.

2044 an § 19 Abs. 1 BVerfSchG zweifeln etwa *Bergemann* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. H Rn. 135 ff.; *Gazeas,* Nachrichtendienstliche Erkenntnisse, 2014, S. 409 ff.; BVerfSchG in BVerfG, NVwZ-RR 2023, 1 – Nachrichtendienstliche Informationsübermittlung beschäftigt sich wegen Verfristung nicht (auch) mit § 19 Abs. 1 BVerfSchG.

grenzt, § 17 Abs. 1 BVerfSchG, § 10 Abs. 3 BNDG, § 10 Abs. 4 MADG.[2045] Die Nachrichtendienste sollen nicht auf Ersuchen anderer Sicherheitsbehörden hin tätig werden.[2046] Andernfalls würden sie zur Ermittlungsperson der jeweiligen ersuchenden Behörde, was das informationelle Trennungsprinzip gerade verhindern soll.

b. Die FIU als Nachrichtendienst?

Eine § 17 Abs. 1 BVerfSchG entsprechende Vorschrift sieht das Anti-Geldwäscherecht nur in Art. 2 Nr. 5 FinanzinformationsRL vor. Die FinanzinformationsRL betrifft in Deutschland aber nur § 32 Abs. 3a GwG.

§ 30 Abs. 3 GwG könnte es deshalb erlauben, dass die FIU auf Ersuchen bestimmter Behörden nach § 32 Abs. 3 GwG Informationen neu beschafft, um diese sodann weiterzuleiten (s. o. III. 2. c.). Dieses Vorgehen passte auch in das Konzept der FIU, deren Aufgabe ja nicht auf die Analyse von Verdachtsmeldungen limitiert ist, sondern allgemein in der Versorgung bestimmter Sicherheitsbehörden mit Finanzinformationen besteht, § 28 Abs. 1 GwG.

Schon aus der Rechtsprechung zur Vorratsdatenspeicherung ergibt sich aber eine Notwendigkeit, das in Art. 2 Nr. 5 FinanzinformationsRL geäußerte Begriffsverständnis auf die Zugriffsregeln der GWRL bzw. des GwG vollständig anzuwenden (oben III. 2. c. bb. & cc.).

Selbst bei einer engen Auslegung der Übermittlungspflichten stellt sich die FIU aber noch immer als proaktive Informationsversorgerin der Sicherheitsbehörden dar. Ein allgemeines, informationelles Trennungsgebot findet sich im Anti-Geldwäscherecht gerade nicht.

aa. Der Begriff der Nachrichtendienste

Da dem informationellen Trennungsgebot in der Rechtsprechung des BVerfG Verfassungsrang zukommt, ist das Fehlen einer Verankerung im

2045 § 10 BNDG und § 10 MADG sind anders als § 17 BVerfSchG mit „Übermittlung von Informationen an den BND/MAD" überschrieben. Auch hier wird aber eine Geltung in beide Richtungen anzunehmen sein.

2046 *Krauß/ Matthias* in BeckOK StPO, RiStBv 205 Rn. 39; *Gazeas,* Nachrichtendienstliche Erkenntnisse, 2014, S. 61 f., 507; vgl. auch BVerfGE 133, 277 (326 f.) – Antiterrordatei I; für dem umgekehrten Fall siehe *Streiß,* Trennungsgebot, 2012, S. 178.

Gesetz gleichgültig, soweit jedenfalls die Grundrechte einschlägig sind (dazu unten). Die Aufgaben der FIU könnten also dem informationellen Trennungsprinzip unterliegen, wenn es sich bei der Behörde um einen *Nachrichtendienst* handelt. Das ganze Konzept des GwG, das zentral auf die FIUs ausgerichtet ist, stünde dann diametral gegen ein verfassungsrechtliches Grundprinzip des Sicherheitsrechts.

Der Gesetzgeber darf die verfassungsrechtlichen Grundsätze, soweit sie Anwendung finden, nicht unterlaufen. Er kann deshalb nicht darüber disponieren, ob eine Behörde im verfassungsrechtlichen Sinne Nachrichtendienst ist oder nicht. Das BVerfG hat in seinen Kernaussagen zum informationellen Trennungsprinzip[2047] in den Urteilen zum ATDG zwar allgemein auf „Nachrichtendienste" abgestellt. Es hat aber auf eine Definition dieses Begriffs verzichten können, da das ATDG abschließend auf die klassischen Nachrichtendienste ausgerichtet war. Es ist somit offen, ob das BVerfG das informationelle Trennungsprinzip ausschließlich auf den Bundesverfassungsschutz, den BND, den MAD und die Landesverfassungsschutzbehörden anwenden will, oder ob es für sämtliche Behörden gilt, die begrifflich einen Nachrichtendienst darstellen.[2048]

Damit stellt sich das Problem ein, dass eine allgemeingültige Definition der Nachrichtendienste nicht vorliegt.[2049] Das Grundgesetz erwähnt nur die „nachrichtendienstliche Tätigkeit" in Art. 45d GG und den „Verfassungsschutz" in Art. 73 Abs.1 Nr. 10 lit. b) c), 87 Abs. 1 S. 2 GG. Es überlässt deren Gründung und Ausgestaltung aber den Bundes- und Landesgesetzgebern. Eine institutionelle Garantie besteht daher nach gängiger Auffassung nur für die nachrichtendienstliche Tätigkeit an sich, nicht für einzelne Behörden.[2050] Ob eine Behörde als Nachrichtendienst einzustufen ist, muss daher allein von der verfassungsrechtlichen Begriffswertung bzw. dem Cha-

2047 BVerfGE 133, 277 (329) – Antiterrordatei I; E 156, 11 (50) – Antiterrordatei II; NJW 2022, 1583 (Rn. 171 ff.) – Bayerisches Verfassungsschutzgesetz.

2048 Allgemein zum Begriff „Nachrichtendienst" *Gröpl,* Nachrichtendienste, 1993, S. 37 f.

2049 Ausf. *Dietrich* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, III § 3 Rn. 2 ff.

2050 Vgl. *Uhle* in Dürig/Herzog/Scholz GG, Art. 73 Rn. 241; *J. Hecker* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, III § 2 Rn. 8 ff.; *Gröpl,* Nachrichtendienste, 1993, S. 64 ff; 82 ff; 133 ff.; *J. Franz Lindner/Unterreitmeier*, DÖV 2019, 165 (167 f.); in Richtung einer institutionellen Garantie für das BfV aber BVerfGE 30, 1 (20); dazu *Badura* in *Bundesamt für Verfassungschutz* (Hrsg.), Deutschland, Bundesamt für Verfassungschutz 1990, 1990, S. 27 (27 ff.).

rakter der Behörde abhängen.[2051] Insofern ist auf die Aufgabenzuweisung der Behörde und deren gesetzlicher Befugnisse abzustellen. Nachrichtendienste zeichnen sich danach durch ihre informationsbezogene Stellung im rechtlichen Sicherheitsgefüge aus.[2052]

Es gibt keinen Grund, den Begriff der Nachrichtendienste auf bestehende Behörden zu beschränken. Betreffend die parlamentarische Kontrolle nach Art. 45d GG scheint es heute herrschende Meinung zu sein, dass diese Verpflichtung „zukunftsoffen" ist, also auch auf weitere Behörden angewandt werden muss, so diese „nachrichtendienstliche Tätigkeiten" ausüben.[2053] Diese Offenheit muss nicht nur für die parlamentarische Kontrolle, sondern für alle verfassungsrechtlichen Grundsätze, die die „Nachrichtendienste" betreffen, gelten.

Stellt sich eine Behörde also als Nachrichtendienst dar, muss das sie betreffende Recht den verfassungsrechtlichen Vorgaben genügen – insbesondere dem informationellen Trennungsprinzip (s. o.).

§ 30 Abs. 3 GwG und § 32 Abs. 3 GwG beinhalten fast keine Voraussetzungen für den Datenaustausch zwischen der FIU und den in § 32 Abs. 3 GwG aufgeführten Sicherheitsbehörden. Auch kann jedenfalls die Staatsanwaltschaft, anders als die FIU, Privatpersonen nicht zu heimlichen informellen Auskünften verpflichten. Sie kann allenfalls um solche Informationen bitten oder Zeugenuntersuchungen und Beschlagnahmen durchführen. Insofern ist jedenfalls auf gesetzlicher Ebene eine deutliche Diskrepanz zwischen den Befugnissen der Behörden festzustellen.

Ob § 30 Abs. 3 GwG und § 32 Abs. 3 GwG daher noch dem informationellen Trennungsprinzip und insb. den Voraussetzungen der hypothetischen Datenneuerhebungen entsprechen, ist daher mehr als fraglich. Es muss folglich zunächst geklärt werden, ob die FIU als Nachrichtendienst einzustufen ist.

2051 Vgl. *Hermes* in Dreier GG, Art. 45d Rn. 22 ff.

2052 *Dietrich* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, III § 3 Rn. 4 ff.; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 21.

2053 *Hermes* in Dreier GG, Art. 45d Rn. 25; ihm folgend *H. Klein* in Dürig/Herzog/Scholz GG, Art. 45d Rn. 40 f.; *S. Unger* in v. Mangoldt/Klein/Starck GG, Art. 45d Rn. 10.

bb. Der **Rechtscharakter** der FIU nach dem GwG

Der Rechtscharakter der – von dem Mitgliedstaaten einzurichtenden – FIUs wird von der GWRL nicht determiniert. Entscheidend ist nur, dass sie als Behörden unabhängig und in ihrem Aufgabenbereich frei sind, Art. 32 Abs. 3 GWRL.[2054] International haben sich deshalb unterschiedliche Modelle für die FIUs durchgesetzt, die gewöhnlich als „administrative"-, „law enforcement"-, „judicial"- oder „hybrid models" klassifiziert werden.[2055] Von Europol etwa wird die deutsche FIU als „law enforcement type" angesehen, wohl da sie eigenständige Ermittlungen vornehmen kann.[2056] Der Begriff „law enforcement" ist aber für eine Einordnung der FIU nach deutschem Recht kaum brauchbar, da er nicht zwischen repressivem und präventivem Polizeihandeln unterscheidet.[2057] Der Begriff „administrative typ", den Europol verwendet, ist deutlich enger als der deutsche Begriff einer Verwaltungsbehörde und wird auf Behörden begrenzt, die selbst keine Gefahrenabwehr oder Strafverfolgung betreiben, wie beispielsweise in Italien, wo die FIU bei der Banca d'Italia angesiedelt ist.[2058]

Zur Einordnung der Problematik hilft ein Blick in die Vergangenheit. Bevor die FIUs europarechtlich obligatorisch wurden, mussten die Verpflichteten verdächtige Transkationen in Deutschland unmittelbar an die zuständigen Strafverfolgungsbehörden übermitteln, § 11 Abs. 1 GwG 1993.[2059] Erst mit Umsetzung der 2. EG-GeldwäscheRL wurde in § 5 GwG 2002[2060] eine

2054 S.a. *FATF,* Recommendations 2012, konsolidierte Fassung März 2022, Empfehlung 29, S. 24, 102.

2055 Vgl. *Europol,* Suspicion to Action, 2017, S. 28 f.; *IWF*, (Weltbank), FIUs Overview, 2004, S. 8 ff.; *FATF,* Recommendations 2012, konsolidierte Fassung März 2022, S. 102; *Maillart* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 71 (119); *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (7 ff.).

2056 *Europol,* Suspicion to Action, 2017, S. 28; s.a. *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (8).

2057 *Möstl* in BeckOK POR NRW, Syst. Vorb. Rn. 86; zur Dichotomie krit. *Danne,* Prävention und Repression, 2022, insb. S. 225 ff.

2058 *Amato* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 303 (354 ff.); *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (8).

2059 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG) vom
25.Oktober 1993 (BGBl. I S. 1770).

2060 Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des
Terrorismus (Geldwäschebekämpfungsgesetz) vom 08. August 2002 (BGBl. I S. 3105).

zentrale Stelle für die Sammlung der Verdachtsanzeigen beim BKA eingerichtet. Deren Aufgabe bestand nach § 5 Abs. 1 GwG 2002 darin, *die Polizeien bei der Verhütung und Verfolgung von Geldwäsche und Finanzierung von Terrorismus zu unterstützen*. Etwa durch das Sammeln der Meldungen, deren statistischer Analyse und dem Veröffentlichen von Berichten, § 5 Abs. 2 GwG. Die Verpflichteten mussten nach § 11 Abs. 1 GwG 2002 aber weiterhin ihre Verdachtsfälle an die zuständigen Strafverfolgungsbehörden melden und dem BKA lediglich eine Kopie vorlegen. Daran änderte sich auch durch die Umsetzung der 3. GWRL, §§ 10, 11 GwG 2008[2061] und die Änderungen in Folge des FATF-Deutschlandberichts nichts, §§ 10, 11 GwG 2011.[2062]

Erst, nachdem die FIU im Jahr 2017 im Rahmen der Umsetzung der 4. GWRL aus dem BKA herausgelöst und bei der Generalzolldirektion als Abteilung innerhalb der Direktion Zollkriminalamt eingegliedert wurde, waren die Meldungen gem. § 43 Abs. 1 GwG nur noch an die FIU und nicht mehr an die Strafverfolgungsbehörden zu richten. Die Eingliederung beim Zollkriminalamt wurde allerdings später revidiert und die FIU als eigene Direktion bei der Generalzolldirektion eingerichtet, § 5a Abs. 2 FVG.[2063] Damit dürfte jedenfalls klargestellt worden sein, dass die FIU keine Aufgaben der Zollfahndung übernimmt, § 5a Abs. 3 S. 2 FVG, und nicht nach § 52 S. 2 ZFdG als Ermittlungsperson der Staatsanwaltschaft angesehen werden kann.

Die Umstrukturierung 2017 veranlasste in der Bundesrepublik eine Diskussion über den Charakter der FIU bzw. ihrer Aufgaben.[2064] Hatte sich zuvor aus der Meldepflicht an die Strafverfolgungsbehörden noch recht klar ein Zusammenhang zur Strafverfolgung ergeben, war nunmehr fraglich, wie die Arbeit der FIU als Zwischenstelle von Finanzwirtschaft und Sicherheitsbehörden innerhalb der deutschen Sicherheitsarchitektur zu verorten sei.

2061 Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäsche-bekämpfungsergänzungsgesetz - GwBekErgG) vom 13. August 2008 (BGBl. I S. 1690).

2062 Gesetz zur Optimierung der Geldwäscheprävention vom 22. Dezember 2011 (BGBl. I S. 2959).

2063 Siebtes Gesetz zur Änderung von Verbrauchsteuergesetzen vom 30.03.2021 (BGBl. I. S. 607).

2064 Vgl. *Da Barreto Rosa* in Herzog GwG, GwG Vorb. zu Abschn. 5 Rn. 7 ff.

(1) „Zentralstellen" in der deutschen Sicherheitsarchitektur

Die deutsche FIU trägt nach § 27 Abs. 1 GwG den Namen „Zentralstelle für Finanztransaktionsuntersuchungen." Der Begriff der Zentralstelle ist dem Verfassungsrecht entnommen. Nach Art 87 Abs. 1 S. 2 GG dürfen durch Bundesgesetz *Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen, für die Kriminalpolizei und zur Sammlung von Unterlagen für Zwecke des Verfassungsschutzes* geschaffen werden. Ausdrücklich als Zentralstelle wird denn auch das BKA bezeichnet, das nach § 2 Abs. 1 BKAG als *Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen* fungiert. Bei Schaffung der FIU, die ursprünglich beim BKA angesiedelt war, wollte der Gesetzgeber durch die Benennung als Zentralstelle an den Charakter des BKA anknüpfen.[2065]

Tatsächlich liegt ein Vergleich der FIU mit dem BKA nahe. Aufgabe des BKA ist das Sammeln, Auswerten und Weitergeben von Informationen zur Gefahrenabwehr und Strafverfolgung, § 2 Abs. 1 BKAG. Gefahrenabwehr und Strafverfolgung als gemeinsame polizeiliche Aufgaben überschneiden sich hier, eine funktional-organisatorische Trennung dieser Rechtsgebiete ist für das BKA gerade nicht bzw. nur intern vorgesehen.[2066] Spätestens mit der Erweiterung der Aufgaben des BKA im Rahmen der Terrorismusbekämpfung[2067] ist eine einheitliche Charakterisierung des BKA aber ohnehin nicht mehr möglich. Es ist Zentralstelle, Kriminalpolizei und Gefahrenabwehrbehörde zugleich.

Anders als die FIU ist die Arbeit des BKA als Zentralstelle auf die Koordinierung[2068] polizeilicher Informationen gerichtet, nicht auf deren Erhebung. Zwar hat das BKA nach § 9 BKAG das Recht, zur Erfüllung seiner Zentralstellentätigkeit Informationen zu erheben. Diese Befugnis ist aber restriktiv dahingehend auszulegen, dass die Erhebung allein dem Ver-

2065 BT-Drs. 14/8739, S. 13 f.

2066 *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 577; *Ibler* in Dürig/Herzog/Scholz GG, Art. 87 Rn. 129; *Hermes* in Dreier GG, Art. 87 Rn. 47.

2067 BVerfGE 141, 220 (224) – BKA-Gesetz; s.a. *A. Schmidt* KJ 2010, 307.

2068 BVerfGE 110, 33 (51).; *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 76; *Ibler* in Dürig/Herzog/Scholz GG, Art. 87 Rn. 117 ff.

ständnis und der Komplementierung bestehender Informationen dienen darf.[2069]

Als Hauptaufgabe des BKA stellt sich in diesem Zusammenhang die Einrichtung und Organisation von Verbundsystemen nach § 29 BKAG sowie Amts- und Zentraldateien nach § 13 BKAG dar. Wichtigstes Verbundsystem ist dabei das zentrale System INPOL.[2070] Gespeichert werden hier sowohl Grunddaten zu Personen als auch Falldaten zur Analyse komplexer Sachverhalte.[2071] Sinn des Verbundsystems ist der Datenaustausch der verschiedenen Polizeien von Bund und Ländern.[2072] Zeitlich und lokal übergreifend relevante Informationen, die im Rahmen der Informationsbeschaffung durch die einzelnen Behörden anfallen, sollen hier zur Verfügung gestellt werden, § 30 BKAG. Verantwortlich für die einzelnen Daten sind immer die einstellenden Behörden, § 31 Abs. 2 BKAG. Das BKA nimmt also nur eine koordinierende und unterstützende Funktion ein. Es analysiert die eingestellten Informationen nicht proaktiv mit dem Ziel, Sicherheitsbehörden zu Ermittlungen anzuregen, sondern übermittelt nach § 2 Abs. 2 BKAG nur dann Informationen, wenn es schon weiß, welche Strafverfolgungsbehörde mit einem Fall betraut ist.[2073] Gegenüber den anderen Sicherheitsbehörden besteht die Arbeit des BKA hinsichtlich der Verbundsysteme also primär in der technischen Bereitstellung. Es ist als koordinierender „Servicedienstleister" und nicht als Informationsbeschaffer zu verstehen.[2074]

Die Aufgaben der FIU sind anders gelagert. Zwar unterhält auch sie ein Informationssystem, ist aber nicht auf eine unterstützende bzw. koordinierende Servicefunktion beschränkt. Die FIU muss die sie erreichenden Informationen eigenständig analysieren, um festzustellen, ob diese für weitere Sicherheitsbehörden relevant sind oder nicht, Art. 32 Abs. 2 S. 3 GWRL, § 30 Abs. 2 GwG. Die FIU ist also nicht nur Sammel- und Koordinations-

2069 *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 133; BT-Drs. 13/1550, S. 24.

2070 BT-Drs. 18/8596.

2071 BT-Drs. 18/8596, S. 1 f.; *BMI,* White Paper Polizei 2020, S. 5; *Arzt* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 1204 f.; *Graulich* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BKAG § 29 Rn. 1 f.

2072 *Graulich* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BKAG § 13 Rn. 3, § 29 Rn. 1 f.

2073 Idem, § 2 Rn. 35.

2074 Vgl. *BMI,* White Paper Polizei 2020, S. 3 "serviceorientierter Dienstleister"; *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 132; *Hermes* in Dreier GG, Art. 87 Rn. 47: "Service".

stelle, sondern aktiv – insbesondere in den Prozess der Einleitung von Ermittlungsverfahren – eingebunden. Sie ist dafür verantwortlich, dass Informationen in Bezug auf Geldwäsche und Terrorismusfinanzierung, die naturgemäß bei Privaten entstehen und nur durch deren umfangreiche Überwachung erkannt werden können, ihren Weg zu den Strafverfolgungsbehörden finden. Sie versorgt damit Sicherheitsbehörden mit *neuen* Informationen, anstatt lediglich polizeilich erlangte Informationen horizontal zur Verfügung zu stellen. Der Aufgabenbereich des BKA als Zentralstelle lässt daher keinen Rückschluss auf den Charakter der Aufgaben der FIU zu.

(2) Die FIU als administrative Gefahrenabwehrbehörden?

Nach Vorstellung des Gesetzgebers unterstrich die Einordnung unter das Dach der Generalzolldirektion und damit des Finanzministeriums den präventivpolizeilich administrativen Charakter der FIU.[2075] Der Bundesrat hatte im Gesetzgebungsverfahren erhebliche Zweifel geäußert, ob eine administrative Ausrichtung für eine Behörde sinnvoll sei, die vorwiegend Vorbewertungen genuin strafrechtlicher Sachverhalte vornehme.[2076]

Der Zweck der FIU besteht laut § 27 Abs. 1 GwG in der Verhinderung, Aufdeckung und Unterstützung bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Daraus ergibt sich, dass die FIU in sachlicher Hinsicht sowohl Gefahrenabwehr durch Verhinderung der Geldwäsche betreiben als auch die Strafverfolgung unterstützen will.[2077] Durch beide Zwecke unterscheidet sie sich elementar von den Nachrichtendiensten. In der Diskussion um die Einordnung der FIU spielt daher auch weniger der Vergleich mit Geheimdiensten eine Rolle, als die Frage, ob die FIU eine Behörde der Gefahrenabwehr oder Strafverfolgung darstellt, oder ob sie überhaupt in eine der beiden Kategorien einsortiert werden kann.

Mit dieser Thematik hat sich jüngst *Bülte* ausführlicher beschäftigt, der dem Gesetzgeber dogmatische Rückendeckung verschafft. Für ihn lassen die Vorschriften der §§ 27 ff. GwG über die Aufgaben der FIU die gesetzgeberische Prämisse erkennen, dass es sich bei der FIU um eine administrative Gefahrenabwehrbehörde handelt. Er stützt diesen Befund darauf, dass neben der Sammlung, Analyse und Weiterleitung von Daten auch Sofort-

2075 BT-Drs. 18/11555, S. 136, 168; zust. etwa *Krais,* Geldwäsche, 2018, Rn. 475.
2076 BR-Drs. 182/1/17, S. 21; BT-Drs. 18/11928, S. 11 f.
2077 *Degen,* Geldwäsche, 2009, S. 148 ff.

maßnahmen zur Verhinderung von Geldwäsche gem. §§ 40 ff. GwG von der FIU ergriffen werden müssen.[2078] Auch aus den FATF-Empfehlungen und der GWRL ergäbe sich, dass die Geldwäschebekämpfung tendenziell dazu gedacht sei, effizient Straftaten in der Zukunft zu verhindern, indem die Verwertung der strafbar erlangten Vermögenswerte erschwert wird.[2079] In der Tat ist das Ziel der Geldwäschebekämpfung die Verhinderung der Geldwäsche zum Schutz des Binnenmarkts.[2080]

Dieser Umstand könne nach *Bülte* aber nicht darüber hinwegtäuschen, dass die Aufgaben der FIU doch ganz primär darauf ausgerichtet sind, strafbares Verhalten aufzudecken, da ja nicht nur die Vortaten, sondern die Vermögensverwertung selbst durch die Einführung der Geldwäschestrafbarkeit (in § 261 StGB) kriminalisiert würde.

Er bezweifelt denn auch, dass sich aus den internationalen Vorgaben Rückschlüsse auf den Charakter der deutschen FIU schließen ließen. In Deutschland würde das Strafrecht gemeinhin als eigenes Rechtsgebiet verstanden[2081], bei dem die Strafe im Vordergrund stünde und Prävention nur einen erwünschten Nebeneffekt darstelle. Diese Strafrechtsphilosophie läge dem Europäischen Gesetzgeber nicht zugrunde, der Strafe zwar als effektive, aber nur als eine von vielen Form der Prävention verstünde.[2082] Für das GwG, dem die deutsche Strafrechtsphilosophie zugrunde liegt, sei damit also noch nichts entschieden.

Daher stellt *Bülte* bei seiner Bewertung des Rechtscharakters der FIU allein auf deren Aufgaben und Ermächtigungen nach dem GwG ab. Hier kommt er sodann aber zu demselben Ergebnis wie der Gesetzgeber und stuft die FIU als Behörde der Gefahrenabwehr ein. Es könne zwar nicht außer Acht bleiben, dass die FIU aktiv bei der Aufklärung von Straftaten mitwirkt, allein die Mitwirkung bzw. Unterstützung der Strafverfolgung sei aber eben noch keine Strafverfolgung. Vielmehr bestünden die Aufgaben der FIU in sog. „Vorermittlungen",[2083] also Ermittlungen, die lediglich abklären sollen, ob in einem bestimmten Fall eventuell ein Anfangsverdacht be-

2078 *Bülte*, NVwZ-Extra 4b/2022, 1 (9 f).
2079 Idem, (15 f.).
2080 Vgl. nur Erwägungsgrund Nr. 1 der 4. EU-GeldwäscheRL
2081 Vgl. etwa *Gärditz,* Strafprozeß & Prävention, 2003, S. 8 ff.; *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 577.
2082 *Bülte*, NVwZ-Extra 4b/2022, 1 (16); dazu *Engelhart* in Engelhart/Roksandić Vidlička (Hrsg.), Terrorism, 2019, S. 287 (295).
2083 *Bülte*, NVwZ-Extra 4b/2022, 1 (17)

stehen könnte.[2084] Etliche Verwaltungsbehörden, etwa im Tierschutz- oder Waffenrecht, würden solche Vorermittlungen vornehmen, die in Strafverfahren münden könnten, ohne dass sie deshalb Strafverfolgung betreiben würden.[2085]. Bei der Frage, ob Ermittlungen eine Strafverfolgung darstellen, müsse deshalb streng auf die Ermittlungsbehörde abgestellt werden. Danach sollen nur solche Ermittlungen einen strafverfahrensrechtlichen Charakter aufweisen, die von einer Behörde geführt werden, die zum Führen von Strafverfahren befugt ist.[2086]

(3) Die FIU als (vorermittelnde) Strafverfolgungsbehörde.

Diese Aussage von *Bülte* klingt nach einem Zirkelschluss. Die Frage, welche Behörden *zum Führen von Strafverfahren befugt sind*, ist ja gerade die zu beantwortende. Mit der Aussage „*strafverfahrensrechtliche Ermittlungen sind Ermittlungen von Strafverfahrensbehörden*" ist nichts gewonnen, wenn nicht klar ist, was eine *Strafverfahrensbehörde* konstituiert.

Offenbar stellt *Bülte* bei der Bestimmung des Begriffs des Strafverfahrens bzw. der Strafverfolgung allein auf die Ermächtigung zur Anklage nach §§ 152 Abs.1, 170 StPO ab, die außerhalb des Steuerstrafrechts (§§ 385 ff. AO) exklusiv der Staatsanwaltschaft zusteht. Nach seiner Auffassung können also allein die Staatsanwaltschaft und deren Ermittlungsbehörden (sowie die Finanzbehörden[2087] im Steuerstrafrecht) eine strafverfahrensrechtliche Behörde sein, denn sie allein sind befugt, einen Strafprozess im engeren Sinne einzuleiten. Er geht somit von einem strikt formellen Begriff des Strafverfahrens oder der Strafverfolgung aus. Damit hätte der Gesetzgeber den Begriff der Strafverfolgung einfachgesetzlich abschließend durch die §§ 152 ff. StPO geklärt. Ob ihm das zusteht, ist aber gerade die Frage, da auch ein verfassungsrechtlicher bzw. materieller Begriff der Strafverfolgung denkbar wäre, der auch Vorermittlungen miteinschließt.[2088]

2084 Dazu insb. Abgrenzung zu „Vorfeldermittlungen": *Zöller,* Informationssysteme, 2002, S. 127 ff.; *Rogall*, ZStW 1991, 907 (945 ff.); *Roxin/Schünemann,* Strafverfahrensrecht, 29. Aufl. 2017, § 39 Rn. 17 f.

2085 *Bülte*, NVwZ-Extra 4b/2022, 1 (17).

2086 Ibid.

2087 Nach § 386 Abs. 1 AO auch die Hauptzollämter, nicht aber die Generalzolldirektion.

2088 BVerfGE 113, 348 (371) für Maßnahmen der Strafverfolgungsvorsorge; *Barreto da Rosa* in Herzog GwG, § 30 Rn. 13; *N. Lange*, DRiZ 2002, 264 (266); vgl. auch

Bekannt ist diese Fragestellung aus der Diskussion um die sog. „Strafverfolgungsvorsorge" durch die Polizei bzw. den „doppelfunktionalen Maßnahmen", bei denen präventive und repressive Elemente vermischt sind.[2089] In diesem Umfeld bewegt sich auch die Tätigkeit der FIU, die im Rahmen ihres großen Bestrebens, Geldwäsche zu verhindern, ja nicht zuletzt die Durchführung von Strafverfahren ermöglichen soll.[2090]

Das BVerfG hat sich hinsichtlich der Gesetzgebungskompetenz für doppelfunktionale Ermächtigungen für einen materiellem Begriff der Strafverfolgung entschieden. Danach fällt grundsätzlich jede Beweisbeschaffung zur Verwendung in künftigen Strafverfahren und mithin auch die Verfolgungsvorsorge unter den Begriff der Strafverfolgung bzw. das *gerichtliche Verfahren* i. S. d. Art. 74 Abs. 1 Nr. 1 GG.[2091] Das BVerfG hat insofern polizeirechtliche Ermächtigungen mit jedenfalls teilweise repressiven Zügen nicht schon deswegen als Verwaltungshandeln eingestuft, weil keine „Strafverfahrensbehörde" ermächtigt wurde, sondern auf den konkreten Zweck der Maßnahme abgestellt. Daraus lässt sich ableiten, dass Vorermittlungen nicht schon deshalb keine Strafverfolgung darstellen können, nur weil sie von einer Behörde durchgeführt werden, die kein Strafverfahren i. S. d. §§ 152 ff., 170 StPO einleiten bzw. die öffentliche Anklage erheben darf.

Man kommt um eine materielle Charakterbeschreibung der FIU also nicht herum. Dabei helfen ihre Aufgaben in der Gesamtschau kaum weiter. Das Sammeln und Analysieren von Daten ist in der modernen Sicherheitsarchitektur eine Standardaufgabe sämtlicher Sicherheitsbehörden. Sie alle sind zur Erhebung und Verarbeitung von Daten ermächtigt. Auch ihre Befugnisse zu heimlichen Maßnahmen unterscheiden sich kaum noch.[2092] Bei

---

Schenke, FS Paeffgen, 2015, S. 393 (396 ff.); allg. zum Begriff der Strafverfolgung *Greco,* Strafprozesstheorie, 2015, S. 119 ff.

2089 Vgl. BVerfGE 150, 244 (275 ff.) – Autom. Kennzeichenerfassung II; *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 2 Rn. 9 ff.; *Brodowski,* Überwachungsmaßnahmen, 2015, S. 327 ff.; *Buchberger* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. K Rn. 17 ff.; *Graulich*, NVwZ 2014, 685 (688 ff.); vgl. zum GwG *Degen,* Geldwäsche, 2009, S. 148 ff.

2090 Zur Abgrenzung von Vorermittlungen und Strafverfolgungsvorsorge *Zöller,* Informationssysteme, 2002, S. 127 ff.; *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 152 Rn. 4b.

2091 BVerfGE 113, 348 (369 ff.); E 103, 21 (30 ff.); dazu *Bäcker,* Kriminalpräventionsrecht, 2015, S. 249 ff.; *Schenke*, FS Paeffgen, 2015, S. 393.

2092 *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 12.

der Einteilung einer Behörde in die deutsche Sicherheitsarchitektur muss es daher auf den Schwerpunkt in der Zielsetzung ihrer Tätigkeit ankommen.

Die Hauptaufgabe der FIU dürfte angesichts der Fülle an Verdachtsmeldungen (s. o. Kap. D. III. 2. c. aa. (1)) in der Analyse verdächtiger Transaktionen bestehen. Die Bundesregierung selbst bezeichnete die Filterfunktion der FIU als deren „zentralen Mehrwert".[2093] Dieser Einschätzung hat sich der *wissenschaftliche Dienst des Bundestages* angeschlossen und festgestellt, dass sich die Funktion der FIU seit der Herauslösung aus dem BKA kaum geändert hat. Er hegt deshalb an der rein administrativen Aufgabe der FIU „gewisse Zweifel".[2094]

Nach der gängigen Definition des Verdachtsfalls müssen die meldenden Verpflichteten zwar keinen Anfangsverdacht i. S. d. § 152 Abs. 2 StPO prüfen, sondern lediglich feststellen, ob geldwäscherechtliche Auffälligkeiten vorliegen (s. o. Kap. D. III. 2. c. aa. (2)). Damit ist aber über die Analysetätigkeit der FIU noch nichts gesagt. Bei dieser kommt es ja gerade darauf an, die Spreu vom Weizen zu trennen. Nach § 32 Abs. 2 GwG ist das Ergebnis der Analyse proaktiv weiterzuleiten, wenn die FIU feststellt, *dass ein Vermögensgegenstand tatsächlich mit Geldwäsche, Terrorismusfinanzierung oder sonst einer Straftat in Zusammenhang steht.*

Nach Vorstellung des Gesetzgebers soll der Verdachtsgrad solcher Feststellungen noch immer unterhalb eines Anfangsverdachts stehen, da die Bewertung des Anfangsverdachts allein der Strafverfolgungsbehörde zustehen soll.[2095] Gleichzeitig muss der Verdachtsgrad aber über jenem der Verpflichteten i. S. d. § 43 GwG liegen, sonst wäre die Analysetätigkeit unnötig.

Schon für den Anfangsverdacht i. S. d. §§ 152 Abs. 2, 160 StPO reichen nach gängiger Definition *zureichende tatsächliche Anhaltspunkte* aus, allein vage Anhaltspunkte oder Vermutungen sollen unzureichend sein.[2096] Die Rechtsprechung geht mit dieser Definition des Anfangsverdachts sehr großzügig um, wie der Mikado-Fall eindrücklich belegt (s. o. Kap E. I. 1. c. bb.). Sie belässt der Staatsanwaltschaft einen Einschätzungsspielraum.[2097] In der Literatur wird der Anfangsverdacht deshalb teilweise als reines

2093 BT-Drs. 18/11928, S. 26; s.a. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248).
2094 *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21 f.
2095 BT-Drs. 18/11555, S. 144
2096 BVerfGE 115, 166 (197 f.); *B. Schmitt* in Meyer-Goßner/Schmitt StPO, § 152 Rn. 4.
2097 BVerfG, NJW 1984, 1451 (1452); BGH, NJW 1970, 1543; NJW 1990, 96 (97 f.); *S. Peters* in MüKo StPO, § 152 Rn. 49 mwN.

Willkürverbot betrachtet.[2098] Unter dieser Schwelle dürfte aufgrund des Rechtsstaatsprinzips keine staatliche Ermächtigung ansetzen.

Schon eine klare Unterscheidung zwischen dem Verdachtsgrad der Meldepflicht nach § 43 Abs. 1 GwG und dem Anfangsverdacht nach § 152 Abs. 2 StPO ist deshalb schwierig und es war lange Zeit umstritten, ob es überhaupt einen Unterschied geben kann und soll (s. o. Kap. D. III. 2. c. aa.). Konsequenterweise stellt sich dann aber erst recht die Frage, ob ein eigener Verdachtsgrad für Weiterleitungen der FIU nach § 32 Abs. 2 GwG zwischen den sehr eng beieinander liegenden Polen der § 43 GwG und §§ 152 Abs. 2, 160 StPO überhaupt beschrieben und praktisch umgesetzt werden kann. Angesichts der kaum zu unterscheidenden Definitionen schon von § 43 Abs. 1 GwG und § 152 Abs. 2 StPO scheint es sich vielmehr um eine völlig abstrakte Vorstellung zu handeln.[2099]

Faktisch werden die Analysetätigkeiten der FIU damit auf die Prüfung eines strafprozessrechtlichen Anfangsverdachts hinauslaufen. Da aufgrund der Kriminalisierung der Geldwäsche nach § 261 StGB eine Strafbarkeit nicht nur mit der Vortat, sondern der Vermögensverschiebung selbst verbunden ist, die das Objekt der operativen Analyse darstellt, beschäftigt sich die FIU letztlich essenziell mit der Aufdeckung von Straftaten.[2100] Selbst wenn die FIU die Transaktion nach § 40 GwG stoppt und damit im Einzelfall präventiv tätig wird, müsste regelmäßig auch dann eine Weiterleitung an die Staatsanwaltschaft zur Einleitung einer Strafverfahrens nach § 32 Abs. 2 GwG erfolgen, da nach § 261 Abs. 3 StGB bereits der Versuch der Geldwäsche strafbar ist. Die Analyse verdächtiger Meldungen i. S. d. § 43 Abs. 1 GwG ist also entweder strafverfahrensrechtlicher und gefahrenabwehrrechtlicher[2101] oder allein strafverfahrensrechtlicher Natur. Dass eine positive Analyse nur gefahrenwehrrechtliche Maßnahmen nach sich zieht, ist hingegen kaum denkbar. Ausschließlich präventiv handelt die FIU nur in der Gesamtschau, wenn man davon ausgeht, dass durch die Menge der repressiven Einzelvorgänge die Nutzung des Finanzsystems zur Geldwäsche letztlich unmöglich gemacht wird. Von diesem Ziel ist die

2098 *Diemer* in KK-StPO, § 152 Rn. 7; *Hoven*, NStZ 2014, 316 (366 ff.); vgl. auch BVerfG, NStZ-RR 2004, 143 (143); NJW 1984, 1451(1452).

2099 *Barreto da Rosa* in Herzog GwG, § 32 Rn. 10.

2100 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248).

2101 Zu Überschneidungen wegen der Versuchsstrafbarkeit s.a. BVerfGE 113, 348 (373) [2005] – TKÜ

Geldwäschebekämpfung offenbar aber noch weit entfernt (s. o. Kap. D. III. 2. c. aa. (1)).[2102]

Angesichts dessen scheint eine Zuordnung der Aufgaben der FIU nach dem GwG allein zum Gefahrenabwehrrecht angesichts der primären Funktion der individuellen Transaktionsanalyse nicht möglich.[2103] Die Primärfunktion der FIU in der Bundesrepublik als Filterstelle verdächtiger Transaktionen stellt sich vielmehr primär als Vorermittlung zur Vorbereitung etwaiger Strafverfahren dar. Auch wenn die FIU keine Ermittlungen im Sinne der StPO durchführt, ist sie vorrangig doch mit Prozessen betraut, die sich im weiteren bzw. verfassungsrechtlichen Sinne als Strafverfolgung identifizieren lassen.

(4) Diskussion auf europäischer Ebene

Auch auf europäischer Ebene wird die Ausrichtung der FIUs als administrative Strafverfolgungs- oder Justizbehörde diskutiert. *Brewczynska*[2104] hat sich dieser Thematik jüngst ausführlich gewidmet.

Sie greift die internationale Unterscheidung zwischen den „administrative", „law-enforcement", „judicial" und „hybrid"[2105] Formen (s. o.) der FIU auf, bemerkt aber, dass die Einordnung letztlich aufgrund der Aufgaben bzw. der Aktivitäten der FIU erfolgen muss, da hiervon abhängt, welches Datenschutzregime für die Maßnahmen der FIU Anwendung findet.[2106]

Die Frage nach dem Rechtscharakter der FIU stellt sich also nicht nur in Deutschland wegen des Prinzips der informationellen Trennung, sondern auch im Rahmen des europäischen Datenschutzrechts.

Die Grenze zwischen der JI-RL und der DSGVO hält *Brewczynska* hinsichtlich der Verwendung bzw. Weitergabe persönlicher Daten von Privaten an Sicherheitsbehörden für schwer bestimmbar, wenn die Daten von den Privaten eigentlich zu anderen als sicherheitsrechtlichen Zwecken gespeichert wurden. Ein solcher Fall liege auch bei der Verarbeitung von Finanz-

2102 Vgl. auch *T. Fischer,* StGB, 69. Aufl. 2021, § 261 Rn. 4b ff.

2103 *Barreto da Rosa* in Herzog GwG, § 30 Rn. 13; vgl. allgemein für das GwG *Degen,* Geldwäsche, 2009, S. 152 ff.

2104 *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612.; s.a. *Quintel*, ERA Forum 2022, 53.

2105 Vgl. *Europol,* Suspicion to Action, 2017, 28 f.; *IWF*, (Weltbank), FIUs Overview, 2004, S. 8; *FATF,* Recommendations 2012, konsolidierte Fassung März 2022, S. 102.

2106 Dazu auch *Quintel*, ERA Forum 2022, 53 (63 ff.).

daten durch die FIU vor.[2107] Soweit eine Datenverarbeitung der FIU als Verantwortlicher nach Art. 3 Nr. 8 der JI-RL zuzurechnen ist, müsste deshalb geklärt werden, ob die JI-Richtlinie oder die DSGVO einschlägig ist. Dies wiederum hänge davon ab, ob es sich bei der FIU um eine „zuständige Behörde" i. S. d. Art. 3 Nr. 7 der JI-RL handle, was der Fall ist, *„wenn sie zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder für die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist"*. Dies hänge schließlich von den Aufgaben der FIU ab.[2108]

Die Aufgaben der FIU würden zunächst recht klar den Anschein erwecken, unter die in Art. 3 Nr. 7 der JI-RL zu fallen, da ihr nach Art. 32 Abs. 1 der 4. GWRL die Bekämpfung, Aufdeckung und Verhinderung von (strafbarer) Geldwäsche und Terrorismusfinanzierung obliege. Andererseits sei fraglich, ob ihre Maßnahmen, die vornehmlich im Sammeln und Auswerten von Informationen bestünden, für diese Zwecke überhaupt ausreichend seien. Diese seien primär auf die Weitergabe an andere Behörden insb. die Staatsanwaltschaften gerichtet, die dann auf Grundlage der Informationen die Strafverfolgung vorantreiben. Die FIU agiere somit mehr als Informationsbeschafferin, als Hilfsperson der eigentlich *zuständigen Behörden*. Andererseits wiederum könne die FIU spätestens seit der 4. GWRL im hohen Maße auch eigenständig ermitteln, was wiederum Ausdruck polizeilicher Arbeit sei.[2109] Dafür spreche weiter auch die Kooperation der FIUs mit Europol durch die Vernetzung von FIU.net mit dem System von Europol,[2110] die erst 2019 vom *EDPS* gestoppt wurde.[2111]

Zuletzt vergleicht *Brewczynska* die FIU mit Experten bzw. Sachverständigen bei der Strafverfolgung. Wie etwa Forensiker arbeite die FIU mit

2107 *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (10) mit Verweis auf *EDPS,* Stellungnahme Datenschutzreform, 07.03.2012, Nr. 38, S. 8.; s. dazu auch EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 102 = NJW 2021, 531; Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 63 ff. = EuZW 2022, 706; *Zerdick* in Ehmann/Selmayr DSGVO, Art. 2 Rn. 13; *ders.* in Ehmann/Selmayr DSGVO; *Bäcker* in BeckOK Datenschutzrecht, DSGVO Art. 2 Rn. 30.

2108 *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (12 ff.).

2109 Ibid.

2110 Ibid. mit Verweis auf *Europäische Kommission*, Report from the Commission to the European Parliament and the Council assessing the framework for cooperation between Financial Intelligence Units, COM(2019) 371 final; s.a. *Europol,* Suspicion to Action, 2017.

2111 *EDPS,* Annual Report, 2019, S. 41.

ihrer technischen Analyse den Strafverfolgungsbehörden zu. Allerdings unterschieden sie sich dadurch von jenen, dass sie nach Art. 32 Abs. 1 der 4. GWRL eigenständig und unabhängig arbeiten würden, also selbst entscheiden könnten, was mit den von ihnen verarbeiteten Informationen geschieht.[2112]

Aus dieser Unabhängigkeit schlussfolgert sie letztlich, dass die europarechtlichen Aufgaben der FIU eine eindeutige Subsumtion der FIU unter Art. 3 Nr. 7 der JI-RL nicht zuließen. Es käme stattdessen im Einzelfall auf die nationalen Gesetze an, wie sehr die jeweiligen *„FIUs an die law-enforcement-Behörden heranrückten"*. Sie entscheidet sich also gegen eine klare rechtliche Bewertung der Natur der FIUs auf europarechtlicher Ebene.

Das ergibt gerade vor dem deutschen Hintergrund Sinn, der zeigt, dass die nationalen Sicherheitsarchitekturen Besonderheiten aufweisen können und eine europarechtliche Determination des Rechtscharakters bestimmter Behörden kaum möglich scheint. Dies gilt jedenfalls solange das Sicherheitsverfassungsrecht strukturell national geprägt bleibt.

(5) Möglichkeit und Konsequenzen einer Abgrenzung von Gefahrenabwehr und Strafverfolgung in Bezug auf die FIU?

Angesichts der diversen Aufgaben der FIU stellt sich die Frage, ob eine klare Zuordnung zu einem Rechtsgebiet überhaupt möglich und sinnvoll ist. Gefahrenabwehr und Strafverfolgung werden in Deutschland traditionell als streng getrennte Rechtsgebiete behandelt.[2113] Die Trennung wurzelt in der Gewaltenteilung. Während die Abwehr von Gefahren eine Aufgabe der Verwaltung ist, obliegt die Strafverfolgung der Justiz. Entsprechend verteilen sich die Gesetzgebungskompetenzen auf verschiedene Körperschaften. Durch die Trennung soll verhindert werden, dass repressive Staatsgewalt zentriert und übereffizient in einer staatlichen Säule versammelt wird.[2114]

Tatsächlich ist die FIU nicht die einzige Behörde, die sowohl Gefahrenabwehr und Strafverfolgung betreibt bzw. unterstützt. Für das BKA

2112 *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (13).

2113 Dazu ausf. und krit. Jüngst *Danne,* Prävention und Repression, 2022, S. 163 ff., 255 ff.

2114 *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 8.

wurde dieser Umstand schon beschrieben (s. o).[2115] Aber auch dem Zollfahndungsdienst obliegt es, im Zuständigkeitsbereich der Zollverwaltung Straftaten aufzudecken, zu verhüten, zu verfolgen sowie Vorsorge für die künftige Verfolgung von Straftaten zu treffen, §§ 4, 5 ZFdG.[2116] Nach § 52 ZFdG kommt den Zollfahndungsbeamten die gleiche Rolle wie der Polizei in der StPO zu: Sie sind Hilfspersonen der Staatsanwaltschaft. Zusätzlich werden sie durch das ZFdG zu verschiedenen Zwangsmaßnahmen mit präventiver Funktion berechtigt. Dasselbe gilt für die Bundespolizei. Diese ist zwar Gefahrenabwehrbehörde, vgl. § 1 Abs. 5 BPolG, nimmt aber ebenfalls für manche Straftaten die Aufgaben der Polizei im Strafverfahren wahr, § 12 BPolG. Die Gesetzgebungskompetenz für Aufgaben der Gefahrenabwehr obliegt dem Bund in diesen Fällen als Annex zu seiner Zuständigkeit über die Aufstellung besonderer Behörden nach Art. 73 Abs. 1 GG.[2117] Die Kompetenz für Zoll und Grenzschutz ist etwa in Art. 73 Abs. 1 Nr. 5 GG normiert.

Was für den Zollfahndungsdienst und die Bundespolizei in einem Gesetz geregelt ist, gilt letztlich in gleicher Weise für den Polizeivollzugsdienst der Länder. Die Aufteilung der polizeilichen Arbeit in Gefahrenabwehr und Strafverfolgung ist allein eine rechtliche. Es werden dieselben Beamten eingesetzt.[2118] Die Unterschiede sind auf Gesetzgebungskompetenzen zurückzuführen und wirken sich vor allem auf den Rechtsschutz aus.[2119] In der Sache unterscheiden sich die präventiven Möglichkeiten der Polizei kaum mehr von jenen, die ihnen das Strafverfahrensrecht zugesteht. [2120] Das ist auch nur konsequent, denn durch die Tendenz einer Vorverlagerung der Strafbarkeit kommt es häufig zu einer Überschneidung von Gefahrenabwehr und Strafverfolgung, die eine saubere Abgrenzung kaum mehr zulässt. [2121]

Kompetenzrechtliche Probleme sind für das GwG nicht ersichtlich. Zwar sind für das Recht der Gefahrenabwehr prinzipiell die Länder zuständig.

2115 *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 577.
2116 Dazu *Zöller,* Informationssysteme, 2002, S. 227 ff.
2117 Vgl. BVerfGE 155, 119 (172 ff.) – Bestandsdatenauskunft II.
2118 *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 2 Rn. 7.
2119 *Brodowski,* Überwachungsmaßnahmen, 2015, S. 327 ff.
2120 *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 12.
2121 *Brodowski,* Überwachungsmaßnahmen, 2015, S. 293 ff; ausführlich zur Abgrenzung S. 327 ff. 338 ff.

Aus den Bundeskompetenzen für bestimmte Bereiche folgt jedoch die Kompetenz zur Einrichtung von entsprechenden Gefahrenabwehrbehörden. Der Gesetzgeber stützte sich im Rahmen seiner Annahme daher zu Recht für den Erlass des GwG auf die Gesetzgebungskompetenz für das Wirtschaftsrecht, (Art. 74 Abs. 1 Nr. 11 GG) und für die Änderungen am ZFdG und FVG auf Art. 73 Abs. 1 Nr. 5 GG.[2122] Charakterisiert man die Rechte und Pflichten der FIU als Strafverfolgung, könnte man stattdessen über eine Bundeskompetenz nach Art. 74 Abs. 1 Nr. 1 GG nachdenken. Eine Kompetenz der Länder ist in diesem Fall erst recht nicht denkbar. Wohl aus diesem Grund wurde bislang nicht an der Kompetenz des Bundesgesetzgebers zum Erlass des GwG gezweifelt.

Interessant ist die Einstufung daher letztlich nur für das informationelle Trennungsprinzip. Wie bereits erläutert, führt die Aufgabentrennung nicht dazu, dass sämtliche Sicherheitsbehörden nur auf einem Teilgebiet tätig werden und Informationen erheben dürfen. Da es im Rahmen von Vorermittlungen, Prävention und Repression zwangsweise zu Überschneidungen bzw. einem Ineinandergreifen kommt[2123], wäre eine solche Vorgehensweise auch nicht sinnvoll. Allein die Voraussetzungen, unter denen die Weiterverwendung und der Austausch von Informationen erfolgen können, hängen nach dem informationellen Trennungsprinzip grundsätzlich von der Einteilung der jeweiligen Behörde in die Sicherheitsstruktur der Bundesrepublik ab.

Das informationelle Trennungsprinzip gilt nur für die Nachrichtendienste auf der einen und Polizeibehörden auf der anderen Seite.[2124] Informationen, die im Rahmen der Gefahrenabwehr bzw. der Strafverfolgung erlangt wurden, können allerdings auch nicht frei zwischen den jeweiligen Behörden, sondern nur gemäß den Prinzipien der Zweckbindung und der

2122 BT-Dr.s 18/11555, S.90.

2123 *Dietrich* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, III § 3 Rn. 8; ebd. *Gusy* IV § 2 Rn. 46, 55; ebd. *Warg* V § 1 Rn. 8; *J. Franz Lindner/Unterreitmeier*, DÖV 2019, 165 (168) *Zöller,* Informationssysteme, 2002, S. 322 ff.; *ders.* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (190 f.); zur Überschneidung von Strafverfahren und Polizeirecht *Gärditz,* Strafprozeß & Prävention, 2003, S. 91 ff.; *Brodowski,* Überwachungsmaßnahmen, 2015, S. 253 ff.; *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 2 Rn. 6; generell krit. zur Dichotomie *Danne,* Prävention und Repression, 2022, insb. S. 225 ff.

2124 Siehe nur: BVerfGE 133, 277 (29) – Antiterrordatei I E 156, 11 (51 f.) – Antiterrordatei II; *Gusy*, GSZ 2021, 141 (142 ff.); *Arzt* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, ATDG § 1 Rn. 35 ff.

hypothetischen Datenneuerhebung ausgetauscht werden[2125], vgl. etwa § 25 BKAG oder § 481 StPO i. V. m. § 15 Abs. 4 PolG BW, § 23 Abs. 5 PolG NRW. [2126]

Angewandt auf die FIU bedeutet dies, dass allein die Weiterleitung von Finanzinformationen an die Strafverfolgungsbehörden nach § 32 Abs. 2 GwG keinen weiteren verfassungsrechtlichen Bedenken begegnet, wenn man sie als vorermittelnde Behörde im Rahmen der Strafverfolgung begreift. Eine Weiterleitung von Daten an die Gefahrenabwehrbehörden ist in § 32 Abs. 2 GwG nicht vorgesehen. Allein die Weiterleitung von Informationen an den BND und das BfV nach § 32 Abs. 1, Abs. 2 S. 2, 3 GwG wecken Zweifel sowie die Weiterleitung an das BKA (als spezielle Gefahrenabwehrbehörde) nach § 32 Abs. 3a GwG, § 3 Abs. 2a S.2 BKAG.

(6) Ein dritter Weg: die FIU als Nachrichtendienst?

Es stellt sich aber weiter die Frage, wenn die Weiterleitung von Informationen nicht nur Recht, sondern Aufgabe der FIU ist, ob ihre Einstufung als Strafverfolgungsbehörde überhaupt Sinn ergeben kann. Schließlich soll sie auch andere Behörden mit Informationen versorgen, etwa eben nach § 32 Abs. 1, 2 S. 2, 3 GwG den BND und das BfV.

Von wissenschaftlicher Seite wird daher noch eine dritte Alternative vorgeschlagen, nach der die FIU weder eine Gefahrenabwehr- noch eine Strafverfolgungsbehörde, sondern eine „Art Finanznachrichtendienst" darstellen soll.[2127] Wie bereits erläutert, ist es gerade nicht die Aufgabe der FIU, Strafverfahren durchzuführen, sondern Informationen für deren Einleitung zu liefern. Zwar hat sie zur Erfüllung ihrer Aufgaben auch operative Möglichkeiten nach § 40 GwG. Diese sind aber von gefahrenabwehrrechtlicher Natur und dienen anders als ihre Primäraufgabe – die Analyse von

2125 BVerfGE 141, 220 (276 ff.) – BKA-Gesetz; E 100, 313 (360 ff.) – Strategische Fernaufklärung; *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 187 ff.; ebd. M.*W. Müller/Schwabenbauer* Kap. G Rn. 578; 884 ff.; *Löffelmann*, GSZ 2019, 16; zum Verhältnis von Zweckbindung und informationellem Trennungsprinzip *Unterreitmeier*, DÖV 2021, 659 (661 f.).

2126 Weitere Bsp. bei *M. W. Müller/Schwabenbauer* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. G Rn. 838.

2127 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.); s.a. *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21: „eine Art Finanz-Nachrichtendienst".

Verdachtsmeldungen[2128] – nicht unmittelbar der Strafverfolgung. Daher wird die Einstufung der FIU als Strafverfolgungsbehörde ja so vehement bestritten.

Das Primat der Informationsvorsorge, das für die FIU in den §§ 28 ff. GwG so stark zum Ausdruck kommt, ist in Deutschland grundsätzlich nicht von den operativen Sicherheitsbehörden, sondern von den Nachrichtendiensten bekannt. Auch steht die Möglichkeit von heimlichen Auskunftsersuchen bei Privaten allein den Nachrichtendiensten zu. So findet sich ein Äquivalent zu § 30 Abs. 3 GwG weder in der StPO noch in den Polizeigesetzen, wohl aber in den Gesetzen über den Verfassungsschutz, z. B. § 8a Abs. 1 Nr. 2 BVerfschG (s. Kap. E. II. 2. a.).

Die Aufgabe der klassischen Nachrichtendienste ist primär die Information der Politik, wodurch sie sich essenziell von der FIU unterscheiden. Was neben dem Zweck aber die Möglichkeiten und die Arbeitsweise der FIU betrifft, sind diese tatsächlich charakteristisch für Nachrichtendienste.[2129] Ihre Befugnisse zur Erhebung und Verarbeitung persönlicher Daten seien auf Heimlichkeit geradezu angelegt. Informationsrechte oder gar Benachrichtigungspflichten gegenüber den Betroffenen enthält das GwG nicht. § 47 GwG stellt vielmehr sicher, dass sämtliche Informationen bezüglich Verdachtsmeldungen und Auskunftsersuchen der FIU geheim gehalten werden. Darüber hinaus hat die FIU extensive Möglichkeiten zum Datenzugriff im automatisierten Verfahren. So kann sie nicht nur nach § 31 Abs. 1 GwG bei verschiedenen Behörden um Auskunft ersuchen, sie kann auch einen automatischen Datenabgleich vornehmen, etwa nach § 31 Abs. 4 GwG mit dem polizeilichen Informationsverbund i. S. d. § 29 BKA, nach § 31 Abs. 4a GwG mit dem Zentralen Verfahrensregister der Staatsanwaltschaft, nach § 31 Abs. 5 GwG mit Daten der Finanzbehörden oder nach § 31 Abs. 8 GwG mit dem Melderegister.

Mit all diesen Daten kann die FIU die Informationen, die sie aus den Meldungen der Geldwäscheverpflichteten erhält, abgleichen, ohne dass dies irgendjemandem offenbar würde. *Vogel* erinnert daran, dass die Daten aus den Verdachtsmeldungen aufgrund des ausschweifenden Verpflichtetenkreises in § 2 GwG und des niedrigschwelligen Verdachtsgrades nach § 43 Abs. 1 GwG einen umfassenden Blick in das gesamte Wirtschaftsgeschehen Deutschlands erlauben. Da die FIU nach § 30 Abs. 3 GwG zusätzlich das

2128 BT-Drs. 18/11982, S. 26: „zentraler Mehrwert".

2129 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.).

Recht hat, bei all diesen Verpflichteten ohne weitere Voraussetzungen Finanzinformationen eigenständig einzuholen, kommandiere sie letztlich ein *Netzwerk privater Informanten* gleich dem Vorgehen der Nachrichtendienste.[2130]

Anders als die Unterscheidung zwischen Gefahrenabwehr und Strafverfolgung hätte die Einstufung der FIU als Nachrichtendienst erhebliche Konsequenzen. Wie bereits dargelegt, wird hinsichtlich der Nachrichtendienste seit jeher diskutiert, inwiefern diese von den restlichen Sicherheitsbehörden getrennt sein müssen. Zwar hat das Bundesverfassungsgericht bislang allein einer informationellen Trennung Verfassungsrang zugesprochen[2131], die Frage nach der organisatorisch-funktionalen[2132] Trennung, die den Nachrichtendiensten Polizeibefugnisse verwehrt, dürfte aber vor allem deshalb noch höchstrichterlich unbeantwortet sein, da sie in den Gesetzen der Verfassungsschutzbehörden ohnehin vorgesehen ist, etwa in § 2 Abs. 1S. 3 BVerfSchG, § 1 Abs. 1 S. 2 BNDG; § 1 Abs. 4 MADG, § 2 Abs. 3 LVSG BW.

Das BVerfG hat in seiner jüngsten Rechtsprechung zwar betont, dass sich seine Ausführungen als Konsequenz des geltenden Rechts darstellen,[2133] und vermieden, die Notwendigkeit der gesetzlichen Trennung ausdrücklich in der Verfassung zu verankern. Es hat aber schon in den Urteilen zum ATDG mehrfach klargestellt, dass es die intensiveren Informationserhebungsbefugnisse der Nachrichtendienste nur deshalb für mit den Grundrechten vereinbar hält, weil ihnen entsprechend schwerwiegende operative Möglichkeiten fehlen.[2134] Dies entspricht letztlich dem Verständnis des

2130 Idem, (249).

2131 BVerfGE 133, 277 (329) – Antiterrordatei I; E 156, 11 (50) – Antiterrordatei II; NJW 2022, 1583 (Rn. 141 ff.) – Bayerisches Verfassungsschutzgesetz.

2132 Übersicht bei *Ibler* in Dürig/Herzog/Scholz GG, Art. 87 Rn. 143; *W. Roth* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BVerfSchG § 2 Rn. 7 ff.; *Roggan/Bergemann*, NJW 2007, 876 (876 f.); zu den Einzelheiten der organisatorischen und funktionalen Trennung *Banzhaf,* Verfassungsschutz, 2021, S. 204 ff.; *Gazeas,* Nachrichtendienstliche Erkenntnisse, 2014, S. 58 ff.; *Poscher/Rusteberg* KJ 2014, 57 (59 ff.); *Gusy*, GSZ 2021, 141 (147 ff.).

2133 BVerfG, NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; *Banzhaf,* Verfassungsschutz, 2021, S. 216.

2134 BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.);, NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Gärditz*, JZ 2013, 633 (634); zur prinzipientheoretischen Erklärung dieser Rechtsprechung *Gusy*, GSZ 2021, 141 (145 ff.).

Trennungsprinzips als *grundrechtliche* Reflexwirkung.[2135] Aus den Grundrechten ließe sich danach ableiten, *dass keine Behörde, die alles kann, auch alles wissen soll und andersherum keine Behörde alles können soll, die alles wissen darf.*[2136] Da die Informationsbefugnisse der Nachrichtendienste unverhältnismäßig würden, wenn sie auch operative Befugnisse erhielten, würde eine Aufgabe der Trennung letztlich die Existenzberechtigung der Nachrichtendienste auslöschen.[2137] Die Vermutung liegt also nahe, dass die vom BVerfG festgestellte Notwendigkeit einer informationellen Trennung letztlich zu einer Trennung auch in funktionaler Hinsicht zwingt, jedenfalls aber begünstigt eine organisatorisch-funktionale Trennung die informationelle Trennung.[2138]

Der § 32 Abs. 2 S. 1, Abs. 3 GwG widerspricht den Anforderungen des informationellen Trennungsprinzips recht eindeutig, da an die Weiterleitung der analysierten Meldungen an die Staatsanwaltschaft keine weiteren Voraussetzungen gestellt werden, als dass die Informationen zur Durchführung der Aufklärung von Straftaten bzw. zur Durchführung von Strafverfahren erforderlich sind. Eine Weiterleitung von Informationen von Nachrichtendiensten an die Strafverfolgungsbehörden soll nach der jüngsten Rechtsprechung des BVerfG aber nur möglich sein, wenn dies zur Verfolgung besonders schwerer Straftaten geschieht und konkrete bzw. in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorhanden sind.[2139]

Die Weiterleitung von Informationen der Nachrichtendienste an die Strafverfolgungsbehörden soll die Ausnahme und nicht die Norm bilden.

cc. Fazit: Die FIU als Bruch der deutschen Sicherheitsarchitektur

Mit dieser Vorstellung lässt sich die Aufgabenbeschreibung der FIU nicht in Einklang bringen. Das informationelle Trennungsprinzip, der Grundsatz der Zweckbindung und die Figur der hypothetischen Datenneuerhebung sind allesamt von der Vorstellung durchdrungen, dass verschiedene Sicher-

2135 *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 245 ff.
2136 *Gusy*, GA 1999, 319 (327).
2137 *Poscher/Rusteberg* KJ 2014, 57 (60 f.).
2138 *Gusy*, GSZ 2021, 141 (147 f.).
2139 BVerfG, NVwZ-RR 2023, 1 (8 ff) – Nachrichtendienstliche Informationsübermittlung;, NJW 2022, 1583 (Rn. 249 ff.) – Bayerisches Verfassungsschutzgesetz.

heitsbehörden jeweils eigene Primäraufgaben wahrnehmen und für diese Informationen erheben. Sollen diese Informationen erkennbar für andere als die eigenen Zwecke genutzt oder weitergeleitet werden, stellt dies einen erheblichen Grundrechtseingriff dar, der besondere sicherheitsrechtliche Vorkehrungen benötigt.[2140]

Zwar ist der Austausch von Informationen zwischen Nachrichtendiensten und anderen Sicherheitsbehörden der Natur nach nicht völlig ausgeschlossen; als Abweichung von der nachrichtendienstlichen Primäraufgabe bleibt er aber rechtfertigungsbedürftig.[2141]

Eine Behörde, die nachrichtendienstliche Mittel verwenden kann, und deren Aufgabe es primär ist, operative Sicherheitsbehörden mit Informationen zu versorgen, war dem deutschen Sicherheitsrecht bislang fremd. Die klassischen Nachrichtendienste sollen gerade nicht final, sondern nur ausnahmsweise als Vorermittler der Polizeibehörden und Strafverfolgung fungieren,[2142] auch wenn dies zu der fragwürdigen Entwicklung geführt hat, dass Polizei- und Strafverfolgungsbehörden vermehrt mit nachrichtendienstlichen Möglichkeiten ausgestattet wurden.[2143]

Mit diesem Grundgerüst der Sicherheitsarchitektur wird im Geldwäschegesetz gebrochen. Die Charakterisierung der FIU streng nach deutschem Verständnis muss scheitern, da eine solche Charakterisierung entweder anhand der Aufgaben oder aber der Befugnisse einer Behörde erfolgen muss. Nun hat die FIU mit § 30 Abs. 3 GwG die Befugnisse eines Nachrichtendienstes, kümmert sich in der Sache aber überwiegend um die Vorermitt-

2140 BVerfGE 133, 277 (329) – Antiterrordatei I; E 156, 11 (50) – Antiterrordatei II;, NJW 2022, 1583 (Rn. 171 ff.) – Bayerisches Verfassungsschutzgesetz; *Gazeas,* Nachrichtendienstliche Erkenntnisse, 2014, S. 237 ff.; *Unterreitmeier*, DÖV 2021, 659 (660 f.).

2141 Zu diesem Verhältnismäßigkeitsaspekt: *Poscher/Rusteberg* KJ 2014, 57 (68 ff.); *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (191).

2142 Ausdrücklich zum Ausnahmecharakter BVerfG, NJW 2022, 1583 (Rn. 302) – Bayerisches Verfassungsschutzgesetz; s.a. *Banzhaf,* Verfassungsschutz, 2021, S. 216; *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2020, S. 79 (S. 89 ff.); *Kingreen/Poscher,* Polizeirecht, 11. Aufl. 2020, § 2 Rn. 17 f.; *Poscher/Rusteberg* KJ 2014, 57 (S. 68 ff.); *Gusy*, GSZ 2021, 141 (146 ff.); *ders.* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, IV § 2 Rn. 44 ff.

2143 Vgl. BT-Drs. 16/12411, S. 9; *M. Baldus*, Die Verwaltung 47 (2014), 1 (3 ff.); *Wolff*, DÖV 2009, 597 (599 ff.); *Paeffgen*, StV 2002, 337; *Gusy* in Röttgen/Wolff (Hrsg.), Parlamentarische Kontrolle, [Electronic ed.] 2008, S. 13 (25 f.) *Thiel,* Entgrenzung, 2012, S. 473 ff. S.a. *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht,Rn. 250; *Dietrich* in Dietrich/Eiffler (Hrsg.), Hdb. Nachrichtendienste, 2017, III § 3 Rn. 8 jeweils mwN.

lung zur Vorbereitung von Strafverfahren, während der Gesetzgeber sie als administrative Gefahrenabwehrbehörde ausgestaltet haben will.

Die einzige verfassungsrechtlich vorgesehene Behördenkategorie, die für die FIU in Betracht kommt, ist die „Zentralstelle" i. S. d. Art. 87 Abs. 1 GG. Dass sich der Gesetzgeber hieran orientieren wollte, offenbart schon der Name der FIU (Zentralstelle für Finanztransaktionsuntersuchungen, §§ 27 ff. GwG). Es wurde aber dargestellt, dass die FIU gerade nicht nur die Aufgabe einer Zentralstelle übernimmt, die primär in der Koordination und Unterstützung gesehen wird,[2144] sondern anderen Sicherheitsbehörden proaktiv zuarbeiten soll.

Dass eine Behörde nicht nur die Aufgaben einer Zentralstelle übernimmt, ist natürlich nichts Neues. Auch das BKA übernimmt verschiedene Aufgaben. Es ist nicht nur Zentralstelle, sondern auch Kriminalpolizei sowie Gefahrenabwehrbehörde.[2145] Soweit es in letzterer Funktion tätig wird, muss das BKA jedoch den für die Polizeien vorgesehenen Beschränkungen unterworfen werden.[2146] Die Diskussion um die Rechtsnatur der FIU erinnert insofern an die Ausführungen zur Umgestaltung des BKA zum Ende der vergangenen Dekade. Auch dort wurde und wird teilweise noch immer der Vorwurf erhoben, dass die Kombination verschiedener Funktionen unter einem Dach letztlich zu einer Grenzverschiebung von Polizei und Nachrichtendiensten geführt hat.[2147] Innerhalb des BKAG werden die verschiedenen Aufgaben allerdings klar benannt und schon durch die Anordnung innerhalb des Gesetzes in jeweils eigene Abschnitte unterteilt, die die jeweils zulässigen Maßnahmen aufführen.[2148] Beim BKA verschwimmen damit zwar Aufgaben unter einem Behördendach, die Aufgaben lassen sich jedoch weiterhin den Bereichen Gefahrenabwehr und Strafverfolgung zuweisen, auch wenn durch die erkennbare Vorfeldverlagerung dieser Rechtsbereiche sicher eine Annäherung der polizeilichen Arbeit ans Aufgabenfeld der Nachrichtendienste stattgefunden hat.

2144 BVerfGE 110, 33 (51).; *Ibler* in Dürig/Herzog/Scholz GG, Art. 87 Rn. 117 ff.

2145 *Burgi* in v. Mangoldt/Klein/Starck GG, Art. 87 Rn. 48; *Wolff*, DÖV 2009, 597 (598 ff.); ausf. *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 125 ff.

2146 BVerfGE 141, 220 – BKA-Gesetz.

2147 *Roggan*, NJW 2009, 257 (262); *Wolff*, DÖV 2009, 597 (598 ff.); *Kutscha,* Stellungnahme BKAG; Innenausschuss A-Drs. 16(4)460D, 2008, S. 1; *Thiel,* Entgrenzung, 2012, 473 ff. *Hermes* in Dreier GG, Art. 45d Rn. 25.

2148 *Graulich* in Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Auflage 2019, BKAG Vorb. Rn. 1.

Für die FIU lässt sich dies nicht behaupten. Zwar könnte ihre Übermittlungspflicht bei Ersuchen gem. Art. 32 Abs. 4 S. 2 GWRL bzw. § 32 Abs. 3 GwG durch eine strenge Ausgestaltung bzw. Auslegung so ausgestaltet werden, dass sie dem Informationsaustausch von Nachrichtendiensten und operativen Sicherheitsbehörden bei Anfragen, bspw. §§ 19, 21 BVerfSchG, entspricht (III. 2. c. bb. (2)). Ihre Existenzberechtigung liegt aber in der proaktiven Versorgung von (auch) operativen Sicherheitsbehörden mit Informationen, die quasi nachrichtendienstlich errungen wurden.[2149] Dies ist eine Aufgabe, die weder funktional noch organisatorisch in die Sicherheitsarchitektur des Grundgesetzes integriert werden kann.

Da die Rechtsprechung des BVerfG aber insbesondere im Bereich der Informationsübermittlung an diese Aufgaben- bzw. Sachbereiche anknüpft, ist die Bewertung der §§ 30 ff. GwG kritisch. Wäre die FIU Nachrichtendienst i. S. d. Art. 87 Abs. 1, 45d GG, verstieße wohl jedenfalls ihre Pflicht zur proaktiven Übermittlung von verdächtigen Verdachtsmeldungen nach § 32 Abs. 2 S. 1 GwG gegen das Prinzip der informationellen Trennung. Die jüngst vom BVerfG noch einmal geforderten Anforderungen an die Übermittlung von nachrichtendienstlich errungenen Informationen an die Strafverfolgung[2150] werden von der Vorschrift gerade nicht eingehalten, da die Informationsversorgung durch die FIU keine Ausnahme, sondern Zweck des GwG ist. Auch die Verhältnismäßigkeit der operativen Befugnisse der FIU müssten vor diesem Hintergrund spezifisch untersucht werden, da Nachrichtendiensten solche typischerweise verwehrt sind. Zu diesem Aspekt der Aufgabentrennung verschiedener Sicherheitsbehörden hat sich das BVerfG aber noch nicht umfassend geäußert, da sie sich schon aus dem einfachen Gesetzesrecht ergibt.[2151]

Unabhängig von den allgemeinen (unions-)grundrechtlichen Anforderungen, die sich aufgrund des Überwachungskomplexes ergeben, kommt also durchaus in Betracht, dass das GwG strukturell gegen die grundgesetzliche Sicherheitsverfassung verstößt.

2149 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.).
2150 BVerfG, NJW 2022, 1583 (Rn. 249 ff.) – Bayerisches Verfassungsschutzgesetz.
2151 Vgl. *Banzhaf,* Verfassungsschutz, 2021, S. 209 ff.

c. Das informationelle Trennungsprinzip in der (europarechtlichen) Verhältnismäßigkeitsprüfung

An dieser Stellte muss jedoch in Erinnerung gerufen werden, dass die Anwendung des informationellen Trennungsprinzips mit all seinen Konsequenzen von der Anwendung der Grundrechte des Grundgesetzes abhängig ist, da jedenfalls das BVerfG diese Trennung bislang allein aus den Grundrechten heraus abgeleitet hat.[2152] Ob die Grundrechte aber im Bereich der Anti-Geldwäschebekämpfung Anwendung finden, hängt vom Harmonisierungsgrad der Vorschriften ab (s. o. III. 1.).[2153]

aa. Informationelle Trennung im Geldwäscherecht und *Effet utile*

Für die Organisation der FIU sehen weder die 4./5. GWRL, noch der Vorschlag zur 6. GWRL spezifische Regeln vor. Allein die Unabhängigkeit und eigenständige Arbeit der FIU müssen gewährleistet sein.[2154] Von der Organisation zu trennen sind die Aufgaben, die die FIU nach den europäischen Vorgaben erledigen *muss*.

Für § 30 Abs. 3 GwG, also die Möglichkeit der FIU, bei Privaten ohne konkreten Anlass Finanzdaten zu erheben, wurde schon festgestellt, dass diese Maßnahme ausdrücklich von Art. 32 Abs. 9 der 5. GeldwäscheRL (und auch Art. 18 Abs. 4 des Vorschlags für eine 6. GWRL) verlangt wird. Insofern ist eine ausdrückliche Determinierung festzustellen.

Für die Weiterleitungsvorschriften des § 32 GwG konnte diese Feststellung nicht gleichermaßen getroffen werden. „Nach Art. 32 Abs. 3 S. 2 GWRL obliegt es der FIU nur*, bei begründetem Verdacht auf Geldwäsche, damit zusammenhängende Vortaten oder Terrorismusfinanzierung die Ergebnisse ihrer Analysen und alle zusätzlichen relevanten Informationen an die zuständigen Behörden weiterzugeben*". In Art. 32 Abs. 4 S. 2 heißt es *weiter: „Die zentralen Meldestellen müssen in der Lage sein, Auskunftsersuchen der zuständigen Behörden ihres jeweiligen Mitgliedstaats zu beantworten,*

2152 BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.); NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Gärditz*, JZ 2013, 633 (634); *Gusy*, GSZ 2021, 141 (142); *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 245 ff.

2153 BVerfGE 73, 339 (374 ff.) [1986] – Solange II; dazu nur *Masing* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 2 Rn. 136 ff.; *Britz*, NJW 2021, 1489; *Lehner*, JA 2022, 177.

2154 Dazu *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (7 ff.).

sofern die Auskunftsersuchen auf Belangen im Zusammenhang mit Geldwäsche, damit im Zusammenhang stehenden Vortaten oder Terrorismusfinanzierung beruhen". (Der Vorschlag zur 6. GWRL übernimmt diese Regeln fast wortgleich in Art. 17 Abs. 3, Art. 19 Abs. 1).

Zu den Voraussetzungen, unter denen diese Informationsweitergabe erfolgen soll, verhält sich die Vorschrift (auch weiterhin) nicht.

Es ließe sich also durchaus argumentieren, dass der deutsche Gesetzgeber, wenn er die Maßnahmen der FIU so ausgestaltet, dass diese den Kompetenzen der Nachrichtendienste entsprechen, er im Rahmen der Weiterleitungsnormen die aus den Grundrechten folgenden Konsequenzen beachten müsste. Allerdings ist der deutsche Gesetzgeber nach Art. 39 Abs. 1 GWRL dazu gezwungen, der FIU einen geheimen Zugriff auf die Daten der Verpflichteten einzuräumen. Auch über den gesamten Unterbau der Informationsgewinnung – nämlich die Sorgfaltspflichten und Meldepflichten der Privaten sowie die Analysepflicht der FIU – kann er nicht disponieren. Die Umstände, aus denen sich ein nachrichtendienstlicher Charakter (i. S. d. Grundgesetzes, s. o.) der FIU ableiten ließe[2155], entziehen sich also der Gewalt der nationalen Gesetzgeber in der EU.

Das informationelle Trennungsprinzip leitet sich aus den Grundrechten des Grundgesetzes ab. Es sieht vor, dass die Ausstattung einer Behörde mit bestimmten Überwachungsrechten, -aufgaben und -mitteln Konsequenzen für die Informationsübermittlung bzw. -teilhabe mit sich bringt, da andernfalls die erhaltenen Überwachungsmöglichkeiten unverhältnismäßig wären (s. o.).[2156] Diese Stoßrichtung geht verloren, wenn der Gesetzgeber überhaupt nicht entscheiden dürfte, mit welchen Instrumenten er eine Behörde ausstatten will. Schon aus diesem Grund ist höchst fraglich, ob die informationelle Trennung von Nachrichtendiensten und Polizei mit all ihren vom BVerfG entwickelten Auswirkungen auch dann gelten soll, wenn die Maßnahmen, die für den infrage stehenden nachrichtendienstlichen Charakter einer Behörde verantwortlich sind, nie zur Disposition des Gesetzgebers standen.

2155 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.).

2156 BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.) – Antiterrordatei II; NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Gärditz*, JZ 2013, 633 (634); *Gusy*, GSZ 2021, 141 (142); *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 245 ff.

Im Hinblick auf das Anti-Geldwäscherecht dürfte eine (nationalstaatlich etablierte) informationelle Trennung jedenfalls dem europarechtlichen Grundsatz der Effektivität (*effet utile*) widersprechen.

Nach diesem Prinzip muss das europäische Recht so ausgelegt werden, dass dessen Ziele am besten und wirkungsvollsten durchgesetzt werden.[2157] Eines der Hauptziele der GWRL ist die strafrechtliche Verfolgung von Geldwäsche durch die Aufdeckung von Transaktionen illegaler Vermögenswerte.[2158] Eine wirkungsvolle Umsetzung der Geldwäscherichtlinie setzt voraus, dass sämtliche Meldungen, die nach Analyse der FIU tatsächlich im Verdacht stehen, einen Zusammenhang mit Geldwäsche, einer damit zusammenhängenden Vortat oder Terrorismusfinanzierung aufzuweisen, an die zuständige Behörde weitergeleitet werden.[2159] Diese Filterfunktion der FIU ist ein primärer Aspekt der Richtlinie. Als *zentrale Stelle* soll die FIU Daten erheben, erhalten und weiterverarbeiten, um diese dann eigenständig an die entsprechenden Behörden weiterzuleiten.[2160]

Würde die proaktive Weiterleitung durch die FIU aufgrund der informationellen Trennung erheblich erschwert, gleichzeitig diese Trennung aber überhaupt erst wegen der eingeräumten Befugnisse bzw. systematischen Stellung der FIU obligatorisch werden, würde die informationelle Trennung den Regelungszweck der Richtlinie aufheben, ja geradezu ad absurdum führen. Eine effektive Umsetzung der Richtlinie setzt also den oben beschriebenen Bruch mit der deutschen Sicherheitsarchitektur schlicht voraus. Die Etablierung eines „Finanzgeheimdienstes"[2161] zur Versorgung weiterer Sicherheitsbehörden mit Informationen ist ein Kernelement des europäischen Geldwäscherechts.

Soweit die informationelle Trennung dem entgegensteht, kann sie wegen des *effet utile* nicht zur Anwendung kommen. Insofern muss Art. 32 Abs. 3 S. 4 GWRL so ausgelegt werden, dass er die FIU zur proaktiven Weiterlei-

2157 Vgl. nur EuGH, Urt. v. 15. 9. 2011, C-53/10, (Mücksch) Rn. 22 ff. = EuZW 2011 (873); *Streinz* in Streinz EUV/AEUV, EUV Art. 4 Rn. 33; *Potacs*, EuR 2009, 465; *Seyr,* effet utile, 2010, S. 94 ff. jeweils mwN aus der Rechtsprechung des EuGH.

2158 Vgl. Erwägungsgrund Nr. 37 der 4. EU-GeldwäscheRL; Erwägungsgrund Nr. 1 der Richtlinie (EU) 2018/1673 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 über die strafrechtliche Bekämpfung der Geldwäsche, ABl. 2018 L 284/22; vgl. auch BR-Drs. 182/1/17, S. 21; BT-Drs. 18/11928, S. 11 f.

2159 *Maillart* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 71 (122) lässt eine Obligation der FIU zur Weiterleitung allerdings offen.

2160 Vgl. Erwägungsgrund Nr. 37, 4. EU-GeldwäscheRL

2161 *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21.

tung einer Verdachtsmeldung im Falle eines erhärteten Verdachts[2162] verpflichtet und diese Weiterleitung nicht von erheblichen Voraussetzungen, insb. nicht dem Konzept der hypothetischen Datenneuerhebung, abhängig gemacht werden kann.

bb. Rückkopplung der informationellen Trennung mit den Unionsgrundrechten

Eine Prüfung insbesondere der proaktiven Weiterleitungsvorschriften in § 32 GwG bzw. Art. 32 Abs. 3 S. 4 der GWRL wird daher nicht generell an deutschen Grundrechten bzw. dem hieraus abgeleiteten Prinzip der informationellen Trennung scheitern können. Diese kann sinnvollerweise trotz einer unvollständigen Determinierung im Wortlaut des Art. 32 Abs. 3 S. 4 der GWRL in der GWRL nicht grundsätzlich zur Anwendung kommen.

An dieser Stelle muss deshalb die Frage in den Raum gestellt werden, ob auch das Unionsrecht eine Art informationelles Trennungsprinzip von Nachrichtendiensten und Polizei kennt, gegen das die Aufgaben, bzw. Ermächtigungen und Pflichten der FIU verstoßen könnten.[2163]

Auf den ersten Blick ist diese Frage schnell beantwortet. Die Europäische Union ist für den Bereich der allgemeinen Strafverfolgung, Gefahrenabwehr und Informationsversorgung, so zwischen diesen Bereichen überhaupt differenziert wird, nicht zuständig, Art. 4 Abs. 2 S. 3 EUV, sondern nur für die justizielle Zusammenarbeit und den Bereich schwerer Kriminalität, Art, 82, 83 AEUV.[2164] Folglich kann auch nicht unmittelbar von der Existenz eines operativen europäischen Sicherheitsrechts gesprochen werden.[2165] Aus den europäischen Grundrechten hat der EuGH aber schon eine ganze Reihe an Vorgaben für das Sicherheitsrecht abgeleitet, insbesondere im Bereich der Datenverarbeitung. Er hat diese stets aus dem Grund-

2162 Zum Verdachtsgrad äußert sich die EU-GeldwäscheRL nicht.

2163 In diese Richtung zur PNR-RL: VG Wiesbaden Beschluss v. 15.05.2020 – 6 K 806/19.WI, Rn. 75 ff.; *Wissenschaftliche Dienste des Bundestags,* PNR-Urteil, 2022, S. 15.

2164 Vgl. *Aden* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. M Rn. 1 ff.; *Möstl* in BeckOK POR NRW, Syst. Vorb. Rn. 65 ff.

2165 Dazu *Schöndorf-Haubold,* Europ.Sicherheitsverwaltungsrecht, 2010, S. 139 f.

satz der Verhältnismäßigkeit entwickelt (s. o. Kap C. II).[2166] Mittlerweile sind die Grundätze sicherheitsrechtlicher Informationsverarbeitung für die Polizeibehörden und Strafverfolgung in der JI-RL konkreter ausgestaltet worden. Das Einfallstor des informationellen Trennungsprinzips steht somit grundsätzlich auch dem EuGH offen.

Es wurde bereits erwähnt, dass der informationellen Trennung im Kern ein Umgehungsgedanke zugrunde liegt.[2167] Einen solchen findet man auch in der Rechtsprechung des EuGH zur Vorratsdatenspeicherung. Dort hatte der Gerichtshof zwar nicht ausdrücklich zum Anstoß genommen, dass durch Auslagerung von Speicherpflichten an Private, die Voraussetzungen der Sicherheitsbehörden zur Datenerhebung bzw. -speicherung nicht unterlaufen werden. Er hat aber, obwohl dies grundsätzlich nicht den europäischen Kompetenzrahmen berührt,[2168] bei der Verhältnismäßigkeit der Speicherpflicht auf das Fehlen von spezifischen Voraussetzungen für die nationalen Zugangsvorschriften abgestellt. Es scheint dem EuGH also durchaus ein Anliegen zu sein, dass eine Arbeitsaufteilung von verschiedenen Akteuren im Bereich der Sicherheitsgesetzgebung nicht dazu führen darf, dass Sicherheitsbehörden an Informationen gelangen, ohne dass das unmittelbar für sie geltende Recht dies zulassen würde. Somit lässt sich der Ausgangspunkt der hypothetischen Datenneuerhebung letztlich auch in der Rechtsprechung des EuGH wiederfinden. Zumindest abstrakt ließe sich also andenken, die europäische Verhältnismäßigkeitsprüfung mit den informationellen Trennungsprinzip aufzuladen, indem bei der Betrachtung der Weiterleitung die verschiedenen Informationszugriffsrechte der beteiligten Behörden berücksichtigt werden.

Auf eine tatsächliche Übertragung des informationellen Trennungsprinzips auf die Anforderungen aus Art. 7, 8 EU-GRC durch den EuGH kann man aber nur spekulieren.

2166 Siehe nur EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 38 ff. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 96 ff. mwN = NJW 2017, 717.

2167 BVerfG, NVwZ-RR, 2023, 1 (8) – Nachrichtendienstliche Informationsübermittlung; *Gärditz*, JZ 2013, 633 (634); *Zöller* in Dietrich/Gärditz/Graulich ua. (Hrsg.), Nachrichtendienste, 2018, S. 185 (191).

2168 *Celeste*, Eur. Const. Law Rev 15 (2019), 134 (139).

d. Fazit

Der Informationsaustausch von Nachrichtendiensten und anderen Sicherheitsbehörden unterliegt in Deutschland strengen Anforderungen gemäß dem informationellen Trennungsprinzip. Die niedrigschwelligen und umfassenden Datenerhebungsmöglichkeiten der Nachrichtendienste sind nur gerechtfertigt, weil ihnen im Gegenzug operative Maßnahmen vorenthalten sind.[2169] Sie dürfen alles wissen, aber nicht alles können.[2170] Um diese Trennung von Informationszugang und operativen Befugnissen zu erhalten, muss der Informationsaustausch von Nachrichtendiensten und Polizeibehörden bzw. der Strafverfolgung streng reglementiert werden.

In diese Architektur lassen sich die Vorschriften des GwG, insb. § 30 Abs. 3 GwG und § 32 Abs. 2, 3 GwG, nicht harmonisch einfügen. Die FIU soll durch ein Netzwerk privater Informanten und heimlichen Zugriffsmöglichkeiten über sämtliche Auffälligkeiten im Finanzverkehr Bescheid wissen. Sie wird deshalb aus guten Gründen als „Finanzgeheimdienst" begriffen.[2171] Anders als die Gesetze der echten Nachrichtendienste, zielt das Recht der FIU aber final auf die Versorgung, insbesondere der Staatsanwaltschaften mit Informationen gerade ab.

Aus Art. 32 Abs. 3 S. 4 GWRL und § 32 Abs. 2 GwG folgt, dass verdächtige Transaktionen, außer in den Fällen des § 32 Abs. 5 GwG, stets zur Überprüfung an die Staatsanwaltschaft gelangen sollen.

Die gefahrenabwehrrechtlichen Befugnisse der FIU nach § 40 GwG stellen sich gegenüber der Transaktionsanalyse lediglich als Nebenschauplatz dar. Die FIU betreibt faktisch primär strafverfahrensrechtliche Vorermittlungen.[2172] Sie ist auch, anders als das BKA, keine echte Zentralstelle i. S. d. Art. 87 Abs. 1 GG, denn ihre Aufgaben liegen nicht primär in der

2169 BVerfGE 133, 277 (323 ff.) – Antiterrordatei I; E 156, 11 (50 ff.); NJW 2022, 1583 (Rn. 153 ff.) – Bayerisches Verfassungsschutzgesetz; s.a. *Gärditz*, JZ 2013, 633 (634); *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 245 ff.

2170 *Gusy*, GA 1999, 319 (327).

2171 *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21; ausf. *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.).

2172 *Barreto da Rosa* in Herzog GwG, § 30 Rn. 13; vgl. auch *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248); allg. für das GwG *Degen,* Geldwäsche, 2009, S. 152 ff.

Koordination[2173] oder Ergänzung[2174], sondern in der aktiven Informationsversorgung. Die Aufgaben und Befugnisse der FIU sind in der deutschen Sicherheitsarchitektur schlicht einzigartig.

Die GWRL überlässt die formal organisatorische Ausgestaltung der FIU den nationalen Gesetzgebern.[2175] Da der deutsche Gesetzgeber insofern einen Spielraum hatte, wären die Vorgaben des Grundgesetzes also prinzipiell zu beachten gewesen. Somit könnte man durchaus die Frage in den Raum stellen, ob er eine Behörde schaffen durfte, die sich als „administrative Gefahrenabwehrbehörde" versteht[2176], strafverfahrensrechtliche Vorermittlungen betreibt und dazu im Bereich der Finanzinformationen auf Befugnisse zurückgreifen darf, die sonst nur den Nachrichtendiensten vorbehalten sind.

Man muss jedoch beachten, dass der Gesetzgeber zu diesem Bruch mit der grundgesetzlichen Sicherheitsarchitektur schlicht gezwungen war. Es ist gerade Sinn der FIU, als Informationsversorgerin von Sicherheitsbehörden zu dienen. Eine solche Aufgabenzuweisung kennt das Grundgesetz aber nicht und sie wäre wohl auch mit der Rechtsprechung des BVerfG zur informationellen Trennung kaum in Einklang zu bringen.[2177]

So ist etwa das heimliche Zugriffsrecht der FIU nach § 30 Abs. 3 GwG spätestens seit Einführung des Art. 32 Abs. 9 der 5. GWRL vollharmonisiert. Dasselbe gilt für die Sorgfalts- und Meldepflichten der Privaten. Die Umstände, aus denen sich der nachrichtendienstliche Charakter der FIU ergibt,[2178], sind somit indisponibel. Auch im Rahmen der Weiterleitungsregeln hatte der deutsche Gesetzgeber nur auf den ersten Blick einen gewissen Spielraum. Hätte er die Informationsweitergabe an die Anforderungen des informationellen Trennungsprinzips angepasst und etwa wie § 19 Abs. 1 BVerfSchG ausgestaltet, müsste er sich wohl vorwerfen lassen, die Richtlinie nicht im Sinne des *effet utile* umgesetzt zu haben, denn die effektive

2173 BVerfGE 110, 33 (51); *Bäcker* in Herdegen/Masing/Poscher ua. (Hrsg.), Hdb. Verfassungsrecht, 2021, § 28 Rn. 76 *Ibler* in Dürig/Herzog/Scholz GG, Art. 87 Rn. 117; *Hermes* in Dreier GG, Art. 87 Rn. 47;

2174 *Bäcker* in Bäcker/Denninger/Graulich (Hrsg.), Lisken/Denninger Hdb. Polizeirecht, Kap. B Rn. 133; BT-Drs. 13/1550, S. 24.

2175 *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (8 ff.); *Bülte*, NVwZ-Extra 4b/2022, 1 (2 ff.).

2176 BT-Drs. 18/11555, S. 136, 168

2177 Vgl. *Gusy*, GSZ 2021, 141 (147 f.).

2178 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.).

Geldwäsche setzt gerade voraus, dass sämtliche verdächtigen Meldungen ihren Weg zur Staatsanwaltschaft finden.[2179]

Eine Prüfung der §§ 30 Abs. 3, 32 Abs. 2, 3 GwG anhand der grundgesetzlichen Vorgaben zur informationellen Trennung dürfte daher nicht angezeigt sein. Es ließe sich allenfalls überlegen, ob man den Umgehungsgedanken, der dem Prinzip zugrunde liegt, im Rahmen einer europarechtlichen Verhältnismäßigkeitsprüfung wieder aufgreift. Die Urteile zur Vorratsdatenspeicherung lassen sich so verstehen, dass klassische Ermittlungsvoraussetzungen nicht durch die Etablierung von Criminal-Compliance-Strukturen unterlaufen werden sollten. Der EuGH scheint in der möglichen Umgehung tradierter Sicherheitsprinzipien durch teilprivatisierte Massenüberwachungskomplexe also durchaus eine strukturelle Beeinträchtigung der Unionsgrundrechte zu erkennen. Den Art. 7, 8 EU-GRC könnte daher ein Verbot allmächtiger Analysestellen durchaus entnommen werden.

IV. Zusammenfassung der Ergebnisse

Die Überprüfung des Anti-Geldwäscherechts in Deutschland, bestehend aus der GWRL und deren Umsetzungsgesetz, dem GwG, anhand der Rechtsprechung von BVerfG, EuGH und EGMR, hat im Kern zu folgenden Ergebnissen geführt:

1. Transaktionsmonitoring

- Das Transaktionsmonitoring, bei dem sämtliche Kontotransaktionsdaten der Kunden insb. von Kreditinstituten automatisiert nach *geldwäscherechtlichen Auffälligkeiten* gerastert werden, stellt ein Phänomen der Massenüberwachung dar, da die Analyse final auf eine Weiterleitung der Daten an Sicherheitsbehörden ausgerichtet ist. Bei der Intensitätsbestimmung muss das Monitoring als Glied einer graduellen Eingriffskette

2179 Erwägungsgrund Nr. 37 der 4. EU-GeldwäscheRL; Erwägungsgrund Nr. 1 der Richtlinie (EU) 2018/1673 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 über die strafrechtliche Bekämpfung der Geldwäsche, ABl. 2018 L 284/22; vgl. auch BR-Drs. 182/1/17, S. 21; BT-Drs. 18/11928, S. 11 f.

betrachtet werden.[2180] Insofern handelt es sich um einen intensiven bzw. schweren Eingriff in die Privatheitsgrundrechte aus Art. 7, 8 EU-GRC, denn betroffen sind besonders sensible Daten[2181] fast der gesamten Bevölkerung.[2182]

Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG findet auf das Transaktionsmonitoring, inkl. der automatisierten Analyse, keine Anwendung, da dieser Überwachungstatbestand von der GWRL vollständig determiniert wird. Dies ergibt sich zwar nicht unmittelbar aus dem Wortlaut des Art. 13 Abs.1 lit. d) GWRL.[2183] Diese Vorschrift kann bei Kreditinstituten aber effektiv nur durch die Einführung einer allgemeinen EDV-Rasterung sämtlicher Kundentransaktionen umgesetzt werden.

- Massenhafte Datenanalysen zur Kriminalitätsbekämpfung sind nicht prinzipiell mit Art. 7, 8 EU-GRC unvereinbar.[2184] Als schwerer Grundrechtseingriff kann das Transaktionsmonitoring aber nur in einer nationalen Gefährdungssituation[2185] oder zur Bekämpfung schwerer Straftaten gerechtfertigt sein.[2186] Soweit die GWRL das Transaktionsmonitoring zur Bekämpfung von Terrorismusfinanzierung vorschreibt, ist letztgenannter Anforderung Genüge getan. Bei der Bekämpfung von Geldwäsche ist dies aber nicht allgemein der Fall, denn aufgrund des *all-crimes-approach* kann es sich bei dem Delikt der Geldwäsche auch um bloße Alltagskriminalität handeln.[2187]

2180 vgl. EGMR, Urt. v. 25.5.2021, Nr. 58170/13, 62322/14, 24960/15 (Big Brother Watch ua/Vereinigtes Königreich), Rn. 325. = NVwZ-Beil. 2021, 11.

2181 BVerfGE 120, 274 (347 f.) – Online-Durchsuchung; *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

2182 Zu diesem Intensittätsaspekt: EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 56 = NJW 2014, 2169.

2183 auch nicht aus *EBA,* Leitlinien Risikofaktoren, EBA/GL/2021/02, 01.03.2021 (dt. Fassung), lfd. Nr. 4.72 ff.

2184 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 176 ff. = EuZW 2022.

2185 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 175 ff. = NJW 2021, 531.

2186 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 148 = EuZW 2022, 706; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

2187 Krit. insofern *Hochmayr* in Frankfurter Kommentar, AEUV Art. 83 Rn. 12; s.a. *Böse/S. Jansen*, JZ 2019, 591 (594).

Eine einschränkende Auslegung des Geldwäschetatbestands ist aufgrund der Determinierung in Art. 1 Abs. 3 GWRL und Art. 3 Geldwäschestrafbarkeits-RL nicht möglich. Eine grundrechtskonforme Auslegung müsste daher unmittelbar an Art. 13 Abs.1 lit. d) GWRL ansetzen. Diese Norm muss im Lichte von Art. 7, 8 EU-GRC dahingehend ausgelegt werden, dass sie das Transaktionsmonitoring nur zur Bekämpfung solcher Geldwäschedelikte erlaubt, die aufgrund der Vortat als schwere Kriminalität einzustufen sind.

Strengere nationale Regelungen sind nicht möglich, da nach Art. 5 GWRL nur im Rahmen des Unionsrechts abgewichen werden darf. Nationale Regelungen, die das Monitoring zur Bekämpfung auch allgemeiner Kriminalität einsetzen, verstoßen daher gegen Art. 5 GWRL sowie mittelbar und unmittelbar gegen Art. 7, 8 EU-GRC.

- Im Übrigen müssen die Prüfkriterien so festgelegt werden, dass die Zahl unschuldiger Personen, die fälschlicherweise mit dem durch die Richtlinie geschaffenen System identifiziert werden, auf ein Minimum beschränkt wird[2188] und nicht zu einer (auch mittelbaren) Diskriminierung bestimmter Personengruppen führen.[2189] Dies muss von der Aufsicht, insbesondere der EBA im Rahmen ihrer Leitlinienkompetenz, Art. 17, 18 Abs. 4 GWRL, sichergestellt werden.
- Da beim Transaktionsmonitoring und der daran eventuell anknüpfenden Verdachtsmeldung besonders sensible Daten verarbeitet werden, muss sichergestellt sein, dass jeder Verarbeitungsschritt effektiv auf die Bekämpfung schwerer Straftaten ausgerichtet ist. Dies ist nur der Fall, wenn die Übermittlung an die Sicherheitsbehörden von einem ausreichenden Anlass abhängig gemacht wird.[2190] Die Übermittlung der Analyseergebnisse von Verdachtsmeldungen von der FIU an die Sicherheitsbehörden i. S. d. Art. 32 Abs. 3 S. 3 der GWRL fordert einen „begründeten Verdacht". Dies ist im Lichte der Art. 7, 8 EU-GRC für Deutschland dahingehend auszulegen, dass bei Straftaten mindestens ein Anfangsverdacht vorliegt. Die Regelung des § 32 Abs. 2 S. 1 GwG ist entsprechend auszulegen.[2191] Andernfalls verstieße sie gegen Art. 5 GWRL bzw. Art. 7, 8 EU-GRC.

2188 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 203 ff. = EuZW 2022, 706.
2189 Idem, Rn. 197.
2190 Idem, Rn. 204.
2191 AA. BT-Drs. 18/11555, S. 144; 18/11928, S. 26.

2. Vorratsdatenspeicherung von Finanzdaten

- Aufgrund der geldwäscherechtlichen Aufzeichnungs- und Aufbewahrungspflicht sind sämtliche Transaktionsdaten zu speichern, da sie für das Monitoring erhoben werden müssen. Aufgrund der Zugriffsrechte und Übermittlungspflichten der FIU, Art. 32 Abs. 9 i. V. m. Abs. 4. S. 2 GWRL, handelt es sich um eine anlasslose Vorratsdatenspeicherung hochsensibler Daten, für die grundsätzlich die Feststellungen des EuGH greifen.
  Dieser erlaubt eine solche Speicherung maximal für sechs Monate.[2192]Diese zeitliche Grenze kann für die geldwäscherechtlichen Speicherpflichten der verpflichteten Privaten aber nicht übertragen werden, da für Finanzdaten, etwa Kontoauszüge, bereits umfangreiche Speicherpflichten aus anderen Rechtsgebieten, insb. dem Wirtschaftsrecht, folgen. In Deutschland besteht etwa eine allgemeine Aufbewahrungspflicht über zehn Jahre nach § 257 Abs. 4 HGB. Die GWRL lässt solche Fristen nach Art. 40 Abs. 1 UAbs. 2 unberührt.
- Die Verhältnismäßigkeit muss daher über die Eingrenzung des Zugriffs erfolgen. Für Daten, die länger als sechs Monate bei Privaten gespeichert sind, ist ein Zugriff der FIU grundsätzlich auszuschließen. Insofern leidet Art. 32 Abs. 9 GWRL an einem Gestaltungsmangel und müsste jedenfalls teleologisch reduziert, eigentlich aber gesetzlich verändert werden.
- Soweit die FIU Daten speichert, die sie durch Zugriff oder im Rahmen einer Verdachtsmeldung erhalten hat, sind die Daten spätestens nach sechs Monaten zu löschen, wenn sich nicht aus der Analyse ergibt, dass die Daten mit Geldwäsche oder Terrorismusfinanzierung in Verbindung stehen. In Deutschland ist § 37 Abs. 2 GwG entsprechend auszulegen. Auf europäischer Ebene ergibt sich die Begrenzung entweder aus Art. 5 JI-RL oder Art. 17 Abs. 1 DSGVO. Welches dieser Datenschutzregime für die FIU gilt[2193], ist daher nicht unmittelbar relevant.
- Die FIU agiert nicht nur als Analyse- sondern auch als Weiterleitungs- und Auskunftsstelle für Finanzdaten. Über sie als Mittlerin wird den Sicherheitsbehörden nach Art. 32 Abs. 4 S. 2 GWRL ein heimlicher Zugriff auf sensible Daten ermöglicht. Dabei folgt Heimlichkeit folgt aus

2192 EuGH Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 255 = EuZW 2022.

2193 Dazu *Quintel*, ERA Forum 2022, 53 (61 ff.); *Brewczyńska*, Computer Law & Security Review 43 (2021), 105612 (11 ff.).

dem Verbot der Verpflichteten, Dritte über geldwäscherechtliche Informationsübermittlungen zu informieren, Art. 39 Abs. 1, 59 Abs. 1 lit. b) GWRL. Ein heimlicher (mittelbarer) Zugriff von Sicherheitsbehörden auf vorratsmäßig gespeicherte sensible Daten kann nur zur Bekämpfung schwerer Kriminalität gerechtfertigt sein.[2194]

Dient die Übermittlung der Bekämpfung von Geldwäsche, stellt sich insofern abermals das Problem ein, dass nicht jedes Geldwäschedelikt eine schwere Straftat darstellt. Die Pflicht der FIU zur Übermittlung muss entsprechend eng ausgelegt werden. § 100a Abs. 2 Nr. 1 lit. m) StPO könnte hier eine Vorbildfunktion einnehmen.

- Bei Übermittlungen zur Bekämpfung allgemeiner schwerer Kriminalität an eine nach Art. 3 Abs. 2 Finanzinformations-RL benannte Behörde, ergibt sich aus Art. 2 Nr. 5 Finanzinformations-RL, dass nur solche Daten übermittelt werden dürfen, die bei der FIU bereits vorliegen. Die FIU darf also nicht auf Ersuchen hin von ihrem Zugriffsrecht Gebrauch machen.

  Diese Einschränkung ist auf Übermittlungen der FIU zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu übertragen, da ihre Zugriffsrechte keine materiellen und formellen Einschränkungen vorsehen. Den Sicherheitsbehörden wäre daher über Art. 32 Abs. 9 i. V. m. Abs. 3. S. 4 GWRL mittelbar ein Zugriff auf anlasslos gespeicherte Daten eingeräumt, der nur unter engen Voraussetzungen erlaubt ist.[2195]

  Auf die bei der FIU vorliegenden Daten dürfen Sicherheitsbehörden ferner nur unter Richtervorbehalt zugreifen.[2196]
- Die Feststellungen zu Art. 32 Abs. 9 i. V. m. Abs. 4. S. 2 GWRL sind auf §§ 30 Abs. 3, 32 Abs. 3 GwG zu übertragen. Die identifizierten Limitierungen ergeben sich aus den Art. 7, 8 EU-GRC. Daher sind nationale strengere Regelungen bzw. Abweichungen nicht möglich, Art. 5 GWRL.

  Auch § 32 Abs. 3 Nr. 1 GwG ist daher so auszulegen, dass eine Weiterleitung nur zur Bekämpfung von Terrorismusfinanzierung und schwerer Geldwäschekriminalität möglich ist. Außerdem muss die Weiterleitung einem Richtervorbehalt unterliegen, bedarf insofern also einer Änderung.

2194 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.
2195 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 60 ff. = NJW 2014, 2169.
2196 EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 51 ff. = NJW 2021, 2103; Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 56 = NJW 2019, 655.

- § 32 Abs. 3 Nr. 2 GwG übererfüllt Art. 32 Abs. 4. S. 2 GWRL, da er eine Weiterleitung auch zur Bekämpfung allgemeiner Straftaten und zur Verhütung allgemeiner Gefahren zulässt. Zwar sieht Art. 7 Finanzinformations-RL eine Weiterleitung von Informationen zur Bekämpfung allgemeiner Kriminalität vor, allerdings nur an spezifisch benannte Behörden und nur bei schwerer *Kriminalität*. Art. 7 Finanzinformations-RL wurde in Deutschland allein durch § 32 Abs. 3a GwG umgesetzt. Für § 32 Abs. 3 Nr. 2 GwG gilt Art. 7 Finanzinformations-RL also nicht.
  § 32 Abs. 3 Nr. 2 GwG geht damit über die Determinierung des Art. 32 Abs. 4. S. 2 GWRL hinaus und ist deswegen nach Art. 5 GWRL an den Unionsgrundrechten zu messen. Insofern ist wegen der Begrenzung intensiver Überwachungsmaßnahmen auf die Bekämpfung schwerer Kriminalität[2197] ein Verstoß gegen Art. Art. 7, 8 EU-GRC festzustellen. Dieser Verstoß könnte nicht nur vom EuGH, sondern nach jüngerer Rechtsprechung auch vom BVerfG festgestellt werden.[2198]
- Die Weiterleitungsrechte der FIU sind aus einem weiteren Grund problematisch. Da die FIU sowohl aufgrund ihrer Filterfunktion als auch ihrer Zugriffrechte in erheblichem Umfang sensible Daten erhebt und analysiert, die ihr aktiv zugespielt werden, überwacht sie letztlich den gesamten Finanzfluss im jeweiligen Mitgliedstaat[2199], quasi als „Finanzgeheimdienst".[2200]
  Mit der Sicherheitsarchitektur des Grundgesetzes wird dadurch gebrochen, denn dieses sieht eine informationelle Trennung von Nachrichtendiensten und (operativen) Sicherheitsbehörden vor, die nur ausnahmsweise durchbrochen werden darf. Bei der FIU ist der Informationsfluss aber keine Ausnahme, sondern primärer Zweck.
  Die GWRL kann allerdings nicht effektiv umgesetzt werden, ohne das Prinzip der informationellen Trennung zu missachten. Die GWRL zwingt also zu einem Systembruch innerhalb des GG. Da das informationelle Trennungsprinzip sich aus den Grundrechten ableitet, findet es keine Anwendung, soweit die Grundrechte aufgrund des Anwendungsvorrangs des Unionsrechts zurücktreten. Es bestünde aber die Möglichkeit, im Rahmen der europarechtlichen Prüfung der Weiterlei-

2197 EuGH, Urteil v. 21.6.2022, C-817/19 (Ligue des droits humains (PNR)), Rn. 219. = EuZW 2022, 706
2198 BVerfGE 152, 216 (236 ff.) – Recht auf Vergessen II.
2199 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (248 ff.).
2200 *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21.

tungsrechte und -pflichten auf die systematische Stellung der jeweiligen Behörden Rücksicht zu nehmen – die Art. 7, 8 EU-GRC also mit einem informationellen Trennungsprinzip aufzuladen.

Literaturverzeichnis

1. UA des 18. Deutschen Bundestags, Beschlussempfehlung und Bericht des 1. Untersuchungsausschusses gemäß Artikel 44 des Grundgesetzes*, Deutscher Bundestag, 2017.

30. Strafverteidigertag (Hrsg.), Wieviel Sicherheit braucht die Freiheit, 30. Strafverteidigertag, Frankfurt/Main, 24.-26.3.2006, Schriftenreihe der Strafverteidigervereinigungen Bd. 30, 2007, Berlin.

IV International Conference on "Information Technology and Nanotechnology // The IV International Conference on Information Technology and Nanotechnology, 24-27 April 2018, Samara, Russian Federation, in Journal of physics Conference series, volume 1096, 2018.

Accenture, Evolving AML Journey, Leveraging Machine Learning Within Anti-money Laundering Transaction Monitoring 2017, https://www.accenture.com/_acnmedia/pdf-61/accenture-leveraging-machine-learning-anti-money-laundering-transaction-monitoring.pdf, zuletzt zugegriffen am 04.04.2022.

Ackermann, Bernd/Reder, Lars, Geldwäscheprävention in Kreditinstituten nach Umsetzung der Dritten EG-Geldwäscherichtlinie, Teil I, in Wertpapier-Mitteilungen (WM) 2009, 158.

Ackermann, Bernd/Reder, Lars, Geldwäscheprävention in Kreditinstituten nach Umsetzung der Dritten EG-Geldwäscherichtlinie, Teil II, in Wertpapier-Mitteilungen (WM) 2009, 200.

Adelberg, Philipp Nikolaus, Rechtspflichten und -grenzen der Betreiber sozialer Netzwerke, Zum Umgang mit nutzergenerierten Inhalten, Heidelberg, 2020, zugl. Diss., Univ. Bonn, 2019.

Adensamer, Angelika, Aspekte einer Überwachungs-Gesamtrechnung, in FIfF-Kommunikation 2019(4), 25.

Adensamer, Angelika, Handbuch Überwachung, Wien, 2020.

Albers, Marion, Data Retention in Germany, in Zubik, Marek/Podkowik, Jan/Rybski, Robert (Hrsg.), European Constitutional Courts towards Data Retention Laws, 2021, S. 117.

Albers, Marion, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin, 2001.

Albers, Marion, Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hrsg.), Informationelle Selbstbestimmung im Digitalen Wandel, 2017, S. 11.

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden, 2005, zugl.: Univ., Habil., Berlin, 2001/2002.

Albers, Marion, Surveillance and Data Protection Rights: Data Retention and Access to Telecommunications Data, in Albers, Marion/Sarlet, Ingo Wolfgang (Hrsg.), Personality and Data Protection Rights on the Internet, Brazilian and German Approaches, 2022, S. 69.

Albers, Marion/Sarlet, Ingo Wolfgang (Hrsg.), Personality and Data Protection Rights on the Internet, Brazilian and German Approaches, 2022.

Albers, Marion/Weinzierl, Ruth (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, Beiträge zur rechtsstaatsorientierten Evaluierung von Sicherheitsgesetzen, Baden-Baden, 2010.

Ambos, Kai, Anmerkung zu EuGH, Urt. v. 30.05.2006, C-317, 318/04, in Juristenzeitung (JZ) 2009, 466.

Ambos, Kai, Der Europäische Gerichtshof für Menschenrechte und die Verfahrensrechte: Waffengleichheit, partizipatorisches Vorverfahren und Art. 6 EMRK, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)2003, 583.

Amnesty International, Suveillance Giants, How the Business Model of Google and Facebook threatens Human Rights, 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en/., zuletzt zugegriffen am 08.08.2023

Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltsvereins (Hrsg.), Strafverteidigung im Rechtsstaat, 25 Jahre Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins, 2009, Baden-Baden.

Arndt, Claus, Die Fernmeldekontrolle im Verbrechensbekämpfungsgesetz, in Neue Juristische Wochenschrift (NJW) 1995, 169.

Article 29 Data Protection Working Party, Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, 13.06.2011, zuletzt zugegriffen am 08.08.2023.

Artopeus, Wolfgang/Findeisen, Michael, (Bundesaufsichtsamt für das Kreditwesen (BAKred), Das Geldwäschegesetz zwischen Erwartung und Wirklichkeit, Anhörung im Deutschen Bundestag am 25.08.1995 (Entwurf), 21.08.1995.

Arzt, Clemens, Antiterrordatei verfassungsgemäß – Trennungsgebot tot? in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2013, 1328.

Arzt, Clemens, Das neue Gesetz zur Fluggastdatenspeicherung, in Die Öffentliche Verwaltung (DÖV) 2017, 1023.

Arzt, Clemens, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Teil IV, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., 2021, München.

Auer, Marietta, Warum der Begriff der Rechtsgeltung nicht zur Bewältigung staatlichen Unrechts taugt, in: Rechtswissenschaft (RW) 2017, 45.

Ayres, Ian/Braithwaite, John, Responsive regulation, Transcending the deregulation debate, 1995, New York.

Bäcker, Matthias, Die Vertraulichkeit der Internetkommunikation, in Rensen, Hartmut/Brink, Stefan (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 99.

Bäcker, Matthias, Grundrechtlicher Informationsschutz gegen Private, in Der Staat 2012, 91.

Bäcker, Matthias, Kapitel B. Die Polizei im Verfassungsgefüge, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., 2021, München.

Bäcker, Matthias, Kapitel D. Polizeiaufgaben und Regelungsmuster des polizeilichen Eingriffsrechts, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., 2021, München.

Bäcker, Matthias, Kriminalpräventionsrecht, Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, 2015, Tübingen, zugl. Uni. Habil., Hamburg, 2015.

Bäcker, Matthias, Strategische Telekommunikationsüberwachung auf dem Prüfstand, in Kommunikation und Recht (K&R) 2014, 556.

Badura, Peter/Dreier, Horst (Hrsg.), Festschrift 50 Jahre Bundesverfassungsgericht, 2001, Tübingen.

Bakaus, Julia/Kruse, Lars-Heiko/Schwerdtner, Cornelia (Hrsg.), Die "Zentrale Stelle" in Kreditinstituten, Anti-Financial Crime in der Praxis, 2019, Frankfurt.

Baldus, Manfred, Entgrenzungen des Sicherheitsrechts, Neue Polizeirechtsgomatik, in Die Verwaltung (Verw 2014, 1.

Bannenberg, Britta/Wabnitz, Heinz-Bernd/Janovsky, Thomas ua. (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 5. Aufl., 2020, München

Bantlin, Franziska, Die G 10-Kommission – Zur Kontrolle der Nachrichtendienste, 2021, Berlin, zugl. Diss., Univ. Freiburg, 2020

Banzhaf, Maximilian, Die Ämter für Verfassungsschutz als Präventionsbehörden, 2021, Berlin, zugl. Diss., Univ. Augsburg, 2020.

Bär, Wolfgang, Der Zugriff auf Computerdaten im Strafverfahren, 1992, Köln, zugl. Diss., Univ. Bayreuth, 1991.

Bär, Wolfgang, Die Neuregelung des § 100j StPO zur Bestandsdatenauskunft, Auswirkungen auf die Praxis der Strafverfolgung, in Zeitschrift für IT-Recht und Recht der Digitalisierung 2013, 700.

Bär, Wolfgang, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Stuttgart.

Bär, Wolfgang, Kapitel 28. EDV-Beweissicherung, in Bannenberg, Britta/Wabnitz, Heinz-Bernd/Janovsky, Thomas ua. (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 5. Aufl., 2020, München

Barczak, Tristan, Der nervöse Staat, Ausnahmezustand und Resilienz des Rechts in der Sicherheitsgesellschaft, 2. Aufl. 2021, Tübingen, zugl. Univ. Habil., Münster, 2019.

Barton, Stephan/Kölbel, Ralf/Lindemann, Michael (Hrsg.), Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens, Interdisziplinäre Studien zu Recht und Staat Band 54, 2015, Baden-Baden.

Bartz, Tim/Böcking, David/Diehl, Jörg/Hesse, Martin/Latsch, Gunther/Seith, Anne, Deutschland, ein Paradies für Geldwäscher, in Der Spiegel vom 27.08.2021.

Basel Committee on Banking Supervision, Guidelines Sound management of risks related to money laundering and financing of terrorism, Bank of International Settlements, January 2014 (rev. July 2020), https://www.bis.org/bcbs/publ/d505.pdf, zuletzt zugegriffen am 08.08.2023.

Basler Ausschuss für Bankenaufsicht, Sorgfaltspflicht der Banken bei der Feststellung der Kundenidentität, Oktober 2001, https://www.bis.org/publ/bcbs85g.pdf, zuletzt zugegriffen am 08.08.2021

Bauernfeind, Tobias, Die Rundschreiben-Praxis der BaFin, in Die Öffentliche Verwaltung (DÖV) 2020, 110.

Baumann, Bastian, Datenschutzkonflikte zwischen der EU und den USA, Angemessenheit des Datenschutzniveaus am Beispiel der PNR-Abkommen, 2016, Berlin, zugl. Diss., Univ. Freiburg, 2015.

Baumgartner, Annina, Anmerkung zu EuGH, Urteil vom 6.10.2020, C-623/17 (Privacy International), in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2021, 36.

Baur, Alexander, Maschinen führen die Aufsicht, Offene Fragen der Kriminalprävention durch digitale Überwachungsagenten, in Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2020, 275.

Bell, Anita, Beschlagnahme und Akteneinsicht bei elektronischen Medien, 2016, Hamburg, zugl. Diss., Univ. Münster, 2015.

Benda, Ernst/Mailhofer, Werner/Vogel, Hans-Jochen (Hrsg.), Handbuch des Verfassungsrechts der Bundesrepublik Deutschland, 1984, Berlin.

Bergemann, *Nils*, Kapitel H. Nachrichtendienste und Polizei, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., 2021, München.

Bergles, Siegfried/Eul, Harald, „Rasterfahndung" zur Geldwäschebekämpfung - ein Konflikt mit dem Datenschutz? in Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2002, 556.

Bergles, Siegfried/Schirnding, Clemens Graf, Geldwäschebekämpfung durch unterstützende Research-Systeme - Umsetzung in der Bankenpraxis, in Zeitschrift für Bankrecht und Bankwirtschaft (ZBB) 1999, 58.

Bertrand, Astrid/Maxwell, Winston/Vamparys, Xavier, Do AI-based anti-money laundering (AML) systems violate European fundamental rights? in International Data Privacy Law 2021, 276.

Beulke, Werner/Meininghaus, Florian, Heimliche Durchsuchung eines PC, Anmerkung zu BGH, Beschluß vom 21.02.2006 - 3 BGs 31/06, in Strafverteidiger (StV) 2007, 60.

Bieker, Felix/Bremert, Benjamin, Rote Linien im Sand, bei Sturm: Die Überwachungs-Gesamtrechnung, in FIfF-Kommunikation 2019(4), 34.

Bieker, Felix/Bremert, Benjamin/Hagendorff, Thilo, Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf, in Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes, Zwischen Systemgestaltung und Selbstregulierung, 2018, S. 139.

Bignami, Francesca, Privacy and Law Enforcement in the European Union: The Data Privacy and Law Enforcement in the European Union: The Data Retention Directive Retention Directive, in Chicago Journal of International Law 2007, 233.

Blankenagel, Alexander, Verfassungsmäßigkeit einer gesetzlichen Impfpflicht gegen Corona? in Juristenzeitung (JZ) 2022, 267.

Bleckmann, Albert/Wiethoff, Claudia, Zur Grundrechtskonkurrenz, in Die Öffentliche Verwaltung (DÖV) 1991, 722.

Bleckmann, Moritz, Nationale Grundrechte im Anwendungsbereich des Rechts der Europäischen Union, Die Kooperation des Grundrechtsschutzes in der Europäischen Union unter Berücksichtigung der besonderen Ausprägungen des nationalen Grundrechtsschutzes, 2012, Tübingen, zugl. Diss., Univ. Köln, 2009/2019.

Bock, Dennis, Criminal Compliance, 1. Aufl. 2011, Baden-Baden, zugl. Univ. Habil., Kiel, 2010/2011.

Böckenförde, Thomas, Auf dem Weg zur elektronischen Privatsphäre, in Juristenzeitung (JZ) 2008, 925.

Bode, Thomas A., Verdeckte strafprozessuale Ermittlungsmaßnahmen, 2012, Berlin/Heidelberg, zugl. Diss., Univ. Frankfurt (Oder), 2011/2012.

Boehm, Franziska, Anlasslose Datensammlungen und die Mitarbeit Privater bei der Strafverfolgung – der neue Trend in der europäischen Verbrechensbekämpfung? in Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV) 2012, 82.

Boehm, Franziska/Andrees, Markus, Zur Vereinbarkeit der Vorratsdatenspeicherung mit europäischem Recht, Bewertung der generellen Speicherpflicht nach EuGH und EGMR Rechtsprechung, in Computer und Recht (CR) 2016, 146.

Boehm, Franziska/Cole, Mark D., Studie zu den Folgen des EuGH-Urteils zur Vorratsdatenspeicherung Auswirkungen auf Mitgliedstaaten, EU-Rechtsakte und internationale Abkommen, in Zeitschrift für Datenschutz (ZD) 2014, 553.

Boehme-Neßler, Volker, Ist eine allgemeine Impfpflicht gegen das SARS-CoV-2 verfassungsgemäß?, Rechtsgutachten Erstattet im Auftrag von Ärztinnen und Ärzte für individuelle Impfentscheidung e.V., Ärztinnen und Ärzte für individuelle Impfentscheidung e.V., 13.03.2022, https://individuelle-impfentscheidung.de/fileadmin/Downloads/Rechtsgutachten_Allgemeine_Impfpflicht_13.03.22.pdf., zuletzt zugegriffen am 08.08.2023

Boerger, Björn Bastian, § 38 Geldwäscherecht, in Momsen, Carsten/Grützner, Thomas (Hrsg,), Wirtschafts- und Steuerstrafrecht, Handbuch für die Unternehmens- und Anwaltspraxis, 2. Aufl., München, 2020

Bonin, Irina, Grundrechtsschutz durch verfahrensrechtliche Kompensation bei Maßnahmen der polizeilichen Informationsvorsorge, 2014, Stuttgart, zugl. Diss., Univ. Freiburg 2012.

Boos, Karl-Heinz/ Fischer, Reinfrid/Schulte-Mattler, Hermann (Hrsg.), Kommentar zu Kreditwesengesetz, VO (EU) Nr. 575/2013 (CRR) und Ausführungsvorschriften, 5. Aufl., 2016, München (zit. als *Bearbeiter* in Boos/Fischer/Schulte-Mattler KWG).

Böse, Martin, Aufsichtsrechtliche Vorermittlungen in der Grauzone zwischen Strafverfolgung und Gefahrenabwehr, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2007, 848.

Böse, Martin/Jansen, Scarlett, Die Vortat der Geldwäsche – unionsrechtliche Vorgaben und ihre Konsequenzen für das deutsche Strafrecht, in Juristenzeitung (JZ) 2019, 591.

Böszörmenyi, Janos/Schweighofer, Erich, A review of tools to comply with the Fourth EU anti-money laundering directive, in International Review of Law, Computers & Technology 2015, 63.

Böszörmenyi, Janos/Schweighofer, Erich, Tracking of Financial Movements, in Schweighofer, Erich/Kummer, Franz/Hötzendorfer, Walter (Hrsg.), Transparenz, Tagungsband des 17. Internationalen Rechtsinformatik Symposions (IRIS 2014) = Transparency, 2014, S. 617.

Brade, Alexander, Die horizontale Eingriffsaddition, in Die Öffentliche Verwaltung (DÖV) 2019, 853.

Brandner, Gert, Die überschießende Umsetzung von Richtlinien, Tatbestand und Rechtsfolgen der autonomen Erstreckung des Regelungsgehalts einer Richtlinie auf Sachverhalte außerhalb ihres Anwendungsbereichs durch den nationalen Gesetzgeber, 2003, Frankfurt (Main), zugl. Univ. Diss, Freiburg, 2003.

Brandt, Karsten, Das Bundesamt für Verfassungsschutz und das strafprozessuale Ermittlungsverfahren, Die Mitwirkung des Bundesamtes für Verfassungsschutz in strafprozessualen Ermittlungsverfahren vor dem Hintergrund des sog. Trennungsgebots, 2015, Berlin, zugl. Diss., Univ. Hamburg, 2012/2013.

Braun, Frank, Die entschädigungslose Indienstnahme Privater am Beispiel der sog. Vorratsdatenspeicherung, in Kommunikation und Recht (K&R) 2009, 386.

Braun, Frank/Albrecht, Florian, Der Freiheit eine Gasse? Anmerkungen zur „Überwachungsgesamtrechnung" des Bundesverfassungsgerichts, in Verwaltungsrundschau (VR) 2017, 151.

Breckwoldt, Maike, Grundrechtskombinationen, 2015, Tübingen, zugl. Diss., Univ. Hamburg, 2014.

Brewczyńska, Magdalena, Financial Intelligence Units: Reflections on the applicable data protection legal framework, in 43 Computer Law & Security Review 2021, 105612.

Breyer, Patrick, Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland (Vorratsspeicherung, traffic data retention), 2005, Berlin, zugl., Diss., Univ. Frankfurt (Main), 2004.

Breyer, Patrick, Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, in Strafverteidiger (StV) 2007, 214.

Brian, Ilka/Frey, Tobias/Pelz, Christian, Aktuelles Geldwäscherecht –, Sommernovellen in Deutschland vor Winterreformen der EU, in Corporate Compliance (CCZ) 2021, 209.

Britz, Gabriele, Freie Entfaltung durch Selbstdarstellung, Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, 2007, Tübingen.

Britz, Gabriele, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, 2010, S. 561.

Britz, Gabriele, Kooperativer Grundrechtsschutz in der EU, Aktuelle Entwicklungen im Lichte neuerer Rechtsprechung des BVerfG, in Neue Juristische Wochenschrift (NJW) 2021, 1489.

Britz, Gabriele, Vertraulichkeit und Integrität informationstechnischer Systeme, in Die Öffentliche Verwaltung (DÖV) 2008, 411.

Brkan, Maja, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, in 20 German Law Journal 2019, 864.

Brodowski, Dominik, BVerfG v. 17.2.2009 – 2 BvR 1372/07 und 2 BvR 1745/07. Automatischer Suchlauf bei Kreditinstituten zur Feststellung bestimmter Überweisungen, in Juristische Rundschau (JR) 2010, 543.

Brodowski, Dominik, Strafprozessualer Zugriff auf E-Mail-Kommunikation, in Juristische Rundschau (JR) 2009, 402.

Brodowski, Dominik, Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht, 2016, Tübingen, zugl. Diss., Univ. Tübingen, 2016.

Brownsword, Roger/Scotford, Eloise/Yeung, Karen (Hrsg.), The Oxford handbook of law, regulation and technology, 2017, Oxford/New York.

Buchner, Benedikt, Die Einwilligung im Datenschutzrecht, in Datenschutz und Datensicherheit (DuD) 2010, 39.

Buermeyer, Ulf, Die "Online-Durchsuchung", Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme, in Onlinezeitschrift für höchstrichterliche Rechtsprechung im Strafrecht (HRRS) 2007, 329.

Buermeyer, Ulf, Informationelle Selbstbestimmung und effektiver Rechtsschutz im Strafvollzug: Informationsrechten im Vollzug von Freiheitsentziehungen, Verwirklichungsbedingungen von Datenschutz und, 2019, zugl. Diss., Univ. Mainz 2014/2015.

Buggel, Thorsten, Research- und Monitoring Maßnahmen, in Bakaus, Julia/Kruse, Lars-Heiko/Schwerdtner, Cornelia (Hrsg.), Die "Zentrale Stelle" in Kreditinstituten, Anti-Financial Crime in der Praxis, 2019, S. 455.

Bull, Hans Peter, Grundsatzentscheidungen zum Datenschutz bei den Sicherheitsbehörden, Rasterfahndung, Online-Durchsuchung, KFZ-Kennzeichenerfassung und Vorratsdatenspeicherung in der Rechtsprechung des Bundesverfassungsgerichts, in Möllers, Martin H. W./van Ooyen, Robert Chr. (Hrsg.), Bundesverfassungsgericht und öffentliche Sicherheit, 2. Aufl. 2012, S. 65.

Bull, Hans Peter, Grundsatzentscheidungen zum Datenschutz im Bereich der inneren Sicherheit., Rasterfahndung, Online-Durchsuchung, Kfz-Kennzeichenerfassung, Vorratsdatenspeicherung und Antiterrordatei in der Rechtsprechung des Bundesverfassungsgerichts, in van Ooyen, Robert Chr./Möllers, Martin H. W. (Hrsg.), Handbuch Bundesverfassungsgericht im politischen System, 2015, S. 627.

Bull, Hans Peter, Informationelle Selbstbestimmung - Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, 2. Aufl. 2011, Tübingen.

Bull, Hans Peter, Netzpolitik: Freiheit und Rechtsschutz im Internet, 2013, Baden-Baden.

Bull, Hans Peter, Polizeiliche und nachrichtendienstliche Befugnisse zur Verdachtsgewinnung, in Osterloh, Lerke/Schmidt, Karsten/Weber, Hermann (Hrsg.), Staat, Wirtschaft, Finanzverfassung, Festschrift für Peter Selmer zum 70. Geburtstag, 2004, S. 29.

Bülte, Jens, Die Risiken des Risikobasierten Ansatzes, - Zu den Pflichten der FIU nach §§ 30, 32 GwG, in Neue Zeitschrift für Verwaltungsrecht– Extra (NVwZ-Extra) 4b/2022, 1.

Bülte, Jens, Zu den Gefahren der Geldwäschebekämpfung für Unternehmen, die Rechtsstaatlichkeit und die Effektivität der Strafverfolgung, in Neue Zeitschrift für Wirtschaftsstrafrecht (NZWiSt) 2017, 276.

Bumke, Christian, Der Grundrechtsvorbehalt, Untersuchungen über die Begrenzung und Ausgestaltung der Grundrechte, 1998, Baden-Baden, zugl.: Diss., Univ. Köln, 1996/1997.

Bumke, Christian, Der Grundsatz der Verhältnismäßigkeit. Beispiel für eine rechtsimmanente Innovation im Recht, in Hoffmann-Riem, Wolfgang (Hrsg.), Innovationen im Recht, 2016, S. 115.

Bundesamt für Justiz, Übersicht Telekommunikationsüberwachung 2020 (Maßnahmen nach § 100g StPO insgesamt) 2020, https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_Verkehrsdaten_2020.pdf?__blob=publicationFile&v=4, zuletzt zugegriffen am 08-08-.2023.

Bundesanstalt für Finanzdienstleistungsaufsicht, Auslegungs- und Anwendungshinweise, Besonderer Teil: Kreditinstitute, Juni 2021, https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_aua_bt_ki_gw.html, zuletzt zugegriffen am 08.08.2023.

Bundesanstalt für Finanzdienstleistungsaufsicht, Auslegungs- und Anwendungshinweise zum Geldwäschegesetz, Mai 2020, https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_gw.pdf;jsessionid=686C6E8197C73EBC2CAABF1BCD924F86.2_cid501?__blob=publicationFile&v=17, zuletzt zugegriffen am 08.08.2023

Bundesanstalt für Finanzdienstleistungsaufsicht, Jahresbericht, 2006, https://www.bafin.de/SharedDocs/Downloads/DE/Jahresbericht/dl_jb_2006.html, zuletzt zugegriffen am 08.08.2023

Bundesanstalt für Finanzdienstleistungsaufsicht, Leitlinien und Q&As der Europäischen Aufsichtsbehörden, https://www.bafin.de/DE/RechtRegelungen/Leitlinien_und_Q_and_A_der_ESAs/Leitlinien_und_Q_and_A_der_ESAs_node.html, zuletzt zugegriffen am 08.08.2023

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz – 19. Tätigkeitsbericht –, 2001-2002.

Bundesministerium der Finanzen (Hrsg.), Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) 2019, https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Abgabenordnung/2019-11-28-GoBD.html, zuletzt zugegriffen am 21.06.2021.

Bundesministerium der Finanzen, Auslegungshinweise des Bundesministerium der Finanzen zur Handhabung des Verdachtsmeldewesen (§ 11 GWG), 06. November 2014.

Bundesministerium der Finanzen, Erste Nationale Risikoanalyse 2018/2019, https://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2019-10-19-erste-nationale-risikoanalyse_2018-2019.pdf?__blob=publicationFile&v=7, zuletzt zugegriffen am 08.08.2023

Bundesministerium des Innern, Polizei 2020, White Paper, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=7, zuletzt zugegriffen am 08.08.2023

Bundesnetzagentur, Mitteilung zur Speicherverpflichtung nach § 113b TKG 2017, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html, zuletzt zugegriffen am 03.03.2021.

Bung, Jochen, Grundlagenprobleme der Privatisierung von Sanktions- und Präventionsaufgaben, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)2014, 536.

Bunjes, Johann/Geist, Reinhold (Begr.) Umsatzsteuergesetz, Kommentar, 20. Aufl., 2021, München (zit. als *Bearbeiter* in Bunjes/UStG)

Bunte, Hermann-Josef/Zahrte, Kai, AGB-Banken AGB-Sparkassen Sonderbedingungen, 5. Aufl., 2019, München (zit. als *Bearbeiter* in Bunte/Zahrte Banken/Sparkassen-AGB).

Burhoff, Detlef, Zurückstellung der Benachrichtigung von der Beschlagnahme – „heimliche Beschlagnahme" (§ 95a StPO), in StrafRechtsReport (StRR) (9) 2021, 6.

Bürkle, Jürgen (Hrsg.), Compliance in Versicherungsunternehmen, Rechtliche Vorgaben und praktische Umsetzung, 3. Aufl., 2020, München.

Burmeister, Frank/Staebe, Erik, Grenzen des sog. Gold Plating bei der Umsetzung europäischer Richtlinien in nationales Recht, in Europarecht (EuR) 2009, 444.

Büro der Vereinten Nationen für Drogen- und Verbrechensbekämpfung, goAML, Anti-Money Laundering System, https://unite.un.org/goaml/, zuletzt zugegriffen am 08.08.2023.

Busch, Dagmar/Teichmann, Helmut, Das neue Geldwäscherecht, 2003, Baden-Baden.

Callies, Christian/Ruffert, Matthias EUV/AEUV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtechart, Kommentar, 6. Aufl., 2022, München (zit. als *Bearbeiter* in Callies/Ruffert EUV/AEUV).

Cameron, Iain, A. Court of Justice Metadata retention and national security: Privacy International and La Quadrature du Net, in 58 Common Market Law Review (Common Market Law Rev) 2021, 1433.

Cameron, Iain, European Union Law Restraints on Intelligence Activities, in 33 International Journal of Intelligence and CounterIntelligence (Int. J. of Intelligence and CounterIntelligence) 2020, 452.

Canaris, Claus-Wilhelm, Handelsrecht, 24. Aufl. 2020, München.

Canhoto, Ana Isabel, Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective, in 131 Journal of Business Research 2020, 441.

Carl, Dieter/Klos, Joachim, Geldwäschegesetz und Datenweitergabe zu Besteuerungszwecken, in Deutsche Steuerzeitung (DStR) 1994, 68.

Carl, Dieter/Klos, Joachim, Verdachtsmeldepflicht und Strafaufhebung in Geldwäschefällen, in Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 1994, 161.

Čas, Jonathan/Bellanova, Rocco/Burgess, J. Peter/Friedewald, Michael/Peissl, Walter, Introduction, Surveillance, privacy and security, in Friedewald, Michael/Burgess, J. Peter/Čas, Jonathan/Bellanova, Rocco/Peissl, Walter (Hrsg.), Surveillance, privacy and security, Citizens' perspectives, 2017, S. 1.

CDU, CSU, SPD, Deutschlands Zukunft Gestalten, Koalitionsvertrag zwischen CDU, CSU und SPD, 18. Aufl., 2013, https://archiv.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf., zuletzt zugegriffen am 08.08.2023.

Celeste, Edoardo, The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios, in 15 European Constitutional Law Review (Eur. Const. Law Rev) 2019, 134.

Clarke, Roger, Information technology and dataveillance, in Communications of the ACM 1988, 498.

Classen, Claus Dieter, Zuviel des Guten? Unionsrechtliche Neuakzentuierungen beim Grundrechtsschutz, in Juristenzeitung (JZ) 2019, 1057.

Comdirect (Hrsg.), Wie lange muss man Kontoauszüge aufbewahren?, https://magazin.comdirect.de/finanzwissen/wie-lange-kontoauszug-aufbewahren#muss-ich-kontoauszuege-aufbewahren, zuletzt zugegriffen am 08.08.2023.

Commerzbank (Hrsg.), Kontoauszüge wegwerfen oder aufbewahren? Das ist die Frage! https://www.commerzbank.de/portal/de/ratgeber/finanzen/aufbewahrungsfrist-Ihrer-kontoauszuege-das-muessen-sie-wissen.html, zuletzt zugegriffen am 08.08.2023.

Costanzo, Paolo, The risk-based approach to anti-money laundering and counter-terrorist financing in international and EU standards: what it is, what it entails, in Unger, Brigitte (Hrsg.), Research handbook on money laundering, 2013, S. 349.

Cremer, Wolfram, Aufenthaltsverbote und offene Drogenszene: Gesetzesvorrang, Parlamentsvorbehalt und grundgesetzliche Kompetenzordnung, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2001, 1218.

Culley, Alexander Conrad, The Third EU Money Laundering Directive: A Banker's Tightrope, in 13 Irish Journal of European Law (Irish J. of EU Law) 2006, 161.

Dahm, Joachim, Banken im Spannungsfeld zwischen Staat und Kunden, - Der Versuch einer Standortbestimmung am Beispiel der Weitergabe von Daten an staatliche Stellen -, in Wertpapier-Mitteilungen (WM) 1996, 1285.

Dahm, Joachim/Hamacher, Rolfjosef, Geldwäschebekämpfung und strafrechtliche Verfahrensgarantien, in Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 1995, 206.

Dalby, Jakob, Grundlagen der Strafverfolgung im Internet und in der Cloud, Möglichkeiten, Herausforderungen und Chancen, 2016, Wiesbaden, zugl. Diss. Münster, 2015.

Danne, Marius, Prävention und Repression im Sicherheitsrecht, 2022, Berlin, zugl. Diss., Univ. Gießen, 2022.

Degen, Andreas, Gesetzliche Mitwirkungspflichten der Kreditwirtschaft bei der Geldwäsche- und Terrorismusbekämpfung, Eine verfassungsrechtliche Betrachtung aus Sicht der Bankkunden am Beispiel des Konten-Screenings und des Kontendatenabrufverfahrens, Berlin 2009, zugl. Diss., Univ. Luxemburg, 2007.

Degenhart, Christoph, Entscheidung unter Unsicherheit – die Pandemiebeschlüsse des BVerfG, in Neue Juristische Wochenschrift (NJW) 2022, 123.

Deloitte, Final Study on the Application of the Anti-Money Laundering Directive, 2011, https://op.europa.eu/en/publication-detail/-/publication/8afd2daa-05cf-49aa-9c5b-f4eca0472a2e, zuletzt zugegriffen am 08.08.2023.

Dencker, Friedrich, Festschrift für Hanns Dünnebier zum 75. Geburtstag am 12. Juni 1982, Zur Zulässigkeit staatlich gesteuerter Deliktsbeteiligung, in Hanack, Ernst-Walter/Rieß, Peter/Wendisch, Günter (Hrsg.), Festschrift für Hanns Dünnebier zum 75. Geburtstag am 12. Juni 1982, 1982, S. 447.

Denninger, Erhard, Prävention und Freiheit, in Huster, Stefan/Rudolph, Karsten (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, 2008, S. 85.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2000, 2000.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit zum 31. Dezember 2005, 2005., https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/jahresbericht/BlnBDI-Jahresbericht-2005-Web.pdf, zuletzt zugegriffen am 08.08.2023

Der Europäische Datenschutzbeauftragte, Opinion 12/2021 on the anti-money laundering and countering the financing of terrorism (AML/CFT) package of legislative proposals, 22.09.2021, https://edps.europa.eu/system/files/2021-12/21-09-22_edps_opinion_aml_de.pdf, z zuletzt zugegriffen am 08.08.2023.

Der Europäische Datenschutzbeauftragte, Stellungnahme 1/2017: Stellungnahme des EDSB zu einem Vorschlag der Kommission zur Änderung der Richtlinie (EU) 2015/849 und der Richtlinie 2009/101/EG, Zugang zu Informationen über den wirtschaftlichen Eigentümer und Implikationen für den Datenschutz, 02.02.2017, https://edps.europa.eu/sites/default/files/publication/17-02-02_opinion_aml_de.pdf, zuletzt zugegriffen am 08.08.2023.

Der Europäische Datenschutzbeauftragte, Stellungnahme 5/2015, Zweite Stellungnahme zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität, 24.09.2015., https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_de.pdf, zuletzt zugegriffen am 08.08.2023.

Der Europäische Datenschutzbeauftragte, Stellungnahme 5/2020, zum Aktionsplan der Europäischen Kommission für eine umfassende Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, 23.07.2020, https://edps.europa.eu/sites/edp/files/publication/20-07-23_edps_aml_opinion_de.pdf, zuletzt zugegriffen am 08.08.2023.

Der Europäische Datenschutzbeauftragte, Stellungnahme des Europäischen Datenschutzbeauftragten über einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und Finanzierung des Terrorismus, und über einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Übermittlung von Angaben zum Auftraggeber bei Geldtransfers, 04. Juli 2013, https://edps.europa.eu/sites/default/files/publication/13-07-04_money_laundering_de.pdf., zuletzt zugegriffen am 08.08.2023.

Derleder, Peter/Knops, Kai-Oliver/Bamberger, Heinz Georg (Hrsg.), Deutsches und europäisches Bank- und Kapitalmarktrecht, Band I und II, 3. Aufl., 2017, Berlin..

Deutsch, Markus, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, 1992, Mannheim, Zugl. Diss., Univ. Mannheim 1991.

Deutsche Bank, Big Data, How it can become a differentiator, 2014, https://cib.db.com/docs_new/GTB_Big_Data_Whitepaper_(DB0324)_v2.pdf, zuletzt zugegriffen am 07.10.2021.

Deutsche Bank, Deutsche Bank and Google Cloud sign pioneering cloud and innovation partnership 4. Dezember, 2020, https://www.db.com/news/detail/20201204-deutsche-bank-and-google-cloud-sign-pioneering-cloud-and-innovation-partnership?language_id=1, zuletzt zugegriffen am 08.08.2023.

Deutsche Bundesbank, Monatsbericht Oktober 2002, https://www.bundesbank.de/de/publikationen/berichte/monatsberichte/monatsbericht-oktober-2002-692074, zugegriffen am 08.08.2023

Deutsche Bundesbank, Zahlungsverhalten in Deutschland 2017, Vierte Studie über die Verwendung von Bargeld und unbaren Zahlungsinstrumenten, 2017, https://www.bundesbank.de/resource/blob/634056/8e22ddcd69de76ff40078b31119704db/mL/zahlungsverhalten-in-deutschland-2017-data.pdf, zugegriffen am 08.08.2023*Deutsche Kreditwirtchaft*, Auslegungs- und Anwendungshinweise der DK zur Verhinderung von Geldwäsche, Terrorismusfinanzierung und „sonstigen strafbaren Handlungen", Februar 2014, https://bankenverband.de/media/uploads/2017/09/13/files-dk-hinweis estand_februar2014.pdf, zuletzt zugegriffen am 03.08.2021.

Diergarten, Achim/Fraulob, Ulrich (Hrsg.), Geldwäsche, Kommentar zum GwG und den einschlägigen Vorschriften des KWG, VAG, ZAG (zit. als *Bearbeiter* in Diergarten/Fraulob GWG).

Dietrich, Jan-Hendrik, § 6 Sicherheitsbegriffe des Sicherheitsrechts, in Dietrich, Jan-Hendrik/Fahrner, Matthias/Gazeas, Nikolaos ua. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, 2022, München

Dietrich, Jan-Hendrik/Eiffler, Sven-R. (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017, Stuttgart (zit. als. *Bearbeiter* in Hdb. Nachrichtendienste).

Dietrich, Jan-Hendrik/Fahrner, Matthias/Gazeas, Nikolaos ua. (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, 2022, München (zit. als *Bearbeiter* in Hdb. Sicherheits- und StaatsschutzR)

Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, Festgabe für Kurt Graulich zum 70. Geburtstag, Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik Bd. 3, 2019, Tübingen.

Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand/Graulich, Kurt ua. (Hrsg.), Nachrichtendienste im demokratischen Rechtsstaat, Kontrolle – Rechtsschutz – Kooperationen, Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik Bd. 1, 2018, Tübingen.

Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand/Graulich, Kurt ua. (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik Bd. 4, 2020, Tübingen.

Dietrich, Jan-Hendrik/Sule, Satish (Hrsg.), Intelligence law and policies in Europe, A handbook, 2019, München; Oxford; Baden-Baden.

Diller, Martin/Brauneisen, Kai/Hütten, Hilmar, CTAs und das neue Geldwäschegesetz –, Wie weit gehen Transparenz- und sonstige Pflichten?, in Neue Zeitschrift für Arbeitsrecht (NZA) 2017, 1512.

Dittrich, Kurt/Trinkhaus, Marc, Die gesetzlichen Regelungen der Geldwäsche und ihre Reform – eine Praxisanalyse, in Deutsches Steuerrecht (DStR) 1998, 342.

Doll, Simone, Strafprozessuale Konturierung des Kernbereichs privater Lebensgestaltung, Dissertation, 2021, Baden-Baden, zugl. Diss., Univ. Freiburg, 2021.

Dombek, Bernhard, Das Geldwäschegesetz aus der Sicht von Anwälten und Vertretern der anderer beratender Berufe, in Kahlert, Joachim (Hrsg.), Geldwäsche, Problemanalyse und Bekämpfungsstrategien; Dokumentation; eine Tagung der Friedrich-Ebert-Stiftung am 7. und 8. Oktober 1993 in Berlin, 1994, S. 103.

Dörr, Oliver/Grote, Rainer/Marauhn, Thilo (Hrsg.), EMRK/GG, Konkordanzkommentar zum europäischen und deutschen Grundrechtsschutz, 3. Aufl., 2022 (zit. als *Bearbeiter* in Konkordanzkommentar).

Dreier, Horst/Bauer, Hartmut (Hrsg.), Grundgesetz, Kommentar, 3. Aufl. (zit. als *Bearbeiter* in Dreier GG).

Droste, Bernadette, Handbuch des Verfassungsschutzrechts, 2007, Stuttgart.

Dürig, Günter, Der Grundrechtssatz von der Menschenwürde: Entwurf eines praktikablen Wertsystems der Grundrechte aus Art. 1 Abs. I in Verbindung mit Art. 19 Abs. II des Grundgesetzes, in Archiv des öffentlichen Rechts (AöR)1956, 117.

Ehmann, Eugen/Selmayr, Martin Datenschutz-Grundverordnung: DS-GVO, Kommentar, 2. Aufl., 2018 (zit. als *Bearbeiter* in Ehmann/Selmayr DSGVO).

Eifert, Martin, Informationelle Selbstbestimmung im Internet, Das BVerfG und die Online-Durchsuchungen, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2008, 521.

Eisenberg, Ulrich, Beweisrecht der StPO, Spezialkommentar, 10. Aufl. 2017, München.

Ellenberger, Jürgen/Bunte, Hermann-Josef (Hrsg.), Bankrechts-Handbuch, 6. Aufl., 2022, München.

Enders, Christoph, Die Menschenwürde in der Verfassungsordnung, Zur Dogmatik des Art. 1 GG, 1997, Tübingen, zugl. Univ. Habil., Freiburg, 1991.

Enders, Christoph, Sozialstaatlichkeit im Spannungsfeld von Eigenverantwortung und Fürsorge, in Enders, Christoph/Wiederin, Ewald/Pitschas, Rainer/Sodan, Helge/al, et (Hrsg.), Der Sozialstaat in Deutschland und Europa, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Jena vom 6. bis 9. Oktober 2004, 2005, S. 7.

Enders, Christoph/Wiederin, Ewald/Pitschas, Rainer ua. (Hrsg.), Der Sozialstaat in Deutschland und Europa, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Jena vom 6. bis 9. Oktober 2004, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer Bd. 2004, 2005.

Engelhart, Marc, Aiming for a New Architecture of Security Law, in Engelhart, Marc/ Roksandić Vidlička, Sunčana (Hrsg.), Dealing with terrorism, Empirical and normative challenges of fighting the Islamic State, 2019, S. 287.

Engelhart, Marc/ Kudlich, Hans/Vogel, Benjamin (Hrsg.), Digitalisierung, Globalisierung und Risikoprävention. Festschrift für Ulrich Sieber zum 70. Geburtstag. Teilbände 1 und 2, 2021, Berlin.

Engelhart, Marc/Roksandić Vidlička, Sunčana (Hrsg.), Dealing with terrorism, Empirical and normative challenges of fighting the Islamic State, Research series of the Max Planck Institute for Foreign and International Criminal Law S, Reports on research in criminal law volume 165, 2019.

Engels, Arne, Die 5. Geldwäscherichtlinie im Überblick: Änderungen der Richtlinie (EU) 2015/849 durch Richtlinie (EU) 2018/843, in Wertpapier-Mitteilungen (WM)2018, 2071.

Engelstätter, Tobias, Die Richtlinie zur Terrorismusbekämpfung (EU) 2017/541 –, Deutsches Staatsschutzstrafrecht unter Anpassungsdruck? in Zeitschrift für das gesamte Sicherheitsrecht (GSZ)2019, 95.

Engert, Marcus, 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, zugegriffen am 08.08.2023.

Epping, Volker; Hillgruber, Christian, Grundgesetz, Kommentar, 3. Aufl., 2020, München (zit. als *Bearbeiter* in Epping/Hillgruber BeckOK GG).

Erb, Volker/Schäfer, Jürgen (Hrsg.), Münchener Kommentar zum Strafgesetzbuch, 4. Aufl., 2021, München (zit. als *Bearbeiter* in MüKo StGB).

Erbs, Georg/Kohlhaas, Max, Strafrechtliche Nebengesetze, Stand: 236. EL, Mai 2021, München (zit. als *Bearbeiter* in Erbs/Kohlhaas).

Escher, Markus, Bankaufsichtsrechtliche Änderungen im KWG durch das Vierte Finanzmarktförderungsgesetz, in Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2002, 652.

Escher-Weingart, Christina/Stief, Markus, Geldwäschebekämpfung im Nichtfinanzbereich, Neues Geldwäschegesetz im Spannungsfeld zwischen europäischen Vorgaben und praktischen Erfordernissen, in Wertpapier-Mitteilungen (WM)2018, 693.

Eser, Albin/Goydke, Jürgen (Hrsg.), Strafverfahrensrecht in Theorie und Praxis, Festschrift für Lutz Meyer-Gossner zum 65. Geburtstag, 2001, München.

Eskens, Sarah, The Ever-Growing Complexity of the Data Retention Discussion in the EU: An In-Depth Review of La Quadrature du Net and Others and Privacy International - Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others [2020] ECLI:EU:C:2020:791; Case C-623/17 Privacy International [2020] ECLI:EU:C:2020:790 Case Notes, in European Data Protection Law Review 2022, 143.

Europäische Aufsichtsbehörden, Endgültige Leitlinien, Gemeinsame Leitlinien nach Artikel 25 der Verordnung (EU) 2015/847 zu den Maßnahmen, mit deren Hilfe Zahlungsdienstleister das Fehlen oder die Unvollständigkeit von Angaben zum Auftraggeber und zum Begünstigten feststellen können, und zu den empfohlenen Verfahren für die Bearbeitung eines Geldtransfers, bei dem die vorgeschriebenen Angaben fehlen, 16.01.2018, dt. Fassung., https://www.eba.europa.eu/regulation-and-policy/anti-money-laundering-and-e-money/guidelines-to-prevent-transfers-of-funds-can-be-abused-for-ml-and-tf, zuletzt zugegriffen am 08.08.2023.

Europäische Bankenaufsichtsbehörden, 23 January 2018 Opinion on the Use of Innovative Solutions by Credit and Financial Insitutions in the Customer Due Dilligence Process, 23.01.2018.

Europäische Bankenaufsichtsbehörden, Leitlinien nach Artikel 17 und Artikel 18 Absatz 4 der Richtlinie (EU) 2015/849 über Sorgfaltspflichten und die Faktoren, die Kredit- und Finanzinstitute bei der Bewertung des mit einzelnen Geschäftsbeziehungen und gelegentlichen Transaktionen verknüpften Risikos für Geldwäsche und Terrorismusfinanzierung berücksichtigen sollten („Die Leitlinien zu den Risikofaktoren für Geldwäsche und Terrorismusfinanzierung"), zur Aufhebung und Ersetzung der Leitlinien JC/2017/37, 01.03.2021 (dt. Fassung), https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/Guidelines%20on%20ML-TF%20risk%20factors%20%28revised%29%202021-02/Translations/1016923/Guidelines%20ML%20TF%20Risk%20Factors_DE.pdf, zuletzt zugegriffen am 08.08.2023.

Evers, Hans-Ulrich, Privatsphäre und Ämter für Verfassungsschutz, 1960, Berlin/Boston.

Fairfield, Joshua/Engel, Christoph, Privacy as a Public Good, in Miller, Russell A. (Hrsg.), Privacy and power, A transatlantic dialogue in the shadow of the NSA-Affair, 2017, S. 95.

Favarel-Garrigues/Godefroy, Thierry/Lascoumes, Pierre, Tools and securitization: the instrumentation of AML/CFT policies in French banks, in Svedberg Helgesson, Karin/Mörth, Ulrika (Hrsg.), Securitization, accountability and risk management, Transforming the public security domain, 2012, S. 88.

Feiler, Harald/Kröger, Jan-Wolfgang, Neue geldwäscherechtliche Pflichten: Einsichtnahme ins Transparenzregister und Unstimmigkeitsmeldung, Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie, in Corporate Compliance (CCZ) 2019, 262.

Fekonja, Benjamin, BaFin-Verlautbarungen, 2014, Baden-Baden, zugl. Diss., Univ. Augsburg, 2013.

Fiedler, Ingo/Krumma, Isabel/Zanconato, Ulrich Andreas/McCarthy, Killian J./Reh, Eva, Das Geldwäscherisiko verschiedener Glücksspielarten, 2017, Berlin.

Financial Action Task Force on Money Laundering, Annual Report 2001-2002, https://www.fatf-gafi.org/media/fatf/documents/reports/2001%202002%20ENG.pdf, zuletzt zugegriffen am 08.08.2023.

Financial Action Task Force on Money Laundering, FATF Annual Report 2019-2020, https://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF-annual-report-2019-2020.pdf., zuletzt zugegriffen am 08.08.2023

Financial Action Task Force on Money Laundering, IX Special Recommendations, 2001, konsolidierte Fassung Feb. 2008., https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Ixspecialrecommendations.html, zuletzt zugegriffen am 08.08.2023.

Financial Action Task Force on Money Laundering, High-Risk Jurisdictions subject to a Call for Action - February 2021, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2021.html, zuletzt zugegriffen am 08.08.2023.

Financial Action Task Force on Money Laundering, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation The FATF Recommendations, The FATF Recommendations, orig. Fassung Feb. 2012, https://www.bayerisches-innenministerium.de/assets/stmi/sus/inneresicherheit/fatf_recommendations_2-2012.pdf, zuletzt zugegriffen am 08.08.2023

Financial Action Task Force on Money Laundering, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation The FATF Recommendations, The FATF Recommendations, konsolidierte Fassung März 2022, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, zuletzt zugegriffen am 10.09.2021.

Financial Action Task Force on Money Laundering, Jurisdictions under Increased Monitoring - June 2021, https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2021.html, zuletzt zugegriffen am 08.08.2023.

Financial Action Task Force on Money Laundering, Report 1990-1991, 1991, https://www.fatf-gafi.org/countries/d-i/france/documents/fatfannualreport1990-1991.html, zuletzt zugegriffen am 23.06.2021.

Financial Action Task Force on Money Laundering, The Forty Recommendations of the Financial Task Force on Money Laundering, 1990, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf, zuletzt zugegriffen am 08.08.203.

Financial Action Task Force on Money Laundering, The Forty Recommendations, 2003, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf, zuletzt zugegriffen am 08.08-2023.

Financial Intelligence Unit, Berichterstattung, Anweisungen und Spezifikationen, Anlage 2 - XML-Schema Dokumentation, Stand 20.08.2018, https://www.zoll.de/DE/FIU/Software-goAML/Publikationen/publikationen_node.html, zuletzt zugegriffen am 08.08.2023.

Financial Intelligence Unit, goAML Web, https://goaml.fiu.bund.de/Home, zuletzt zugegriffen am 08.08.2023.

Financial Intelligence Unit, Jahresbericht 2011, Bundeskriminalamt (BKA), 2011.

Financial Intelligence Unit, Jahresbericht 2019, 2019.

Fincke, Martin, Zum Begriff des Beschuldigten und den Verdachtsgraden, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)1983, 918.

Findeisen, Michael, Bankgeheimnis und Verhinderung der Geldwäsche, in Hadding, Walther/Hopt, Klaus/Schimansky, Herbert (Hrsg.), Basel II: Folgen für Kreditinstitute und ihre Kunden. Bankgeheimnis und Bekämpfung von Geldwäsche, Bankrechtstag 2003, 2004, S. 95.

Findeisen, Michael, Deliktspezifische Strukturprävention gegen Geldwäsche im Finanzsektor, in Wertpapier-Mitteilungen (WM)1998, 2410.

Findeisen, Michael, Der Präventionsgedanke im Geldwäschegesetz, Anforderungen der Bankenaufsicht an die internen Sicherungsmaßnahmen der Kreditinstitute gem. § 14 Abs. 2 GwG zur Bekämpfung der Geldwäsche, in Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 1997, 121.

Fischer, Thomas, Strafgesetzbuch, mit Nebengesetzen, Kommentar, 69. Aufl. 2021, München (zit. als *Bearbeiter* in Fischer StGB).

Flores, Denys A./Angelopoulou, Olga/Self, Richard J., An Anti-Money Laundering Methodology: Financial Regulations, Information Security and Digital Forensics Working Together, in 3 Journal of Internet Services and Information Security (J. of Internet Services & Information Security) 2013, 101.

Florian, Ulrich, Anmerkung zu BVerfG, Beschluß vom 22. 3. 2005 - 1 BvR 2357/04, in Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2005, 202.

Flynn, Cathal, Data Retention, the Separation of Power in the EU and the Right to Privacy: A Critical Analysis of the Legal Validity of the 2006 Directive on the Retention of Data, in University College Dublin Law Review 2008, 1.

Frantangelo, Pierpaolo, The CDD Obligations Following a Risk- Based Approach, in Siclari, Domenico (Hrsg.), The New Anti-Money Laundering Law, 2016, S. 11.

Fremuth, Michael Lysander, Wächst zusammen, was zusammengehört? Das Trennungsgebot zwischen Polizeibehörden und Nachrichtendiensten im Lichte der Reform der deutschen Sicherheitsarchitektur, in Archiv des öffentlichen Rechts (AöR) 2014, 32.

Frey, Tobias/Pelz, Christian (Hrsg.), Beckscher' Online-Kommentar GwG, 14. Edition, Stand 01.06.2023 (zit. als *Bearbeiter* in BeckOK GwG).

Friedewald, Michael/Burgess, J. Peter/Čas, Jonathan ua. (Hrsg.), Surveillance, privacy and security, Citizens' perspectives, PRIO new security studies, 2017, London.

Friedewald, Michael/Lamla, Jörn/Roßnagel, Alexander (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, Research, 2017, Wiesbaden.

Friedrich, Dirk, Die Verpflichtung privater Telekommunikationsunternehmen, die staatliche Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, 2001, Aachen, zugl.: Diss., Univ. Regensburg, 2000/2001.

Frister, Helmut, Der Anspruch des Beschuldigten auf Mitteilung der Beschuldigung aus Art. 6 Abs. 3 lit. a EMRK, in Strafverteidiger (StV) 1998, 159

Frister, Helmut, Kapitel F. Polizeihandeln im Strafverfahren, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., 2021, München.

Frowein, Jochen Abraham./Peukert, Wolfgang (Hrsg.), Europäische Menschenrechtskonvention, EMRK-Kommentar, 3. Aufl., 2009, Kehl (zit. als *Bearbeiter* in Frowein/Peukert EMRK, 3. Aufl. 2009).

Fülbier, Andreas, GwG, Kommentar zum Geldwäschegesetz, 5. Aufl., 2006, Köln (zit. als *Bearbeiter* in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006).

Fülbier, Andreas/ Aepfelbach, Rolf R, Das Geldwäschegesetz, Eine einführende Kommentierung, 2. Aufl., 1994, Köln (zit. als *Bearbeiter* in Fülbier/Aepfelbach GWG, 2. Aufl. 1994).

Fülbier, Andreas/ Aepfelbach, Rolf R, Das Geldwäschegesetz, Eine einführende Kommentierung, 1. Aufl., 1994, Köln (zit. als *Bearbeiter* in Fülbier/Aepfelbach GWG, 1. Aufl. 1993).

Gaede, Karsten, Fairness als Teilhabe, Das Recht auf konkrete und wirksame Teilhabe durch Verteidigung gemäss Art. 6 EMRK ; Ein Beitrag zur Dogmatik des fairen Verfahrens in europäischen Strafverfahren und zur wirksamkeitsverpflichteten Konventionsauslegung unter besonderer Berücksichtigung des Rechts auf Verteidigungsbeistand, 2010, Berlin, zugl. Diss., Univ. Zürich, 2005.

Gallant, M. Michelle, AML: maintaining the balance between controlling serious crime and human rights, in Rider, Barry Alexander K. (Hrsg.), Research handbook on international financial crime, 2015, S. 532.

Gallus, Nico/Zeyher, Lukas, § 95 a StPO als „Rettungsanker" für die heimliche Beschlagnahme von E-Mails beim Provider?, in Neue Zeitschrift für Strafrecht (NStZ) 2022, 462.

Gander, Hans-Helmuth/Perron, Walter/Poscher, Ralf ua. (Hrsg.), Resilienz in der offenen Gesellschaft, Symposium des Centre for Science and Security, 2012, Baden-Baden.

Gärditz, Klaus Ferdinand, Kapitel VI § 1 Auskunftsersuchen gegenüber der Privatwirtschaft, in Dietrich, Jan-Hendrik/Eiffler, Sven-R. (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017.

Gärditz, Klaus Ferdinand, Anmerkung zu BVerfG, 24.4.2013 — 1 BvR 1215/07. Antiterrordatei und nachrichtendienstrechtliches Trennungsgebot, in Juristenzeitung (JZ) 2013, 633.

Gärditz, Klaus Ferdinand, Bundesnachrichtendienst semper reformanda, in Deutsches Verwaltungsblatt (DVBl) 2021, 905.

Gärditz, Klaus Ferdinand, Die Rechtsbindung des Bundesnachrichtendienstes bei Auslandstätigkeiten, in Die Verwaltung 2015, 463.

Gärditz, Klaus Ferdinand, Innere Sicherheit, in *Stern, Klaus/Sodan, Helge/Möstl, Markus* (Hrsg.), Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl., 2022, München, § 22.

Gärditz, Klaus Ferdinand, Sicherheitsrecht als Perspektive, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2017, 1.

Gärditz, Klaus Ferdinand, Strategische Fernmeldebeschränkung und Netzknotenüberwachung für den Verfassungsschutz? in Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, Festgabe für Kurt Graulich zum 70. Geburtstag, 2019, S. 153.

Gassner, Ulrich, Parlamentsvprbehalt und Bestimmtheitsgrundsatz, in Die Öffentliche Verwaltung (DÖV) 1996, 18.

Gazeas, Nikolaos, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, Berlin, zugl. Diss., Univ. Köln, 2013/2014.

Gehra, Bernhard/Gittfried, Norbert/Lienke, Georg ua. (Hrsg.), Prävention von Geldwäsche und Terrorismusfinanzierung, Praktische Umsetzung der aufsichtsrechtlichen Anforderungen durch Banken, 2. Aufl., 2020, Heidelberg.

Gellert, Raphaël/Gutwirth, Serge, The legal construction of privacy and data protection, in 29 Computer Law & Security Review 2013, 522.

Gemmin, Christian, Zur Institutionalisierung einer Überwachungsgesamtrechnung, in Die Öffentliche Verwaltung (DÖV) 2022, 789.

Geppert, Martin/Schütz, Raimund (Hrsg,), Beck'scher TKG-Kommentar, 4. Aufl., 2013, München (zit. als *Bearbeiter* in Geppert/Schütz Beck'scher TKG Kommentar).

Gercke, Marco, Die Entwicklung des Internetstrafrechts 2015/2016, in Zeitschrift für Urheber- und Medienrecht (ZUM) 2016, 825.

Gerhard, Torsten, Gutachterliche Stellungnahme zu Zulässigkeit und Möglichkeiten der Ausgestaltung einer allgemeinen Impfpflicht gegen COVID19, im Auftrag des Staatsministeriums Baden-Württemberg, Oppenländer, 2022, https://www.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/211212_Gutachterliche_Stellungnahme_zu_Impfpflichten_Korrigierte_Fassung_Seite67.pdf?msclkid=9d8980abb57b11eca90b8588550ef1d5, zuletzt zugegriffen am 08.08.2023

Gerhardt, Jens, Corona-Impfpflicht zur Herstellung einer Herdenimmunität?, in Arbeitsschutz in Recht und Praxis (ARP) 2021, 149.

Germann, Michael, Gefahrenabwehr und Strafverfolgung im Internet, 2000, Berlin, zugl. Diss., Univ. Erlangen, Nürnberg, 1999.

Gersdorf, Hubertus, Hate Speech in sozialen Netzwerken, Verfassungswidrigkeit des NetzDG-Entwurfs und grundrechtliche Einordnung der Anbieter sozialer Netzwerke, in Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR) 2017, 439.

Gersdorf, Hubertus/Paal, Boris P. (Hrsg.), Informations- und Medienrecht, Kommentar, 2. Aufl., 2021 (zit. als *Bearbeiter* in BeckOK Informations-/MedienR).

Gerson, Oliver Harry, Wunsch und Wirklichkeit einer sog. „Überwachungsgesamtrechnung, Rechtstheoretische Grundlagen eines innovativen Evaluationsinstruments in der Sicherheitsgesetzgebung, in Kriminalpolitische Zeitschrift (KriPoZ) 2022, 404.

Geurts, Matthias/Koch, Christian/Schebesta, Michael/Weber, Ahrend, Bankgeheimnis und Bankauskunft in der Praxis, 6. Aufl. 2000, Köln.

Gitter, Rotraud/Schnabel, Christoph, Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht, in Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR) 2007, 411.

Glaab, Sebastian/Neu, Jasmin/Scherp, Dirk, Umsetzung der 5. EU-Geldwäscherichtlinie –, Was kommt auf die Verpflichteten zu? in Betriebs-Berater (BB) 2020, 322.

Gnüchtel, Ralf, Das Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen auf Grundlage der dritten Evaluation, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 13.

Goerlich, Helmut, Grundrechte als Verfahrensgarantien, Ein Beitrag zum Verständnis des Grundgesetzes für d. Bundesrepublik Deutschland, 1981, Baden-Baden, zugl. Univ. Habil., 1981, Hannover.

Götz, Frank, § 85 Innere Sicherheit, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. VIII, 3. Aufl., 2006, Heidelberg, § 85.

Gola, Peter/Heckmann, Dirk, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2022 (zit. als *Bearbeiter* in Gola/Heckmann DSGVO/BDSG).

Golla, Sebastian, Datenschutzrechtliche Schattengewächse in den Ländern, Herausforderungen bei der Umsetzung der JI-Richtlinie für die Polizei, in Kriminalpolitische Zeitschrift (KriPoZ) 2019, 238.

Golla, Sebastian/Skobel, Eva, „Sie haben doch nichts zu verbergen?", Zur Möglichkeit einer Einwilligung in die Datenverarbeitung im Geltungsbereich der Richtlinie (EU) 2016/680, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ)2019, 140.

González Fuster, Gloria, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Dissertation, Vrije Universiteit Brussel (VUB), 2013.

González Fuster, Gloria/Gutwirth, Serge, Opening up personal data protection: A conceptual controversy, in 29 Computer Law & Security Review 2013, 531.

Göres, Ulrich, Zur Rechtmäßigkeit des automatisierten Abrufs von Kontoinformationen, Ein weiterer Schritt zum gläsernen Bankkunden, in Neue Juristische Wochenschrift (NJW) 2005, 253.

Górski, Maciej, Freedom of Communication and Data Retention in Judgments of the European Court of Human Rights, in Zubik, Marek/Podkowik, Jan/Rybski, Robert (Hrsg.), European Constitutional Courts towards Data Retention Laws, 2021, S. 19.

Grabenwarter, Christoph, Europäischer Rechtsprechungsdialog in Grundrechtsfragen – am Beispiel der Vorratsdatenspeicherung, in Stumpf, Cordula/Kainer, Friedemann/Baldus, Christian (Hrsg.), Privatrecht, Wirtschaftsrecht, Verfassungsrecht, Privatinitiative und Gemeinwohlhorizonte in der europäischen Integration, 2015, S. 1386.

Grabenwarter, Christoph/Breuer, Marten/Bungenberg, Marc ua. (Hrsg.), Europäischer Grundrechteschutz, 2. Aufl., Enzyklopädie Europarecht Band 2, 2022., Baden-Baden; Zürich; St. Gallen; Wien

Grabenwarter, Christoph/Pabel, Katharina, Europäische Menschenrechtskonvention, Ein Studienbuch, 7. Aufl. 2021, München.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union, 77. Aufl., 2022, München (zit. als *Bearbeiter* in Grabitz/Hilf/Nettesheim Recht der EU).

Grabowska-Moroz, Barbara, Data Retention in the European Union, in Zubik, Marek/Podkowik, Jan/Rybski, Robert (Hrsg.), European Constitutional Courts towards Data Retention Laws, 2021, S. 3.

Graf, Jürgen (Hrsg.), Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Stand: 47. Edition, 01.04.2023 (zit. als *Bearbeiter* in BeckOK StPO).

Grafe, Adina, Die Auskunftserteilung über Verkehrsdaten nach §§ 100g, 100h StPO, Staatliche Kontrolle unter Mitwirkung Privater, 2008, Freiburg, zugl. Diss., Univ. Freiburg 2008.

Granger, M. P./Irion, Kristina, The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection, in 39 European Law Review (Eur. Law Rev.) 2014, 834.

Graulich, Kurt, Befugnisse und Kontrolle des Bundesnachrichtendienstes bei der Fernmeldeaufklärung, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ)2021, 121.

Graulich, Kurt, Bestandsdatenauskunft II, Doppeltüren-Modell und Verhältnismäßigkeitsgrundsatz, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) - Beilage 2020, 47.

Graulich Kurt, Kapitel E. Das Handeln von Polizei- und Ordnungsbehörden zur Gefahrenabwehr, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., 2021, München.

Graulich, Kurt, Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation, Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisbeschlusses BND-26. Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisbeschlusses BND-26, 1. UA des 18. Deutschen Bundestags, 23.10.2015, https://www.bundesregierung.de/resource/blob/974430/386718/35c213a9c86b6de99ef60e78fd3d7d91/2015-10-30-bericht-svp-data.pdf?download=1, zuletzt zugegriffen am 08.08.2023

Graulich, Kurt, Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und internationale Datenkooperation, in Kriminalpolitische Zeitschrift (KriPoZ) 2017, 43.

Graulich, Kurt, Sicherheitsrecht, in Deutsches Verwaltungsblatt (DVBl) 2013, 1210.

Greco, Luís, Strafprozesstheorie und materielle Rechtskraft, Grundlagen und Dogmatik des Tatbegriffs, des Strafklageverbrauchs und der Wiederaufnahme im Strafverfahrensrecht, 2015, Berlin, zugl.: Univ., Habil., München 2014/2015.

Gregor, Andreas, Verfassungsmäßigkeit des automatisierten Abrufs von Kontostammdaten, in Entscheidungen zum Wirtschaftsrecht (EWiR) 2008, 189.

Greve, Holger, Das neue Bundesdatenschutzgesetz, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2017, 737.

Griebel, Thorsten, Der Makler als „Hilfssheriff" im Kampf gegen Geldwäsche und Terrorismusfinanzierung – Das neue „Geldwäschepräventions-Optimierungsgesetz", Ein aus dem Wesen der Makelei heraus begründeter Widerspruch, in Neue Zeitschrift für Miet- und Wohnungsrecht (NZM) 2012, 482.

Grimm, Dieter (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, Die Verwaltung. Beiheft 4, 2001, Berlin

Grimm, Dieter, in Hassemer, Winfried/Starzacher, Karl (Hrsg.), Organisierte Kriminalität - geschützt vom Datenschutz?, 1993, S. 28.

Groß, Thomas, Terrorbekämpfung und Grundrechte, Zur Operationalisierung des Verhältnismäßigkeitsgrundsatzes, in Kritische Justiz 2002, 1.

Guckelberger, Anette, Veröffentlichung der Leistungsempfänger von EU-Subventionen und unionsgrundrechtlicher Datenschutz, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW)2011, 126.

Gürkan, David, Der risiipikoorientierte Ansatz zur Geldwäscheprävention und seine Folgen, Geldwäschegesetz und Kreditwesengesetz im Lichte von Rechtsdogmatik und Rechtsökonomie, 2019.

Gurlit, Elke, Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, in Neue Juristische Wochenschrift (NJW) 2010, 1035.

Gusy, Christoph, Das Trennungsprinzip zwischen Informationen von Nachrichtendiensten und Polizei, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ)2021, 141.

Gusy, Christoph, Die Rechtstellung der Nachrichtendienste, in Juristische Ausbildung (JURA)1986, 296.

Gusy, Christoph, Die Verfassungsbeschwerde, in van Ooyen, Robert Chr./Möllers, Martin H. W. (Hrsg.), Handbuch Bundesverfassungsgericht im politischen System, 2015, S. 333.

Gusy, Christoph, Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, in Weber-Dürler, Béatrice/Kokott, Juliane/Vesting, Thomas (Hrsg.), Die Staatsrechtslehre und die Veränderung ihres Gegenstandes, Konsequenzen von Europäisierung und Internationalisierung ; Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Hamburg vom 1. bis 4. Oktober 2003, 2004, S. 153.

Gusy, Christoph, Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang?, in Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV) 2000, 52.

Gusy, Christoph, IV § 1 Organisation und Aufbau der deutsche Nachrichtendienste, in Dietrich, Jan-Hendrik/Eiffler, Sven-R. (Hrsg.), Handbuch des Rechts der Nachrichtendienste, 2017.

Gusy, Christoph, Mehr als der Polizei erlaubt ist?, Die Nachrichtendienste im Anti-Terrorkampf, in Huster, Stefan/Rudolph, Karsten (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, 2008, S. 120.

Gusy, Christoph, Organisierte Kriminalität zwischen Polizei und Verfassungsschutz., in Goltdammer's Archiv für Strafrecht 1999, 319.

Gusy, Christoph, Polizeiliche Befragung am Beispiel des § 9 NRWPolG, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 1991, 614.

Gusy, Christoph, Sicherheitsrecht als Rechtsgebiet? Ein Streit um Worte oder um die Sache und wenn ja, welche Sache?, in Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, Festgabe für Kurt Graulich zum 70. Geburtstag, 2019, S. 9.

Gusy, Christoph/Eichenhofer, Johannes, in, Beck'scher Online-Kommentar Datenschutzrecht, 34. Edition, Stand 01.11.2020, München.

Haas, Evelyn, Abweichende Meinung der Richterin Haas zum Beschluss des Ersten Senats vom 4. April 2006 - 1 BvR 518/02-, in abw. Meinung zu BVErfGE 115, 320.

Habersack, Matthias/Mayer, Christian, § 14 Die überschießende Umsetzung von Richtlinien, in Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021.

Hadding, Walther/Hopt, Klaus/Schimansky, Herbert (Hrsg.), Basel II: Folgen für Kreditinstitute und ihre Kunden. Bankgeheimnis und Bekämpfung von Geldwäsche, Bankrechtstag 2003, Schriftenreihe der Bankrechtlichen Vereinigung Bd. 22, 2004.

Hamacher, Rolfjosef, Der heimliche Kontenzugriff und das Grundgesetz. Finanzbehörden als Geheimdienst?, in Deutsches Steuerrecht (DStR) 2006, 633.

Hamacher, Rolfjosef, Rasterfahndung in Banken? in Die Bank 09/2006, 40.

Hamm, Rainer/Leipold, Klaus (Hrsg.), Beck'sches Formularbuch für den Strafverteidiger, 6. Aufl., München, 2018.

Hanack, Ernst-Walter/Rieß, Peter/Wendisch, Günter (Hrsg.), Festschrift für Hanns Dünnebier zum 75. Geburtstag am 12. Juni 1982, 1982, Berlin.

Hancox, Emily, The meaning of "implementing" EU law under Article 51(1) of the Charter: Åkerberg Fransson, in Common Market Law Review 51 (Common Market Law Rev.) 2013, 1411.

Hannich, Rolf, (Hrsg.) Karlsruher Kommentar zur Strafprozessordnung, 8. Aufl. 2019, München (zit. als *Bearbeiter* in KK-StPO).

Hartmann, Moritz, Internationale Finanzströme und Geldwäsche. Eine spiegelbildliche Phänomenologie sicherheitsarchitektonischer Legislation, in Kritische Justiz (KJ) 2007, 2.

Hassemer, Winfried, Das Geldwäschegesetz und der Datenschutz, in Kahlert, Joachim (Hrsg.), Geldwäsche, Problemanalyse und Bekämpfungsstrategien ; Dokumentation ; eine Tagung der Friedrich-Ebert-Stiftung am 7. und 8. Oktober 1993 in Berlin, 1994, S. 123.

Hassemer, Winfried, Sicherheit durch Strafrecht, in 30. Strafverteidigertag (Hrsg.), Wieviel Sicherheit braucht die Freiheit, 30. Strafverteidigertag, Frankfurt/Main, 24.-26.3.2006, 2007, S. 9.

Hassemer, Winfried/Starzacher, Karl (Hrsg.), Organisierte Kriminalität - geschützt vom Datenschutz? Forum Datenschutz Bd. 2, 1993, Baden-Baden.

Hauschka, Christoph E./Moosmayer, Klaus/Lösler, Thomas (Hrsg.), Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, 3. Aufl., 2016, München

Hauser, Markus, Das IT-Grundrecht, Schnittfelder und Auswirkungen, 2015, Berlin, zugl.: Diss., Univ. Hamburg, 2014.

Hawickhorst, Katrin, § 129a StGB - ein feindstrafrechtlicher Irrweg zur Terrorismusbekämpfung, Kritische Analyse einer prozessualen Schlüsselnorm im materiellen Recht, 2011, Berlin, zugl.: Diss., Univ. Berlin, 2011.

Heckmann, Dirk, Polizeiliche Datenerhebung und -verarbeitung, in Verwaltungsblätter für Baden-Württemberg (VBlBW) 1992, 164.

Hefendehl, Roland, Die neue Ermittlungsgeneralklausel der §§ 161, 163 StPO, Segen oder Fluch? in Strafverteidiger (StV) 2001, 700.

Heinemann, Marcus, Grundrechtlicher Schutz informationstechnischer Systeme, Unter besonderer Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2015, Berlin, Zugl.: Diss., Univ. Passau 2014.

Hellwig, Hans-Jürgen, Die neue Geldwäscherichtlinie, in Anwaltsblatt (AnwBl) 2002, 144.

Henn, Martin/Kuballa, Dirk-Peter, Steuerliche Einordnung und Anerkennung von Bankkontoauszügen und Kontoumsatzdaten, in Der Betrieb (DB) 2016, 1900.

Herdegen, Matthias/Masing, Johannes/Poscher, Ralf/Gärditz, Ferdinand (Hrsg.), Handbuch des Verfassungsrechts, 2021, München

Herresthal, Carsten/Brink, Ulrich, Münchener Kommentar zum Handelsgesetzbuch Bd. 6: Bankvertragsrecht: Recht des Zahlungsverkehrs, Kapitalmarkt- und Wertpapiergeschäft, Ottawa Übereinkommen über Internationales Factoring, 2019, München (zit. als *Bearbeiter* in MüKo HGB Bd. VI BankvertragsR).

Hert, Paul de/Papakonstantinou, Vagelis, The New Police and Criminal Justice Data Protection Directive: A First Analysis, 7 in New Journal of European Criminal Law (New J. Europ. Crim. Law) 2016, 7.

Hert, Paul de/Papakonstantinou, Vagelis, The PNR Agreement and Transatlantic anti-terrorism Cooperation: No firm human rights framework on either side of the Atlantic, in 46 Common Market Law Review (Common Market Law Rev) 2009, 885.

Herzog, Felix (Hrsg.), Geldwäschegesetz, (GwG), Kommentar, 2. Aufl., 2014, München (zit. als *Bearbeiter* in Herzog GwG, 2. Aufl. 2014).

Herzog, Felix (Hrsg.) Geldwäschegesetz (GwG), Kommentar, 4. Aufl., 2020 (zit. als *Bearbeiter* in Herzog GwG).

Herzog, Felix, Das Bankgeheimnis – eine Schranke staatlicher und staatlich veranlasster Ermittlungen?, in Hadding, Walther/Hopt, Klaus/Schimansky, Herbert (Hrsg.), Basel II: Folgen für Kreditinstitute und ihre Kunden. Bankgeheimnis und Bekämpfung von Geldwäsche, Bankrechtstag 2003, 2004, S. 47.

Herzog, Felix, Der Banker als Fahnder?, Von der Verdachtsanzeige zur systematischen Verdachtsgewinnung - Entwicklungstendenzen der Geldwäschebekämpfung -, in Wertpapier-Mitteilungen (WM)1996, 1753.

Herzog, Felix, Finanzermittlungen vor der Verdachtsschwelle, in Hirsch, Hans Joachim (Hrsg.), Festschrift für Günter Kohlmann zum 70. Geburtstag, 2003, S. 427.

Herzog, Felix, Geldwäschebekämpfung - quo vadis?, in Wertpapier-Mitteilungen (WM) 1999, 1905.

Herzog, Felix (Hrsg.), Geldwäschegesetz (GwG), Kommentar, 3. Aufl., 2018, München (zit. als *Bearbeiter* in Herzog GwG, 3. Aufl. 2018).

Herzog, Felix/Christmann, Rainer, Geldwäsche und „Bekämpfungsgesetzgebung", Ein Plädoyer für rechtsstaatliche Sensibilität, in Wertpapier-Mitteilungen (WM) 2003, 6.

Herzog, Felix/Hoch, Temba, Politisch exponierte Personen unter Beobachtung, Konsequenzen aus der 3. EU-Geldwäscherichtlinie und damit verbundene Fragen des Datenschutzes, in Wertpapier-Mitteilungen (WM) 2007, 1997.

Heß, Reinhold, Grundrechtskonkurrenzen, 2000, Berlin, zugl. Diss., Univ. Marburg, 1999.

Hesse, Konrad, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Aufl. 1995.

Hetzer, Wolfgang, Deutsche Umsetzung neuer europäischer Vorgaben zur Bekämpfung der Geldwäsche und der Terrorismusfinanzierung, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW)2008, 560.

Hetzer, Wolfgang, Geldwäsche und Terrorismus, in Zeitschrift für Rechtspolitik (ZRP)2002, 407.

Hilgendorf, Eric, Die mißbrauchte Menschenwürde, Probleme des Menschenwürdetopos am Beispiel der bioethischen Diskussion, in Jahrbuch für Recht und Ethik (JRE) 1999, 137.

Hilgendorf, Eric, Grundfragen strafrechtlicher Compliance am Beispiel der strafrechtlichen Produkthaftung für Teilautonome technische Systeme, in Rotsch, Thomas (Hrsg.), Criminal Compliance vor den Aufgaben der Zukunft, 2013, S. 19.

Hilger, Hans, Zum Strafverfahrensrechtsänderungsgesetz 1999 (StVÄG 1999) - 1. Teil 1, in Neue Zeitschrift für Strafrecht (NStZ)2000, 561.

Hillgruber, Christian, § 210 Grundrechtsschranken, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. IX, 3. Aufl., 2011, Heidelberg.

Hirsch, Burkhard, Auf dem Weg in den Überwachungsstaat, in Huster, Stefan/Rudolph, Karsten (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, 2008, S. 164.

Hirsch, Conrad, Auskünfte durch Kreditinstitute im straf- und steuerstrafrechtlichen Ermittlungsverfahren, 1991, Konstanz, zugl.: Diss., Univ. Konstanz, 1991 u.d.T.: Das Bankgeheimnis im Strafverfahren, 1991.

Hirsch, Hans Joachim (Hrsg.), Festschrift für Günter Kohlmann zum 70. Geburtstag, 2003, Köln.

Hobbes, Thomas, Grundzüge der Philosophie, Edition Holzinger, 3. Aufl. 2014, Berlin, orig. 1642, London.

Höche, Thorsten, Der Entwurf einer dritten EU-Richtlinie zur Verhinderung der Nutzung des Finanzsystems zu Zwecken der Geldwäsche und der Finanzierung des Terrorismus, in Wertpapier-Mitteilungen (WM) 2005, 8.

Höche, Thorsten/Rößler, Gernot, Das Gesetz zur Optimierung der Geldwäscheprävention und die Kreditwirtschaft, in Wertpapier-Mitteilungen (WM) 2012, 1505.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht, Rechtsfragen des elektronischen Geschäftsverkehrs, 2020, München.

Hoffmann, Jan Martin, Unionsgrundrechte als verfassungsrechtlicher Prüfungsmaßstab, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2020, 33.

Hoffmann-Riem, Wolfgang (Hrsg.), Innovationen im Recht, 2016, Tübingen

Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, 2010, Tübingen.

Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, in Juristenzeitung (JZ) 2008, 1009.

Hoffmann-Riem, Wolfgang, Grundrechtsanwendung unter Rationalitätsanspruch, Eine Erwiderung auf Kahls Kritik an neueren Ansätzen in der Grundrechtsdogmatik, in Der Staat 2004, 203.

Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft., Auf dem Wege zu einem neuen Konzept des Datenschutzes, in Archiv des öffentlichen Rechts (AöR)1998, 513.

Holznagel, Bernd, Das Compliance-System des Entwurfs des Netzwerkdurchsetzungsgesetzes, in Zeitschrift für Urheber- und Medienrecht (ZUM) 2017, 615.

Honer, Matthias, Die Grundrechte der EU-Grundrechtecharta, in Juristische Ausbildung (JURA) 2021, 219.

Hong, Mathias, Der Menschenwürdegehalt der Grundrechte, Grundfragen, Entstehung und Rechtsprechung, 2019, Tübingen, zugl. Univ. Habil., Freiburg, 2016.

Hong, Matthias, Grundrechte als Instrumente der Risikoallokation, in Scharrer, Jörg/Dalibor, Marcel/Fröhlich, Katja/Debus, Alfred G. (Hrsg.), Risiko im Recht - Recht im Risiko, 50. Assistententagung Öffentliches Recht; Tagung der wissenschaftlichen Mitarbeiterinnen und Mitarbeiter, wissenschaftlichen Assistentinnen und Assistenten, 2011, S. 111.

Hoppe, Corinne, Vorfeldermittlungen im Spannungsverhältnis von Rechtsstaat und der Bekämpfung organisierter Kriminalität, 1999, Frankfurt (Main), zugl.: Diss., Univ. Hamburg, 1998.

Horn, Hans-Detlef, Die grundrechtsunmittelbare Verwaltung, Zur Dogmatik des Verhältnisses zwischen Gesetz, Verwaltung und Individuum unter dem Grundgesetz, 1999, Tübingen, Zugl.: Univ. Habil., Bayreuth, 1998.

Hornung, Gerrit, Die Festplatte als „Wohnung"? in Juristenzeitung (JZ) 2007, 828.

Hornung, Gerrit, Die kumulative Wirkung von Überwachungsmaßnahmen: Eine Herausforderung an die Evaluierung von Sicherheitsgesetzen, in Albers, Marion/Weinzierl, Ruth (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik, Beiträge zur rechtsstaatsorientierten Evaluierung von Sicherheitsgesetzen, 2010, S. 65.

Hornung, Gerrit/Schindler, Stephan/Schneider, Jana, Die Europäisierung des strafverfahrensrechtlichen Datenschutzes Zum Anwendungsbereich der neuen Datenschutz-Richtlinie für Polizei und Justiz, in Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) 2018, 566.

Hornung, Gerrit/Schnabel, Christoph, Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung -, in Deutsches Verwaltungsblatt (DVBl) 2010, 824.

Huber, Bertold, „Massenüberwachung" vor dem EGMR, Die Entscheidungen in den Rechtssachen Big Brother Watch und Rättvisa, in Neue Zeitschrift für Verwaltungsrecht - Beilage (NVwZ-Beilage) 2021, 3.

Huber, Bertold, Die strategische Rasterfahndung des Bundesnachrichtendienstes –, Eingriffsbefugnisse und Regelungsdefizite, in Neue Juristische Wochenschrift (NJW) 2013, 2572.

Hund, Horst, Überwachungsstaat auf dem Vormarsch - Rechtsstaat auf dem Rückzug?, in Neue Juristische Wochenschrift (NJW) 1992, 2118.

Huster, Stefan/Kingreen, Thorsten (Hrsg.), Handbuch Infektionsschutzrecht, 2. Aufl., 2022, München.

Huster, Stefan/Rudolph, Karsten (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, 2008, Frankfurt (Main).

Ibel, Fabian, EGMR: Big Brother Watch u. a. vs. Vereinigtes Königreich, in ZD-Aktuell 2021, 5246.

IBM, Fighting financial crime with AI, How cognitive solutions are changing the way institutions manage AML compliance, fraud and conduct surveillance 2019, https://www.ibm.com/downloads/cas/WKLQKD3W, zuletzt zugegriffen am 04.04.2022.

Insitut für Gesetzesfolgenabschätzung und Evaluation, Ziekow, Jan/Piesker, Axel/Vallée, Tim (Hrsg.), Evaluation nach Artikel 5 Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen vom 3. Dezember 2015, Bundesministeriums des Innern, für Bau und Heimat, Juli 2018, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/sonstige-downloads/anpassung-verfassungsschutzrecht/abschlussbericht.pdf?__blob=publicationFile, zuletzt zugregriffen am 08.08.2023..

Ioannides, Emmanuel, Fundamental Principles of EU Law Against Money Laundering, 2016, London.

Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., 2003, Heidelberg

Jäger, Torsten, Überschießende Richtlinienumsetzung im Privatrecht, 2006, Baden-Baden, zugl. Diss., Univ. Augsburg, 2006.

Jahn, Joachim, Verschärfte Finanzkontrollen nach Terroranschlägen, in Zeitschrift für Rechtspolitik (ZRP)2002, 109.

Jakobs, Günther, Terroristen als Personen im Recht?, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2006, 839.

Jansen, Frank, Zulässigkeit und Grenzen des schriftlichen staatsanwaltlichen Erkenntnisgewinns am Beispiel des Bankauskunftsersuchens und der Provideranfrage, Zugleich ein Beitrag zum Bankgeheimnis und Fernmeldegeheimnis als Ermittlungsschranken, Zugl.: Konstanz, Univ., Diss., 2009, 2010.

Jarass, Hans D., Charta der Grundrechte der Europäischen Union. Unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK, Kommentar, 4. Aufl., 2021 (zit. als *Bearbeiter* in Jarass EU-GRC).

Jasserand, Catherine, Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?, in 34 Computer Law & Security Review 2018, 154.

Jestaedt, Matthias, Verhältnismäßigkeit als Verhaltensmaß, Gesetzgebung angesichts der Vielfalt der Rationalitäten und des Eigenwert des politischen Kompromisses, in Jestaedt, Matthias/Lepsius, Oliver (Hrsg.), Verhältnismäßigkeit, Zur Tragfähigkeit eines verfassungsrechtlichen Schlüsselkonzepts, 2021, S. 293.

Jestaedt, Matthias/Lepsius, Oliver (Hrsg.), Verhältnismäßigkeit, Zur Tragfähigkeit eines verfassungsrechtlichen Schlüsselkonzepts, Recht - Wissenschaft - Theorie Bd. 8, 2021, Tübingen.

Jestaedt, Matthias/Lepsius, Oliver/Möllers, Christoph ua. (Hrsg.), Das entgrenzte Gericht, Eine kritische Bilanz nach sechzig Jahren Bundesverfassungsgericht, 2011, Berlin.

Johannes, Paul C./Weinhold, Robert, Das neue Datenschutzrecht bei Polizei und Justiz, Europäisches Datenschutzrecht und deutsche Datenschutzgesetze, 2018, Baden-Baden

Junge Wissenschaft Öffentlichen Recht e.V. (Hrsg.), Kollektivität - Öffentliches Recht zwischen Gruppeninteressen und Gemeinwohl, 52. Assistententagung Öffentliches Recht, 2012, Baden-Baden.

Juszczak, Adam/Sason, Elisa, Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this only the Beginning?, in eucrim: The Europeam Crminal Law Association's Forum (eucrim) 2021, 238.

Kaetzler, Joachim, Anforderungen an die Organisation der Geldwäscheprävention bei Bankinstituten, ausgewählte Einzelfragen, in Corporate Compliance (CCZ) 2008, 174.

Kahl, Wolfgang, Die Schutzergänzungsfunktion von Art. 2 Abs. 1 Grundgesetz, Zugleich ein Beitrag zur Lehre der Grundrechtskonkurrenzen, 2000, Tübingen.

Kahl, Wolfgang, Vom weiten Schutzbereich zum engen Gewährleistungsgehalt, Kritik einer neuen Richtung der deutschen Grundrechtsdogmatik, in Der Staat 2004, 167.

Kahler, Thomas, Massenzugriff der Staatsanwaltschaft auf Kundendaten von Banken zur Ermittlung von Internetstraftaten, 2017, Baden-Baden, zugl. Diss., Univ. Frankfurt (Main), 2016.

Kahlert, Joachim (Hrsg.), Geldwäsche, Problemanalyse und Bekämpfungsstrategien; eine Tagung der Friedrich-Ebert-Stiftung am 7. und 8. Oktober 1993 in Berlin, 1994.

Kaiser, Carolin, Privacy and identity issues in financial transactions, The proportionality of the European anti-money laundering legislation, 2018, zugl. Diss., Univ. Groningen, 2018.

Kalscheuer, Fiete/Jacobsen, Annika, Der Parlamentsvorbehalt: Wesentlichkeitstheorie als Abwägungstheorie, in Die Öffentliche Verwaltung (DÖV) 2018, 523.

Karpenstein, Ulrich/Sangi, Roya, Nationale Sicherheit im Unionsrecht, zur Bedeutung von Art. 4 II 3 EUV, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2020, 162.

Kaufmann, Michael, Die Bedeutung der Einbeziehung von Bankmitarbeitern in die strafrechtliche Bekämpfung der Geldwäsche, 2001, Frankfurt (Main), zugl.: Univ., Diss. Bremen, 2000.

Kaysers, Hans Henning, Die Unterrichtung Betroffener über Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses, in Archiv des öffentlichen Rechts (AöR) 2004, 121.

Kilchling, Michael/Lukas, Tim, Bundesministerium der Justiz (Hrsg.), Gefährdung von Rechtsanwälten, Steuerberatern, Notaren und Wirtschaftsprüfern durch Geldwäsche, Forschungsprojekt im Auftrag der Bundesministerien der Justiz und des Innern - Endbericht, Max-Planck-Institut für Ausländisches und Internationales Strafrecht, Recht, 2004, 2005, Godesberg.

Kingreen, Thorsten, Whatever it takes II? Verfassungsblog vom 15.02.2022, https://verfassungsblog.de/whatever-it-takes-ii/., zuletzt zugregriffen am 08.08.2023

Kingreen, Thorsten/Poscher, Ralf, Grundrechte, 37. Aufl. 2021, Heidelberg

Kingreen, Thorsten/Poscher, Ralf, Polizei- und Ordnungsrecht, mit Versammlungsrecht, 11. Aufl. 2020, München

Kipker, Dennis-Kenji, Informationelle Freiheit und staatliche Sicherheit, 2016, Tübingen, zugl. Diss., Univ. Bremen, 2015.

Kipker, Dennis-Kenji/Schefferski, Julia/Stelter, Mattea, Anmerkung zu EuGH, Urteil vom 21.12.2016 – C-203/15 u. C-698/15 – Tele2 Sverige, in Zeitschrift für Datenschutz (ZD) 2017, 124.

Kirchhof, Paul, Bankgeheimnis und Geldwäsche aus verfassungsrechtlicher Sicht, in Hadding, Walther/Hopt, Klaus/Schimansky, Herbert (Hrsg.), Basel II: Folgen für Kreditinstitute und ihre Kunden. Bankgeheimnis und Bekämpfung von Geldwäsche, Bankrechtstag 2003, 2004, S. 79.

Klein, Eckart, Zur objektiven Funktion der Verfassungsbeschwerde, in Die Öffentliche Verwaltung (DÖV) 1982, 797.

Klein, Franz/Orlopp, Gerd (Begr.), Abgabenordnung, Einschließlich Steuerstrafrecht, Kommentar, 15. Aufl., 2020 (zit. als *Bearbeiter* in Klein AO).

Klement, Jan Henrik, Die Kumulation von Grundrechtseingriffen im Umweltrecht, in Archiv des öffentlichen Rechts (AöR) 2009, 35.

Klement, Jan Henrik, Grundrechtseingriffe, in *Stern, Klaus/Sodan, Helge/Möstl, Markus* (Hrsg.), Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl., 2022, München, § 80.

Klugmann, Marcel, Das Gesetz zur Optimierung der Geldwäscheprävention und seine Auswirkungen auf die anwaltliche Praxis, in Neue Juristische Wochenschrift (NJW) 2012, 641.

Knauer, Christoph/Kudlich, Hans/Schneider, Harmut (Hrsg.) Münchener Kommentar zur Strafprozessordnung, Kommentar, 2. Aufl., München (zit. als *Bearbeiter* in MüKo StPO).

Knierim, Antonie, Kumulation von Datensammlungen auf Vorrat, Vorratsspeicherung von TK- und Fluggastdaten und das Verbot umfassender Überwachung, in Zeitschrift für Datenschutz (ZD) 2011, 17.

Knierim, Thomas, Kapitel 10: Straftaten im Bankbereich, in Bannenberg, Britta/Wabnitz, Heinz-Bernd/Janovsky, Thomas ua. (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 5. Aufl., 2020, München

Kniesel, Michael/Vahle, Jürgen, Zur Novellierung des nordrhein-westfälischen Polizeirechts, in Die Öffentliche Verwaltung (DÖV) 1990, 646.

Koch, Martin, Datenerhebung und -verarbeitung in den Polizeigesetzen der Länder, 1999, Baden-Baden, zugl. Diss., Univ. Hamburg, 1998 u.d.T.: Vergleich der Regelungen zur Datenerhebung und -verarbeitung in den Polizeigesetzen der Länder

Kockel, Martin/Vossen-Kempkens, Stefanie, Zur Sachbehandlung von unschlüssigen, haltlosen, beschimpfenden, sich inhaltlich wiederholenden „querulatorischen" Strafanzeigen, in Neue Zeitschrift für Strafrecht (NStZ) 2001, 178.

Koenig, Ulrich (Hrsg.), Abgabenordnung, Kommentar, 4. Aufl., 2021 (zit. als *Bearbeiter* in Koenig AO).

Kokemoor, Axel, Der Automatisierte Abruf von Kontoinformationen nach § 24c KWG, in Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2004, 135.

Kokott, J./Sobotta, C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, in International Data Privacy Law 2013, 222.

Kolany-Raiser, Barbara/Heil, Reinhard/Orwat, Carsten ua. (Hrsg.), Big Data und Gesellschaft, Technikzukünfte, Wissenschaft und Gesellschaft / Futures of Technology, Science and Society, 2018, Wiesbaden.

Kölbel, Ralf, Criminal Compliance – ein Missverständnis des Strafrechts? in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2014, 499.

Köndgen, Johammes, Das neue Recht des Zahlungsverkehrs, in Juristische Schulung 2011, 481.

Korff, Niklas, § 45 Überweisungsverkehr, in Derleder, Peter/Knops, Kai-Oliver/Bamberger, Heinz Georg (Hrsg.), Deutsches und europäisches Bank- und Kapitalmarktrecht, Band I, 3. Auflage 2017.

Korioth, Stefan/Vesting, Thomas (Hrsg.), Der Eigenwert des Verfassungsrechts, Was bleibt von der Verfassung nach der Globalisierung?, 2011, Tübingen.

Kostov, Iva, Die Fluggastdatenverarbeitung zu Sicherheitszwecken, Teil 1 – Mit Anmerkungen zur Eingriffsintensität und Rechtfertigung nach dem EuGH, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2022, 267.

Krais, Jürgen, Geldwäsche und Compliance, Praxisleitfaden für Güterhändler, 2018, München.

Krais, Jürgen, Zu den Neuregelungen der 4. EU-Geldwäscherichtlinie, in Corporate Compliance (CCZ) 2015, 251.

Krämer, Gregor, Die Bekämpfung von Geldwäsche und Terrorismusfinanzierung, Die Tätigkeit der FATF als internationaler Standardsetter, 2008, Baden-Baden, zugl. Habil., Univ. Saarbrücken, 2007.

Krehl, Christoph, Die Erkundigungspflicht des Zeugen bei fehlender oder beeinträchtigter Erinnerung und mögliche Folgen ihrer Verletzung, in Neue Zeitschrift für Strafrecht (NStZ) 1991, 416.

Kreissl, Reinhard/Norris, Clive/Krlic Marija/Groves, Leroy/Amicelle, Anthony, Surveillance: Preventing and detecting crime and terrorism, in Wright, David/Kreissl, Reinhard (Hrsg.), Surveillance in Europe, 2015, S. 150.

Kretschmer, Joachim, Das Bankgeheimnis in der deutschen Rechtsordnung, - ein Überblick, in Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 2009, 181.

Kritische Justiz (Hrsg.), Verfassungsrecht und gesellschaftliche Realität: Dokumentation: Kongress "60 Jahre Grundgesetz: Fundamente der Freiheit stärken" der Bundestagsfraktion Bündnis90/Die Grünen am 13./14. März 2009 in Berlin, Sonderheft Kritische Justiz, 2009, Baden-Baden.

Kube, Hanno, § 148 Persönlichkeitsrecht, in: Josef Isensee/Paul Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Bd. VII, 3. Aufl., 2009, Heidelberg.

Kübler, Johanna, Die Säulen der Europäischen Union: einheitliche Grundrechte? zur Grundrechtsdivergenz zwischen der ersten und dritten Säule am Beispiel des Datenschutzes, 2002, Baden-Baden, zugl. Diss., Uni. Frankfurt (Main) 2002.

Kühling, Jürgen, Datenschutzrechtlicher Überarbeitungsbedarf beim „Steuerehrlichkeitsgesetz", Datenschutz zwischen Desinteresse und Alarmismus, in Zeitschrift für Rechtspolitik (ZRP) 2005, 196.

Kühling, Jürgen, Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2014, 681.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung, BDSG, Kommentar, 3. Aufl., 2020, München (zit. als *Bearbeiter* in Kühling/Buchner DSGVO/BDSG).

Kühling, Jürgen/Heitzer, Sonja, Returning through the National Back Door? The future of data retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere, in 40 European Law Review (Eur. Law Rev) 2015, 263.

Kuhn, Tomas, Überschießende Umsetzung bei mindest- und vollharmonisierenden Richtlinien: Einheitliche oder gespaltene Anwendung?, in Europarecht (EuR) 2015, 216.

Kunz, Jens, Die neue Geldtransferverordnung – Überblick zu den wesentlichen Änderungen, in Compliance Berater (CB) 2016, 54.

Kunz, Jens/Schirmer, Matthias, 4. EU-Geldwäsche-RL:, Auswirkungen auf Unternehmen, Banken und Berater, in Betriebs-Berater (BB) 2015, 2435.

Kurz, Constanze/Engling, Dirk/Rehak, Rainer, Stellungnahme an das Bundesverfassungsgericht zum BND-Gesetz und zur Ausland-Ausland-Fernmeldeaufklärung, Chaos Computer Club, 2017, 1 BvR 2835/17, https://www.ccc.de/system/uploads/290/original/BNDgesetz_CCC-Stellungnahme.pdf, zuletzt zugegriffen am 08.08.2023

Kutscha, Martin, Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung*, in Neue Juristische Wochenschrift (NJW) 2007, 1169.

Lachenmann, Matthias, Das Ende des Rechtsstaates aufgrund der digitalen Überwachung durch die Geheimdienste?, in Die Öffentliche Verwaltung (DÖV) 2016, 501.

Ladeur, Karl-Heinz, Das Recht auf informationelle Selbstbestimmung, Eine juristische Fehlkonstruktion?, in Die Öffentliche Verwaltung (DÖV) 2009, 45.

Ladeur, Karl-Heinz, Datenschutz - vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken: Zur "objektiv-rechtlichen Dimension" des Datenschutzes, in Datenschutz und Datensicherheit (DuD) 2000, 12.

Landerer, Lukas Martin, The Anti-Money-Laundering Directive and the ECJ's Jurisdiction on Data Retention, in eucrim: The Europeam Crminal Law Association's Forum (eucrim) 2022, 67.

Landesbeauftragter für Datenschutz in Baden-Württemberg, Fünfundzwanzigster Tätigkeitsbericht, 2004, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/25.-T%C3%A4tigkeitsbericht-2004.pdf, zuletzt zugegriffen am 08.08.2023

Landesbeauftragter für Datenschutz Nordrhein-Westfalen, Siebzehnter Datenschutz- und Informationsfreiheitsbericht, 2004, https://www.ldi.nrw.de/system/files/media/document/file/17_datenschutz-_und_informationsfreiheitsbericht.pdf ,zuletzt zugegriffen am 08.08.2023.

Landesbeauftragter für den Datenschutz Sachsen-Anhalt, 8. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Sachsen-Anhalt, 2007, https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Veroeffentlichungen/Taetigkeitsberichte/TB_8/8._Taetigkeitsbericht_Datenschutz.pdf ,zuletzt zugegriffen am 08.08.2023.

Lang, Volker/Schwarz, Anne/Kipp, Rudolf, Regelungen zur Bekämpfung der Geldwäsche, 3. Aufl. 1999, Stuttgart.

Lange, Claudia/Höche, Thorsten, Basel II: Was verbirgt sich dahinter für Kreditinstitute und ihre Kunden? Bankgeheimnis und Bekämpfung von Geldwäsche, Bericht über den Bankrechtstag am 4. Juli 2003 in Düsseldorf, in Wertpapier-Mitteilungen (WM) 2003, 1645.

Lange, Nicole, Staatsanwaltschaftliche Vorermittlungen -, ohne rechtliche Grundlage? in Deutsche Richterzeitung 2002, 264.

Lehner, Roman, Deutscher und europäischer Grundrechtsschutz nach den Entscheidungen zum „Recht auf Vergessen", – Von der Alternativität zur Komplementarität?, in Juristische Ausbildung (JURA) 2022, 177.

Lehnhoff, Jochen, Geplante Kontenüberwachung und Kundenrasterung bei Wertpapiergeschäften gehen zu weit!, in Wertpapier-Mitteilungen (WM) 2002, 687.

Leidenmühler, Franz, Die freiwillige „Übererfüllung" unionsrechtlicher Vorgaben durch die Mitgliedstaaten., Ein Beitrag zur rechtsdogmatischen und rechtspolitischen Diskussion um das sog. „Gold Plating", in Europarecht (EuR) 2019, 383.

Lemieux, Frédéric, Intelligence and state surveillance in modern societies, An international perspective, 2019, Bingley.

Lenk, Maximilian, Sanktionsbewehrte Melde- und Anzeigepflichten – Zu den materiell-rechtlichen Problemen einer privatisierten Kriminalitätsbekämpfung, in Juristische Rundschau (JR) 2020, 103.

Lepsius, Oliver, Das Computer-Grundrecht, Herleitung-Funktion-Überzeugungskraft, in Roggan, Fredrik (Hrsg.), Online-Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008; Dokumentation einer Fachtagung der Humanistischen Union und der Friedrich-Naumann-Stiftung für die Freiheit am 28. April 2008 in Berlin, 2008, S. 21.

Lepsius, Oliver, Die Chancen und Grenzen des Grundsatzes der Verhältnismäßigkeit, in Jestaedt, Matthias/Lepsius, Oliver (Hrsg.), Verhältnismäßigkeit, Zur Tragfähigkeit eines verfassungsrechtlichen Schlüsselkonzepts, 2021, S. 1.

Lepsius, Oliver, Die Maßstabssetzende Gewalt, in Jestaedt, Matthias/Lepsius, Oliver/Möllers, Christoph/Schönberger, Christoph (Hrsg.), Das entgrenzte Gericht, Eine kritische Bilanz nach sechzig Jahren Bundesverfassungsgericht, 2011, S. 159.

Lepsius, Oliver, Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland, in Leviathan 2004, 64.

Lepsius, Oliver, Sicherheit und Freiheit, - ein zunehmend asymmetrisches Verhältnis, in Schuppert, Gunnar Folke/Merkel, Wolfgang/Nolte, Georg/Zürn, Michael (Hrsg.), Der Rechtsstaat unter Bewährungsdruck, 2010, S. 23.

Leutheusser-Schnarrenberger, Sabine, Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa, in Datenschutz und Datensicherheit (DuD) 2014, 589.

Leutheusser-Schnarrenberger, Sabine, Vorratsdatenspeicherung - Ein vorprogrammierter Verfassungskonflikt, in Zeitschrift für Rechtspolitik (ZRP) 2007, 9.

Lilie, Hans, Anmerkung zu LG Kaiserslautern, Beschluß vom 19.03.1981 - 5 Os 346/80, in Neue Zeitschrift für Strafrecht (NStZ)1981, 438.

Lindner, Bernd Michael/Lienke, Georg/Aydur, Ebru, Die neue EU-Geldtransferverordnung – Wesentliche Neuerungen für zwischengeschaltete Zahlungsdienstleister, in Corporate Compliance (CCZ) 2016, 90.

Lindner, Josef Franz/Unterreitmeier, Johannes, »Überwachungsgesamtrechnung«: Karlsruhe calculat?, in Juristenzeitung (JZ) 2022, 915.

Lisken, Hans/Denninger, Erhard Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 6. Aufl., 2018, München (zit. als *Bearbeiter* in Lisken/Denninger Hdb. Polizeirecht, 6. Aufl. 2018).

Lisken, Hans, Über Aufgaben und Befugnisse der Polizei im Staat des Grundgesetzes, in Zeitschrift für Rechtspolitik (ZRP) 1990, 15.

Lisken, Hans, Verdachts- und ereignisunabhängige Personenkontrollen zur Bekämpfung der grenzüberschreitenden Kriminalität, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 1998, 22.

Lisken, Hans, Vorfeldeingriffe im Bereich der „Organisierten Kriminalität" — Gemeinsame Aufgabe von Verfassungsschutz und Polizei? in Zeitschrift für Rechtspolitik (ZRP) 1994, 264.

Löffelmann, Markus, "Kaum betroffen", Die sogenannte Vorratsdatenspeicherung ist mitnichten ein besonders schwerer Grundrechtseingriff. Es handelt sich um ein Verkehrsdatenregister. FAZ Online vom 29.04.2015, https://www.faz.net/aktuell/politik/staat-und-recht/gastbeitrag-kaum-betroffen-13566596-p2.html?service=printPreview, zuletzt zugegriffen am 08.08.2023.

Löffelmann, Markus, Anmerkung zu BVerfG, Beschluss vom 10.11.2020 – 1 BvR 3214/15, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2021, 25.

Löffelmann, Markus, Datenerhebung aus dem „Smart Home" im Sicherheitsrecht, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2020, 244.

Löffelmann, Markus, Die Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung, - Schema oder Struktur?, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2019, 16.

Löffelmann, Markus, Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz, 2022, Berlin.

Löhnig, Martin, BGH v. 8. 11. 2005 – ZR 90/05, Anspruch auf Erteilung von Kontoauszügen wird nicht mit Hauptforderung mitgepfändet, in Juristische Rundschau (JR) 2007, 73.

Lorenz, Dieter, Allgemeines Persönlichkeitsrecht und Gentechnologie, in Juristenzeitung (JZ) 2005, 1121.

Lowe, David, The European Union's Passenger Name Record Data Directive 2016/681: Is it Fit for Purpose?, in 17 International Criminal Law Review (ICL) 2017, 78.

Löwe, Ewald/Rosenberg, Werner, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, 27. Aufl., 2018, Berlin, Boston (zit. als *Bearbeiter* in Löwe/Rosenberg StPO).

Löwe-Krahl, Oliver, Das Geldwäschegesetz, Ein taugliches Instrument zur Verhinderung der Geldwäsche?, in Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 1994, 121.

Lübbe-Wolff, Gertrude, Die Grundrechte als Eingriffsabwehrrechte, Struktur und Reichweite der Eingriffsdogmatik im Bereich staatlicher Leistungen, 1988, Baden-Baden, Zugl. Habil., Univ. Bielefeld, 1987.

Ludwig, Thomas Claus, Zum Verhältnis zwischen Grundrechtecharta und allgemeinen Grundsätzen, in Europarecht (EuR) 2011, 715.

Lynskey, Orla, Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order, in 63 International and Comparative Law Quarterly (Int. & Comp. Law Quarterly) 2014, 569.

Lyon, David, Surveillance Studies, An overview, in Monahan, Torin/Wood, David Murakami (Hrsg.), Surveillance studies, A reader, 2018, S. 18.

Lyon, David, Surveillance studies: an overview, 2012, Cambridge.

Lyon, David, The electronic eye, The rise of surveillance society, 1994, Minneapolis

Maillart, Jean-Baptiste, The Anti-Money Laundering Architecture of the FATF, in Vogel, Benjamin/Maillart, Jean-Baptiste (Hrsg.), National and international anti-money laundering law. Rethinking the architecture of criminal justice, regulation and data protection, 2020, S. 11.

Makrutzki, Patric, Verdeckte Ermittlungen im Strafprozeß, Rechtswissenschaftliche Analyse - Rechtsvergleichende Studie mit dem U.S.-amerikanischen Prozeßrecht, 2000, Berlin, zugl. Diss., Univ. Freiburg 1997/1998.

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian, Grundgesetz, Kommentar, 7. Aufl., 2018 (zit. als *Bearbeiter* in Mangoldt/Klein/Starck GG).

Mann, Thomas/Sennekamp, Christoph/Uechtritz, Michael (Hrsg.), Verwaltungsverfahrensgesetz, Großkommentar, 2. Aufl., 2019 (zit. als *Bearbeiter* in Mann/Sennekamp/Uechtritz VwVfG).

Marquenie, Thomas, The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework, in 33 Computer Law & Security Review 2017, 324.

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht, Grundlagen – Dimensionen – Verflechtungen, 2018, Tübingen, zugl. Habil., Univ. Freiburg, 2017.

Marsch, Nikolaus, Die objektive Funktion der Verfassungsbeschwerde in der Rechtsprechung des Bundesverfassungsgerichts, in Archiv des öffentlichen Rechts (AöR) 2012, 592.

Marxsen, Christian, Strategische Fernmeldeaufklärung, in Die Öffentliche Verwaltung (DÖV) 2018, 218.

Masing, Johannes, Die Ambivalenz von Freiheit und Sicherheit, in Juristenzeitung (JZ) 2011, 753.

Masing, Johannes, Die Ambivalenz von Freiheit und Sicherheit, in Gander, Hans-Helmuth/Perron, Walter/Poscher, Ralf/Riescher, Gisela/Würtenberger, Thomas (Hrsg.), Resilienz in der offenen Gesellschaft, Symposium des Centre for Science and Security, 2012, S. 41.

Masing, Johannes, Herausforderungen des Datenschutzes, in Neue Juristische Wochenschrift (NJW) 2012, 2305.

Maurer, Hartmut/Waldhoff, Christian, Allgemeines Verwaltungsrecht, 20. Aufl. 2020, München.

Meinicke, Dirk, Anmerkung zu BVerfG, Beschluss vom 24.1.2012 - 1 BvR 1299/05, in Zeitschrift für IT-Recht und Recht der Digitalisierung 2012, 410.

Merten, Detlef/Papier, Hans-Jürgen/Bernhardt, Rudolf (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, 2009, Heidelberg.

Meyer, Jürgen/Hölscheidt, Sven, Charta der Grundrechte der Europäischen Union, Kommentar, 5. Aufl., 2019, Baden-Baden (zit. als *Bearbeiter* in Meyer/Hölscheidt EU-GRC).

Meyer-Goßner, Lutz (Begr.), *Schmitt, Bertram/Köhler, Marcus* (Hrsg.), Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 63. Aufl., 2020, München (zit. als *Bearbeiter* in Meyer-Goßner/Schmitt StPO).

Meyer-Ladewig, Jens (Begr.), *Nettesheim*, *Martin/Raumer, Stefan von* (Hrsg.), EMRK Europäische Menschenrechtskonvention, Handkommentar, 5. Aufl., 2023 Baden-Baden (zit. als *Bearbeiter* in Meyer-Ladewig/Nettesheim/von Raumer EMRK).

Michalke, Reinhart, Wenn der Staatsanwalt klingelt, - Verhalten bei Durchsuchung und Beschlagnahme, in Neue Juristische Wochenschrift (NJW) 2008, 1490.

Michl, Fabian, Sicherstellung von Daten durch die Polizei, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2019, 1631.

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh — zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, in Datenschutz und Datensicherheit (DuD) 2017, 349.

Milaj, Jonida/Kaiser, Carolin, Retention of data in the new Anti-money Laundering Directive— 'need to know' versus 'nice to know', in 17 International Data Privacy Law (Int. Data Privacy Law) 2017, 115.

Miller, Russell A. (Hrsg.), Privacy and power, A transatlantic dialogue in the shadow of the NSA-Affair, 2017, Cambridge.

Mitsilegas, Valsamis/Gilmore, Bill, The Eu Legislative Framework Against Money Laundering and Terrorist Finance: A Critical Analysis in the Light of Evolving Global Standards, in 56 International and Comparative Law Quarterly (Int. & Comp. Law Quarterly) 2007, 119.

Mitsilegas, Valsamis/Guild, Elspeth/Kuskonmaz, Elif/Vavoula, Niovi, Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks, in European Law Journal 2022 (online preprint), 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3972218, zuletzt zugegriffen am 08.08.2023.

Mitsilegas, Valsamis/Vavoula, Niovi, The Evolving EU Anti-Money Laundering Regime, in 23 Maastricht Journal of European and Comparative Law (Maastricht J. of EU and Comp. Law) 2016, 261.

Möllers, Martin H. W./van Ooyen, Robert Chr. (Hrsg.), Bundesverfassungsgericht und öffentliche Sicherheit, 2. Aufl., Jahrbuch öffentliche Sicherheit Sonderband Bd. 3.1, 2012, Frankfurt (Main).

Momsen, Carsten/Grützner, Thomas (Hrsg,), Wirtschafts- und Steuerstrafrecht, Handbuch für die Unternehmens- und Anwaltspraxis, 2. Aufl., München, 2020 (zit. als *Bearbeiter* in Hdb. Wirtschafts- & SteuerstrafR).

Monahan, Torin/Wood, David Murakami (Hrsg.), Surveillance studies, A reader, 2018, New York.

Moser-Knierim, Antonie, Vorratsdatenspeicherung, Zwischen Überwachungsstaat und Terrorabwehr, 2014, Wiesbaden, zugl. Diss., Univ. Kassel, 2013.

Möstl, Markus, Die Beschlüsse des BVerfG zu Kfz-Kennzeichenkontrollen, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2019, 101.

Möstl, Markus, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, 2002, Tübingen, zugl. Habil., Univ. München 2001/2002.

Möstl, Markus, Eingreifschwellen im polizeilichen Informationsrecht, in Spiecker gen. Döhmann, Indira/Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 239.

Möstl, Markus/Kugelmann, Dieter (Hrsg.), Beck'scher Online-Kommentar, Polizei- und Ordnungsrecht Nordrhein-Westfalen, 19. Edition, Stand 01.09.2021, München (zit. als *Bearbeiter* in BeckOK POR NRW).

Möstl, Markus/Weiner/Bernhard (Hrsg.), Beck'scher Online-Kommentar, Polizei- und Ordnungsrecht Niedersachsen, 21. Edition, Stand 01.11.2021, München (zit. als *Bearbeiter* in BeckOK NdsPOG).

Mülhausen, Dieter/Herzog, Felix (Hrsg.), Geldwäschebekämpfung und Gewinnabschöpfung, Handbuch der straf- und wirtschaftsrechtlichen Regelungen, 2006, München.

Müller, Eckhart/Schlothauer, Reinhold/Knauer, Christoph (Hrsg.), Münchener Anwalts-Handbuch Strafverteidigung, 3. Aufl., 2022, München (zit. als *Bearbeiter* in MAH Strafverteidigung)

Müller, Michael W./Schwabenbauer, Thomas, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht; Teil II-III, Teil V, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl. 2021.

Müller, Michael W./Schwabenbauer, Thomas, Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden, in Neue Juristische Wochenschrift (NJW) 2021, 2079.

Müller, Nadja, Transparenz auf allen Ebenen – Zur Umsetzung der Vierten Geldwäscherichtlinie – Teil 1, in Neue Zeitschrift für Wirtschaftsstrafrecht (NZWiSt) 2017, 87.

Müller, Nadja, Transparenz auf allen Ebenen – Zur Umsetzung der Vierten Geldwäscherichtlinie – Teil 2, in Neue Zeitschrift für Wirtschaftsstrafrecht (NZWiSt) 2017, 121.

Müller, Rolf-Georg, Polizeiliche Datenerhebung durch Befragung, Zugleich eine Analyse des § 9 NW. PolG, 1997, Berlin, zugl. Diss., Univ. Bochum, 1997.

Müller, Rudolf, Die Grenzen des Bankgeheimnisses, in Neue Juristische Wochenschrift (NJW) 1963, 831.

Münch, Ingo von/Kunig, Philipp, Grundgesetz, Kommentar, 7. Aufl., 2021, München (zit. als *Bearbeiter* in von Münch/Kunig GG).

Murswiek, Dietrich, Die Corona-Waage, Kriterien für die Prüfung der Verhältnismäßigkeit von Corona-Maßnahmen, in Neue Zeitschrift für Verwaltungsrecht – Extra (NVwZ-Extra) 5/2021.

Nachbaur, Andreas, Vorratsdatenspeicherung „light" – Rechtswidrig und allenfalls bedingt von Nutzen, in Zeitschrift für Rechtspolitik (ZRP) 2015, 215.

Naumann, Kolja, Art. 52 Abs. 3 GrCh zwischen Kohärenz des europäischen Grundrechtsschutzes und Autonomie des Unionsrechts, in Europarecht (EuR) 2008, 424.

Nave, Susana Campos, Das Know Your Customer-Prinzip und die Geldwäscheprävention, in Compliance Berater (CB) 2018, 166.

Nettesheim, Martin, Grundrechtsschutz der Privatheit, in Nettesheim, Martin/Diggelmann, Oliver/Lege, Joachim/Kingreen, Thorsten (Hrsg.), Der Schutzauftrag des Rechts, Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, 2011, S. 7.

Nettesheim, Martin/Diggelmann, Oliver/Lege, Joachim ua. (Hrsg.), Der Schutzauftrag des Rechts, Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, VVDStRL, BD. 70, 2011, Berlin.

Neumann, Dieter, Vorsorge und Verhältnismäßigkeit, Die kriminalpräventive Informationserhebung im Polizeirecht, 1994, Berlin, zugl. Diss., Univ. Bielefeld, 1993,

Nitschke, Peter, Kapitel 15 Das PNR-Abkommen zwischen der EU und den USA: Eine transatlantische (innere) Sicherheitsarchitektur, in Jahrbuch Terrorismus 2007, 209.

Oberste Finanzbehörden der Länder, Anweisungen für das Straf- und Bußgeldverfahren (Steuer) – AStBV (St) 2019, S 0720 BStBl 2018 01. Dezember 2018, https://datenbank.nwb.de/Dokument/769703/, zuletzt zugegriffen am 08.08.2023.

Oehmichen, Anna/Mickler, Christina, Die Vorratsdatenspeicherung – Eine never ending story?, in Neue Zeitschrift für Wirtschaftsstrafrecht (NZWiSt) 2017, 298.

Oermann, Markus/Staben, Julian, Mittelbare Grundrechtseingriffe durch Abschreckung, Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken, in Der Staat 2013, 630.

Ogorek, Markus, Anmerkung zu EuGH, Urteil vom 6.10.2020 – C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua/Premier ministre ua), in Neue Juristische Wochenschrift (NJW) 2021, 531.

Orantek, Kerstin, Die Vorratsdatenspeicherung in Deutschland, in Neue Justiz (NJ) 2010, 193.

Orrù, Elisa, The European PNR Directive as an instance of pre-emptive, risk-based algorithmic security and its implications for the regulatory framework, in 27 Information Polity 2022, 131.

Osterloh, Lerke/Schmidt, Karsten/Weber, Hermann (Hrsg.), Staat, Wirtschaft, Finanzverfassung, Festschrift für Peter Selmer zum 70. Geburtstag, Schriften zum Öffentlichen Recht Band 960, 2004, Berlin

Oswald, Katharina, Money-Laundering Legislation in Germany: Selected Results from a Recent Research Project, in 5 European Journal of Crime, Criminal Law and Criminal Justice (Eur. J. of Crime, Criminal Law & Justice)1997, 196.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3. Aufl., 2021, München (zit. als *Bearbeiter* in Paal/Pauly DSGVO/BDSG).

Pache, Eckhardt, in, Frankfurter Kommentar zu EUV, GRC und AEUV, München, Tübingen 2017.

Papier, Hans-Jürgen, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) – Extra 15/2016, 1.

Park, Tido, Durchsuchung und Beschlagnahme, 4. Aufl. 2018, München.

Payrhuber, Melanie/Stelkens, Ulrich, 1:1-Umsetzung" von EU-Richtlinien: Rechtspflicht, rationales Politikkonzept oder (wirtschafts)politischer Populismus? zugleich zu Unterschieden zwischen Rechtsangleichungs- und Deregulierungsrichtlinien, in Europarecht (EuR) 2019, 190.

Pechstein, Matthias/Nowak, Carsten/Häde, Ulrich (Hrsg.), Frankfurter Kommentar zu EUV, GRC und AEUV, 2017 (zit. als *Bearbeiter* in Frankfurter Kommentar).

Pedersen, Anja Møller/Udsen, Henrik/Jakobsen, Søren Sandfeld, Data retention in Europe—the Tele 2 case and beyond, in 8 International Data Privacy Law (Int. Data Privacy Law) 2018, 160.

Penney, Jonathon, Understanding Chilling Effects, in 106 Minnesota Law Review 2022, 1451.

Petersen, Jens, Das Bankgeheimnis zwischen Individualschutz und Institutionsschutz, 2005, Tübingen,

Petersen, Niels, Verhältnismäßigkeit als Rationalitätskontrolle, Eine rechtsempirische Studie verfassungsgerichtlicher Rechtsprechung zu den Freiheitsgrundrechten, 2015, Tübingen, zugl. Habil., Univ. Bonn, 2014.

Petri, Thomas, Auskunftsverlangen nach § 161 StPO gegenüber Privaten, - eine verdeckte Rasterfahndung? in Strafverteidiger (StV) 2007, 266.

Pfeffer, Kristin, Stille Europäisierung, – Wie europäisch wird das deutsche Polizeirecht? in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2022, 294.

Pfisterer, Valentin, »Finanzprivatsphäre« in Deutschland, in Jahrbuch des öffentlichen Rechts der Gegenwart (JöR) 2017, 393.

Picot, Arnold/Berchtold, Yvonne/Neuburger, Rahild, Big Data aus ökonomischer Sicht: Potenziale und Handlungsbedarf, in Kolany-Raiser, Barbara/Heil, Reinhard/Orwat, Carsten/Hoeren, Thomas (Hrsg.), Big Data und Gesellschaft, 2018, S. 309.

Placzek, Thomas, Allgemeines Persönlichkeitsrecht und privatrechtlicher Informations- und Datenschutz, Eine schutzgutbezogene Untersuchung des Rechts auf informationelle Selbstbestimmung, 2006, Hamburg, zugl.: Diss., Univ. Regensburg, 2005.

Pohle, Jörg, Freiheitsbestandsanalyse statt Überwachungsgesamtrechnung – Ein Alternativvorschlag, in FIfF-Kommunikation 2019(4), 37.

Popp, Andreas, Strafvereitelung durch Schweigen – der Zeuge als Garant für die Verwirklichung straf- und maßregelrechtlicher Sanktionierungsbefugnisse? in Juristische Rundschau (JR) 2014, 418.

Poscher, Ralf, Die Zukunft der Informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in Gander, Hans-Helmuth/Perron, Walter/Poscher, Ralf/Riescher, Gisela/Würtenberger, Thomas (Hrsg.), Resilienz in der offenen Gesellschaft, Symposium des Centre for Science and Security, 2012, S. 167.

Poscher, Ralf, Eingriffsschwellen im Recht der Inneren Sicherheit, Ihr System im Licht der neueren Verfassungsrechtsprechung, in Die Verwaltung 2008, 345.

Poscher, Ralf, Sicherheitsverfassungsrecht im Wandel, in Korioth, Stefan/Vesting, Thomas (Hrsg.), Der Eigenwert des Verfassungsrechts, Was bleibt von der Verfassung nach der Globalisierung? 2011, S. 245.

Poscher, Ralf, The Right to Data Protection, A No-Right Thesis, in Miller, Russell A. (Hrsg.), Privacy and power, A transatlantic dialogue in the shadow of the NSA-Affair, 2017, S. 129.

Poscher, Ralf/Kilchling, Michael/Landerer, Lukas Martin, Ein Überwachungsbarometer für Deutschland, Entwicklung eines Konzeptes zur periodischen Erfassung staatlicher Überwachungsmaßnahmen, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2021, 225.

Poscher, Ralf/Kilchling, Michael/Landerer, Lukas Martin, Überwachungsbarometer für Deutschland, Ein Modellkonzept, Friedrich-Naumann-Stiftung für die Freiheit, 2022, https://shop.freiheit.org/download/P2@1168/542535/Analyse_Ueberwachung_Teil2_260122_final.pdf, zuletzt zugegriffen am 08.08.2023.

Poscher, Ralf/Rusteberg, Benjamin, Die Aufgabe des Verfassungsschutzes, Zur funktionalen Trennung von Polizei und Nachrichtendiensten, in Kritische Justiz (KJ) 2014, 57.

Poscher, Ralf/Rusteberg, Benjamin, Ein Kooperationsverwaltungsrecht des Verfassungsschutzes?, in Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand/Graulich, Kurt/Gusy, Christoph/Warg, Gunter (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2020, S. 145.

Potacs, Klagenfurt, Effet utile als Auslegungsgrundsatz, in Europarecht (EuR) 2009, 465.

Prantl, Heribert, Ende der Maßlosigkeit, in Süddeutsche Zeitung (SZ) vom 08.04.2014, https://www.sueddeutsche.de/politik/urteil-zur-vorratsdatenspeicherung-ende-der-masslosigkeit-1.1932057, zuletzt zugegriffen am 23.01.2023, zuletzt zugegriffen am 08.08.2023.

Priebe, Reinhard, Vorratsdatenspeicherung und kein Ende, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2017, 136-130.

Purtova, Nadezhda, Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships, in 8 International Data Privacy Law (Int. Data Privacy Law) 2018, 52.

Puschke, Jens/Singelnstein, Tobias, Telekommunikationsüberwachung, Vorratsdatenspeicherung und (sonstige) heimliche Ermittlungsmaßnahmen der StPO nach der Neuregelung zum 1. 1. 2008, in Neue Juristische Wochenschrift (NJW) 2008, 113.

Quintel, Teresa, Data protection rules applicable to Financial Intelligence Units: still no clarity in sight, in 23 ERA Forum 2022, 53.

Radtke, Henning, Aktive Mitwirkungspflichten und die "freiwillige " aktive Mitwirkung des Betroffenen bei dem Zugriff auf elektronisch gespeicherte Daten im Strafprozess, in Eser, Albin/Goydke, Jürgen (Hrsg.), Strafverfahrensrecht in Theorie und Praxis, Festschrift für Lutz Meyer-Gossner zum 65. Geburtstag, 2001, S. 321.

Ransiek, Andreas, Die Information der Kunden über strafprozessuale und steuerrechtliche Ermittlungsmaßnahmen bei Kreditinstituten, in Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra) 1999, 401.

Rath, Christian, Karlsruhe und der Einschüchterungseffekt – Praxis und Nutzen einer Argumentationsfigur des Bundesverfassungsgerichts, in Kritische Justiz (Hrsg.), Verfassungsrecht und gesellschaftliche Realität: Dokumentation: Kongress "60 Jahre Grundgesetz: Fundamente der Freiheit stärken" der Bundestagsfraktion Bündnis 90/Die Grünen am 13./14. März 2009 in Berlin, Sonderheft Kritische Justiz, 2009, Baden-Baden., 2009, S. 65.

Reichling, Tilman, Der staatliche Zugriff auf Bankkundendaten im Strafverfahren, Die Kontenabfrage als strafprozessuale Ermittlungsmaßnahme, mögliche Folgemaßnahmen und verfassungsrechtliche Legitimationsprobleme, 2010, Frankfurt (Main), zugl. Diss., Univ. Bielefeld, 2009.

Reichling, Tilman, Strafprozessuale Ermittlungen bei Kreditinstituten – ein Überblick, in Juristische Rundschau (JR) 2011, 12.

Reifner, Udo, Bankentransparenz und Bankengeheimnis: Zu den Prinzipien der EG-Bankrechtsangleichung, in Juristenzeitung (JZ) 1993, 273.

Rensen, Hartmut/Brink, Stefan (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, Erörtert von den wissenschaftlichen Mitarbeitern, Bd. 1, 2009, Berlin.

Richard Král/Petr Mádr, On the (in)applicability of the EU Charter of Fundamental Rights to national measures exceeding the requirements of minimum harmonisation Directives, in 46 European Law Review (Eur. Law Rev.) 2021, 81.

Richter, Christian, Verfassungsmäßigkeit einer allgemeinen Impfpflicht gegen das SARS-CoV-2, Unter Berücksichtigung einer etwaigen Schutzpflicht, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2022, 204.

Rider, Barry Alexander K. (Hrsg.), Research handbook on international financial crime, Research handbooks in financial law, 2015, Cheltenham, UK; Northampton, MA, USA.

Riegel, Reinhard, Der Quantensprung des Gesetzes zu Art. 10 GG (G 10), in Zeitschrift für Rechtspolitik (ZRP) 1995, 176.

Rieger, Thomas, Der Bundesnachrichtendienst im demokratischen Rechtsstaat, 1986, Ellwangen, zugl. Diss., Univ. Hannover, 1984.

Riepl, Frank, Informationelle Selbstbestimmung im Strafverfahren, 1998, Tübingen, Zugl.: Diss., Univ. Tübingen, 1994.

Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 4. Aufl., 2021, Berlin/Boston.

Rogall, Klaus, Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)1991, 907.

Rogall, Klaus, Informationseingriff und Gesetzesvorbehalt im Strafprozeßrecht, 1992.

Roggan, Fredrik (Hrsg.), Online-Durchsuchungen, Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008; Dokumentation einer Fachtagung der Humanistischen Union und der Friedrich-Naumann-Stiftung für die Freiheit am 28. April 2008 in Berlin, 2008, Berlin-

Roggan, Fredrik, Der Einsatz von Automatischen Kennzeichenlesesystemen (AKLS) zu Fahndungszwecken, Der Einsatz von Automatischen Kennzeichenlesesystemen (AKLS) zu Fahndungszwecken Eine Kommentierung der Neuregelung des § 163 g StPO, in Neue Zeitschrift für Strafrecht (NStZ) 2022, 19.

Roggan, Fredrik, Verfassungsrechtliche Grenzen von automatisierten Kfz-Kennzeichenkontrollen, Zur Fortschreibung der Leitplanken des Sicherheitsrechts durch das BVerfG, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2019, 344.

Roggan, Fredrik/Bergemann, Nils, Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland, Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz, in Neue Juristische Wochenschrift (NJW) 2007, 876.

Roggan, Fredrik/Kutscha, Martin (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl. 2006, Berlin.

Rojszczak, Marcin, The uncertain future of data retention laws in the EU: Is a legislative reset possible? in 41 Computer Law & Security Review 2021, 105572.

Ross, Stuart/Hannan, Michelle, Money laundering regulation and risk-based decision-making, in 10 Journal of Money Laundering Control (J. of Money Laundering Control) 2007, 106.

Rößler, Gernot, Auswirkungen der vierten EU-Anti-Geldwäsche-Richtlinie auf die Kreditwirtschaft, in Wertpapier-Mitteilungen (WM) 2015, 1405.

Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, München.

Roßnagel, Alexander, Die „Überwachungs-Gesamtrechnung", Das BVerfG und die Vorratsdatenspeicherung, in Neue Juristische Wochenschrift (NJW) 2010, 1238.

Roßnagel, Alexander, Die neue Vorratsdatenspeicherung, Der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, in Neue Juristische Wochenschrift (NJW) 2016, 533.

Roßnagel, Alexander, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff, in Neue Juristische Wochenschrift (NJW) 2019, 1.

Roßnagel, Alexander, Vorratsdatenspeicherung - was geht noch und was nicht mehr? Einordnung und Handlungsmöglichkeiten nach der neueren EuGH-Rechtsprechung, in Zeitschrift für Datenschutz (ZD) 2022, 650.

Roßnagel, Alexander, Vorratsdatenspeicherung rechtlich vor dem Aus? in Neue Juristische Wochenschrift (NJW) 2017, 696.

Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes, Zwischen Systemgestaltung und Selbstregulierung, DuD-Fachbeiträge, 2018, Wiesbaden.

Rotsch, Thomas (Hrsg.), Criminal Compliance vor den Aufgaben der Zukunft, Schriften zu Compliance Bd. 7, 2013, Baden-Baden.

Rotsch, Thomas (Hrsg.), Criminal Compliance, Handbuch, 2015, Baden-Baden

Rotsch, Thomas, Criminal Compliance in Theorie und Praxis des Wirtschaftsstrafrechts, in Rotsch, Thomas (Hrsg.), Criminal Compliance vor den Aufgaben der Zukunft, 2013, S. 3.

Roxin, Claus/Schünemann, Bernd, Strafverfahrensrecht, ein Studienbuch, 29. Aufl. 2017, München.

Ruce, Philip J., Anti-Money Laundering: The Challenges of Know Your Customer Legislation for Private Bankers and the Hidden Benefits for Relationship Management (the Bright Side of Knowing Your Customer), in 128 Banking Law Journal 2011, 548.

Rudolphi, Hans-Joachim/Wolter, Jürgen/Degener, Wilhelm (Hrsg.), SK-StPO, Systematischer Kommentar zur Strafprozessordnung; mit GVG und EMRK, 4. Aufl., 2010, Köln (zit. als *Bearbeiter* in SK-StPO).

Ruffert, Matthias/Schröder, Meinhard (Hrsg.), Dynamik und Nachhaltigkeit des Öffentlichen Rechts, Festschrift für Professor Meinhard Schröder zum 70. Geburtstag, Schriften zum Öffentlichen Recht Bd. 1215, 2012, Berlin.

Ruppert, Stefan, Gesetz zur Optimierung der Geldwäscheprävention: Neue Pflichten für Steuerberater, in Deutsches Steuerrecht 2012, 100.

Ruppert, Stefan, Vierte Geldwäscherichtlinie verabschiedet – Was ändert sich für Steuerberater? in Deutsches Steuerrecht (DStR) 2015, 1708.

Rusteberg, Benjamin, Der grundrechtliche Gewährleistungsgehalt, Eine veränderte Perspektive auf die Grundrechtsdogmatik durch eine präzise Schutzbereichsbestimmung, 2009, Tübingen, zugl. Diss., Univ. Freiburg, 2008

Rusteberg, Benjamin, Die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz – Eine Zwischenbilanz des allgemeinen Sicherheitsrechts, in Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV) 2017, 24.

Rusteberg, Benjamin, Grundrechtsdogmatik als Schlüssel zum Verhältnis von Gemeinschaft und Individuum, in Junge Wissenschaft Öffentlichen Recht e.V. (Hrsg.), Kollektivität - Öffentliches Recht zwischen Gruppeninteressen und Gemeinwohl, 52. Assistententagung Öffentliches Recht, 2012, S. 13.

Rux, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, in Juristenzeitung (JZ) 2007, 285.

Säcker, Franz-Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch, 8. Aufl., 2018 (zit. als *Bearbeiter* in MüKo BGB).

Safferling, Christoph/Rückert, Christian, Europäische Grund- und Menschenrechte im Strafverfahren, - ein Paradigmenwechsel?, in Neue Juristische Wochenschrift (NJW) 2021, 287.

Salas, Mariano Fernández, The third anti-money laundering directive and the legal profession 2005, https://www.anti-moneylaundering.org/Document/Default.aspx?DocumentUid=7B528765-CB1F-4748-9733-68935E2C4745, zuletzt zugegriffen am 08.08.2023

Samson, Erich/Langrock, Marc, Der "gläserne" Bankkunde? Automatisierter Abruf von Kontoinformationen und Grundrecht auf informationelle Selbstbestimmung; zur verfassungsrechtlichen Problematik der §§ 93 Abs. 7, 8, 93 b der Abgabenordnung, 2005, Köln.

Sandhu, Aqilah, Anmerkung zu EuGH, Urteil vom 6.10.2020 – C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua/Premier ministre ua), in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2021, 209.

Sandhu, Aqilah, Die Tele2-Entscheidung des EuGH zur Vorratsdatenspeicherung in den Mitgliedstaaten und ihre Auswirkungen auf die Rechtslage in Deutschland und in der Europäischen Union, in Europarecht (EuR) 2017, 453.

Saperstein, Lanier/Sant, Geoffrey/Ng, Michelle, The Failure of Anti-Money Laundering Regulation: Where is the Cost-Benefit Analysis?, in 91 Notre Dame Law Review Online 2015, 1.

Sapozhnikova, M. U./Gayanova, M. M./Vulfin, A. M./Nikonov, A. V./Chuykov, A. V., Distributed Infrastructure for Big Data Processing in the Transaction Monitoring Systems, in IV International Conference on "Information Technology and Nanotechnology, 24-27 April 2018, Samara, Russian Federation, 2018, S. 228.

Sauerland, Thomas, Die Verwaltungsvorschrift im System der Rechtsquellen, 2005, Berlin, zugl. Diss., Univ. Marburg, 2003.

Savigny, Eike von (Hrsg.), Ludwig Wittgenstein: philosophische Untersuchungen, 2. Aufl., Klassiker auslegen Bd. 13, 2011, Berlin.

Schantz, Peter, Rechtsschutz gegen die strategische Fernmeldeüberwachung: Ein „blinder Fleck" im Rechtsstaat? in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2015, 873.

Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht, Datenschutz-Grundverordnung und Bundesdatenschutzgesetz in der Praxis, 2017, München.

Scharrer, Jörg/Dalibor, Marcel/Fröhlich, Katja ua. (Hrsg.), Risiko im Recht - Recht im Risiko, 50. Assistententagung Öffentliches Recht ; Tagung der wissenschaftlichen Mitarbeiterinnen und Mitarbeiter, wissenschaftlichen Assistentinnen und Assistenten vom 23. bis 26. Februar 2010 in Greifswald, 2011, Baden-Baden.

Schatz, Andreas, Automatisierter Abruf von Kontoinformationen, in Bakaus, Julia/Kruse, Lars-Heiko/Schwerdtner, Cornelia (Hrsg.), Die "Zentrale Stelle" in Kreditinstituten, Anti-Financial Crime in der Praxis, 2019, S. 549.

Schatz, Andreas, Umsetzung der Geldtransferverordnung 2015/847, in Bakaus, Julia/Kruse, Lars-Heiko/Schwerdtner, Cornelia (Hrsg.), Die "Zentrale Stelle" in Kreditinstituten, Anti-Financial Crime in der Praxis, 2019, S. 525.

Schenke, Wolf-Rüdiger, Die Gesetzgebungskompetenz für die Strafverfolgungsvorsorge, in Stuckenberg, Carl-Friedrich/Gärditz, Klaus Ferdinand (Hrsg.), Strafe und Prozess im freiheitlichen Rechtsstaat, Festschrift für Hans-Ullrich Paeffgen zum 70. Geburtstag am 2. Juli 2015, 2015, S. 393.

Schenke, Wolf-Rüdiger, Polizeiliches Handeln bei Anscheinsgefahr und Gefahrverdacht, in Juristische Schulungn (JuS) 2018, 505.

Schenke, Wolf-Rüdiger/Graulich, Kurt/Ruthig, Josef (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl., Beck'sche Kurz-Kommentare, 2019, München (zit. als *Bearbeiter* in Sicherheitsrecht des Bundes).

Scherp, Dirk, Gesetze gegen die Geldwäsche und gegen die Finanzierung des ?, Terrorismuseine stille Verfassungsreform, in Wertpapier-Mitteilungen (WM) 2003, 1254.

Schiedermair, Stefanie, Der Schutz des Privaten als internationales Grundrecht, 2012, Tübingen, zugl. Habil., Univ. Mainz, 2011/2012.

Schild, Hans-Hermann, Anmerkung zu EuGH, Urteil vom 21.6.2022 – C-817/19 – Ligue des droits humains, in Zeitschrift für Datenschutz (ZD) 2022, 553.

Schily, Otto, Gesetze gegen die Geldwäsche und gegen die Finanzierung des Terrorismus, eine stille Verfassungsreform? in Wertpapier-Mitteilungen (WM)2003, 1249.

Schimansky, Herbert/Bunte, Hermann-Josef/Lwowski, Hans-Jürgen (Hrsg.), Bankrechts-Handbuch, 5. Aufl., 2017, München (zit. als *Bearbeiter* in Bankrechts-Hdb.)

Schlaich, Klaus/Korioth, Stefan, Das Bundesverfassungsgericht, Stellung, Verfahren, Entscheidungen: ein Studienbuch, 12. Aufl. 2021, München.

Schlegel, Stephan, Das Akteneinsichtsrecht des Beschuldigten im Strafverfahren, in Onlinezeitschrift für höchstrichterliche Rechtsprechung im Strafrecht (HRRS) 2004, 411.

Schlink, Bernhard, Abwägung im Verfassungsrecht, 1976, Berlin, zugl. Diss., Univ. Heidelberg, 1975.

Schlink, Bernhard, Das Nachrichtendienstliche Mittel, in Neue Juristische Wochenschrift (NJW) 1980, 552.

Schlink, Bernhard, Das Recht der Informationellen Selbstbestimmung, in Der Staat 1986, 233.

Schlink, Bernhard, Der Grundsatz der Verhältnismäßigkeit, in Badura, Peter/Dreier, Horst (Hrsg.), Festschrift 50 Jahre Bundesverfassungsgericht, 2001, S. 445.

Schmahl, Stefanie, Grundrechtsbindung der deutschen Staatsgewalt im Ausland, in Neue Juristische Wochenschrift (NJW) 2020, 2221.

Schmidbauer, Wilhelm/Steiner, Udo, Polizeiaufgabengesetz, Polizeiorganisationsgesetz, Kommentar, 5. Aufl., 2020, München (zit. als *Bearbeiter* in Schmidbauer/Steiner BayPAG).

Schmidt, Hubert (Hrsg.), COVID-19, Rechtsfragen zur Corona-Krise, 3. Aufl., Beck-Online Bücher, 2022, München.

Schmidt-Aßmann, Eberhard, Das allgemeine Verwaltungsrecht als Ordnungsidee, Grundlagen Und Aufgaben der Verwaltungsrechtlichen Systembildung, 2. Aufl. 2006, Dordrecht,

Schmidt-Bleibtreu, Bruno ua. (Hrsg). *Maunz, Theodor* (Begr.) Bundesverfassungsgerichtsgesetz, Kommentar, Stand- 61. EL 2021 (zit. als *Bearbeiter* in Schmidt-Bleibtreu/Klein/Betghe BVerfGG).

Schnabel, Christoph, Das „Mikado-Prinzip", in Datenschutz und Datensicherheit (DuD) 2007, 426.

Schnabl, Robert, Kapitel 6. Geldwäsche, in Bannenberg, Britta/Wabnitz, Heinz-Bernd/Janovsky, Thomas/Schmitt, Lothar/Bär, Wolfgang/Beck, Siegfried (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 5. Aufl. 2020.

Schnarr, Karl Heinz, Zur Verknüpfung von Richtervorbehalt, staatsanwaltschaftlicher Eilanordnung und richterlicher Bestätigung, in Neue Zeitschrift für Strafrecht (NStZ) 1991, 209.

Schneider, Franziska, Die Hypothetische Datenneuerhebung – Begriff ohne Konzept, in Zeitschrift für das gesamte Sicherheitsrecht (GSZ) 2022, 1.

Schneider, Franziska, Kernbereich privater Lebensgestaltung, in Juristische Schulung (JuS) 2021, 29.

Schneider, Jens-Peter, Stand und Perspektiven des Europäischen Datenverkehrs- und Datenschutzrechts, in Die Verwaltung 2011, 499.

Schnieders, Ralf, Anmerkung zu BVerfG, Beschl. v. 18.12.2018 – 1 BvR 142/15, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2019, 381.

Schober, Patrice, Das „Mysterium" der Aufbewahrungspflichten – Hier finden Sie die Antworten in 45 Minuten, in Zeitschrift für Bilanzierung, Rechnungswesen & Controlling (BC) 2013, 528.

Schoch, Friedrich, Abschied vom Polizeirecht des liberalen Rechtstaats? Vom Kreuzberg-Urteil des Preußischen Oberverwaltungsgerichts zu den Terrorismusbekämpfunsggesetzen unserer Tage, in Der Staat 2004, 347.

Schoch, Friedrich, Besonderes Verwaltungsrecht, 2018, München.

Schoch, Friedrich, Das Recht auf Informationelle Selbstbestimmung, in Juristische Ausbildung (JURA) 2008, 352.

Schoch, Friedrich, Der Prüfungs- und Entscheidungsmaßstab im Normenkontroll-Eilverfahren, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2022, 1.

Schoch, Friedrich, Der verfassungsrechtliche Schutz des Fernmeldegeheimnisses (Art. 10 GG), in Juristische Ausbildung (JURA) 2011, 194.

Schoch, Friedrich, Die Ambivalenz von Freiheit und Sicherheit, in Gander, Hans-Helmuth/Perron, Walter/Poscher, Ralf/Riescher, Gisela/Würtenberger, Thomas (Hrsg.), Resilienz in der offenen Gesellschaft, Symposium des Centre for Science and Security, 2012, S. 63.

Schoch, Friedrich/Schneider, Jens-Peter – Verwaltungsrecht - VwGO, Kommentar, Stand: August 2022, München (zit. als *Bearbeiter* in Schoch/Schneider VerW).

Schomburg, Wolfgang/Lagodny, Otto (Hrsg), Internationale Rechtshilfe in Strafsachen, = International cooperation in criminal matters, 6. Aufl., 2020, München (zit. als *Bearbeiter* in Schomburg/Lagodny Int. Rechtshilfe in Strafsachen).

Schönke, Adolf/Schröder, Horst (Begr.), *Eser/Albin* (Hrsg.), Strafgesetzbuch, Kommentar, 2019, München (zit. als *Bearbeiter* in Schönke/Schröder StGB).

Schramm, Marc/Shvets, Iryna, Verkehrsdaten zwischen ePrivacy-RL und ePrivacy-VO, Nutzung von TK-Diensten und personalisierter Werbung, in Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR) 2019, 568.

Schubert, Peter, Das neue Geldwäschegesetz – Versuch einer ersten Annäherung aus Sicht des rechtlichen Beraters und Kautelarjuristen – Teil 1, in Neue Juristische Online Zeitschrift (NJOZ) 2018, 41.

Schünemann, Bernd, Die großen wirtschaftsstrafrechtlichen Fragen der Zeit, in Goltdammer's Archiv für Strafrecht (GA) 2013, 191.

Schünemann, Bernd, Verfassungsrechtliche Vorgaben für die Struktur des Strafverfahrens, in Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltsvereins (Hrsg.), Strafverteidigung im Rechtsstaat, 25 Jahre Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins, 2009, S. 827.

Schuppert, Gunnar Folke/Merkel, Wolfgang/Nolte, Georg ua. (Hrsg.), Der Rechtsstaat unter Bewährungsdruck, Schriften zur Governance-Forschung Bd. 20, 2010, Baden-Baden.

Schuster, Leo, Die Verantwortung der Banken bei der Geldwäsche, 1994, Regensburg.

Schwabenbauer, Thomas, Heimliche Grundrechtseingriffe, Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, 2013, Tübingen, zugl. Diss., Univ. München 2012/2013.

Schwabenbauer, Thomas, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Teil I, in Bäcker, Matthias/Denninger, Erhard/Graulich, Kurt (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr - Strafverfolgung - Rechtsschutz, 7. Aufl., 2021, München.

Schwark, Eberhard/Zimmer, Daniel (Hrsg.), Kapitalmarktrechts-Kommentar, Börsengesetz mit Börsenzulassungsverordnung, Wertpapierprospektgesetz, Verkaufsprospektgesetz mit Vermögensanlagen-Verkaufsprospektverordnung, Wertpapierhandelsgesetz, Wertpapiererwerbs- und Übernahmegesetz, 4. Aufl., 2010, München (zit. als *Bearbeiter* in Schwark/Zimmer, KMRK, 4. Aufl. 2010).

Schwarze, Jürgen; Becker, Ulrich; Hatje, Armin; Schoo, Johann, EU-Kommentar, 4. Aufl., 2019, Baden-Baden, (zit. als *Bearbeiter* in Schwarze/Becker/Hatje/Schoo, EU-Recht).

Schweighofer, Erich/Kummer, Franz/Hötzendorfer, Walter (Hrsg.), Transparenz, Tagungsband des 17. Internationalen Rechtsinformatik Symposions; IRIS 2014; 20. bis 22, Februar 2014, Universität Salzburg = Transparency, booksocg.at Bd. 302, 2014.

Sciurba, Michele, The incompatibility of global anti-money laundering regimes with human and civil rights, Reform needed?, 2019, Baden-Baden.

Seedorf, Sebastian, Der Grundsatz der Verhältnismäßigkeit bei der Gesetzgebung, in Jestaedt, Matthias/Lepsius, Oliver (Hrsg.), Verhältnismäßigkeit, Zur Tragfähigkeit eines verfassungsrechtlichen Schlüsselkonzepts, 2021, S. 129.

SEON, Top 14 Anti Money Laundering (AML) Software & Tools 2023, https://seon.io/resources/comparisons/aml-software-tools/, zuletzt zugegriffen am 08.08.2023

Seyr, Sibylle, Der effet utile in der Rechtsprechung des Europäischen Gerichtshofs, 2008, Berlin, zugl. Diss., Univ. Göttingen, 2006/2007.

Shaugnessy, Patricia, The New EU Money-Laundering Directive: Lawyers as Gate-Keepers and Whistle-Blowers, in Law and Policy in International Business 2002, 25.

Shin, Sangwoo, Bank- und kapitalmarktrechtliche Organisationspflichten, Ein Vergleich des deutschen und koreanischen Rechts, 2013, Baden-Baden, zugl. Diss., Univ. Halle-Wittenberg 2012.

Sichtermann, Siegfried, Bankgeheimnis und Bankauskunft, systematische Darstellung mit besonderer Berücksichtigung der Rechtsprechung und unter Heranziehung ausländischen Rechts, 2. Aufl. 1966, Frankfurt (Main).

Siclari, Domenico (Hrsg.), The New Anti-Money Laundering Law, 2016, Cham.

Sieber, Ulrich, Compliance-Programme im Unternehmensstrafrecht, in Sieber, Ulrich/Dannecker, Gerhard/Kindhäuser, Urs/Vogel, Joachim/Walter, Tonio (Hrsg.), Strafrecht und Wirtschaftsstrafrecht, Dogmatik, Rechtsvergleich, Rechtstatsachen ; Festschrift für Klaus Tiedemann zum 70. Geburtstag, 2008, S. 449.

Sieber, Ulrich, Informationsrecht und Recht der Informationstechnik, Die Konstituierung eines Rechtsgebietes in Gegenstand, Grundfragen und Zielen, in Neue Juristische Wochenschrift (NJW) 1989, 2569.

Sieber, Ulrich, Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt, Eine Analyse der Vorfeldtatbestände im „Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten, in Neue Zeitschrift für Strafrecht (NStZ) 2009, 353.

Sieber, Ulrich, Straftaten und Strafverfolgung im Internet, Gutachten C zum 69. Deutschen Juristentag, 2012, München.

Sieber, Ulrich/Dannecker, Gerhard/Kindhäuser, Urs ua. (Hrsg.), Strafrecht und Wirtschaftsstrafrecht, Dogmatik, Rechtsvergleich, Rechtstatsachen ; Festschrift für Klaus Tiedemann zum 70. Geburtstag, 2008, Köln

Simitis, Spiros, Die informationelle Selbstbestimmung, Grundbedingung einer verfassungskonformen Informationsordnung, in Neue Juristische Wochenschrift (NJW) 1984, 398.

Simitis, Spiros, Übermittlung der Daten von Flugpassagieren in die USA: Dispens vom Datenschutz?, in Neue Juristische Wochenschrift (NJW) 2006, 2011.

Simitis, Spiros/Hornung, Gerrit/Spiecker Döhmann, Indra ua. (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, 2019, Baden-Baden (zit. als *Bearbeiter* in Simitis/Hornung/Spieker Datenschutzrecht).

Singelnstein, Tobias, Informationelle Selbstbestimmung und Sachverhaltserforschung im Ermittlungsverfahren, verfassungsrechtliche Anforderungen an Datenerhebung und Datenverarbeitung, in Barton, Stephan/Kölbel, Ralf/Lindemann, Michael (Hrsg.), Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens, 2015, S. 251.

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen, - Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, in Neue Zeitschrift für Strafrecht (NStZ) 2012, 593.

Singelnstein, Tobias, Strafprozessuale Verwendungsregelungen zwischen Zweckbindungsgrundsatz und Verwertungsverboten. Voraussetzungen der Verwertung von Zufallsfunden und sonstiger zweckentfremdender Nutzung personenbezogener Daten im Strafverfahren seit dem 1. Januar 2008, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW) 2008, 854.

Skyrius, Rimvydas/Giriūnienė, Gintarė/Katin, Igor/Kazimianec, Michail/Žilinskas, Raimundas, The Potential of Big Data in Banking, in Srinivasan, S. (Hrsg.), Guide to Big Data Applications, 2018, S. 451.

Sölch, Otto, *Ringleb/Karl* (Begr.), *Treiber, Andreas* (Hrsg.), Umsatzsteuergesetz, Kommentar, Stand: 88. EL 2020, München (zit. als *Bearbeiter* in Sölch/Ringleb UStG).

Son, Jae-Young, Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, 2006, Berlin, zugl. Diss., Univ. Mannheim, 2005.

Sotiriadis, Georgios, Die Entwicklung der Gesetzgebung über Gewinnabschöpfung und Geldwäsche, Unter Berücksichtigung der jeweiligen kriminalpolitischen Tendenzen, 2010, Berlin, zugl. Diss., Univ. Bremen, 2008.

Sotiriadis, Georgios/Heimerdinger, Dominik, Die Umsetzung der 3. EG-Geldwäscherichtlinie und ihre Bedeutung für die Finanzwirtschaft, in Zeitschrift für Bank- und Kapitalmarktrecht 2009, 234.

SPD/Bündnis 90/Die Grünen/FDP, Mehr Fortschritt wagen, Bündnins für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag 2021-2025. 2021, https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf., zuletzt zugegriffen am 08.08.2023.

Specht, Louisa/Mantz, Reto (Hrsg.), Handbuch europäisches und deutsches Datenschutzrecht, Bereichsspezifischer Datenschutz in Privatwirtschaft und öffentlichem Sektor, 2019, München (zit. als *Bearbeiter* in Hdb. Europ. & Deutsches Datenschutzrecht).

Spiecker gen. Döhmann, Indira/Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, Tübingen.

Spielmann, Christoph, Konkurrenz von Grundrechtsnormen, 2008, Tübingen, zugl. Diss., Univ. Münster, 2007.

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien, Kommentar, 4. Aufl., 2019, München (zit. als *Bearbeiter* in Spindler/Schuster Elektronische Medien, 4. Aufl. 2019).

Spoerr, Wolfgang/Roberts, Marc, Die Umsetzung der Vierten Geldwäscherichtlinie: Totale Transparenz, Geldwäschebekämpfung auf Abwegen? in Wertpapier-Mitteilungen (WM) 2017, 1142.

Srinivasan, S. (Hrsg.), Guide to Big Data Applications, 2018, Cham.

Stackowiak, Robert/Mantha, Venu/Licht, Art/Khanna, Ambreesh, Big Data in Financial Services and Banking Oracle Corp., 2015, https://de.scribd.com/document/362910285/big-data-in-financial-services-wp-2415760-pdf, zuletzt zugegriffen am 08.08.2023.

Starnecker, Tobias, Videoüberwachung zur Risikovorsorge, Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse, 2017, Berlin, zugl. Diss., Univ. Passau, 2016.

Stavros, Stephanos, The Guarantees for Accused Persons under Article 6 of the European Convention on Human Rights, An Analysis of the Application of the Convention and a Comparison with Other Instruments, 1993, Boston.

Steenwijk, Peter, A Balanced Package: Fighting Money Laundering with the 4th European Directive, in Zwaan, Jaap de/Lak, Martijn/Makinwa, Abiola/Willems, Piet (Hrsg.), Governance and Security Issues of the European Union, Challenges Ahead, 2016, S. 209.

Stefanou, Constantin/Xanthaki, Helen, The New EU Draft Money Laundering Directive: A Case of Inter-Institutional Synergy, in 3 Journal of Money Laundering Control (J. of Money Laundering Control) 2000, 325.

Stern, Klaus, Das Staatsrecht der Bundesrepublik Deutschland, 1994, München .

Stern, Klaus/Sachs, Michael (Hrsg.), Europäische Grundrechte-Charta, GRCh, Kommentar, 2016 (zit. als *Bearbeiter* in Stern/Sachs EU-GRC).

Stern, Klaus/Sodan, Helge/Möstl, Markus (Hrsg.), Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl., 2022, München (zit. als *Bearbeiter* in Stern/Sodan/Möstl Staatsrecht, Bd.).

Stief, Matthias, Die Richtlinie (EU) 2016/680 zum Datenschutz in der Strafjustiz und die Zukunft der datenschutzrechtlichen Einwilligung im Strafverfahren in Strafverteidiger (StV) 2017, 470.

Streinz, Rudolf/Michl, Walther (Hrsg.), EUV/AEUV, Vertrag über die Europäische Union, Vertrag über die Arbeitsweise der Europäischen Union, Charta der Grundrechte der Europäischen Union, Kommentar, 3. Aufl., 2018 (zit. als *Bearbeiter* in Streinz EUV/AEUV).

Stuckenberg, Carl-Friedrich/Gärditz, Klaus Ferdinand (Hrsg.), Strafe und Prozess im freiheitlichen Rechtsstaat, Festschrift für Hans-Ullrich Paeffgen zum 70. Geburtstag am 2. Juli 2015, Schriften zum Strafrecht v.280, 2015, München.

Stumpf, Cordula/Kainer, Friedemann/Baldus, Christian (Hrsg.), Privatrecht, Wirtschaftsrecht, Verfassungsrecht, Privatinitiative und Gemeinwohlhorizonte in der europäischen Integration, 2015, Baden-Baden.

Svedberg Helgesson, Karin/Mörth, Ulrika (Hrsg.), Securitization, accountability and risk management, Transforming the public security domain, PRIO new security studies Bd. 10, 2012, London/New York.

Sydow, Gernot. (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. Aufl., 2021, Baden-Baden (zit. als *Bearbeiter* in Sydow DSGVO).

Szuba, Dorothee, Vorratsdatenspeicherung, Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, 2011, Baden-Baden, zugl. Diss., Univ. Frankfurt (Main), 2011.

Taeger, Jürgen/Gabel, Detlef DSGVO - BDSG, Kommentar, 4. Aufl.,2021 (zit. als *Bearbeiter* in Taeger/Gabel DSGVO - BDSG).

Tanneberger, Steffen, Die Sicherheitsverfassung, Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts. Zugleich ein Beitrag zu einer induktiven Methodenlehre, 2014, Tübingen, zugl. Diss., Univ. Freiburg, 2013.

Thiel, Markus, Die Entgrenzung der Gefahrenabwehr, Grundfragen von Freiheit und Sicherheit im Zeitalter der Globalisierung, 2012, Tübingen, zugl. Habil., Univ. Düsseldorf, 2009/2010.

Thönnes, Christian, A Directive altered beyond recognition, On the Court of Justice of the European Union's PNR decision (C-817/19) 2022, https://verfassungsblog.de/pnr-recognition/, zuletzt zugegriffen am 08.08.2023.

Thönnes, Christian, Fluggastdatenspeicherung: Die Zukunft von Vorratsdatenspeicherung und automatisierter Verdachtsgenerierung, in Die Verwaltung 2022, 527.

Timan, Tjerk/Galič, Maša/Koops, Bert-Jaap, Surveillance Theory and its Implications for Law, in Brownsword, Roger/Scotford, Eloise/Yeung, Karen (Hrsg.), The Oxford handbook of law, regulation and technology, 2017, S. 731.

Tolani, Madelaine, Existiert in Deutschland ein Bankgeheimnis? - Das Bankgeheimnis gegenüber dem Staat unter Berücksichtigung der jüngsten gesetzlichen Veränderungen, in Zeitschrift für Bank- und Kapitalmarktrecht (BKR) 2007, 275.

Tonnara, Pierluigi, Risk Assesment, in Siclari, Domenico (Hrsg.), The New Anti-Money Laundering Law, 2016, S. 57.

Tracol, Xavier, Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it, in 6 Computer Law & Security Review 2014, 736.

Treppmann, Helmut, Archivierung von Geschäftsunterlagen, Rationalisierung und Aufbewahrungspflichten gem. HGB im Spannungsverhältnis?, in Der Betrieb (DB) 1989, 1482.

Trüg, Gerson, Beweisantrag auf Verlesung eines E-Mail-Ausdrucks als präsentes Beweismittel, in Strafverteidiger (StV) 2016, 343.

Trute, Hans-Heinrich, Der Schutz personenbezogener Informationen in der Informationsgesellschaft, in Juristenzeitung (JZ) 1998, 822.

Trute, Hans-Heinrich, Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, in Die Verwaltung 2009, 85.

Tschohl, Christoph/Scheucher, Ewald/Kargl, Dieter/Luksan, Julia/Czadilek, Alexander/Waloschek, Herbert/Kreissl, Reinhard/Klinger, Kilian/Hötzendorfer, Walter/Möchel, Erich, HEAT – Handbuch zur Evaluation der-Anti-Terror-Gesetze, epicenter.works, 2016, https://epicenter.works/sites/default/files/heat_v1.2.pdf, zuletzt zugegriffen am 08.08.2023.

Tuba, Maphuti/van der Westhuizen, Chinelle, An analysis of the 'know your customer' policy as an effective tool to combat money laundering: is it about who or what to know that counts?, in 4 International Journal of Public Law and Policy (Int. J. of Public Law and Policy)2014, 53.

Turner, David/Schroeck, Michael/Shockley, Rebecca, Analytics: The real-world use of big data in financial services, IBM Institute for Business Value; Saïd Business School at the University of Oxford, 2013, https://www.ibm.com/downloads/cas/E4BWZ1PY, zuletzt zugegriffen am 08.08.2023.

Tzanou, Maria/Karyda, Spyridoula, Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga? in 28 European Public Law 2022, 123.

Unger, Brigitte (Hrsg.), Research handbook on money laundering, 2013, Cheltenham.

Unterreitmeier, Johannes, Es ist wieder da – das „informationelle Trennungsprinzip", in Die Öffentliche Verwaltung (DÖV) 2021, 659.

Vahle, Jürgen, Polizeiliche Aufklärungs- und Observationsmaßnahmen, (unter Berücksichtigung der Tätigkeit des Verfassungsschutzes), 1983, Diss., Uni. Bielefeld, 1983.

Vainio, Niklas/Miettinen, Samuli, Telecommunications data retention after Digital Rights Ireland : legislative and judicial reactions in the Member States, in 23 International Journal of Law and Information Technology (Int. J. of Law and Information Technology) 2015, 290.

van Ooyen, Robert Chr./Möllers, Martin H. W. (Hrsg.), Handbuch Bundesverfassungsgericht im politischen System, 2015, Wiesbaden.

Vassilaki, Irini, Heimliche Beschlagnahme von digital gespeicherten Informationen, Auf dem Weg zu einer neuen Ermittlungsmaßnahme, in Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR) 2022, 103.

Verhage, Antoinette, Supply and demand: anti-money laundering by the compliance industry, in 12 Journal of Money Laundering Control (J. of Money Laundering Control) 2009, 371.

Villalón, 12.12.2013 – C-293/12.

Vogel, Benjamin, Conclusions and Recommendations, in Vogel, Benjamin/Maillart, Jean-Baptiste (Hrsg.), National and international anti-money laundering law. Rethinking the architecture of criminal justice, regulation and data protection, 2020, S. 881.

Vogel, Benjamin, The Anti-Money Laundering Architecture of Germany, in Vogel, Benjamin/Maillart, Jean-Baptiste (Hrsg.), National and international anti-money laundering law. Rethinking the architecture of criminal justice, regulation and data protection, 2020, S. 157.

Vogel, Benjamin/Maillart, Jean-Baptiste (Hrsg.), National and international anti-money laundering law. Rethinking the architecture of criminal justice, regulation and data protection, 2020, Mortsel.

Vogelgesang, Klaus, Grundrecht auf informationelle Selbstbestimmung?, 1987, Baden-Baden, zugl.: Diss. Univ. Göttingen, 1986/1987.

Volkmann, Uwe, Anmerkung, in Juristenzeitung (JZ) 2006, 918.

Volkmann, Uwe, Prävention durch Verwaltungsrecht: Sicherheit, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2022, 1408.

Vollmuth, Eva-Maria, Die Geldwäscheprävention in den Instituten der Finanzbranche als integraler Bestandteil ihres Compliance-Management-Systems, 2020, Baden-Baden, zugl. Diss., Univ. Würzburg, 2020.

Voßkuhke, Andreas, „Regulierte Selbstregulierung", Zur Karriere eines Schlüsselbegriffs*, in Grimm, Dieter (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, 2001, S. 197.

Voßkuhke, Andreas/Kaiser, Anna-Bettina, Grundwissen – Öffentliches Recht: Funktionen der Grundrechte, in Juristische Schulung (JuS) 2011, 411.

Wägenbaur, Bertrand, Der zweite Feldzug gegen die Geldwäsche, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2002, 293.

Wahlers, Kristin, Die rechtliche und ökonomische Struktur von Zahlungssystemen inner- und außerhalb des Bankensystems, 2013, Heidelberg, zugl. Diss. Univ. Hamburg, 2012.

Walden, Marcus, Zweckbindung und -änderung präventiv und repressiv erhobener Daten im Bereich der Polizei, 1996, Berlin, zugl. Diss., Univ. Freiburg, 1996.

Weber, Kathrin, Die Sicherung rechtsstaatlicher Standards im modernen Polizeirecht, Eine Untersuchung neuartiger Standardmaßnahmen unter besonderer Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts, 2011, Frankfurt (Main), zugl. Diss., Univ. Gießen, 2010.

Weber-Dürler, Béatrice/Kokott, Juliane/Vesting, Thomas (Hrsg.), Die Staatsrechtslehre und die Veränderung ihres Gegenstandes, Konsequenzen von Europäisierung und Internationalisierung; Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Hamburg vom 1. bis 4. Oktober 2003, VVDStRL Bd. 63, 2004, Berlin.

Wegner, Carsten, Die Reform der Geldwäsche-Richtlinie und die Auswirkungen auf rechtsberatende Berufe, in Neue Juristische Wochenschrift (NJW) 2002, 794.

Weichert, Thilo, Wider das Verbot mit Erlaubnisvorbehalt im Datenschutz?, in Datenschutz und Datensicherheit (DuD) 2013, 246.

Weidemann, Matthias, Aussageverweigerung bei Vernehmung durch Polizeibeamte als Strafvereitelung? in Juristische Ausbildung (JURA) 2008, 532.

Weiß, Wolfgang, Grundrechtsschutz durch den EuGH, Tendenzen seit Lissabon, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2013, 287.

Weißer, Bettina, Der »Kampf gegen den Terrorismus« – Prävention durch Strafrecht? in Juristenzeitung (JZ) 2008, 388.

Weisser, Niclas-Frederic, Der Richtervorbehalt im Nachrichtendienstrecht, in Die Öffentliche Verwaltung (DÖV) 2014, 831.

Welsing, Ruth, Das Recht auf informationelle Selbstbestimmung im Rahmen der Terrorabwehr, Darstellung anhand einer Untersuchung der präventiven Rasterfahndung,2009, Hamburg zugl. Diss., Univ. Marburg, 2008/2009.

Wendel, Mattias, Europäischer Grundrechtsschutz und nationale Spielräume: Grundlagen und Grundzüge eines Spielraumtests im europäischen Grundrechtspluralismus, in Europarecht 2022, 327.

Wendel, Mattias, Wider die Mär vom Grundrechtsblinden: Der EuGH und die Vorratsdatenspeicherung, Verfassungsblog 09.04.2014, https://verfassungsblog.de/wider-maer-vom-grundrechtsblinden-eugh-und-vorratsdatenspeicherung/, zuletzt zugegriffen am 08.08.2023.

Wennerberg, Hjalmar, 3 Der Begriff der Familienähnlichkeit in Wittgensteins Spätphilosophie, in Savigny, Eike von (Hrsg.), Ludwig Wittgenstein: philosophische Untersuchungen, 2. Aufl. 2011, S. 33.

Werner, Gerhard, Bekämpfung der Geldwäsche in der Kreditwirtschaft, 1996, Freiburg, zugl.: Diss. Univ. Freiburg., 1995,

Weßlau, Edda, Vorfeldermittlungen, Probleme der Legalisierung »vorbeugender Verbrechensbekämpfung« aus strafprozeßrechtlicher Sicht, 1989, Berlin, zugl. Diss., Univ. Hamburg, 1988.

Westermeier, Carola, Money is data – the platformization of financial transactions, in 23 Information, Communication & Society 2020, 2047.

Westphal, Dietrich, Die Richtlinie zur Vorratsspeicherung von Verkehrsdaten – Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der „Post-911-Informationsgesellschaft", in Europarecht (EuR) 2006, 706.

Westphal, Dietrich, Leitplanken für die Vorratsdatenspeicherung – Abrücken von „Solange", Das Urteil des BVerfG vom 2. 3. 2010, in Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2010, 494.

Wetzling, Thorsten/Vieth, Kilian, Massenüberwachung bändigen, Gute Rechtsnormen und innovative Kontrollpraxis im internationalen Vergleich, Stiftung Neue Verantwortung, 2019, https://www.stiftung-nv.de/de/publikation/massenueberwachung-baendigen-gute-rechtsnormen-und-innovative-kontrollpraxis-im, zuletzt zugegriffen am 08.08.2023.

Widmaier, Gunter, Der automatisierte Abruf von Kontostammdaten in der Kritik und in der praktischen Anwendung, in Wertpapier-Mitteilungen (WM) 2006, 116.

Will, Rosemarie, Anlass und Folgen eines Routineverkehre, Gutachtens. Zu den Rechtsbindungen des BND bei der strategischen Telekommunikationsüberwachung der sogenannten, in Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand (Hrsg.), Sicherheitsverfassung – Sicherheitsrecht, Festgabe für Kurt Graulich zum 70. Geburtstag, 2019, S. 207.

Wimmers, Jörg/Heymann, Britta, Zum Referentenentwurf eines Netzwerkdurchsetzungsgesetzes (NetzDG) – eine kritische Stellungnahme, in Zeitschrift für Medien- und Kommunikationsrecht (AfP) 2017, 93.

Winkler, Daniela, Der „additive Grundrechtseingriff": Eine adäquate Beschreibung kumulierender Belastungen?, in Juristische Ausbildung (JURA) 2014, 881.

Wissenschaftliche Dienste des Bundestags, Die Umsetzung der Vorgaben des Bundesverfassungsgerichts zur Vorratsdatenspeicherung durch den Gesetzentwurf der Bundesregierung vom 27. Mai 2015, Deutscher Bundestag, WD 3 - 3000 - 108/15, 2015, https://www.bundestag.de/resource/blob/405516/3e022415be167538b39ea8f0396003 70/wd-3-108-15-pdf-data.pdf, zuletzt zugegriffen am 08.08.2023.

Wissenschaftliche Dienste des Bundestags, Titel: Das Urteil des Europäischen Gerichtshofs vom 21. Juni 2022 zur Auslegung der PNR-Richtlinie: Auswirkungen auf das Fluggastdatengesetz und dessen Auswirkungen auf das Fluggastdatengesetz und dessen Anwendung, Deutscher Bundestag, WD 3 - 3000 - 100/22, 2022, https://www.bundestag.de/resource/blob/906594/ca5eb21ee26acfbf0189b1428dddf3e3/WD-3-100-22-pdf-data.pdf, zuletzt zugegriffen am 08.08.2023.

Wissenschaftliche Dienste des Bundestags, Zu möglichen erweiterten Befugnissen der Nachrichtendienste bei der Überwachung von „Finanzströmen", Deutscher Bundestag, WD 3 - 3000 - 040/19, 2019, https://www.bundestag.de/resource/blob/645672/a002254b01fl1cdd9c3eaf2d3723dcc4/WD-3-040-19-pdf-data.pdf, zuletzt zugegriffen am 08.08.2023.

Wissenschaftliche Dienste des Bundestags, Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht, Deutscher Bundestag, WD 3 - 282/06, 2006, https://www.bundestag.de/resource/blob/413200/f5536b8536ef1e1d78716cf912 48fac5/WD-3-282-06-pdf-data.pdf, zuletzt zugegriffen am 08.08.2023.

Wittgenstein, Ludwig, Philosophische Untersuchungen, 1971, Frankfurt am Main.

Wolf, Joachim, Die Kompetenz der Verwaltung zur "Normsetzung" durch Verwaltungsvorschriften, in Die Öffentliche Verwaltung (DÖV) 1992, 849.

Wolff, Heinrich Amadeus, Das Urteil des Bundesverfassungsgerichts zum BKA-Gesetz, in Zeitschrift für Gesetzgebung (ZG) 2016, 361.

Wolff, Heinrich Amadeus, Die Grenzverschiebung von polizeilicher und nachrichtendienstlicher Sicherheitsgewährleistung, in Die Öffentliche Verwaltung (DÖV) 2009, 597.

Wolff, Heinrich Amadeus, Vorratsdatenspeicherung, Der Gesetzgeber gefangen zwischen Europarecht und Verfassung?, in Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2010, 751.

Wolff, Heinrich Amadeus/Brink, Stefan, Beck'scher Online-Kommentar Datenschutzrecht, 34. Edition, Stand 01.11.2020 (zit. als *Bearbeiter* in BeckOK Datenschutzrecht).

Wollenschläger, Ferdinand, Schriftliche Stellungnahme, Öffentliche Anhörung des Innenausschusses am 24.4.2017, Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG)" (BT-Drs. 18/11501), 2017.

Wollenschläger, Ferdinand/Krönke, Lukas, Telekommunikationsüberwachung und Verkehrsdatenspeicherung, eine Frage des EU-Grundrechtsschutzes?, in Neue Juristische Wochenschrift (NJW) 2016, 906.

Wonka, Julia, Die Rechtmäßigkeit staatlicher Auskunftsersuchen gegenüber Banken, in Neue Juristische Wochenschrift (NJW) 2017, 3334.

Wright, David/Kreissl, Reinhard (Hrsg.), Surveillance in Europe, 2015, London/New York.

Würtenberger, Thomas, Entwicklungslinien des Sicherheitsverfassungsrechts, in Ruffert, Matthias/Schröder, Meinhard (Hrsg.), Dynamik und Nachhaltigkeit des Öffentlichen Rechts, Festschrift für Professor Drth Meinhard Schröder zum 70. Geburtstag, 2012, S. 285.

Zalnieriute, Monika, A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union, in 85 The Modern Law Review (Modern Law Rev) 2022, 198.

Zentes, Uta/Glaab, Sebastian (Hrsg.), GwG, Geldwäschegesetz, Kommentar, 2. Aufl., 2020 (zit. als *Bearbeiter* in Zentes/Glaab GwG).

Zentes, Uta/Glaab, Sebastian, Referentenentwurf zur Umsetzung der 4. EU Geldwäscherichtlinie, - Was kommt auf die Verpflichteten zu?, in Betriebs-Berater (BB) 2017, 67.

Zentraler Kreditausschuss, Stellungnahme des Zentralen Kreditausschusses zum Regierungsentwurf eines Gesetzes zur weiteren Fortentwicklung des Finanzplatzes Deutschlandes, 13. Februar 2002, https://die-dk.de/media/files/020213_ZKA-Stn_Regierungsentwurf.pdf, zuletzt zugegriffen am 08.08.2023.

Ziegenhorn, Gero, Der Einfluss der EMRK im Recht der EU-Grundrechtecharta, Genuin chartarechtlicher Grundrechtsschutz gemäß Art. 52 Abs. 3 GRCh, 2009, Berlin, zugl. Diss., Univ. Bonn, 2007/2008.

Zöller, Mark A., Der Rechtsrahmen für die Übermittlung personenbezogener Daten unter Beteiligung der Nachrichtendienste, in Dietrich, Jan-Hendrik/Gärditz, Klaus Ferdinand/Graulich, Kurt/Gusy, Christoph/Warg, Gunter (Hrsg.), Nachrichtendienste im demokratischen Rechtsstaat, Kontrolle – Rechtsschutz – Kooperationen, 2018, S. 185.

Zöller, Mark A., Heimliche und verdeckte Ermittlungsmaßnahmen im Strafverfahren, in Zeitschrift für die gesamte Strafrechtswissenschaft (ZStW)2012, 411.

Zöller, Mark A., Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz, 2002, Heidelberg, Zugl.: Diss., Univ. Mannheim 2001.

Zubik, Marek/Podkowik, Jan/Rybski, Robert (Hrsg.), European Constitutional Courts towards Data Retention Laws, Springer eBook Collection Bd. 45, 2021, Cham.

Zubrod, Andreas, Automatisierter Abruf von Kontoinformationen nach § 24c KWG, Rechtliche Voraussetzungen und Grenzen, in Wertpapier-Mitteilungen (WM) 2003, 1210.

Zuck, Rüdiger, Geldwäsche: Die verfassungswidrige Indienstnahme des Rechtsanwalts für die Zwecke der Strafverfolgung, in Neue Juristische Wochenschrift (NJW) 2002, 1397.

Zurawski, Nils (Hrsg.), Surveillance Studies, Perspektiven eines Forschungsfeldes, 2007, Opladen.

Zurawski, Nils, Einleitung: Surveillance Studies. Perspektiven eines Forschungsfeldes, in Zurawski, Nils (Hrsg.), Surveillance Studies, Perspektiven eines Forschungsfeldes, 2007, S. 7.

Zwaan, Jaap de/Lak, Martijn/Makinwa, Abiola ua. (Hrsg.), Governance and Security Issues of the European Union, Challenges Ahead, 2016, The Hague.