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.

I. 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 „*1.)*

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.