Kapitel F: Diskussion der massenhaften Speicherung und Nutzung von Finanzdaten zu sicherheitsrechtlichen Zwecken

Über die Speicherung von Finanzdaten, deren Verwendung bei den Instituten und den Zugriff der Sicherheitsbehörden auf diese Daten wird bereits seit geraumer Zeit diskutiert (zur Gesetzeshistorie oben Kap. D. III. 2. a.) Die jeweiligen Änderungen an den entsprechenden Gesetzen wurden fachbereichsübergreifend sowohl im banken- als auch im sicherheitsrechtlichen Kontext kommentiert.

Dabei wurden immer wieder verfassungs- und europarechtliche Zweifel gegenüber der Bestandsdatenspeicherung und dem Geldwäscherecht erhoben. In diese Kritik wird sich diese Arbeit einreihen und die jüngsten strukturellen und konkreten Entwicklungen des Sicherheitsverfassungsrechts ergänzen (s. Kap. G).

Da sie insofern an Vorarbeiten bzw. frühere Kritiken anschließt und nicht in Anspruch nehmen will, erstmals allgemeine rechtliche Zweifel an den geldwäscherechtlichen Überwachungsmaßnahmen zu formulieren, soll die historische Diskussion über die verschiedenen Speicherpflichten und Zugriffsrechte im Anti-Geldwäscherecht in vollem Umfang chronologisch dargestellt und kommentiert werden.

I. Kontobestandsdaten

Zunächst soll die Diskussion über die Bestandsdatenauskunft nach § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO dargestellt werden. Anders als bzgl. der Speicherung von Kontoinhaltsdaten hat das BVerfG hierzu bereits in einem Beschluss aus dem Jahr 2007 Stellung bezogen.[1274] Diese Rechtsprechung soll für die Darstellung der Kommentierung als Anker dienen. Die folgenden Abschnitte sind daher chronologisch in die Zeit bis zum Beschluss und jener danach aufgeteilt.

1274 BVerfGE 118, 168 – Kontostammdaten

1. Diskussion bis zur Klärung durch das BVerfG

§ 24c KWG war gleich bei seiner Einführung und in den unmittelbar darauffolgenden Jahren auf breite Kritik aus verschiedenen Fach- und Rechtsbereichen gestoßen. Die Beeinträchtigung der informationellen Selbstbestimmung durch die Bestandsdatenabfrage sah bereits der Bundesrat kritisch.[1275] In seiner Stellungnahme zum Regierungsentwurf stellte er den Umfang der zu speichernden Daten und das Fehlen einer Kontrollinstanz beim Datenzugriff, etwa durch Richtervorbehalt, infrage.[1276] Außerdem sollte die Bundesregierung prüfen, ob durch die Möglichkeit des Auskunftsersuchen durch die Strafverfolgungsbehörden bei der BaFin nicht Voraussetzungen der StPO, die bestimmte Auskunftsersuchen auf schwere Straftaten begrenzt, umgangen würden.[1277]

Trotz dieser Zweifel regte der Bundesrat aber auch Änderungen an, die den Umfang der Bestandsdatenauskunft erweiterten.[1278] So war im Regierungsentwurf noch vorgesehen[1279], dass eine Auskunft nicht solchen Behörden erteilt werden darf, die Steuerstraftaten verfolgen. Der Bundesrat fürchtete einerseits eine Auslegung dieser Einschränkung dahingehend, dass somit alle Strafverfolgungsbehörden ausgenommen werden könnten, die zumindest auch Steuerstraftaten verfolgen. Da dies den gesamten Strafverfolgungsapparat beträfe, könnte die Norm leerlaufen.[1280] Andererseits würden bei der intendierten Auslegung, die nur die spezifischen Behörden zur Verfolgung von Steuerstraftaten adressierte, Steuerstraftaten privilegiert, was der Bundesrat ebenfalls ablehnte. Er schlug daher vor, die Bereichsausnahme für Steuerstraftaten zu streichen.[1281]

Auch aus der Finanzwirtschaft wurde schon im Zuge der Gesetzeseinführung Kritik laut. Der Zentrale Kreditausschuss (heute: „Deutsche Kreditwirtschaft" – DK) machte in seiner Stellungnahme zum Gesetzesentwurf darauf aufmerksam, dass von der Regelung über 400 Millionen Konten betroffen wären.[1282] Auf diese könnte die BaFin – und über sie die Strafver-

1275 BT-Drs. 14/8017, S. 168
1276 Ibid.
1277 Ibid.
1278 Vgl. *Zubrod*, WM 2003, 1210 (1211).
1279 BT-Drs. 14/8017, S. 48, 168.
1280 Idem, S. 169.
1281 Ibid.
1282 *ZKA,* Stellungnahme zum 4. Finanzmarktförderungsgesetz, AZ: 413-FPLD, 13. Februar 2002, S. 8.

folgungsbehörden – ohne Anfrage, ohne Kenntnismöglichkeit und gänzlich ohne Kontrollmechanismen zugreifen.[1283] Das Verfahren sei letztlich eine „Outsourcing-Variante" des gesellschaftlich umstrittenen Kontenzentralregisters und greife unverhältnismäßig in die Rechte der betroffenen Kunden ein.[1284] Die Bestandsdaten seien auch an sich nutzlos und dienten nur einer Verkürzung der Verfahrensdauer, da im Anschluss an das Auffinden eines Konto ja weiterhin noch im Einzelfall die Umsatzdaten angefragt werden müssten. Eine Kontaktaufnahme mit den ca. 2.900 Kreditinstituten gleichzeitig zur Feststellung, ob und wo eine bestimmte Person ein Konto führt, sei aber derzeit technisch gar kein Problem mehr. Es bestünde sogar schon ein internes System, mit dem das BKA Suchanfragen automatisch an alle Institute weiterleiten könne.[1285] Das (voll-)automatisierte System mit heimlichem Zugriff direkt durch eine staatliche Stelle sei daher nicht erforderlich.[1286]

Lehnhoff, Mitglied des Vorstands des Bundesverbandes der Deutschen Volks- und Raiffeisenbanken, meldete ebenfalls verfassungsrechtliche Kritik an.[1287] Die Möglichkeit von Auskunftsersuchen an die Kreditinstitute stelle den milderen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Kontoinhaber dar. Dass diese so zeitaufwendig wären, läge an der ineffizienten Verwaltung.[1288] Dies sei aber nicht das Problem der Bürger, sondern des Staates und dürfe deshalb nicht zulasten der Grundrechtsträger gelöst werden.[1289] Die automatisierte geheime Abfrage bedeute, dass jeder Bürger ständig mit einem Eingriff in seine Daten rechnen müsse. Insofern würden die Bürger unter einen Generalverdacht gestellt.[1290] Weiter sei es rechtsstaatlich bedenklich, dass die Prüfung der Legitimität eines Auskunftsersuchens bei der BaFin nur im Ausnahmefall kontrolliert würde.[1291]

Vergleichbare Äußerungen wurden auch von rechtswissenschaftlicher Seite vorgetragen. Aufgrund der fehlenden Kontrollmechanismen, der Heimlichkeit des Eingriffs und der breiten Betroffenheit der Bevölkerung

1283 Ibid.
1284 Ibid.
1285 Idem, S. 8 f.
1286 Idem, S. 9.
1287 *Lehnhoff*, WM 2002, 687.
1288 Ibid.
1289 Ibid.
1290 Ibid.
1291 Ibid.

wurde die Maßnahme von einigen Autoren ebenfalls als unverhältnismäßig erachtet.[1292] Teilweise war dieses Ergebnis aber auf bestimmte Einzelregelungen begrenzt, etwa auf den erweiterten Kreis der abfrageberechtigten Behörden in § 93 Abs. 8 AO, und nicht generell auf die Bestandsdatenabfrage i. S. d. § 24c KWG.[1293]

Diejenigen Autoren, die die Bestandsdatenabfrage umfänglich für einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung erachteten, stützten diesen Befund auf die fehlenden Eingriffsvoraussetzungen. Das KWG selbst sah und sieht keine besonderen Voraussetzungen vor. Die Ersuchen richten sich stattdessen nach den Vorschriften der jeweiligen Behörden (s. Kap. D. I. 2.). Für die Staatsanwaltschaften kommt dabei nur die Generalklausel für behördliche Ersuchen des § 161 Abs. 1 S. 1 Hs. 1 Alt. 1 StPO in Betracht.[1294] Diese erfordert lediglich einen Anfangsverdacht.

Von den Kritikern wurde nun vorgebracht, dass diese Anforderung nicht der intensiven Wirkung der Bestandsdatenabfrage gerecht würde. Diese sei nicht mit einer gewöhnlichen Auskunft zu vergleichen, sondern mit einer Rasterfahndung oder Telekommunikationsüberwachung, da sie flächendeckend und heimlich erfolge und in eine vertrauliche Beziehung eingreife.[1295]

Vonseiten einiger Datenschutzbeauftragter wurde des Weiteren das Fehlen datenschutzrechtlicher Standards angemahnt. Insbesondere erfordere das Transparenzgebot, dass die Betroffenen über eine Anfrage informiert würden. Entsprechende Schutzvorschriften wurden jedenfalls für § 93 Abs. 7, 8 AO gefordert.[1296]

Neben der Verhältnismäßigkeit nahmen verschiedenen Beiträge auch die Bestimmtheit der Vorschriften, insb. des § 93 Abs. 8 AO, ins Visier. In

1292 *Degen,* Geldwäsche, 2009, S. 273 ff.; *Samson/Langrock,* Gläserner Bankkunde, 2005, S. 17 ff., 57 ff., 78 ff., 85 ff.; *Zubrod*, WM 2003, 1210; *Herzog/Christmann*, WM 2003, 6 (12 f.); *Göres*, NJW 2005, 253 (256 f.); *Hamacher*, DStR 2006, 633 (637 f.); *ders.* Die Bank 09/2006, 40 *Widmaier*, WM 2006, 116 (118 ff.); Übersicht bei *Pfisterer*, JöR 2017, 393 (409 f.); aA. *Kokemoor*, BKR 2004, 135; *Rüpke* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 55 Rn. 8 ff., 13.

1293 *Göres*, NJW 2005, 253 (256).

1294 *Zubrod*, WM 2003, 1210 (1214).

1295 *Samson/Langrock,* Gläserner Bankkunde, 2005, 17 ff., 78 ff.; *Degen,* Geldwäsche, 2009, S. 293 ff.; *Zubrod*, WM 2003, 1210 (1214); *Widmaier*, WM 2006, 116 (118 ff.); *Hamacher*, DStR 2006, 633 (637).

1296 *DSB BW,* 25. Tätigkeitsbericht, 2004, S. 141; *DSB NRW,* 17. Datenschutzbericht, 2004, S. 145.

seiner Ursprungsfassung aus dem Jahr 2003 sah § 93 Abs. 7, 8 AO[1297] noch vor, dass nur Finanzbehörden über das BZSt eine Bestandsdatenabfrage entsprechend § 24c KWG vornehmen können. Nach § 93 Abs. 8 AO 2003 sollten aber alle Behörden, die für ein Gesetz zuständig sind, das an *„Begriffe des EstG anknüpft"*, ein Finanzamt um Auskunft erbeten können, das dann über das BZSt eine Bestandsdatenabfrage durchführt.

Diese Formulierung wurde in der Literatur umgehend kritisiert. Es sei nicht klar, wann ein Gesetz an *„Begriffe des EStG anknüpfen"* würde, da schon nicht festgeschrieben wurde, welche Begriffe damit gemeint sein sollten. Der Gesetzgeber hatte zwar in der Gesetzesbegründung einige Beispielsbegriffe genannt, etwa „Einkünfte, Einkommen oder zu versteuerndes Einkommen",[1298] die Aufzählung war aber nicht abschließend. Da das EStG eine Vielzahl weiterer vergleichbarer Begriffe enthielt, die zwangsläufig in anderen Gesetzen vorkamen, wurde der Kreis der berechtigten Behörden als zu unbestimmt kritisiert.[1299] Um Abhilfe bei der Auslegung zu schaffen, erließ das Finanzministerium einen Anwendungserlass (AEAO).[1300] In Nr. 3.2. AEAO wurde festgestellt, dass sich § 93. Abs. 9 AO 2003 ausschließlich auf Sozialbehörden und Sozialgerichte bezieht.

Dieser Anwendungserlass führte immerhin dazu, dass das BVerfG einem Eilantrag gegen § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO nicht stattgab.[1301] Zwar erkannte es ebenfalls, dass § 93 Abs. 8 AO nicht zu entnehmen ist, welche Behörden und Gerichte bei den Finanzbehörden anfragen dürfen. Aufgrund des Anwendungserlasses sei aber anzunehmen, dass diese nur auf Anfragen der in Nr. 3.2. AEAO bezeichneten Behörden reagieren würden. Die mangelnde Bestimmtheit würde sich daher faktisch nicht negativ auswirken, weshalb im Rahmen der Folgenabwägung (noch) zugunsten des Gesetzgebers entschieden werden müsste.[1302]

1297 Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003, BGBl. I, S. 2928

1298 BT-Drs. 15/1309, S. 12; BR-Drs. 542/03, S. 19.

1299 *Göres*, NJW 2005, 253 (255); *Kühling*, ZRP 2005, 196 (198 f.) *DSB NRW,* 17. Datenschutzbericht, 2004, S. 145; *DSB BW,* 25. Tätigkeitsbericht, 2004, S. 141; krit. auch *Widmaier*, WM 2006, 116 (117).

1300 *BFM*, Anwendungserlass zur Abgabenordnung (AEAO); Regelungen zu §§ 92 und 93 AO (Auskunftsersuchen; Kontenabruf) vom 10.03.2005, BStBl. I, S. 422.

1301 BVerfGE 112, 284.

1302 Idem, (301 f.); krit. *Florian*, BKR 2005, 202 (204).

2. Die Entscheidung des BVerfG im Jahr 2007

In der Hauptsache stellte das BVerfG dann jedoch fest, dass § 93 Abs. 8 KWG 2003 in der Tat unbestimmt und daher nichtig sei.[1303] Eine weite Auslegung der Vorschrift würde dazu führen, dass bei jeder begrifflichen Übereinstimmung eines Gesetzes mit dem EStG der Anwendungsbereich des § 93 Abs. 8 KWG eröffnet würde. Da das EStG alle möglichen Begriffe beinhalte, wäre die Menge der nach § 93. Abs. 8 KWG berechtigten Behörden letztlich unübersehbar.[1304] Das würde selbst dann gelten, wenn man § 93 Abs. 8 KWG eng auslegte und nur auf spezifisch steuerrechtliche Begriffe abstellen würde, wie es die Gesetzesbegründung nahelegte[1305], da auch diese in allen möglichen Gesetzen vorkämen.[1306] Dem Gesetzgeber wäre es ohne weiteres möglich gewesen, die berechtigten Stellen einfach aufzuzählen, wie es letztlich in Nr. 3.2. AEAO denn auch geschehen war.[1307] Die gesetzliche Unbestimmtheit würde durch den Anwendungserlass auch nicht geheilt.[1308]

a. Verhältnismäßigkeit

Im Übrigen stellte das BVerfG keine Unverhältnismäßigkeit der Bestandsdatenabfrage nach § 24c KWG, §§ 93b, 93. Abs. 7AO fest.

Die automatisierte Bestandsdatenabfrage wäre erforderlich im Sinne eines mildesten Mittels. Zwar befand auch das BVerfG, dass Einzelabfragen bei sämtlichen Instituten prinzipiell möglich wären, da sie aber aufwendiger seien und in ihrem Rahmen sämtliche Banken und andere Institute Kenntnis von den Ermittlungen erhielten, seien Einzelabfragen weder gleich geeignet noch ein milderes Mittel.[1309] Hierbei ist bemerkenswert, dass das BVerfG in der Heimlichkeit aufgrund der Automatisierung nach § 24c Abs. 1 S. 6 KWG nicht nur ein intensivierendes Merkmal, sondern einen Umstand erkannte, der sich als schützend für die Rechte des Betroffenen herausstellte. Auf diese Ambivalenz der Heimlichkeit bei Auskunftser-

1303 BVerfGE 118, 168 (188 ff.) – Kontostammdaten.
1304 Idem, (189).
1305 BT-Drs. 15/1309, S. 12.
1306 BVerfGE 118, 168 (189.) – Kontostammdaten.
1307 Idem, (190) mit Verweis auf *Kühling*, ZRP 2005, 196 (199).
1308 BVerfGE 118, 168 (191) – Kontostammdaten.
1309 Idem, (194 f.)

suchen gegenüber privaten Dritten ging das Gericht aber nicht vertiefend ein.

Die Kontobestandsdatenabfrage sei auch nicht unangemessen. Sowohl die funktionierende Strafverfolgung, die Herstellung von Steuergerechtigkeit als auch das Bekämpfen von Betrug bei Sozialleistungen seien Gemeinwohlbelange von erheblicher Bedeutung.[1310] Dazu stünde der Eingriff in das Recht auf informationelle Selbstbestimmung der von den Auskünften Betroffenen nicht außer Verhältnis. Bei der Prüfung dessen Intensität berücksichtigte das BVerfG die Heimlichkeit, den Charakter der erlangten Daten und die Wahrscheinlichkeit des kausalen Eintretens weiterer Nachteile aufgrund der Datenabfrage.

Die Heimlichkeit bewertete das BVerfG dabei anders als noch im Rahmen der Erforderlichkeit pauschal als intensivierend.[1311] Das war mit Blick auf die frühere Rechtsprechung auch nur konsequent.[1312] Es stellte fest, dass aufgrund der heimlichen Erhebung eine Benachrichtigung des Betroffenen notwendig sein kann, da diesem ansonsten ein effektiver Rechtsschutz verwehrt bliebe. Insofern ging es auf die Kritik der Datenschützer ein, die auf das Fehlen von Benachrichtigungspflichten aufmerksam gemacht hatten. Zum Zeitpunkt des Beschlusses war jedenfalls für § 93 AO auch schon die Einführung einer Benachrichtigungspflicht vorgesehen (heute § 93 Abs. 9 S. 2 AO).[1313]

Aber auch die zum Zeitpunkt der Entscheidung bestehenden Fassungen der § 93 Abs. 7,8 AO und § 24c KWG, der noch heute keine Benachrichtigungspflicht vorsieht, hielt das BVerfG nicht wegen fehlender Benachrichtigungspflichten für unverhältnismäßig. Eine Benachrichtigungspflicht würde sich stattdessen nach dem jeweils einschlägigen Verfahrensrecht bestimmen. Die Behörden könnten ausgehend vom Verhältnismäßigkeitsprinzip im Einzelfall eigenständig entscheiden, ob sie ihr Vorgehen nachträglich offenbaren würden oder nicht. Dies hielt das BVerfG für ausreichend und verlangte nicht, dass eine grundsätzliche Benachrichtigungspflicht eigens deklariert werden müsste.[1314]

1310 Idem, (195 f.).

1311 BVerfGE 118, 168 (197 f.) – Kontostammdaten.

1312 BVerfGE 115, 166 (194); E 141, 220 (269 ff.) – BKA-Gesetz; *Tanneberger,* Sicherheitsverfassung, 2014, S. 247 ff.; *Schwabenbauer,* Heimliche Grundrechtseingriffe, 2013, S. 165 ff.; *Löffelmann*, GSZ 2019, 16 (19) jeweils mwN.

1313 BT-Drs. 16/4841, S. 23.

1314 BVerfGE 118, 168 (200, 210 ff.) – Kontostammdaten.

Aus dem Charakter der Daten und aufgrund der Auskunft drohender weiterer Nachteile folgerte das Gericht keine gesteigerte Intensität. Stattdessen stellte es fest, dass es sich bei Kontobestandsdaten prinzipiell um die am wenigsten sensiblen Daten im Finanzbereich handelt. Es sei fast ausgeschlossen, dass sie allein zu einem Ermittlungserfolg führen. Vielmehr dienten sie lediglich als Bestimmung des Ortes, an dem dann Inhaltsdaten erhoben werden können, etwa Kontobewegungen. Das bedeute zwar, dass die Bestandsdaten stets zu weiteren Ermittlungen und damit zu einem Nachteil führen, dieser Nachteil sei aber gerade der offensichtliche Zweck der Erhebung. Die Rechtmäßigkeit der darauffolgenden Erhebung sei davon abzugrenzen und eigenständig zu berücksichtigen.[1315]

b. Das Urteil aus heutiger Sicht

Das Verhältnis der verschiedenen in § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO enthaltenen Ermächtigungen wurde in dem Beschluss zu den Kontobestandsdaten nur rudimentär behandelt. Blickt man mit dem heutigen Kenntnisstand bzw. mit dem von der Rechtsprechung entwickelten Modell der „Doppeltür"[1316] auf die Vorschriften, erkennt man in den Normen drei separate Teilregelungen.

Zunächst ergibt sich aus § 24c Abs. 1 KWG und § 93b Abs. 1 AO die Pflicht verschiedener Institute, eine automatisch zugängliche Datei über Kontobestandsdaten für die BaFin und das BZST bereitzuhalten. Diese Pflicht wird heute durch § 27 Abs. 2 ZAG und § 28 Abs. 1 S. 2 KAGB auf weitere Institute ausgedehnt. § 24c Abs. 2 KWG, § 93 Abs. 2 S. 1 Hs. 1 AO ermächtigen sodann die BaFin und das BZSt, auf dieses Dateisystem zuzugreifen und Daten abzurufen. Aus diesen Vorschriften ergibt sich aber noch nicht das Recht, diese Daten an verschiedene Behörden weiterzuleiten. Dieses folgt erst aus § 24c Abs. 3 KWG, §§ 93b Abs. 2 S. 1 HS. 2, 93 Abs. 7, 8 AO.

Was die § 24c KWG, §§ 93b, 93 Abs. 7, 8 AO nicht regeln, ist das Recht der einzelnen Behörde, bei der BaFin oder dem BZSt um Auskunft zu ersuchen. Dieser vierte Schritt wird in dem Recht der jeweiligen Behörde geregelt. Diese Erkenntnis hatte das BVerfG im Jahr 2007 jedenfalls noch

1315 Idem, (198 f.).

1316 BVerfGE 130, 151 (184, 193 ff.) – Bestandsdatenauskunft I; E 155, 119 (142 ff.) – Bestandsdatenauskunft II; dazu *Graulich*, NVwZ-Beilage 2020, 47 (48 f.).

nicht vollständig erlangt. So stellte es fest: *„§ 24 c Abs. 3 Satz 1 Nr. 2 KWG ermächtigt (…) die zur Verfolgung und Ahndung von Straftaten zuständigen Behörden und Gerichte dazu, Abrufersuchen zu stellen*".[1317] Offenbar ging das Gericht also davon aus, dass §24c Abs. 3 KWG auch als Ermächtigung der anfragenden Behörde für das Ersuchen gegenüber der BaFin bzw. dem BZSt zu verstehen ist. Das wäre heute nicht mehr haltbar. Gleichzeit erkannte es aber, dass § 24c Abs. 3 KWG die Auskunftserteilung davon abhängig mache, dass das Ersuchen aus Sicht der anfragenden Behörde erforderlich ist.[1318] Daraus leitete es eine (Rechtsgrund-)Verweisung des § 24c Abs. 3 auf das jeweilige Verfahrensrecht der Behörde ab und stellte fest, dass ein Ersuchen der Staatsanwaltschaft ein konkretes Ermittlungsverfahren voraussetzt.[1319] Es ging aber nicht den entscheidenden Schritt einer Festlegung der Ermächtigungsgrundlage in der StPO, obwohl schon der Gesetzgeber in der Gesetzesbegründung erkannt hatte, dass sich das Ersuchen aus Sicht der Staatsanwaltschaft nach den allgemeinen Regeln der §§ 152 Abs. 2, 160 StPO richten müsste.[1320] Wie auch das Gericht ging er also von einer Art hybriden Konstellation aus, nach der § 24c Abs. 3 KWG zwar eine Ermächtigung u. a. der Staatsanwaltschaft enthielt, die Voraussetzungen aber aus der StPO folgen würden.

Dogmatisch korrekt wäre es (jedenfalls nach dem heutigen Erkenntnisstand) gewesen, die Ermächtigungsgrundlage für das Ersuchen an die BaFin in § 161 Abs. 1 S. 1 Alt. 1 StPO zu verorten. Diesen finalen Schritt ist der Gesetzgeber aber wie auch das BVerfG nicht gegangen.

In der Literatur war dieses – heute gängige[1321] – Ergebnis hingegen schon früh vorgeschlagen worden[1322]. Sie blieb insofern aber vom BVerfG unberücksichtigt.

c. **Reaktion**

Seit dem Beschluss des BVerfG ist die Diskussion über die Kontostammdatenauskunft verständlicherweise etwas eingeschlafen. Dabei geben die

1317 BVerfGE 118, 168 (191) – Kontostammdaten.
1318 Ibid.
1319 Ibid.
1320 BT-Drs. 14/8017, S. 123.
1321 OLG Stuttgart, NStZ 2016, 48 (48); *T. Knierim* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 10 Rn. 55.
1322 *Zubrod*, WM 2003, 1210 (1214).

Beschlüsse zur Bestandsdatenauskunft im Bereich der Telekommunikation durchaus Anlass, die Entscheidung aus dem Jahr 2007 einer Revision zu unterziehen.

Die unmittelbaren Reaktionen auf den Beschluss zu den Kontobestandsdaten waren zunächst ernüchtert. Teilweise wurde die Entscheidung als Erweiterung der gesetzlichen Spielräume zu heimlichen Überwachungsmaßnahmen eingeschätzt, die weitere Eingriffe in die Persönlichkeitsrechte im Rahmen der Terrorismusbekämpfung und Steuererhebung befürchten ließen.[1323] Manche sahen durch die Aufrechterhaltung von § 24c KWG und §§ 93b, 93 Abs. 7, 8 AO gar den „gläsernen Bankkunden" zur Realität werden.[1324]

Erwartungsgemäß wurden in der Urteilskritik die schon zuvor diskutierten Verhältnismäßigkeitsaspekte vorgebracht. Dem Gericht wurde vorgeworfen, die aufgrund der Streubreite und Heimlichkeit sehr hohe Eingriffsintensität verkannt zu haben und deshalb fälschlicherweise auf notwendige Voraussetzungen sowohl in materieller als auch verfahrensrechtlicher Hinsicht verzichtet zu haben.[1325]

In einer späteren Betrachtung wurden die strukturellen Aussagen des Beschlusses kritisiert. Durch die Darstellung der Bestandsdatenabfrage als prinzipiell geringfügigen Eingriff würde eine Datenkategorisierung vorgenommen und damit von der ehemaligen Vorstellung des BVerfG abgerückt, sodass die Art der Daten sich auf deren Aussagekraft nicht mehr auswirken könne.[1326] Anders als das BVerfG meint, sei die Bestandsdatenerhebung nicht isoliert von den Maßnahmen zu betrachten, die auf ihrer Basis erst ermöglicht würden. Gerade in der komplexen Betrachtung von Daten bzw. deren Verarbeitungs- und Verknüpfungsmöglichkeiten[1327] habe die Originalität des Volkszählungsurteils gelegen.[1328] Die Abkehr von diesem Blickwinkel sei unbefriedigend.[1329] Insgesamt zeige das BVerfG danach die Bereitschaft, eine breite Präventivzugänglichkeit von Daten in Abhängigkeit

1323 *Gregor*, EWiR 2008, 189 (190).
1324 *Tolani*, BKR 2007, 275 (281); so schon *Samson/Langrock,* Gläserner Bankkunde, 2005.
1325 Ausf. *Reichling,* Kontenabfrage, 2010, S. 129 ff.
1326 *Pfisterer*, JöR 2017, 393 (412 ff.).
1327 BVerfGE 65, 1 (45) – Volkszählung.
1328 *Pfisterer*, JöR 2017, 393 (413).
1329 Ibid.

der Datenart zuzulassen, wobei den Finanzdaten nicht der angemessene Persönlichkeitswert zuteil würde.[1330]

3. Klärung durch den EuGH? *Ministerio Fiscal.*

Auch der EuGH hat sich mit der Zulässigkeit sicherheitsrechtlicher Abfragen von (Telekommunikations-)Bestandsdaten befasst. Die Wertung des Gerichtshofs kann aufgrund der Vergleichbarkeit der Datensätze auf die Kontobestandsdatenabfrage übertragen werden.

In der Sache *Ministerio Fiscal*[1331] hatte ein spanisches Gericht dem EuGH die Frage vorgelegt, ob das EU-Recht ein polizeiliches Auskunftsersuchen nach Vertragsdaten bei Telekommunikationsprovidern unter die Voraussetzung stellt, dass die Abfrage der Verfolgung oder Verhütung einer schweren Straftat dient. Bei dem Verfahren ging es damit ausdrücklich nicht um die Speicherpflicht der Bestandsdaten, sondern allein um die Voraussetzungen, unter denen das nationale Sicherheitsrecht der Mitgliedstaaten einen Zugriff von Bestandsdaten zulassen dürfe.[1332]

In den Entscheidungen zur Vorratsdatenspeicherung von TK-Verkehrsdaten hatte der EuGH darauf bestanden, dass eine retrograde Abfrage solcher Daten nur zur Bekämpfung schwerer Straftaten zulässig sei.[1333] Dies folge aus Art. 15 der ePrivacy-RL (s. o. Kap. C. II. 1. a. bb.).[1334] Ob diese Rechtsprechung auf Bestandsdaten zu übertragen sei, war Gegenstand der Vorlagefrage.

In seiner Antwort stellte der Gerichtshof diesbezüglich klar, dass Art. 15 der ePrivacy-RL nicht in jedem Fall den Zugang zu Telekommunikationsdaten auf den Bereich der schweren Kriminalität begrenze. Die Norm eröffne vielmehr grundsätzlich die Möglichkeit zur Beeinträchtigung der Privatheitsrechte im Bereich der Telekommunikation durch das nationa-

1330 *Hartmann* KJ 2007, 2 (17 f.); *Pfisterer*, JöR 2017, 393 (421).

1331 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal) = NJW 2019, 655.

1332 Idem, Rn. 49.

1333 EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 115 ff. = NJW 2017, 717; EuGH, Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 27 ff. = NJW 2021, 2103.

1334 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation, ABl. 2002, L 201/37.

le Sicherheitsrecht. Die besonderen Voraussetzungen für den Zugang zu Verkehrs- oder Standortdaten ergäben sich erst aus der Anwendung des Verhältnismäßigkeitsgrundsatzes.[1335] Ursächlich für die gesteigerten Anforderungen an die Abfrage von Verkehrsdaten sei die Erheblichkeit des damit verbundenen Eingriffs. Für diese wiederum kommt es nach dem EuGH darauf an, wie ausführlich sich die privaten Lebensumstände einer Person aus den entsprechenden Daten ableiten lassen („profiling", dazu auch Kap. III. 1. b. bb. (1)).[1336]

Unter Rückgriff auf diese Maßstäbe kam der EuGH in *Ministerio Fiscal* zu dem Ergebnis, dass der Zugriff von Sicherheitsbehörden auf Bestandsdaten, d. h. Daten, aus denen sich allein die Identität eines SIM-Karteninhabers, bzw. Geräte- oder Nummerninhabers ergebe, keine schwere Beeinträchtigung der Grundrechte aus Art. 7, 8 EU-GRC darstelle. Aus solchen Daten ließen sich keine weitergehenden Rückschlüsse auf das Privatleben des Betroffenen erzielen.[1337] Konsequenterweise verlange das EU-Recht bzw. Art. 15 der ePrivacy-RL in Verbindung mit Art. 7, 8 EU-GRC nicht, dass die nationalen Gesetzgeber die Abfrage von TK-Bestandsdaten nur zur Verhütung schwerer Kriminalität erlauben.[1338]

Ähnlich wie das BVerfG stellt der EuGH also keine spezifischen materiellen Voraussetzungen an den heimlichen sicherheitsrechtlichen Zugang zu (TK-)Bestandsdaten. Der Gerichtshof teilt die Auffassung, dass es sich bei Bestandsdaten um wenig sensible Informationen handelt, deren Abfrage allgemein zur Kriminalitätsverhütung möglich sein kann.

Mehr Gehalt lässt sich aus der Entscheidung nicht ziehen. Der EuGH beantwortete ausschließlich die Vorlagefrage, ob die Bestandsdatenabfrage allein zur Verhütung schwerer Kriminalität zulässig sein kann. Zur konkreten Ausgestaltung der Zugangsnormen, insbesondere hinsichtlich der Bestimmtheit und der Notwendigkeit eigenständiger Rechtsgrundlagen, zur Unterscheidung von automatisierten- und manuellen Abfrageverfahren

---

1335 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 55 = NJW 2019, 655 mit Verweis auf Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 115 = NJW 2017, 717.

1336 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 27 f. = NJW 2014, 2169; Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 99 f. = NJW 2017, 717 EuGH, Urt. v. 6.10.2020 – C-511/18, C-512/18, C-520/18, *La Quadrature du Net* = NJW 2021, 531, Rn. 117; Urteil v. 2.3.2021, C-746/18 (Prokuratuur), Rn. 35 f. = NJW 2021, 2103; s.a. *M. W. Müller/Schwabenbauer*, NJW 2021, 2079 (2084).

1337 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 58 ff. = NJW 2019, 655.

1338 Idem, Rn. 62 f.

oder zur Notwendigkeit datenschutzrechtlicher Formvorschriften, etwa Berichts-, Protokoll- oder Benachrichtigungspflichten, äußerte sich der Gerichtshof nicht.

4. Zusammenfassung und Stellungnahme

Obwohl die Kontobestandsdatenabfrage vor und unmittelbar nach ihrer Einführung stark kritisiert wurde[1339], hat sich das Instrument – ebenso wie die Überwachung von TK-Bestandsdaten – mittlerweile etabliert. Das BVerfG hatte in seiner Entscheidung von 2007 keine grundsätzlichen Bedenken geäußert.[1340]

Auch die Speicherung und Abfrage von TK-Bestandsdaten beanstandete die Rechtsprechung in den folgenden Jahren nicht prinzipiell.[1341] Da es sich bei den Bestandsdaten um wenig sensible Daten handelt, die nur als Türöffner für weitere Ermittlungen dienen, stellt die Abfrage durch Sicherheitsbehörden grundsätzlich einen leichter zu rechtfertigenden Grundrechtseingriff dar.[1342]

Im Zuge der Entscheidungen zur TK-Bestandsdatenspeicherung stellte das BVerfG aber bedeutende Grundsätze fest, die analog auf die Kontostammdatenabfrage anzuwenden sind und 2007 noch keine Berücksichtigung fanden. Dazu gehört insbesondere das Prinzip der Doppeltür,[1343] wonach die Ermächtigungen zu Auskunftsersuchen und entsprechender Übermittlung eigenständig geregelt werden müssen.

1339 *ZKA,* Stellungnahme zum 4. Finanzmarktförderungsgesetz, AZ: 413-FPLD, 13. Februar 2002, S. 8 f.; *Degen,* Geldwäsche, 2009, S. 273 ff.; *Samson/Langrock,* Gläserner Bankkunde, 2005; *Lehnhoff*, WM 2002, 687; *Zubrod*, WM 2003, 1210 (1210); *Herzog/Christmann*, WM 2003, 6 (12 f.); *Göres*, NJW 2005, 253 (256 f.); *Widmaier*, WM 2006, 116 (118 ff.); *Hamacher*, DStR 2006, 633 (637 f.); *ders.* Die Bank 09/2006, 40; kritisch auch der *Bundesrat,* BT-Drs. 14/8017, S. 168; aA. *Kokemoor*, BKR 2004, 135; *Rüpke* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 55 Rn. 8 ff., 13.

1340 BVerfGE 118, 168 (188 ff.) – Kontostammdaten; krit. *Reichling,* Kontenabfrage, 2010, S. 129 ff.; *Pfisterer*, JöR 2017, 393 (421); *Hartmann* KJ 2007, 2 (17 f.); *Tolani*, BKR 2007, 275 (281); *Gregor*, EWiR 2008, 189 (190).

1341 BVerfGE 130, 151– Bestandsdatenauskunft I; E 155, 119 – Bestandsdatenauskunft II.

1342 so auch EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 58 ff. = NJW 2019, 655.

1343 BVerfGE 130, 151 (184, 193 ff.) – Bestandsdatenauskunft I; E 155, 119 (142 ff.) – Bestandsdatenauskunft II; dazu *Graulich*, NVwZ-Beilage 2020, 47 (48 f.).

Die Auskunftsanfragen müssen dabei aber nur im Rahmen von manuellen Übermittlungen, d. h., die die unmittelbar durch die Privaten ergehen, in spezifischen Ermächtigungen geregelt werden. Bei automatisierten Auskünften, die auf bestimmte Vertragsdaten begrenzt sind, reichen die allgemeinen Datenerhebungsklauseln aus.[1344]

Dass die Kontobestandsabfrage in den meisten Sicherheitsgesetzen nicht spezifisch normiert wurde, dürfte daher unproblematisch sein. Allerdings bedürfte die unterschiedliche Behandlung von automatisierter und manueller Bestandsdatenabfrage einer tiefergehenden Untersuchung.

II. Kontoinhaltsdaten

Anders als die Bestandsdatenauskunft, ist der heimliche staatliche Zugriff auf Kontoinhaltsdaten nicht zentral geregelt. Mangels umfassender Zahlen lässt sich keine Aussage darüber treffen, auf welche Grundlage sich staatliche Sicherheitsbehörden in der Praxis primär stützen, wenn sie auf solche Finanzdaten zugreifen wollen. Bankenauskunftsersuchen der Staatsanwaltschaften nach § 161 Abs. 1 S. 1 Alt. 1 StPO gehören jedenfalls zu deren Standardrepertoire (s. o. Kap. E. I. 1. c.).[1345]

1. Einleitung: Abgrenzung von individuellen Auskunftsersuchen und Geldwäscheprävention

Zu individuellen bzw. individualisierten Auskunftsersuchen nach Kontodaten hat sich das BVerfG schon mehrfach verhalten. Besondere Aufmerksamkeit erlangte die Entscheidung im „Mikado"-Fall, in dem die Staatsanwaltschaft Kreditkartenunternehmen aufforderte, ihre Datenbestände nach bestimmten Zahlungsvorgängen zu rastern. Das BVerfG erklärte dieses Vorgehen, das auf die Ermittlungsgeneralklausel des § 161 Abs. 1 S. 1 Alt. 2 StPO gestützt wurde, für verfassungsgemäß.[1346]

1344 BVerfGE 130, 151 (184, 193 ff.) – Bestandsdatenauskunft I; *Bär* in Bannenberg/Wabnitz/Janovsky ua. (Hrsg.), Hdb. Wirtschafts- & Steuerstrafrecht, 5. Aufl. 2020, Kap. 28 Rn. 113 f.

1345 Siehe nur *F. Jansen,* Bankauskunftsersuchen, 2010, S. 1 ff.; *Reichling*, JR 2011, 12 (12).

1346 BVerfG, NJW 2009, 1405; krit. *Buermeyer,* Informationelle Selbstbestimmung, 2019, 152 f.; *Brodowski*, JR 2010, 543 (547); *Singelnstein*, NStZ 2012, 593 (603); *Petri*, StV 2007, 266 (268).

Auch zu den nachrichtendienstlichen Auskunftsverlangen, die ausdrücklich zur heimlichen Abfrage von Kontodaten ermächtigen (s. o. E. II. 2. a.), hat das BVerfG Stellung genommen. Solche Auskünfte würden zwar erheblich in die informationelle Selbstbestimmung der Betroffenen eingreifen, da es sich um besonders sensible Daten handle. Bei entsprechender Ausgestaltung durch Anknüpfung an „qualifizierte Gefährdungstatbestände" und verfahrensrechtliche Sicherungen seien solche Zugriffe aber zulässig.[1347]

Gegenstand dieser Untersuchung ist nicht die Verhältnismäßigkeit individueller Abfragen von Kontoumsätzen, sondern das Normgefüge, mittels dessen diese traditionellen Ermittlungswege umgangen werden können: das Anti-Geldwäscherecht.

Substanzielle grundrechtliche Kritik an den Vorschriften des Anti-Geldwäscherechts gab es dabei schon seit dessen Einführung und wird auch aktuell noch vorgetragen. Die kritische Besprechung lässt sich in fünf Phasen unterteilen, bei denen verschiedene Aspekte der Geldwäschebekämpfung im Fokus der Auseinandersetzung standen.

Zunächst wurden – das Geldwäscherecht war in dieser ersten Phase noch rudimentär ausgestaltet – die unmittelbaren Pflichten der Verpflichteten zur Identifizierung und anschließenden Zusammenarbeit mit staatlichen Behörden besprochen, die zwar als Beeinträchtigung der informationellen Selbstbestimmung erkannt wurden, aber allgemein auf wenig Widerstand stießen. Erst als Mitte der 1990er Jahre das EDV-Monitoring etabliert wurde, keimten erste beachtliche Zweifel an der Vereinbarkeit des Geldwäscherechts mit den Privatheitsgrundrechten auf, wobei vor allem die Suche nach einer rechtlichen Grundlage der Datenverarbeitungsmaßnahmen im Zentrum stand.

Zu einem Versuch, das EDV-Monitoring in Gesetzesform zu gießen, kam es nämlich erst nach der Jahrtausendwende. Hierdurch wurde die dritte Phase der Kritik ausgelöst, in der zwar weiterhin ganz zentral über das Monitoring gestritten wurde, nun aber unter breiterem Interesse und mit stärkerem Fokus auf die Verhältnismäßigkeit der gesetzlichen Regelung.

Die vierte Phase ist von der Einführung des Anti-Geldwäscherechts in der Struktur der 3. GWRL geprägt. Erstmals war in den Gesetzen nun ausdrücklich von einer Überwachungspflicht der Institute die Rede. Gleichzeitig war das Monitoring mittlerweile gängige Praxis, weshalb die Diskussion um die Implikationen der Überwachung trotz der damals intensiven Dis-

1347 BVerfGE 120, 274 (348 ff.) – Online-Durchsuchung.

kussion um die TK-Vorratsdatenspeicherung weniger kontrovers geführt wurde.

In der fünften und aktuellen Phase wird das Monitoring zwar noch immer kritisiert. Der Fokus insbesondere der europäischen Literatur liegt aber primär auf den vorgehaltenen Datenbeständen der Banken und den Zugriffs- und Analyserechten der FIU.

Diese fünf Phasen sollen im Folgenden chronologisch erläutert und im Einzelnen kommentiert werden. Die Darstellung folgt somit der zuvor vorgenommenen historischen Darstellung der Entwicklung des Anti-Geldwäscherechts (s. Kap. D. III. 2. a.) und bezieht sich vornehmlich auf die deutsche Perspektive der Debatte.

Zuletzt sollen dann noch die knappen Ansätze der Rechtsprechung zum Verhältnis des Anti-Geldwäscherechts und der informationellen Selbstbestimmung bzw. den Privatheitsgrundrechten kurz beleuchtet werden.

2. Verdachtsmeldepflichten und „Bankgeheimnis"

In seiner ursprünglichen Form aus dem Jahr 1993 sah das GwG noch keine ausdrückliche Pflicht zur Überwachung, sondern lediglich Identifizierungspflichten und eine Meldepflicht bei Verdachtsmomenten vor. Diese Pflichten gingen mit einer Aufzeichnungs- und Aufbewahrungspflicht einher.

a. Erste Annäherungen bei der FES-Tagung zur Geldwäsche 1994

Die Beeinträchtigung der informationellen Selbstbestimmung der Bankkunden durch das GwG war dementsprechend unmittelbar nach der Einführung des Gesetzes noch ein untergeordnetes Thema. Zumeist wurde lediglich festgestellt, dass die geldwäscherechtlichen Pflichten mit dem Bankgeheimnis kollidieren würden.[1348] Dass dieses – soweit es in der Rechtsordnung überhaupt Ausdruck findet –[1349] aber keinen absoluten

1348 Etwa *Reifner*, JZ 1993, 273 (277 f.); *Carl/Klos*, wistra 1994, 161 (162).

1349 Hierzu übersichtlich *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 8 Rn. 4 ff.

Schutz genießt, sondern allgemein bei der Strafverfolgung durchbrochen wird, war dabei schon anerkannt.[1350]

So stellten zwei Regierungsjuristen etwa fest, dass durch die flächendeckende Mitteilung von Informationen der Banken an den Staat tief in die Privatsphäre der Bürger eingegriffen würde.[1351] Aber anstatt diesen Umstand verfassungsrechtlich zu prüfen, kritisierten sie, dass die aufgrund des Geldwäschegesetzes erlangten Informationen nicht bzw. nicht unmittelbar für die Steuerbekämpfung genutzt werden könnten.[1352]

Erste kritische Töne waren indes bereits auf einer Tagung der Friedrich-Ebert-Stiftung zum Geldwäschegesetz im Oktober 1993 laut geworden.[1353] Hier machten der Vorsitzende der Berliner Anwaltskammer[1354] auf die Beeinträchtigung der Geheimhaltungspflichten der Berufsgeheimnisträger und der Hessische Datenschutzbeauftragte auf Implikationen mit der Privatsphäre der Bankkunden[1355] aufmerksam.

Zwar wurde von beiden auf eine unmittelbare verfassungsrechtliche Einschätzung verzichtet. Sie legten jedoch gewissermaßen den Grundstein der aufkeimenden Diskussion, indem sie die verschiedenen durch das Anti-Geldwäscherecht betroffenen Rechtspositionen kompakt darstellten. Diese sind einerseits die wirtschaftlichen Rechte der verpflichteten Institute und Personen, die aber nicht Thema dieser Arbeit sind, sowie das Recht auf informationelle Selbstbestimmung der betroffenen Kunden.

b. Frühe Betrachtungen von GwG und informationeller Selbstbestimmung

Mit diesem setzte sich die erste umfassende Kommentierung des GwG von *Aepfelbach* und *Fülbier* im Hinblick auf die Melde-, Aufzeichnungs- und Aufbewahrungspflicht nach § 10 GwG 1993 auseinander.[1356] Hinsichtlich der Meldepflicht wurde zunächst ein Vergleich mit dem US-Recht ange-

1350 LG Frankfurt, NJW 1954, 688 (690); *R. Müller*, NJW 1963, 831 (836 ff.); *Carl/Klos*, DStZ 1994, 68 (70); ausf. *Sichtermann,* Bankgeheimnis, 2. Aufl. 1966, S. 289 ff.

1351 *Carl/Klos*, DStZ 1994, 68 (68).

1352 Idem, (71 ff.).

1353 *Kahlert* (Hrsg.), Friedrich-Ebert-Stiftung, Tagung Geldwäsche, 1994.

1354 *Dombek* in Kahlert (Hrsg.), Friedrich-Ebert-Stiftung, Tagung Geldwäsche, 1994, S. 103.

1355 *Hassemer* in Kahlert (Hrsg.), Friedrich-Ebert-Stiftung, Tagung Geldwäsche, 1994, S. 123.

1356 *Fülbier* in Aepfelbach/Fülbier GwG, 1. Aufl., 1993, S. 126 ff.

strengt, das eine allgemeine Meldepflicht für Bartransaktionen ab einem gewissen Schwellenwert vorsah. Solch eine Meldepflicht wäre aber eine Informationserhebung auf Vorrat und ins Blaue hinein, weshalb sie mit deutschem Verfassungsrecht nicht in Einklang zu bringen wäre.[1357] Zurecht hätte sich die EG daher für eine Verdachtsmeldepflicht entschieden. Diese würde zwar ebenfalls in das Recht auf informationelle Selbstbestimmung eingreifen, aufgrund der Filterung auf verdächtige Fälle jedoch nur in einem geringen Maße, das mit dem gesellschaftlichen Interesse an Strafverfolgung gerechtfertigt werden könnte.[1358]

Hinsichtlich der Aufzeichnungs- und Aufbewahrungspflicht wurde ebenfalls bemerkt, dass Private durch das GwG dazu verpflichtet werden, Informationen zu erheben und dem Staat zur Verfügung zu stellen.[1359] Auf eine Prüfung der Verhältnismäßigkeit anhand des deutschen Verfassungsrechts wurde jedoch verzichtet, da die Informationserhebung auf europäischem Recht beruhte.[1360] Nur soweit die Daten zu anderen als geldwäscherechtlichen Zwecken verwendet werden sollten, wäre das deutsche Verfassungsrecht einschlägig, da nach der Präambel der 1. GWRL die Datenverwendung auf geldwäscherechtliche Zwecke begrenzt sei.[1361] Hier wurde wohl übersehen, dass das Verwertungsverbot nicht nur in der Präambel, sondern ausdrücklich in Art. 6 Abs. 3 der 1. GWRL normiert wurden. Nach Art. 6 Abs. 3 S. 2 der 1. GWRL sollte es den Mitgliedstaaten aber möglich bleiben, die nach dem Anti-Geldwäscherecht zu speichernden Daten auch für andere Zwecke zu öffnen.

Das GwG 1993 sah dementsprechend in § 10 noch eine Verwertungsbeschränkung auf Strafverfahren vor, in denen wegen Geldwäsche i. S. d. § 261 StGB[1362] oder einer der Vortaten des § 261 StGB ermittelt wurde. Unter diese Vortaten fielen Verbrechen, Vergehen nach § 29 Abs. 1 Nr. 1 BtMG oder Vergehen des Mitglieds einer kriminellen Vereinigung i. S. d. § 129 StGB. Damit war die Verwertungsbeschränkung also gerade nicht auf Geldwäschedelikte beschränkt. Vielmehr durften die nach dem GwG gespeicherten Daten auch zur Aufklärung von Verbrechen genutzt werden,

1357 Idem, S. 138 ff.
1358 Idem, S. 140.
1359 Idem, S. 126; s.a. BT-Drs. 12/2704, S. 16 f.
1360 Grundlegend BVerfGE 73, 339 – Solange II.
1361 *Fülbier* in Aepfelbach/Fülbier GwG, 1. Aufl., 1993, S. 127; siehe BVerfG, NJW 1990, 974
1362 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15.7.1992, BGBl. I 1302.

ohne dass zusätzlich wegen Geldwäsche ermittelt wurde.[1363] Insofern hätte die Datenverarbeitung an deutschem Verfassungsrecht gemessen werden müssen.

Wenige Jahre später wurde die grundrechtliche Dimension des GwG auch in Zeitschriftenbeiträgen angesprochen.[1364] Von *Dahm* wurde bemerkt, dass die Geldwäschebekämpfung auf der Verarbeitung ganz besonders sensibler Daten beruht.[1365] Da in Form der Strafverfolgung ein staatlicher Zweck verfolgt würde, verlangte er die grundsätzlich unmittelbare Anwendung des Verfassungsrechts. Dabei ging er so weit, die Banken als Beliehene anzusehen.[1366] Dieser Ansatz erweist sich aber als Fehlsubsumption und konnte sich nicht durchsetzen, da die Banken gegenüber Dritten nicht hoheitlich tätig werden.[1367] Sie verarbeiten lediglich Daten, die aus einem privatrechtlichen Verhältnis stammen.

Im Mittelpunkt seiner Untersuchung steht *Dahms* früher Versuch, die geldwäscherechtlichen Pflichten der Banken und anderer Institute mit unmittelbar staatlichen Überwachungsmaßnahmen zu vergleichen und die dazu vorliegende Rechtsprechung des BVerfG als Maßstab für das GwG vorzuschlagen. Hierfür bot sich der 1995 ergangene Gerichtsbeschluss[1368] zur Auslandsfernmeldeaufklärung durch den BND an.[1369] In diesem hatte das BVerfG die Auswertung von Kommunikationsinhalten, die der BND im Rahmen der verdachtslosen Rasterung erhalten würde, vorläufig außer Vollzug gesetzt. Die Nachteile, die eine Auswertung anlasslos abgefangener Kommunikation für die unverdächtigen Betroffenen hätte, seien zu groß.[1370]

Dahm schlug nun vor, diese kritische Betrachtung anlassloser Datensammlung zur Sicherheitsprävention auf das GwG übertragen.[1371] Zwar war im Jahr 1996 noch nicht näher geklärt, auf welchem Wege die Verpflichteten verdächtige Transaktionen entdecken sollten. Es war jedoch bekannt geworden, dass das Bundesaufsichtsamt für das Kreditwesen (BAKred)

1363 *Carl/Klos*, DStZ 1994, 68 (71); vgl. auch BT-Drs. 12/2704, S. 17.
1364 *Dahm*, WM 1996, 1285; *Herzog*, WM 1996, 1753.
1365 *Dahm*, WM 1996, 1285 (1289).
1366 *Dahm/Hamacher*, wistra 1995, 206 (213 f.); *Dahm*, WM 1996, 1285 (1288); auch *Findeisen*, wistra 1997, 121 (124 f.) .
1367 Vgl. nur *Degen*, Geldwäsche, 2009, S. 130 ff.
1368 BVerfGE 93, 181.
1369 *Dahm*, WM 1996, 1285 (1290).
1370 BVerfGE 93, 181 (191).
1371 *Dahm*, WM 1996, 1285 (1290).

das anglo-amerikanische „Know-Your-Customer" System implementieren wollte, wonach die Banken alle verdächtigen Transaktionen zu untersuchen hätten (dazu gleich unten). Daraus wurde gefolgert, dass die Banken eine Art Rasterfahndung durchführen müssten, um solche verdächtigen Transaktionen zu identifizieren, wodurch sie letztlich den Geschäftsverkehr aller Kunden überwachen müssten. Die Rechtsprechung des BVerfG stünde dieser Bestrebung entgegen. Noch nicht einmal die Strafverfolgung selbst wäre zu einer solchen Vorfeldaufklärung berechtigt,[1372] Private sollten es erst recht nicht sein.[1373]

Eine weitere differenzierte Besprechung der Auswirkungen des GwG auf die informationelle Selbstbestimmung findet sich in der Dissertation von *Werner* aus dem Jahr 1996.[1374] Die bestehenden geldwäscherechtlichen Pflichten wurden hier allerdings nicht separat, sondern als einheitlicher Eingriffskomplex dargestellt. Dieser sei trotz des vordergründigen Tätigwerdens von Privaten aufgrund der gesetzlichen Anordnung und des klar definierten Zwecks der Strafverfolgung dem Staat zuzurechnen.[1375] Die Pflichten wurden einer hypothetischen Verhältnismäßigkeitsprüfung im Sinne des deutschen Verfassungsrechts unterzogen – hypothetisch, da im Voraus ebenfalls bemerkt wurde, dass dieses nach der Rechtsprechung des BVerfG aufgrund der dahinterliegenden Richtlinie keine Anwendung finden würde.[1376] Diese Prüfung kam zu dem Ergebnis, dass der Eingriff in die informationelle Selbstbestimmung gerechtfertigt wäre. Die Identifizierungspflicht sei schon kein erheblicher Eingriff, da Transparenz im Wirtschaftsverkehr normal und erwünscht sei.[1377] Die Aufzeichnungspflichten wären durch die Verwendungsbeschränkung und die Meldepflicht durch das Verdachtsmoment ausreichend eingehegt.[1378]

3. Diskussion um die Einführung des Konten-Monitorings ab Mitte der 1990er Jahre

Die Diskussion wurde intensiviert, nachdem Mitte der 1990er Jahre Überlegungen des BAKred zur Überwachung von Transaktionen durch die Geld-

1372 Ibid.
1373 Ibid.
1374 *Werner,* Geldwäsche, 1996, S. 94 ff.
1375 Idem, S. 96.
1376 Idem. S. 91 f.
1377 Idem, S. 102 f.
1378 Idem, S. 103.

wäscheverpflichteten bekannt wurden. Gemäß Art. 5 der 1. GWRL sollten die Mitgliedstaaten sicherstellen, dass die Verpflichteten alle Transaktionen, die einen Verdacht der Geldwäsche besonders nahelegten, sorgfältig prüfen würden. Eine solche Pflicht fand sich aber im GwG nicht ausdrücklich. Dieses sah in § 14 Abs. 2 Nr. 2 GwG 1993 lediglich generalklauselartig vor, dass bestimmte Verpflichtete, insbesondere Kreditinstitute, interne Grundsätze, Verfahren und Kontrollen zur Verhinderung der Geldwäsche entwickeln.

Das BAKred war deshalb besorgt, das Art. 5 der 1. GWRL nicht ausreichend umgesetzt war. Bei einer Tagung der CDU/CSU-Bundestagsfraktion stellten dessen Beamte deshalb vor, wie dieser vermeintliche Umsetzungsmangel behoben werden sollte.[1379] Aus der Verpflichtung zur Entwicklung interner Sicherungsmaßnahmen wollte man ableiten, dass die Banken zur Rasterung der Kundentransaktionen nach einem bestimmten Verfahren verpflichtet sind. Diesen Prozess bezeichnete man als „*Kontenresearch*"[1380]. Konkret vorgeschlagen wurde zunächst aber nur die Überwachung („Monitoring") bestimmter Kunden, wenn bei diesen Transaktionen gefunden wurden, die zwar auffällig waren, aber noch nicht die Schwelle zur Verdachtsmeldung überschritten.[1381] Für diesen Prozess sollten die Banken ihre hauseigene EDV nutzen, um anhand konkreter Suchparameter Auffälligkeiten bei Kundentransaktionen zu entdecken, die sodann im Sinne des Art. 5 der 1. GWRL besonders sorgfältig geprüft werden sollten.[1382] Das heute standardmäßige EDV-Monitoring war damit quasi geboren.

a. Erste Kritik von *Felix Herzog*

Der Vorstoß des BAKred wurde zeitnah von *Felix Herzog* besprochen, der die Beeinträchtigungen der informationellen Selbstbestimmung durch das

1379 *Artopeus/Findeisen*, (BAKred), Entwurfspapier Anhörung CDU/CSU im Bundestag, 21.08.1995, S. 10 ff. aus der Anhörung selbst zitieren *Dahm*, WM 1996, 1285 (1290) und *Herzog*, WM 1996, 1753 (1755 ff.).

1380 Vgl. *BAKred,* Jahresbericht, 1998, S. 92 f.; *Herzog*, WM 1996, 1753 (1755).

1381 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, Ziff. 30; abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.

1382 So jedenfalls *Herzog*, WM 1996, 1753 (1755 ff.); *Dahm*, WM 1996, 1285 (1290) jeweils mit Verweis auf die Anhörung der BAKred durch die CDU/CSU-Fraktion am 25.08.1995. Aus dem Entwurfspapier der BAKred (oben Fn 1380) und der Verlautbarung (oben Fn 1867 1382) ergibt sich das nicht in dieser Ausdrücklichkeit.

Anti-Geldwäscherecht seitdem immer wieder infrage gestellt hat. In einem 1996 erschienen Aufsatz unterzog er die Vorschläge des BAKred einer datenschutz- und verfassungsrechtlichen Prüfung. [1383] Die unmittelbar zuvor von *Dahm* vorgebrachten *Vorbehalte*[1384] erhielten dadurch erstmals echte Substanz. Der Aufsatz behandelt bereits alle Punkte, die auch aus heutiger Perspektive dringlich erscheinen und soll daher an dieser Stelle recht umfassend zusammengefasst werden.

Herzog befand, dass ein EDV-Monitoring von Kundendaten durch die Banken als Eingriff in die informationelle Selbstbestimmung zu werten wäre. Dabei verstand er diese begrifflich ganz im Sinne des Volkszählungsurteil als Quasi-Eigentum[1385] an Daten bzw. dem Recht jeder Person zu wissen, was andere über sie wissen.[1386] In dieses Recht würde eingegriffen, auch wenn die Datenverarbeitung durch die Banken als Private stattfinde. Schon in der Speicherung der Daten identifizierte *Herzog* eine Beeinträchtigung der informationellen Selbstbestimmung der Kunden,[1387] unterließ insofern aber eine rechtliche Prüfung.

Diese beschränkte er auf die übrigen EDV-Prozesse. Aufgrund der staatlichen Anordnung und dem staatlichen Zweck würde das Bank-Kunde-Verhältnis (bei der Suche nach geldwäscherechtlichen Auffälligkeiten) transformiert und damit zu einem öffentlich-rechtlichen.[1388] *Herzog* ordnete die Banken aber deswegen nicht als Beliehene oder Verwaltungshelfer ein. Auch käme es nicht darauf an, ob das Handeln der Banken eine mittelbare oder unmittelbare Grundrechtsbeeinträchtigung sei, da jedenfalls die Verpflichtung der Banken auf den Staat zurückzuführen ist und damit in jedem Fall unmittelbar dem Verfassungsrecht unterliegt.

Ausgehend von dieser Feststellung warf *Herzog* die Frage auf, ob ein Kontenmonitoring gestützt auf § 14 Abs. 2 Nr. 2 GwG 1993 nach dem damals geltenden Datenschutzrecht zulässig sein könnte. Dieses sah in § 4 Abs. 1 BDSG 1990[1389] bereits vor, dass jede Datenverarbeitung eine Einwilligung oder gesetzliche Grundlage voraussetzt. Für gesetzliche Eingriffe in die informationelle Selbstbestimmung hatte das BVerfG spezifische Be-

1383 *Herzog*, WM 1996, 1753 (1756 ff.).
1384 *Dahm*, WM 1996, 1285 (1290).
1385 Vgl. nur *Poscher* in Miller (Hrsg.), Privacy and Power, 2017, S. 129 (132 f.).
1386 *Herzog*, WM 1996, 1753 (1757) mit Verweis auf BVerfGE 65, 1 (43) – Volkszählung.
1387 Idem, (1757).
1388 Idem, (1757).
1389 Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990, BGBl. I, S. 2954

stimmtheitsanforderungen formuliert. Danach müssen die Art, Umfang und Zweck der Datenverarbeitung präzise und bereichsspezifisch festgelegt werden.[1390] Diese Bestimmtheitsanforderungen sah *Herzog* von § 14 Abs. 2 Nr. 2 GwG 1993 nicht erfüllt, da die Vorschrift keine Voraussetzungen für eine Datenerhebung artikulierte.[1391]

Auch § 28 Abs. 1 Nr. 2 BDSG 1990 sah er nicht als taugliche Ermächtigungsgrundlage. Nach dieser Vorschrift dürften Private nur für eigene Zwecke Daten erheben. Die Bekämpfung der Geldwäsche sei primär aber nicht für die Imagepflege des Finanzstandorts Deutschlands, sondern für die Strafverfolgung gedacht und widmet sich damit einem genuin öffentlichen Zweck.[1392] Dennoch nähmen die Institute keine hoheitlichen Aufgaben i. S. d. § 2 Abs. 4 S. 2 BDSG 1990 wahr, weshalb auch die gesetzlichen Grundlagen des BDSG für die Datenverarbeitung durch öffentliche Stellen nicht einschlägig seien.[1393] Sie seien lediglich in die Pflicht genommene Private. Damit stellte sich *Herzog* gegen *Dahms* Einschätzung[1394], dass die Banken verwaltungsrechtlich als Beliehene anzusehen wären. Seine Meinung hat sich heute weitestgehend durchgesetzt. Die geldwäscherechtlichen Pflichten werden gemeinhin als gewerberechtliche Pflichten oder Pflichten *sui generis* und nicht als Kompetenzübertagung angesehen.[1395]

Obwohl es damit schon an einer Rechtsgrundlage für das Monitoring fehlen würde, nahm *Herzog* eine recht umfassende Verhältnismäßigkeitsprüfung anhand des Rechts auf informationelle Selbstbestimmung vor. Einen unionsrechtlichen Vorrang sprach er dabei nicht an.

Mit dem Zweck der Strafverfolgung – insbesondere der Aufklärung schwerer Straftaten – läge ein wesentlicher Auftrag des staatlichen Gemeinwesens vor.[1396] Allerdings erfasse das Kontenmonitoring aufgrund des groben Rasters notwendigerweise eine Unzahl unauffälliger Transaktionen des allgemeinen Lebens. Selbst die vom Raster erfassten „Vorverdachtsfälle" würden in den allermeisten Fällen noch keinen Anfangsverdacht begrün-

1390 BVerfGE 65, 1 (44 ff.) – Volkszählung.
1391 *Herzog*, WM 1996, 1753 (1758).
1392 Ibid.
1393 Idem, 1758 f.
1394 *Dahm/Hamacher*, wistra 1995, 206 (213 f.) *Dahm*, WM 1996, 1285 (1288).
1395 Übersicht bei *Degen,* Geldwäsche, 2009, S. 130 ff.; Für eine gewerberechtliche Pflicht BT-Drs. 18/11928, S. 26; *BaFin,* Auslegungs und Anwendungshinweise GwG: AT, Mai 2020, S. 76; *Kaetzler*, CCZ 2008, 174 (174); „Pflicht sui generis": *Barreto da Rosa* in Herzog GwG, § 43 Rn. 5; *Lenk*, JR 2020, 103 (105 Fn 15).
1396 *Herzog*, WM 1996, 1753 (1759) mit Verweis auf BVerfG, JZ 1987, 1118 (1119).

den.[1397] Dennoch sollten diese Fälle festgehalten und von der Aufsichtsbehörde kontrollierbar, dem Staat also zugänglich, sein. Eine solche Vorfeldaufklärung bedürfe einer besonders strengen Verhältnismäßigkeitskontrolle.[1398]

Schon im Rahmen der Erforderlichkeitsprüfung bestünden erhebliche Zweifel. Ein gleich geeigneter Zweck könnte auch dann erreicht werden, wenn die Überwachung des Finanzverkehrs von materiellen und formellen Voraussetzungen abhängig wäre und durch bestimmte Verfahrensvorschriften eingehegt – wie etwa die Überwachung des Fernmeldeverkehrs.[1399] In diesem Fall wäre die Beeinträchtigung deutlich milder.

Im Übrigen sei das Monitoring nicht angemessen.[1400] Es teile Charakteristika staatlicher Überwachungsmaßnahmen wie der Rasterfahndung oder Telefonüberwachung. Massenhaft würden Daten verarbeitet, die alltägliches legales Verhalten beträfen. Jeder betroffene Bürger befinde sich im *Vorhof des Verdachts*.[1401] Wie auch *Dahm* verglich *Herzog* das EDV-Monitoring mit der Auslandsfernmeldeaufklärung durch den BND. Diese sei vom BVerfG zutreffend als verdachtslose Rasterfahndung gewertet worden.[1402]

Dass Private zu einer Datensammlung auf Vorrat in die Pflicht genommen würden, sei dabei noch skeptischer zu betrachten als vergleichbare Sammlungen durch die Polizei. Die Indienstnahme führe zu einer umfassenden Strukturveränderung im staatlichen Sicherheitsgefüge.[1403]

Weiter würde der Grundsatz der Offenheit des Strafverfahrens unterlaufen. Die vorrätige Datensammlung und geheime Verdachtsanzeigen würden dazu führen, dass die Strafverfolgungsbehörden auf eine Inkulpation verzichten könnten, falls sich ein Anfangsverdacht nicht erhärtet. Die Betroffenen würden daher nie von den Ermittlungen im Vorfeld erfahren und wären faktisch vom Rechtsschutz ausgeschlossen.[1404]

Aufgrund dieser Umstände könne das Interesse der Strafverfolgung den Eingriff in die informationelle Selbstbestimmung nicht rechtfertigen. Die massenhafte Inanspruchnahme Unverdächtiger sei mit rechtsstaatlichen Grundsätzen nicht vereinbar. Selbst wenn eine ausreichende gesetzliche

1397 *Ders.*, WM 1996, 1753 (1759).
1398 Idem, (1760).
1399 Idem, (1760 f.).
1400 Idem, (1761 f.).
1401 Idem, (1761).
1402 Idem, (1761) mit Verweis auf BVerfGE 93, 181 (182).
1403 Idem, (1762).
1404 Ibid.

Grundlage geschaffen würde, wäre fraglich, ob sie sich in den Grenzen des Verfassungsrechts halten könne.[1405]

Herzogs Kritik stieß zwar zunächst nicht auf größeres Echo, erhielt aber durchaus Zustimmung. *Dittrich/Trinkhaus* etwa sahen ebenfalls datenschutzrechtliche Probleme bei der Ermächtigung zur Speicherung von Verdachtsmeldungen.[1406] Sie teilten auch die Vorbehalte gegenüber dem EDV-Monitoring. Weder § 14 Abs. 2 Nr. 2 GwG 1993 noch § 28 Abs. 1 Nr. 2 BDSG 1990 seien ausreichende Grundlagen für eine solch umfassende Verarbeitung der Kundendaten zum Primärzweck der Strafverfolgung.[1407] Zur prinzipiellen verfassungsrechtlichen Zulässigkeit des Monitorings äußerten sie sich aber nicht.

b. Verteidigung des (EDV-)Research und -Monitorings durch *Michael Findeisen*

Die Lesart des § 14 Abs. 2 Nr. 2 GwG 1993 als Verpflichtung zur Errichtung interner Sicherheitsmaßnahmen einschließlich EDV-Monitoringsysteme wurde von *Findeisen*, dem zuständigen Referatsleiter bei dem BAKred, verteidigt.[1408] Die Vorschrift sei nicht nur ein Annex der konkreten Pflichten aus dem GwG, sondern bringe das Präventionsprinzip als eigene Säule des Anti-Geldwäscherechts zum Ausdruck.[1409]

Zur Inhaltsbestimmung verwies *Findeisen* auf die grundlegenden Normen der internationalen Geldwäschebekämpfung. § 14 Abs. 2 Nr. 2 GwG 1993 setzte Art. 11 der 1. EG-Geldwäscherichtlinie um und dieser wiederum die FATF-Empfehlungen von 1990.[1410]

Der Erkenntnisgewinn dieser Rechtsverweisung ist überschaubar. Weder Art. 11 der 1. EG-Geldwäscherichtlinie noch Nr. 20 der FATF-Empfehlungen 1990 schrieben konkrete Sicherungsmaßnahmen vor. Sie verpflichteten allenfalls zur Bereitstellung geeigneter bzw. adäquater Systeme und lesen sich somit wie Parallelvorschriften zu § 14 Abs. 2 Nr. 2 GwG 1993. Dennoch wollte *Findeisen* aus der Verpflichtung zur internen Sicherung die Pflicht

1405 Idem, (1763).
1406 *Dittrich/Trinkhaus*, DStR 1998, 342 (346).
1407 Idem, (347).
1408 *Findeisen*, wistra 1997, 121.
1409 Idem, (123 f.)
1410 *FATF*, 40 Recommendations, 1990.

zur Auswertung und Analyse der bei den Banken vorhandenen Datenbanken herleiten.[1411] Die aus dem GwG Verpflichteten hätten gravierende Erkennungsprobleme. Die Mehrzahl der Transaktionen im Geschäftsverkehr würden unbar durchgeführt und wären oberflächlich nicht auffällig. Auf diese Transaktionen seien die Identifizierungspflicht und die starren Schwellenwerte für Bargeschäfte nicht ausgerichtet. Diese orientierten sich vielmehr am klassischen Geschehen vor dem Bankschalter, das in der Praxis aber keine Relevanz mehr habe.[1412] Daher müsse stattdessen mit „Research" und „Monitoring" gearbeitet werden. Die Nutzbarmachung von Datenbanken zur Risikoprävention gehöre zum gewöhnlichen Sicherungsmanagement der Banken und sei daher auch für die Geldwäschebekämpfung fruchtbar zu machen. Das Research führe nicht zur Ausforschung des Kunden im Interesse der Strafverfolgungsbehörden, sondern diene dem Selbstschutz der Kreditinstitute. Insofern sei es datenschutzrechtlich unbedenklich.[1413]

c. Einführung des EDV-Monitorings durch Verlautbarung der BAKred im Jahr 1998 und anschließende Diskussion

Als ersten greifbaren Schritt hin zum verpflichtenden EDV-Monitoring wurde die Verlautbarung vom 30. März 1998[1414] verstanden.[1415] Nach Ziffer 30 der Verlautbarung („Abbruch der Geschäftsbeziehung") sollten Kreditinstitute Geschäftsbeziehungen längerfristig überwachen, wenn zuvor eine einzelne Transaktion zwar noch keinen Verdacht ausgelöst hatte, die Verdichtung eines Verdachts durch weitere Transaktionen aber möglich erschien. Nach Ziffer 34 (Bestellung eines Geldwäschebeauftragten) lit d.) sollten weiter durch den Geldwäschebeauftragten interne Organisationsanweisungen geschaffen werden, die gewährleisteten, dass solche Transaktionen mit besonderer Aufmerksamkeit behandelt werden, die bereits in der Vergangenheit aus dem Blickwinkel der Geldwäschebekämpfung auffällig geworden waren. Die Art und Weise dieser Sicherstellung wurde den Insti-

1411 *Findeisen*, wistra 1997, 121 (128).
1412 Ibid.
1413 Ibid.
1414 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.
1415 Etwa *Langweg* in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, § 14 Rn. 101.

tuten freigestellt. Rein faktisch dürfte es aber, wie *Findeisen* selbst bemerkt hatte[1416], schon damals nicht möglich gewesen sein, Auffälligkeiten in unbaren Transaktionen ohne die Verwendung einer EDV-Rasterung zu finden. Auch wenn in der Verlautbarung nicht ausdrücklich von EDV-Research bzw. – Monitoring gesprochen wurde, waren diese Prozesse durchaus intendiert.

aa. Erläuterung durch das BAKred bzw. *Michael Findeisen*

Dies wurde spätestens klar, als das BAKred noch im selben Jahr ein „Geldwäsche-Typologienpapier"[1417] als Rundschreiben an die deutschen Kreditinstitute versandte. In diesem wurden erstmals typische Auffälligkeiten beschrieben, die den geldwäscherechtlich Verpflichteten bei der Erkennung von Verdachtsfällen helfen sollten. Hier wurde erstmals ausdrücklich davon gesprochen, dass es sich um „*(EDV-gestützte Systeme) zur Sichtbarmachung geldwäscherelevanter Sachverhalte*"[1418] handle, die in Ziffer 34 lit. d) der Verlautbarung vom 30. März 1998 angesprochen würden.

Die Verlautbarung des BAKred vom 30. März 1998 wurde abermals vom Referatsleiter *Findeisen* in einem Fachbeitrag[1419] erläutert. Neue Argumente lieferte der Aufsatz zwar nicht, beschrieb aber erstmals in einigermaßen konkreter Form, wie sich das BAKred den Research- und Monitoring-Prozess bei den Kreditinstituten vorstellte. Im Rahmen der Bonitätsprüfung der Kunden würden Banken schon länger *Scoringsysteme* verwenden, bei denen aus den bankeigenen Datenbeständen Informationen extrahiert und zu einem Kundenwert verdichtet würden. Außerdem würden die gesammelten Massendaten mithilfe von Data-Mining-Algorithmen analysiert und in der Folge für Akquisitionszwecke genutzt.[1420]

Dieses Modell des „*Data Based Marketing*" ließe sich auf die Geldwäschebekämpfung übertragen. Aus den Transaktionen der Kunden könnten Sekundärinformationen gewonnen werden, die sich zu einem Kundenprofil vervollständigen ließen. Durch eine EDV-Analyse der Kundentransaktio-

1416 *Findeisen*, wistra 1997, 121 (128); *ders.*, WM 1998, 2410.
1417 *BAKred,* Rundschreiben 19/1998, Typologienpapier-Geldwäsche, 02.11.1998.
1418 Idem, S. 49.
1419 *Findeisen*, WM 1998, 2410.
1420 Idem, (2418).

nen anhand dieser Profile könnten die Grenzen des Massengeschäfts überwunden werden.[1421]

Das Research-Vorgehen würde im Ausland bereits eingesetzt. Dort hätten die Banken Computerprogramme entwickelt, die Listen mit ungewöhnlichen Transaktionen ausdrucken könnten. Die Ungewöhnlichkeit ergebe sich eben aus den im Rahmen des Research gewonnenen Kundenprofilen.[1422]

bb. Erneute Kritik von Felix Herzog

Kritik an der Verlautbarung kam abermals von *Felix Herzog*,[1423] der sein Vorbringen aus dem Jahr 1996 wieder aufgriff und insbesondere auch auf die fachlichen Erläuterungen von *Findeisen* einging. In seinem Beitrag sprach *Herzog* zunächst formelle bzw. Fragen des allgemeinen Verwaltungsrechts in Bezug auf die Verlautbarung an. Deren Rechtscharakter sei fraglich. Anders als *Findeisen* meine[1424], sei die Einordnung als faktisch bindende norminterpretierende Verwaltungsvorschrift nicht unproblematisch, da eine solche Bindung nur intern stattfinden kann, d. h. innerhalb des Verwaltungsapparats.[1425] Die Verlautbarung möchte das Gesetz aber faktisch[1426] bindend für Private auslegen und sieht recht konkrete Handlungspflichten vor. Sie ähnelte damit mehr einer Allgemeinverfügung, da die angestrebte Bindungswirkung nach außen zielt. Andererseits sei die Verlautbarung aber nicht unmittelbar zwangsbewehrt, was gegen den Charakter einer Allgemeinverfügung spräche. *Herzog* konstatierte daher, dass die Verlautbarung einer rechtlich strittigen, neuartigen Form von Verwaltungshandeln zuzuordnen sei, nämlich den „normkonkretisierende[n] Verwaltungsvorschriften, die Außenwirkung für sich beanspruchen."[1427] Die rechtliche Einordnung der Verlautbarungen bzw. Rundschreiben des BAKred und nun der BaFin konnte auch bis heute nicht abschließend geklärt werden.[1428]

1421 Ibid.
1422 Ibid.
1423 *Herzog*, WM 1999, 1905.
1424 *Findeisen*, WM 1998, 2410 (2410 f.).
1425 *Herzog*, WM 1999, 1905 (1911); dazu *Sennekamp* in Mann/Sennekamp/Uetrichtz VwVfG, 2. Aufl., § 9 Rn. 15.
1426 *Findeisen*, WM 1998, 2410 (2411).
1427 *Herzog*, WM 1999, 1905 (1911) mit Verweis auf *Wolf*, DÖV 1992, 849.
1428 *Bauernfeind*, DÖV 2020, 110; *Fekonja,* Verlautbarungen, 2013, S. 91 ff., 181 ff.

Schon *Herzog* erkannte aber, dass es für die Bewertung des Verlautbarungsinhalts auf deren Rechtscharakter letztlich nicht ankommen kann, da jedes belastende Verwaltungshandeln mit Außenwirkung ohnehin an höherrangigem Recht, insbesondere den Grundrechten, zu messen sei.[1429]

Ausgehend von dieser Prämisse prüfte er zunächst, ob das GwG eine ausreichende Zuständigkeitsbestimmung des BAKred zum Erlass solcher Verlautbarungen vorsah. *Findeisen* hatte sich für das BAKred insofern auf § 6 Abs. 2 KWG und § 16 Nr. 2 GwG 1993 berufen.[1430] Nach diesen Vorschriften war das BAKred mit der Durchführung des GwG betraut und sollte Missständen im Kredit- und Finanzdienstleistungswesen entgegenwirken, welche u. a. die ordnungsmäßige Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen. Nach *Herzog* handelte es sich um reine Aufgabenzuweisungen, aus denen keine Ermächtigungen zum Erlass von grundrechtsbeeinträchtigenden Verlautbarungen hervorgehen würden.[1431]

Außerdem würde die Verlautbarung gegen den Vorbehalt des Gesetzes bzw. verfassungsrechtlichen Wesentlichkeitsgrundsatz verstoßen, nach dem der Gesetzgeber wesentliche Entscheidungen selbst treffen muss.[1432] Auch diese Grundsatzfrage hinsichtlich der Verlautbarungspraxis des BAKred bzw. der BaFin wird noch heute diskutiert.[1433]

Im Rahmen der Wesentlichkeitsbestimmung wird regelmäßig auf die „Grundrechtsrelevanz" des geregelten Sachbereichs abgestellt.[1434] Kurz gesagt bedeutet das, dass die Wesentlichkeit und damit die Notwendigkeit einer Regelung durch Gesetz steigt, je intensiver die Materie in Grundrechte eingreift.[1435]

1429 *Herzog*, WM 1999, 1905 (1912); siehe allgemein *Starck* in v. Mangoldt/Klein/Starck GG, Art. 1 Rn. 227; ausf. zu Verwaltungsvorschriften als Grundrechtseingriff und Rechtsschutz *Sauerland,* Verwaltungsvorschrift, 2005, S. 391 ff., 417 ff.

1430 *Findeisen*, WM 1998, 2410 (2410 f.).

1431 *Herzog*, WM 1999, 1905 (1912).

1432 Idem, (1915) mit Verweis auf BVerfGE 61, 260 (275)

1433 *Fekonja,* Verlautbarungen, 2013, S. 194 ff.; *F. A. Schäfer* in Boos/Fischer/Schulte-Mattler KWG, 5. Aufl. 2016, § 6 Rn. 16 ff.

1434 BVerfGE 49, 89 (126 f.); *Kotzur* in v. Münch/Künig GG, GG Art. 20 Rn. 157; *Kalscheuer/Jacobsen*, DÖV 2018, 523 (525).

1435 *Maurer/Waldhoff,* Verwaltungsrecht, 20. Aufl. 2020, § 6 Rn. 14; *Sauerland,* Verwaltungsvorschrift, 2005, S. 304 Fn 513 mit Verweis auf *Horn,* Verwaltung, 2020, S. 85 f. Fn 239.

Im Rahmen dieser Darstellung bezog er sich auf seine Ausführungen aus dem Jahr 1996,[1436] die er durch die Verlautbarung als bestätigt ansah. Das EDV-Research und -Monitoring käme in den Ziff. 18, 30 und 34 lit. d) zum Ausdruck.[1437] Die Vorgänge beeinträchtigten die informationelle Selbstbestimmung der Kunden. Zwar würde schon die Speicherung der Inhaltsdaten, deren Rechtsgrund nicht erwähnt wird, die informationelle Selbstbestimmung berühren, deren Verarbeitung sei aber ein „qualitativer Sprung" und somit eine eigenständig zu wertende Belastung.[1438]

Da ein Grundrechtseingriff vorliegt, greife der Vorbehalt des Gesetzes in Verbindung mit der Wesentlichkeitstheorie. Eine gesetzliche Grundlage für die in der Verlautbarung geforderten Maßnahmen gäbe es aber nicht. Weder § 14 Abs. 2 Nr. 2 GwG 1993 noch § 28 Abs. 1 BDSG 1990 kämen infrage. Eine hypothetische Verhältnismäßigkeitsprüfung der EDV-Prozesse unter der Prämisse einer geeigneten gesetzlichen Grundlage nahm *Herzog* in dem Beitrag nicht mehr vor.

Im Grunde zustimmend, aber differenziert äußerte sich *Kaufmann*[1439] zu den Argumenten *Herzogs.* Bei der bankinternen Datenrasterung handele es sich in der Tat um einen erheblichen Eingriff, da sich aus der Summe der Transaktionen eines Kunden ein wirtschaftliches Tätigkeits- und Leistungsprofil der Person ergeben würde.[1440] Solange der Eingriff aber bankintern bliebe, hätte er aufgrund des Privatrechtsverhältnisses keine Grundrechtsrelevanz. Erst die Verdachtsmeldung bilde die Schnittstelle zum hoheitlichen Tätigwerden.[1441] Würden die Banken eine Tätigkeit melden, deren Verdacht sich aus dem EDV-Research ergeben hätte, würde aufgrund der Meldung eine Verbindung zur Strafverfolgung hergestellt. Der gesamte Prozess würde dadurch einen staatlichen Charakter erhalten. Dies hätte zur Folge, dass der Staat sich bankinterne Daten beschafft hätte. So ein Vorgehen wäre aber in der StPO nicht vorgesehen und bräuchte eine spezifische Ermächtigungsgrundlage. Hierfür käme § 14 Abs. 2 Nr. 2 GwG aufgrund dessen Unbestimmtheit nicht infrage.[1442] Nach Ansicht *Kaufmanns* durften Banken die Daten ihrer Kunden also grundsätzlich rastern, die Ergebnisse

1436 *Herzog*, WM 1996, 1753 (1757 ff.).
1437 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.
1438 *Herzog*, WM 1999, 1905 (1916).
1439 *Kaufmann,* Geldwäsche, 2001, S. 174 ff.
1440 Idem, S. 176 f.
1441 Idem, S. 177.
1442 Ibid.

dieser Recherche aber nicht an die Staatsanwaltschaft übermitteln. Diese Vorstellung kann angesichts der Synergie bzw. der Wechselwirkung von Datenverarbeitungsschritten im Rahmen von Überwachungsmaßnahmen nicht überzeugen (s. Kap. B. I. 1. c.).

cc. Diskussionsbeiträge aus der Bankwirtschaft

Auch von Autoren aus der Bankwirtschaft wurde die Einführung des EDV-Research bzw. Monitoring mitunter kritisch besprochen. Der Geldwäschebeauftragte der Citibank *Bergles* und der Rechtsreferent beim Bankenfachverband *Schirnding* veröffentlichten gemeinsam einen Beitrag zur Umsetzung der EDV-Systeme in der Praxis.[1443] Auch sie begriffen die Ziff. 30 und 34 d der BAKred-Verlautbarung vom 30.03.1998 als Grundlage für die Anforderung zur Implementierung bankinterner Research-Systeme. Dabei versuchten sie zunächst, Ordnung in die bislang meist noch undifferenziert verwendeten Begriffe des „Research" und „Monitoring" zu bringen.[1444] Unter Research verstanden sie die personenunabhängige Recherche nach Auffälligkeiten im Datensatz der Banken. Als Monitoring bezeichneten sie die Überwachung eines konkreten Kontos.

Im Folgenden versuchten sie die Funktionsweise eines Research-Systems, das aus der großen Masse der Bankkonten die geldwäscheverdächtigen Fälle herausfiltert, näher zu umschreiben.[1445] Zunächst sollten in periodischen Abständen alle Konten auf zuvor definierte „Auffälligkeiten" untersucht werden. Die „Auffälligkeiten" müssten dann von dem Geldwäschebeauftragten oder einem Mitarbeiter kontrolliert und das entsprechende Konto einer Überwachung, also dem Monitoring, unterzogen werden. Falls sich kein Verdacht ergibt, sollte dies dem System klar gemacht werden, damit das Konto bei der nächsten periodischen Prüfung nicht unnötigerweise wegen den schon kontrollierten Kontobewegungen erneut gemeldet wird. Ergibt sich hingegen ein Verdacht, würde dieser nach § 11 GwG 1993 gemeldet.

Die Auffälligkeiten könnten nach relativen oder starren Mustern erkannt werden – also entweder an den regelmäßigen Bewegungen des geprüften Kontos oder festgelegten Schwellenwerten. Zentral sei die Höhe einer

1443 *Bergles/Schirnding*, ZBB 1999, 58.
1444 Idem, (59).
1445 Idem, (60 f.).

Transaktion. Es müssten aber weitere elektronisch greifbare Indikatoren hinzukommen – etwa ein Auslandsbezug, die Nationalität des Kunden, der Wohnort, ein Abbruch der Geschäftsbeziehung schon kurz nach Eröffnung des Kontos, die Anzahl der in Anspruch genommenen Bankprodukte und weitere.[1446]

Eine Betrachtung der Verfassungsmäßigkeit der von ihnen vorgeschlagenen Funktionsweise des EDV-Research und –Monitoring nahmen *Bergles/Schirnding* nicht vor. Sie wiesen lediglich auf die Kritik durch *Herzog* hin, ohne diese zu bewerten.

Einen Anschluss an dessen Argumente findet man jedoch in einer ausführlichen Besprechung des GwG samt den Verlautbarungen des BAKred durch die Mitarbeiter der Sparkasse Bonn *Lang/Schwarz/Kipp*.[1447] Aufbauend auf der Klarstellung von *Bergles/Schirnding* definierten sie die Begrifflichkeiten der EDV-Prozesse noch konkreter. *Lang/Schwarz/Kipp* verzichteten erstmals auf den Begriff des Research, der auch heute kaum mehr verwandt wird,[1448] und unterschieden stattdessen verschiedene Formen bzw. Phasen des Monitorings. Das bislang als Research bekannte Suchen nach Auffälligkeiten in nicht näher konkretisierten Datenbeständen bezeichneten sie als „Monitoring ohne Verdacht". Das Überwachen von Konten, bei denen eine Auffälligkeit entdeckt wurde, definierten sie hingegen als „Monitoring mit Verdacht". Bei diesem gäbe es einen speziell zu betrachtenden Unterfall, wenn der Verdacht auf einer externen Anfrage etwa einer Staatsanwaltschaft beruht. Diese dritte Kategorie bezeichneten sie als „Monitoring aufgrund externer Anfrage".[1449]

Die so identifizierten drei Varianten des Monitorings unterzogen sie in der Folge einer umfassenden verfassungsrechtlichen Prüfung. Am kritischsten wurde dabei das Monitoring ohne Verdacht beleuchtet.[1450]

Herzogs Ansicht[1451], dass schon die Speicherung der Kontoinhaltsdaten das Recht auf informationelle Selbstbestimmung tangiert, wollten sie in dieser Pauschalität nicht gelten lassen. Die Speicherung im Rahmen einer Geschäftsbeziehung erfolge mit Wissen und Wollen des jeweiligen Kunden,

1446 Idem, (61) mit Verweis auf *BAKred,* Rundschreiben 19/1998, Typologienpapier-Geldwäsche, 02.11.1998.
1447 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 610 ff.
1448 Vgl. *BaFin,* Auslegungs- und Anwendungshinweise GwG, BT: Kreditinstitute, Juni 2021, S. 14 lfd. Nr. 6.1.
1449 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 642 ff., Rn. 8.77.
1450 Idem, S. 644 ff., Rn. 8.4.2.X
1451 Idem, (1757).

da die Durchführung des Bankvertrags andernfalls nicht möglich wäre.[1452] Dabei verkannten sie aber offenbar, dass *Herzog*[1453] nicht von einer Verletzung des Rechts auf informationelle Selbstbestimmung durch die Speicherung gesprochen hatte, sondern nur von einer „Berührung".

Hinsichtlich der Verarbeitung der Datenbestände durch das anlasslose Monitoring teilten *Lang/Schwarz/Kipp* die verfassungsrechtlichen Bedenken *Herzogs*. Der Wortlaut des § 14 Abs. 2 Nr. 2 GwG 1993 spräche keinesfalls dafür, dass es sich um eine gesetzliche Grundlage für einen Eingriff in das Recht auf informationelle Selbstbestimmung handelte. Ebenso wenig wäre eine solche Grundlage nach Art. 5 der 1. EG-GWRL notwendig gewesen, denn auch deren Wortlaut erfordere nur die Prüfung beim Vorliegen von Auffälligkeiten und verpflichte nicht zur Vorfeldsuche.[1454] Differenzierter betrachteten die Autoren die Frage, ob sich eine gesetzliche Grundlage aus dem Datenschutzrecht und dort aus § 28 Abs. 1 Nr. 2 BDSG 1990 zur „Wahrung berechtigter Interessen" ergeben könnte.[1455] Die Früherkennung von Geldwäschefällen wäre schon deshalb im Interesse der Banken, da § 261 Abs. 5 StGB 1992[1456] das leichtfertige Nichterkennen von Geldwäsche unter Strafe stellte, was vor allem Bankmitarbeiter beträfe. Allerdings müsse das berechtigte Interesse i. S. d. § 28 Abs. 1Nr. 2 BDSG 1990 in Abwägung der entgegenstehenden Interessen ausgelegt werden.[1457] Diese Abwägung könnte nur zugunsten der Kunden ausfallen, da die Rasterung theoretisch aller Kundendaten schon aufgrund der Vielzahl der Kunden einen erheblichen Eingriff darstellte, dem ein höchst unsicheres Ergebnis gegenüberstünde.[1458] Dieser Datennutzung würde der Kunde, wenn er entscheiden könnte, sicher widersprechen. Auch sei zu berücksichtigen, dass Kunden als auffällig erkannt werden könnten, die tatsächlich mit Geldwäsche nichts zu tun haben. Dies würde das Vertrauensverhältnis zwischen Bank und Kunde zerrütten.[1459] Die Ansicht des BAKred, dass das anlasslose Monitoring auf

1452 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 650 Rn. 8.100.
1453 *Herzog*, WM 1996, 1753 (1757).
1454 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 651 Rn. 8.103.
1455 Idem, S. 654 ff., Rn. 8.106 ff.
1456 Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15. Juli 1992, BGBL. I, S. 1302
1457 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 658 f. Rn. 8.109 mit Verweis auf BGH, NJW 1986, 2505 (2506).
1458 Iden, S. 661 Rn. 8.111.
1459 Idem. S. 662, Rn. 8.111.

§ 28 Abs. 1 Nr. 2 BDSG 1990 gestützt werden könne, sei deshalb unzutreffend.[1460]

Dem anlasslosen Monitoring stünde weiter entgegen, dass ein *hinreichender Anlass* von der Rechtsprechung als notwendige Mindestvoraussetzung von Eingriffen in die informationelle Selbstbestimmung gefordert würde. Je erheblicher ein solcher Eingriff sei, desto enger müsste er auf bestimmte Anlässe begrenzt sein.[1461] Über diesen Umstand herrsche aufgrund mehrerer Entscheidungen des BVerfG Einigkeit.[1462] Ermittlungen, die erst einen Anfangsverdacht zutage fördern sollten, verstießen deshalb gegen den Grundsatz der Verhältnismäßigkeit.[1463] Um genau so eine anlasslose Ermittlungsmaßnahme handle es sich aber bei dem EDV-Research, das das BAKred in der Verlautbarung vom 30.03.1998[1464] gefordert hatte.[1465]

Wie auch *Herzog* (s.o.)[1466] befanden *Lang/Schwarz/Kipp*, dass es sich bei der Durchführung des EDV-Monitoring nicht um eine hoheitliche Tätigkeit handeln könne.[1467] Es müsse sich schon deshalb lediglich um eine Inpflichtnahme Privater handeln, da die geforderte Maßnahme einer hoheitlich handelnden Behörde gar nicht zustehe.[1468] Gleichzeitig könne es aber nicht angehen, dass Private zu einem Eingriff aufgefordert werden, der dem Staat selbst nicht zustünde, da andernfalls der Grundrechtsschutz umgangen würde. Die Inpflichtnahme zum anlasslosen EDV-Monitoring sei insofern nicht zu rechtfertigen.[1469]

Etwas anderes gelte für das anlassbezogene Monitoring.[1470] Hier fehle die notwendige Voraussetzung eines hinreichenden Anlasses gerade nicht. Auch könnte man hier durchaus von einer Datenverarbeitung im berechtigten Interesse der Verpflichteten ausgehen, denn wenn eine Auffälligkeit bekannt ist, liefen die jeweils betrauten Mitarbeiter tatsächlich Gefahr, einer

1460 Idem, S. 661 ff., Rn. 8.111 f.
1461 Idem, S. 666. ff., Rn. 8.119 ff.
1462 Idem, S. 668 ff., Rn. 8.122 ff. mit Verweis vor Allem auf BVerfG, WM 1994, 691 = NJW 1994, 2079 und BVerfG ZIP 1995, 100 = NJW 1995, 2839.
1463 Idem, S. 680, Rn. 8.151 mit Verweis auf BVerfG, NJW 1997, 2163; Hamacher, WM 1997, 2149 (2151).
1464 *BAKred,* Verlautbarung Geldwäsche, 30.03.1998, abgedruckt in Fülbier/Aepfelbach/Langweg GWG, 5. Aufl. 2006, Anhang III.1.
1465 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 683 Rn. 8.156.
1466 *Herzog*, WM 1996, 1753 (1758).
1467 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 685 Rn. 8.159 f.
1468 Idem, S. 685 Rn. 8.160.
1469 Ibid.
1470 *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 690 ff., Rn. 8.172 ff.

Strafverfolgung wegen § 261 Abs. 5 StGB 1992 ausgesetzt zu werden.[1471] Außerdem seien die Institute an einer hohen „Qualität" der Verdachtsanzeigen interessiert. Sie wollen fehlerhafte Meldungen vermeiden. Hierzu können konkrete Nachforschungen im Wege eines anlassbezogenen Monitorings nützlich sein.[1472]

Das anlassbezogene Monitoring soll dabei auch dann möglich sein, wenn der Verdacht von außen herangetragen wird – etwa von einer Staatsanwaltschaft.[1473] Diese „dritte Kategorie"[1474] des Monitorings sollte aber von spezifischen Voraussetzungen abhängig gemacht werden. So müsse der Name des Verdächtigten genannt werden, denn eine Anregung zum Monitoring „ins Blaue hinein" sei aus den zuvor genannten Gründen zum anlasslosen Monitoring unzulässig.[1475]

4. Gesetzliche Einführung des EDV-Monitoring im Jahr 2002

Die Diskussion um das Kontenmonitoring ging weiter, nachdem § 14 Abs. 2 Nr. 2 GwG durch das Geldwäschebekämpfungsgesetz[1476] abgeändert und § 25a Abs. 1 Nr. 4 KWG mit dem vierten Finanzmarktförderungsgesetz[1477] neu eingefügt wurde.

Anstatt zur *„Entwicklung interner Grundsätze, Verfahren und Kontrollen zur Verhinderung der Geldwäsche"* waren die betroffenen Institute nunmehr nach § 14 Abs. 2 Nr. 2 GwG 2002 verpflichtet, *„interne Grundsätze, angemessene geschäfts- und kundenbezogene Sicherungssysteme und Kontrollen zur Verhinderung der Geldwäsche und Finanzierung terroristischer Vereinigungen"* zu entwickeln. In § 25a Abs. 1 Nr. 4 KWG 2002 hieß es zudem: *„Ein Institut muss über angemessene (…) Sicherungssysteme (…) verfügen; bei Sachverhalten, die aufgrund des Erfahrungswissens über die Methoden der Geldwäsche zweifelhaft oder ungewöhnlich sind, hat es diesen vor dem*

1471 Idem, S. 690 ff., Rn. 8.175 ff.
1472 Idem, S. 694 ff., Rn. 8.182.
1473 Idem, S. 698 ff., Rn. 8.190 ff.
1474 Idem, S. 642 ff. Rn. 8-77 ff., insb. S. 644 Rn. 8.78, 8.80.
1475 Idem, S. 699 ff., Rn. 8.193 ff.
1476 Gesetz zur Verbesserung der Bekämpfung der Geldwäsche und der Bekämpfung der Finanzierung des Terrorismus (Geldwäschebekämpfungsgesetz) vom 08. August 2002 (BGBl. I S. 3105).
1477 Gesetz zur weiteren Fortentwicklung des Finanzplatzes Deutschland (Viertes Finanzmarktförderungsgesetz) vom 21 Juni 2002 (BGBl. I, S. 2010).

Hintergrund der laufenden Geschäftsbeziehung und einzelner Transaktionen nachzugehen."

Die Einführung dieser *Sicherungssysteme* wurde in den Gesetzesmaterialien zu § 25a Abs. 1 Nr. 4 KWG 2002 ausdrücklich als gesetzliche Verankerung der EDV-Monitoringsysteme verstanden.[1478] Aus Sicht der Bundesregierung waren die Regelungsgehalte von § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002 aber, anders als der Bundesrat meinte, unterschiedlicher Natur.[1479]

Offenbar wich die Bundesregierung damit von der Vorstellung des BAKred ab, dass sich die Pflicht zum EDV-Monitoring aus § 14 Abs. 2 Nr. 2 GWG 1993 ergeben würde, und bevorzugte eine Regelung im KWG, damit ausschließlich Banken betroffen waren. Die Kritik an der zuvor vom BAKred geäußerten Rechtsauffassung, insbesondere bzgl. des Fehlens einer ausdrücklichen Ermächtigung zur Datennutzung, wurde aber bei der Schaffung des § 25a Abs. 1 Nr. 4 KWG 2002 nicht berücksichtigt. Auch diese Norm ließ eine entsprechende Klarstellung noch vermissen.

a. Stellungnahme des ZKA

Der ZKA hatte zu der Einführung des § 25a Abs. 1 Nr. 4 KWG 2002 durch das vierte Finanzmarktförderungsgesetz im Rahmen des Gesetzgebungsprozesses ausführlich Stellung genommen.[1480] Mit dem BAKred sei man sich prinzipiell einig, dass bei entsprechendem Anlass (sic), der kunden- oder transaktionsbezogen sein könne, alle Maßnahmen zur Aufklärung getroffen würden – auch die Verwendung der bankinternen EDV.[1481] Das sei aber schon auf Grundlage der aktuellen Gesetzeslage möglich. Eine Gesetzesänderung wäre also nur notwendig, wenn vom Gesetzgeber eine anlassunabhängige (sic) bzw. permanente Überwachung der Bürger für notwendig erachtet würde.[1482] Dies aber stellte eine Instrumentalisierung der Institute zu Zwecken der Strafverfolgung dar und ginge mit einem erheblichen Vertrauensverlust bei ihren Kunden einher. Auch würde § 25a

1478 BT-Drs. 14/8017, S. 125.
1479 BT-Drs. 14/9043, S. 11; aA. der Bundesrat idem, S. 5 f.
1480 *ZKA,* Stellungnahme zum 4. Finanzmarktförderungsgesetz, AZ: 413-FPLD, 13. Februar 2002.
1481 Idem, S.10.
1482 Ibid.

Abs. 1 Nr. 4 KWG 2002 die Anforderungen an eine gesetzliche Grundlage für eine solche permanente Rasterung nicht erfüllen. Die Vorschrift sei schon nicht bestimmt genug und hätte darüber hinaus aufgrund des Sachzusammenhangs im GwG normiert werden müssen.[1483]

b. Diskussion in der Literatur

In der Literatur war umstritten, ob die gesetzlichen Neuregelungen als endgültige Pflicht der Kreditinstitute bzw. der übrigen nach dem GwG Verpflichteten zum anlasslosen (EDV-)Monitoring verstanden werden mussten.[1484] Der damalige FAZ-Wirtschaftsredakteur *Jahn* verstand jedenfalls § 25a Abs. 1 Nr. 4 KWG 2002 als ausdrückliche gesetzliche Verpflichtung der Kreditinstitute zur aktiven und systematischen Durchforschung ihrer Kundendaten nach Geldwäschefällen.[1485] Eine verfassungsrechtliche Prüfung dieser Pflicht nahm er zwar nicht vor. *Jahn* stellte jedoch fest, dass die *„flächendeckende Präventivkontrolle und Datenspeicherung von Finanztransaktionen ein Ausmaß erreicht hätten, dass sich die Bürger eines Rechtsstaats in keinem anderen Lebensbereich bieten lassen würden.*"[1486]

Der Rechtsanwalt *Escher* hingegen war der Meinung, dass sich eine Pflicht zur anlasslosen Überwachung aus den § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002 nicht ergeben würde. Die betroffenen Institute müssten vielmehr ein Scoring-Verfahren etablieren, wonach bestimmte Transaktionen bzw. Transaktionstypen oder Kundentypen auf Auffälligkeiten durch die EDV zu prüfen wären und gegebenenfalls individuelle Nachforschungen angestellt werden sollten.[1487] Wie aber die so bestimmten Transaktionen gefunden werden sollten, wenn nicht alle verfügbaren Daten in die Rasterung einbezogen würden, ließ er offen.

Differenzierter sahen es Autoren aus der Bankwirtschaft selbst. So meinten *Bergles/Eul* etwa, dass sich aus der gesetzlichen Formulierung zwar

1483 Idem, S. 11.
1484 Siehe *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 52, der sich aber klar positionier und auf die Widersprüchlichkeit eines „anlassbezogenen" Monitorings hinweist; offen dagegen noch immer bei *Hartmann* KJ 2007, 2 (16 f.): „angedeutete Präventivkontrolle und Datenspeicherung".
1485 *Jahn*, ZRP 2002, 109 (110).
1486 Idem, (111).
1487 *Escher*, BKR 2002, 652 (661 f.).

nicht unmittelbar eine Pflicht der Kreditinstitute zur anlasslosen Überwachung ihrer Kunden ergäbe. Durch die neuen gesetzlichen Regelungen würden sie aber mehr denn je zu solch einer „Rasterung" gedrängt.[1488] Derweil waren sie der Auffassung, dass die geänderten bzw. neu gefassten Vorschriften § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002 nichts an der bisher vorgetragenen Kritik hinsichtlich der Normbestimmtheit ändern würden.[1489] Die neuen Begrifflichkeiten, insbesondere die Einführung „angemessener Sicherungssysteme", seien *„wenig geeignet allgemeine akzeptierte Datenschutzgrundsätze zu überschreiben."*[1490]

Allerdings käme § 28 Abs. 1 Nr. 2 BDSG 1991, der eine Datennutzung zu eigenen Zwecken erlaubt, hierzu durchaus in Betracht. Die im Rahmen des Research ermittelten Daten würden nicht unmittelbar und uneingeschränkt an die Sicherheitsbehörden übergeben, sondern wären Teil eines Riskmanagements, das den Banken im Vorfeld erlaube, ihre eigenen Risiken zu erkennen. Erst dieses Management erlaube eine effektive Geldwäschebekämpfung und mithin eine Verhinderung negativer Publicity, an der die Kreditinstitute ein eigenständiges wirtschaftliches Interesse hegten, wofür *Bergles/Eul* einige Beispiele aus der Presse anführten.[1491]

Ob dieses Interesse aber ein EDV-„Research/Screening" rechtfertigten könnte, sei fraglich. Im Rahmen des Durchlaufs der Transaktionsdaten könnten Bankkunden in einen falschen Verdacht geraten. Die Systeme bzw. deren Parameter müssten daher so konfiguriert werden, dass der Kreis der Personen, über den nach dem EDV-Programm weitere Nachforschungen angestellt werden, möglichst klein bliebe.[1492] Andererseits träte ein Vertrauensverlust bei den Kunden ein, den die Institute mit den Aktivitäten zur Verhinderung der Geldwäsche gerade zu verhindern suchten. Da insofern kein klarer Ausgang der Interessenabwägung im Rahmen des § 28 Abs. 1 Nr. 2 BDSG 1991 möglich sei, wäre der rechtliche Konflikt zwischen dem EDV-„Research/Screening" weiterhin ungelöst.[1493]

Der Anwalt *Scherp* betrachtete die Einwände gegen die „Researchpflicht", die er einheitlich mit § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG

1488 *Bergles/Eul*, BKR 2002, 556 (556); *Eul* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, S. 1085 (1098 ff.).
1489 *Bergles/Eul*, BKR 2002, 556 (562 f.).
1490 Idem, (562).
1491 Idem, (562 f.).
1492 Idem, (563).
1493 Idem, (564).; ausf. *Eul* in Roßnagel (Hrsg.), Hdb. Datenschutzrecht, 2003, S. 1085 (1100 ff.).

2002 überschrieb, als unschlüssig.[1494] Durch deren Einführung sei zunächst dem Argument, es bestünde keine taugliche Rechtsgrundlage, der Boden entzogen.[1495] Damit sei zwar noch nichts über die verfassungsrechtliche Zulässigkeit gesagt, auch hier könnten sich die kritischen Argumente aber nicht durchsetzen. Insbesondere kritisierte *Scherp* den Vergleich mit der Rasterfahndung i. S. d. § 98a StPO. Beim Kontenresearch würden nicht verschiedene Datenbanken abgeglichen, sondern nur die des jeweiligen Instituts. Betroffen seien somit nur Daten, die die Kunden freiwillig herausgegeben hätten. Die Daten seien in den Häusern vorhanden und deshalb dürften die Institute damit auch zu Zwecken der Geldwäschebekämpfung arbeiten.[1496] Bevor die Ergebnisse des Research analysiert und eventuell zu einer Meldung an staatliche Behörden führten, wäre lediglich das private Verhältnis von Bank und Kunde betroffen. Hier entfalteten die Grundrechte nur eine Ausstrahlungswirkung, weshalb die informationelle Selbstbestimmung nur begrenzt tangiert sei.[1497] Angesichts dessen sei das Research verhältnismäßig. Eine effektive Geldwäsche funktioniere nur durch einen risikoanalytischen Ansatz, der auf verschiedenen Risikograden und davon abhängenden Maßnahmen basierte. Durch die anschließenden Folgemaßnahmen würde gerade verhindert, dass es zu flächendeckenden Verdachtsmeldungen käme.[1498]

Von einer „tatbestandlichen Grundlage des Kontenscreening" sprachen auch *Herzog/Christmann*.[1499] Ihrer Meinung nach waren die § 14 Abs. 2 Nr. 2 GwG 2002 und § 25a Abs. 1 Nr. 4 KWG 2002, die sie ebenfalls komplementär verstanden, eine ausdrückliche Ermächtigung der Banken zur digitalen Kontrolle der Transaktionen ihrer Kunden. Die Vorschriften würden aber den verfassungsrechtlichen Anforderungen an solch einen Eingriff in die informationelle Selbstbestimmung nicht gerecht werden.[1500] Ob die Banken durch die Vorschriften verpflichtet würden, ließen sie offen.

Bemerkenswert ist, dass *Herzog/Christmann* nicht nur die Ermächtigung der Banken ansprachen, sondern das Monitoring in einen Kontext mit den weiteren Änderungen des GwG stellten. Sie erkannten, ohne sich auf die ausdrückliche Auszeichnungs- und Aufbewahrungspflicht in § 9 GwG 2002

1494 *Scherp*, WM 2003, 1254 (1257 f.).
1495 Idem, (1257)
1496 Idem, (1257 f.).
1497 Idem, (1258).
1498 Ibid.
1499 *Herzog/Christmann*, WM 2003, 6 (11).
1500 Ibid.

zu berufen, dass die Banken aufgrund des *Kontenmonitoring „auf Vorrat Informationen für eine durch die Auskunftsbehörde oder Strafverfolgungsbehörden nach Bedarf einzuholende Auskunft verfügbar"* halten mussten. Ferner könne die neu geschaffene FIU im BKA nach § 5 Abs. 3 S. 2 GwG 2002 i. V. m. § 7 Abs. 2 BKAG 2002[1501] auf Daten bei den Banken zugreifen.[1502] Dem BKA käme durch diese Befugnis eine „Vorermittlungskompetenz" zu, die der Gesetzgeber eigentlich nicht einführen wollte.[1503]

Auch auf dem Bankrechtstag 2003, dokumentiert in einem Tagungsband[1504], wurde über die Auswirkungen des neuen Geldwäscherechts auf die informationelle Selbstbestimmung diskutiert. *Herzog* trug hier erneut vor, dass durch die „*Geldwäschebekämpfungsstrategie des Monitoring und Kontenscreening*" der Weg für eine umfassende Rasterung der Kontotransaktionen sämtlicher Bankkunden geebnet würde.[1505] Außerdem betonte er abermals, dass schon die Speicherung der Bankkundendaten einen Eingriff in die informationelle Selbstbestimmung der Kunden darstelle, da die weitere Datenverarbeitung zu verschiedenen Zwecken darauf aufbaue.[1506] Mit einem Verweis auf *Benda*[1507] machte *Herzog* aber klar, dass für ihn die Sammlung der Daten an sich kein Problem darstelle. Erst die (anschließende) Verarbeitung der Daten, die dem Betroffenen nicht gewahr wird, insbesondere durch staatliche Ermittlung, bedürfe einer gesonderten Ausgestaltung zur Wahrung des Verhältnismäßigkeitsprinzips.[1508] Eine solche Ausgestaltung verlangte eigentlich, dass im Rahmen des „Research" nur ein kleiner Kreis von Transaktionen ausgefiltert würde. Die Gesetzesbegründung des § 25a Abs. 1 Nr. 4 KWG 2002 sei aber so zu verstehen, dass zum Auffinden verdächtiger Transaktionen im Massengeschäft eine Vielzahl von

1501 Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 09. Januar 2002 (BGBl. I, S. 361).
1502 *Herzog/Christmann*, WM 2003, 6 (12).
1503 Ibid. mit Verweis auf BT-Drs. 14/9043, S.9
1504 *Hadding/Hopt/Schimansky* (Hrsg.), Bankrechtstag 2003, Basel II, 2004; zusammenfassend *C. Lange/Höche*, WM 2003, 1645.
1505 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (72); s.a. *ders.*, FS Kohlmann, 2003, S. 427 (448 ff.).
1506 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (59).
1507 *Benda* in Benda/Mailhofer/Vogel (Hrsg.), Hdb. Verfassungsrecht, 1984, S. 107 (123 f.).
1508 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (59 f.).

Transaktionen in den Verdachtsbereich gekehrt würden.[1509] Die umfangreiche Einbeziehung Unverdächtiger und deshalb geringe Trefferquote des Monitorings seien bei der Bewertung der Verhältnismäßigkeit zu berücksichtigen.[1510]

Verteidigt wurden § 25a Abs.1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 auf dem Bankrechtstag von *Findeisen*.[1511] Die Vorschriften verstünden sich im Lichte des international forcierten Paradigmenwechsels[1512] hin zu einem risikoorientierten, strukturpräventiven Ansatz (s. o. Kap. D. III. 2. a. ee.) bei der Geldwäschebekämpfung.[1513] Monitoring und Screening bestehender bzw. laufender Geschäftsbeziehungen erlaubten eine beständige Einschätzung des jeweiligen Kundenrisikos. Solche Risikoprofile erlaubten es wiederum, die Überwachung risikoarmer Kunden zu beschränken. Erst wenn der Abgleich eines Kundenrisikos mit dem Transaktionsmuster Ungewöhnlichkeiten hervorbrächte, wären weitere Aufklärungsschritte erforderlich. [1514] Die Bankenaufsicht würde dabei nur prüfen, ob ein solches System überhaupt integriert sei. Eine vollumfängliche Rasterung der Kundendaten und deren Herausgabe an staatliche Stellen verlange sie gerade nicht.[1515]

Dass ein vollumfänglicher Datensatz für das Funktionieren eines solchen Systems, insbesondere für den regelmäßigen Abgleich des Risikoprofils, notwendig ist, ließ aber auch *Findeisen* nicht unerwähnt. Die Verwendung und Aufbewahrung der Transaktionsdaten zu Zwecken der Geldwäschebekämpfung hielt er jedoch für verfassungs- bzw. datenschutzrechtlich unbedenklich. § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 seien Teil einer konsequenten „Customer Due Diligence-Politik" und taugliche Rechtsgrundlage des nunmehr etablierten EDV-Monitorings.[1516] Die Bank dürfe mit den aufgrund der Bankverträge vorhandenen Kundendaten arbeiten, um Reputations-, Organisations- und Rechtsrisiken zu vermeiden.

1509 Idem, (73).
1510 Ibid.
1511 *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95.
1512 *FATF,* 40 Recommendations, 2003, Nr. 5, 15; *Basler Ausschuss für Bankenaufsicht,* Sorgfaltspflichten, Oktober 2001, lfd. Nr. 53.
1513 *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95 (113 ff.).
1514 Idem, S. 115.
1515 Idem, S. 116.
1516 Idem, S. 117

Die bankinterne Geldwäschebekämpfung sei keine staatliche Fahndungsmaßnahme, sondern verantwortungsbewusste Risikominderung der jeweiligen Häuser.[1517] Interessant an den Ausführungen *Findeisens* ist, dass er ebenfalls – anders als der Gesetzgeber (s.o.) – § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 als einheitlich zu verstehende Rechtsgrundlage des Kontenmonitorings verstand.

Eine umfassende verfassungs- und menschenrechtliche Prüfung des – inhaltlich unveränderten – § 25a Abs. 1 S. 3 Nr. 6 KWG 2005[1518] findet sich in der Dissertation von *Degen*.[1519] Dieser begriff die Vorschrift als *„Verpflichtung, alle Kundendaten auf Verdachtsmomente bzgl. der Geldwäsche zu überprüfen"*.[1520] Dieses „Konten-Screening" stelle einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Die Kundendaten seien zwar vom Kunden in dem Wissen an die Bank übertragen worden, dass sie dort verarbeitet werden. Sie würden dazu jedoch nicht zu Daten der Bank, sondern seien weiterhin dem Kunden zuzuordnen.[1521] Mit Verweis auf *Herzog* erkannte *Degen*, dass schon durch die Speicherung der Grundstein für eine mögliche außervertragliche Verwendung gelegt würde. Erst aber, wenn diese Verwendung auch stattfindet, sei der Schutzbereich in verstärktem Maß berührt. [1522] Auch *Degen* äußerte somit an der Speicherung an sich keine grundrechtlichen Zweifel. Seine Kritik zielte allein auf die Monitoring-Pflicht. Diese hielt er – aufgrund einer ausführlichen Prüfung, die hier nur ganz knapp wiedergegeben werden kann, – im Ergebnis für verfassungs- und menschenrechtswidrig.[1523]

Zunächst sei § 25a Abs. 1 S. 3 Nr. 6 KWG 2005 unbestimmt, da weder die typologisierten Geldwäscheverdachtsmomente noch eingriffsbegrenzende Merkmale und die Anforderungen an die Systeme hinreichend konkretisiert wurden.[1524] Auch sei die Vorschrift unverhältnismäßig. Die Rasterung massenhafter Daten mit Sozialbezug, die die Schaffung eines Persönlichkeitsbildes theoretisch zuließen, ohne individuellen Anlass stelle letztlich

1517 Idem, S. 118
1518 Gesetz zur Umsetzung der Richtlinie 2002/87/EG des Europäischen Parlaments und des Rates vom 16 Dezember 2002 (Finanzkonglomeraterichtlinie-Umsetzungsgesetz) vom 21. Dezember 2004 (BGBl. I. S. 3610).
1519 *Degen*, Geldwäsche, 2009, S. 196 ff.
1520 Idem, S. 197.
1521 Idem, S. 200.
1522 Idem, S. 200 mit Verweis auf *Herzog*, WM 1999, 1905 (1916).
1523 Idem, zusammenfassend S. 270 ff.
1524 Idem, S. 205 ff., zusammenfassend S. 216.

eine Pauschalüberwachung dar, die den Wesensgehalt der informationellen Selbstbestimmung tangierte.[1525] Unabhängig vom Ausgang einer Güterabwägung sei das Konten-Screening daher verfassungswidrig. Auch dies ginge aber zulasten des Staates aus. Das Konten-Screening führe zu einer systematischen Überwachung einer großen Zahl Unbeteiligter, die keine Chance auf einen effektiven Rechtsschutz hätten. Da die Geldwäschevortaten mittlerweile auch Bagatelldelikte einschließen, sei das Screening nicht mehr auf Schwerstkriminalität begrenzt. Das Gemeininteresse an der Maßnahme sei daher reduziert und könne den schwerwiegenden Eingriff nicht rechtfertigen.[1526] Alles zu § 25a Abs. 1 S. 3 Nr. 6 KWG 2005 Gesagte gelte im Übrigen auch für § 14 Abs. 2 Nr. 2 GwG, da diese als Parallelnorm dieselbe Verpflichtung enthalte.[1527] Beide Normen seien überdies auch nicht mit Art. 8 Abs. 1 EMRK in Einklang zu bringen, da es auch hier an der Verhältnismäßigkeit bzw. der Notwendigkeit i. S. d. Art 8 Abs. 2 EMRK fehlte.[1528]

c. Kritik der Datenschutzbeauftragten

Wie die Literatur, stuften auch Datenschutzbeauftragte die § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 als Versuch einer Etablierung des Kontenmonitoring im Gesetz ein.[1529] Der Bundesbeauftragte stellte im Jahresbericht 2001-2002 (nur) in Bezug auf § 25a Abs. 1 Nr. 4 KWG 2002 zwar fest, dass die Analyse von Transaktionen mittels EDV *„doch erheblich in die Persönlichkeitsrechte der Betroffenen“* eingreife. Die Analyse und Kontrolle sei aber auf den Zweck der Geldwäschebekämpfung und Terrorismusfinanzierung begrenzt und daher akzeptabel.[1530] Hinsichtlich der Verwendung umfassender Datensätze und der Notwendigkeit deren Anlegung zu einem sicherheitsrechtlichen Zweck äußerte sich der Bundesdatenschutzbeauftragte nicht. Auch die Frage nach der spezifischen Rechtsgrundlage für das Vorgehen der verpflichteten Institute beantwortete er nicht ausdrücklich, wenngleich es in dem Bericht so klingt, als ob § 25a Abs. 1 Nr. 4 KWG 2002 selbst als Rechtsgrundlage angesehen würde.

1525 Idem, S. 222 ff.
1526 S. 227 ff.
1527 S. 236 ff.
1528 S. 245 ff.
1529 *DSB Bund,* 19. Tätigkeitsbericht, 2001-2002, S. 67; *DSB Berlin,* Jahresbericht, 2005, S. 51 ff.
1530 *DSB Bund,* 19. Tätigkeitsbericht, 2001-2002, S. 67.

Deutlich kritischer äußerte sich der Berliner Datenschutzbeauftragte im Jahresbericht 2005. Dieser hatte zuvor schon die Forderungen des BAKred nach EDV-Monitoring-Maßnahmen in Zweifel gezogen[1531] und nahm die gesetzliche Verankerung zum Anlass einer erneuten Besprechung.[1532]

Der Berliner Datenschützer besprach § 25a Abs. 1 Nr. 4 KWG 2002 und § 14 Abs. 2 S. 2 GwG 2002 einheitlich als „Rasterfahndung zur Bekämpfung der Geldwäsche". Allerdings seien diese Normen keine tauglichen Rechtsgrundlagen für einen Dateneingriff, da sie hierfür zu unbestimmt seien. Als Rechtsgrundlage komme allenfalls § 28 Abs. 1 Nr. 2 BDSG 1991[1533] in Betracht. Um danach rechtmäßig zu sein, müsste sich das Kontenmonitoring aber an bestimmte Grenzen halten. Transaktionen sollten nur bereichsspezifisch gerastert werden. Nur bei Banken, die insgesamt ein hohes Risiko für sich feststellen, wäre ein Monitoring sämtlicher Transaktionen möglich. Sobald Risiken bei Transaktionen erkannt würden, müssten diese entsprechend gekennzeichnet und separat gespeichert werden. Außerdem müssten die Bankkunden über die Anwendung von EDV-Systemen in den jeweiligen Instituten informiert werden.[1534] Im Übrigen müssten die verwendeten Parameter einer Plausibilitätskontrolle unterzogen werden, die sich am Ende am Ergebnis messen lassen muss. Nur ein effektives Monitoring, bei der die positiven Ergebnisse in einem angemessenen Verhältnis zu den einbezogenen Daten stünden, könne danach rechtmäßig sein.[1535]

d. Zusammenfassung und Stellungnahme

Das EDV-Monitoring wurde also nach der gesetzlichen Verankerung im Jahr 2002 stärker unter allgemein datenschutzrechtlichen und Aspekten der Wesentlichkeit diskutiert. Es findet sich zwar auch eine umfassende und sehr kritische Prüfung der verfassungsrechtlichen Verhältnismäßigkeit,[1536] besondere Aufmerksamkeit wurde dieser Frage aber nicht mehr gewidmet. Die Argumente lagen im Kern ja auch schon seit 1996 auf dem Tisch.[1537] Darüber hinaus war der ursprünglich angestellte Vergleich mit der strategi-

1531 *DSB Berlin,* Jahresbericht, 2000, S. 48 ff.
1532 *Ders.,* Jahresbericht, 2005, S. 50 ff.
1533 Idem, S. 51 f.
1534 Idem, S. 52 f.
1535 Idem, S. 53.
1536 *Degen,* Geldwäsche, 2009, S. 196 ff, zusammenfassend S. 270 ff.
1537 *Herzog*, WM 1996, 1753 (1757 ff.).

schen Fernmeldeaufklärung des BND[1538] kaum mehr fruchtbar zu machen, da das BVerfG in der Hauptsache die strategische Fernmeldeüberwachung für verfassungskonform befunden hatte.[1539]

Mit der Aufbewahrungspflicht setzten sich die Autoren größtenteils noch immer nicht vertieft auseinander. Immerhin *Herzog/Christmann* erkannten jedoch, dass die Pflicht zum EDV-Monitoring gemeinsam mit der Aufbewahrungspflicht zu einem Vorhalten der Daten für sicherheitsrechtsrechtliche Zwecke führen müsse und kritisierten, dass die neu geschaffene, beim BKA angesiedelte FIU auf diese Daten zugreifen könnte.[1540] Zwar hielt *Herzog* die Speicherung von Bankdaten grundsätzlich für kein Problem, sondern kanalisierte die Kritik auf die anschließende Monitoring-Pflicht.[1541] Das Problem, dass das Anti-Geldwäscherecht nicht nur eine Art strategische Rasterung vorsieht, sondern auch als Vorratsdatenspeicherung verstanden werden kann, war jedoch erstmals formuliert – und zwar, bevor die verfassungs- und europarechtliche Diskussion über eine Vorratsdatenspeicherung im Kontext der Telekommunikationsdaten überhaupt Fahrt aufnehmen konnte.[1542]

5. Kritik in Deutschland seit Einführung der Überwachungspflicht

In § 3 Abs. 1 Nr. 4 GwG 2008[1543] wurden die Verpflichteten des GwG in Umsetzung von Art. 8 Abs. 1 lit. d) der 3. GWRL bzw. Grundsatz 5 lit. d) der FATF-Empfehlungen[1544] zur *kontinuierlichen Überwachung ihrer Geschäftsbeziehungen einschließlich der in ihrem Verlauf durchgeführten Transaktionen* verpflichtet. Damit wurde die geldwäscherechtliche Überwachungspflicht, die in dieser Form noch heute besteht, als eine der allgemeinen Sorgfaltspflichten etabliert.

1538 *Dahm*, WM 1996, 1285 (1290) mit Verweis auf BVerfGE 93, 181

1539 BVerfGE 100, 313 – strategische Fernaufklärung.

1540 *Herzog/Christmann*, WM 2003, 6 (12).

1541 *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (59 f.); *ders.*, WM 1996, 1753 (1757); *ders.*, WM 1999, 1905 (1916); ebenso *Degen,* Geldwäsche, 2009, S. 200.

1542 Übersicht der frühen Diskussion bei *Breyer,* Vorratsspeicherung, 2005, S. 29 ff.

1543 Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz - GwBekErgG) vom 13.08.2008 (BGBl. I, S. 1690).

1544 *FATF,* 40 Recommendations, 2003.

An diese Sorgfaltspflichten knüpft seitdem, wenngleich dies politisch durchaus kontrovers diskutiert wurde (s. o. Kap. D. III. 2. a. ff. (3)),[1545] die Aufzeichnungs- und Aufbewahrungspflicht des § 8 GwG 2008 an.

Auch die Verpflichtung zur Schaffung interner Sicherungsmaßnahmen war im GwBekErG neu gefasst worden. Nach § 25c Abs. 2 KWG 2008[1546] waren die Kreditinstitute nunmehr gehalten, *„angemessene Datenverarbeitungssysteme zu betreiben (…), mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen zu erkennen, die (…) als zweifelhaft oder ungewöhnlich anzusehen sind. (…). Die Institute dürfen personenbezogene Daten erheben, verarbeiten und benutzen, soweit dies zur Erfüllung dieser Pflicht erforderlich ist.*" Erstmals fand sich somit ausdrücklich eine unmittelbare Ermächtigung zur Datenverarbeitung für die systematische Erkennung von ungewöhnlichen Transaktionen.

Eine entsprechend ausdrückliche Verpflichtung bzw. Ermächtigung wurde im GwG hingegen nicht geschaffen. Hier war in § 9 Abs. 2 Nr. 2 GwG 2008 weiter nur von *angemessenen Sicherungssystemen* die Rede. Die bisher bestehende Regelung des § 14 Abs. 2 Nr. 2 GwG 2002 wurde lediglich verschoben. Damit war klargestellt, dass die Pflicht zum EDV-Monitoring ausschließlich Kreditinstitute (später alle Finanzinstitute sowie Finanzholding-Gesellschaften) betraf.

a. Akzeptanz des Monitorings in der deutschen Literatur

Von der Literatur wurde die Überwachungspflicht nach § 3 Abs. 1 Nr. 4 GwG 2008 im Kontext der bestehenden Debatte um das EDV-Monitoring besprochen. So stellten die Autoren meist fest, dass die Überwachungspflicht eine sachliche Nähe zu den internen Sicherungsmaßnahmen i. S. d. § 25c Abs. 2 KWG 2008 aufwiesen.[1547]

1545 BT-Drs. 16/9647, S. 3 f.

1546 Gesetz zur Ergänzung der Bekämpfung der Geldwäsche und der Terrorismusfinanzierung (Geldwäschebekämpfungsergänzungsgesetz - GwBekErgG) vom 13.08.2008 (BGBl. I, S. 1690); zuvor § 25a Abs.1 Nr. 4 KWG 2002; § 25a Abs. 1 Satz 3 Nr. 6 KWG 2005; § 25a Abs. 1 Satz 6 Nr. 3 KWG 2007; zur Änderungsgeschichte *Achtelik* in Herzog GwG, 3. Aufl. 2018, KWG § 25h Rn. 1 f.

1547 *Warius* in Herzog GWG, 1. Aufl. 2010, § 3 Rn. 26, § 9 Rn. 55; *Ackermann/Reder*, WM 2009, 158 (164).

In der Praxis waren die Systeme mittlerweile flächendeckend etabliert.[1548] Die Diskussion um die Zulässigkeit des Monitorings stellte sich angesichts dieser neuen Faktenlage weitestgehend ein. Selbst in einem mitherausgegebenen Handbuch von *Herzog*, der sich bislang als beständigster Kritiker gezeigt hatte,[1549] wurde die Kritik am EDV-Monitoring von *Mülhausen* nunmehr als unberechtigt bezeichnet. Auffällige Transaktionen könnten faktisch und sicher nur durch EDV-Systeme erfasst werden. Zur Effektivität der Geldwäschebekämpfung seien die Systeme also obligatorisch.[1550]

Ähnlich äußerten sich die BaFin Mitarbeiter *Ackermann/Reder*.[1551] Diese fassten die kritischen Äußerungen der vorigen Jahre zusammen und kamen zu dem Schluss, dass zuletzt nur noch die Rechtsgrundlage des EDV-Monitorings ernsthaft diskutiert worden war.[1552] Mit der Neufassung des § 25c Abs. 2 KWG 2008 sei diese rein akademisch geführte Diskussion nunmehr obsolet, da die Vorschrift ausdrücklich zur Datenverarbeitung ermächtigte.[1553]

Verfassungsrechtliche Bedenken stellten sie nicht an. Das EDV-Monitoring müsse seiner Natur nach anlasslos sein, denn es ziele gerade nicht auf die Prüfung von anlassgebenden Fällen.[1554] Stattdessen verfolge es den Zweck, aus der großen Menge der irrelevanten Transaktionen typischerweise verdächtige Fälle zu identifizieren. Dies könne nur gelingen, wenn für alle Kunden ein Risiko- und Verhaltensprofil anhand ihrer Transaktionen erstellt würde, damit Abweichungen erkannt werden könnten.[1555] Eine anlasslose Rasterung aller Transkationen solle aber dennoch nicht erfolgen, da bestimmte Risikobereiche nach der institutsinternen Analyse aus dem Raster herausgenommen werden könnten.[1556]

1548 *BaFin,* Jahresbericht, 2006, S. 195.
1549 *Herzog*, WM 1996, 1753; *ders*., WM 1999, 1905; *ders*., FS Kohlmann, 2003, S. 427; *ders.* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47; *Herzog/Christmann*, WM 2003, 6.
1550 *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 53.
1551 *Ackermann/Reder*, WM 2009, 158 (164 f.).
1552 Idem, (164).
1553 Idem, (165).
1554 Ibid., so auch schon *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 52.
1555 *Ackermann/Reder*, WM 2009, 158 (165).
1556 Ibid.

Über die Auswirkungen der Überwachungspflicht auf die Aufbewahrungspflicht äußerten sich *Ackermann/Reder* nicht. Sie stellten lediglich fest, dass die Pflicht zur Aufbewahrung von Belegen über Geschäftsbeziehungen und Transaktionen neu in das Gesetz aufgenommen wurde.[1557] Dass eine solche Pflicht auch aus der Verknüpfung von sorgfaltspflichtiger Überwachung und entsprechender Aufzeichnung bzw. Aufbewahrung folgen könnte, bemerkten sie nicht. Sie erklärten allerdings, dass eine Kohärenz zur handelsrechtlichen Aufbewahrungspflicht wegen verschiedener Fristenläufe nicht hergestellt werden konnte.[1558] Offensichtlich gingen sie also davon aus, dass diese Regelungen zumindest inhaltlich identisch sein mussten. Dass eine sicherheitsrechtliche Pflicht zur Speicherung von Transaktionsbelegen verfassungsrechtlich problematisch sein könnte, kam den Autoren dabei nicht in den Sinn.

Weniger überzeugt zeigte sich der Rechtsanwalt *Kaetzler*. § 25c KWG 2008 sei zwar als Einführung einer datenschutzrechtlichen Grundlage hervorzuheben, die Norm schüfe aber nur einen groben Eingriffs- und Rechtfertigungstatbestand. Die datenschutzrechtliche Zulässigkeit von Rasterungen nach persönlichen Merkmalen, etwa der Staats- oder Religionsangehörigkeit im Rahmen der EDV-Systeme, seien durchaus zweifelhaft.[1559] Auch er meldete aber an der Verpflichtung der Banken zur elektronischen Rasterung ihrer Kundendaten keine grundsätzlichen verfassungsrechtlichen Bedenken mehr an.

Ein ähnliches Bild zeigte sich in der Kommentarliteratur. Laut *Achtelik* hätte sich der Streit um die datenschutzrechtliche Grundlage *„spürbar entschärft"*.[1560] Er wies jedoch darauf hin, dass die früher angemeldeten datenschutz- und verfassungsrechtlichen Bedenken durch die Schaffung einer rechtlichen Grundlage nicht ausgeräumt worden seien.[1561] Eine eigene Einschätzung gab er jedoch nur insofern ab, als dass er die Unbedenklichkeit der Monitoringsysteme zurückwies.[1562]

1557 *Ackermann/Reder*, WM 2009, 200 (207 f.).
1558 Idem, (208).
1559 *Kaetzler*, CCZ 2008, 174 (179 f.); zust. *Warius* in Herzog GWG, 1. Aufl. 2010, § 9 Rn. 63.
1560 *Achtelik* in Herzog GWG, 1. Aufl. 2010, KWG § 25c Rn. 25.
1561 Idem, KWG § 25c Rn. 26.
1562 Ibid.

b. Unzureichende Betrachtung der Aufzeichnungs- und Aufbewahrungspflicht unter dem Aspekt der Vorratsdatenspeicherung

Mit dem Abfallen der Kritik am Monitoring ging einher, dass eine kritische Betrachtung der ausgedehnten Aufbewahrungspflichten weitestgehend ausblieb. Dies vermag durchaus zu überraschen, denn die Neufassung des GwG im Jahr 2008 fiel in eine Zeit, in der kontrovers über das Thema Vorratsdatenspeicherung diskutiert wurde.[1563] Wie bereits dargestellt, war auch der Politik nicht verborgen geblieben, dass ein Anknüpfen der Aufbewahrungspflicht an die Überwachungspflicht zu einer umfassenden Speicherpflicht von Kontoinhaltsdaten aus sicherheitsrechtlichen Gründen führen könnte. Die FDP-Fraktion hatte diesen Umstand offen angesprochen und gefordert, dass die Aufbewahrungspflicht nicht an die Überwachungspflicht anknüpfte.[1564] Ohne Erfolg.

Man muss hier natürlich sehen, dass Art. 30 lit b.) der 3. GWRL ohnehin festlegte, dass *„bei Geschäftsbeziehungen und Transaktionen die Belege und Aufzeichnungen (…), für die Dauer von mindestens fünf Jahren nach Durchführung der Transaktion oder nach Beendigung der Geschäftsbeziehung"* aufbewahrt werden müssten. Die umfassende Speicherpflicht von Transaktionsbelegen konnte man daher auch unabhängig von der umfassenden Überwachungspflicht als obligatorisch ansehen. Wieso aber diese neue Pflicht in der GWRL grundsätzlich keine Kontroverse in Gang setzte, ist mit dieser Erkenntnis noch nicht beantwortet.

aa. Überblick der knappen Ansätze in der Literatur zum GwG

Völlig unbeachtet blieb der Komplex indes nicht. *Achtelik* etwa stellte in Bezug auf § 25c Abs. 2 KWG 2008 fest, dass das EDV-Monitoring, auch wenn der Gesetzgeber nach eigener Aussage datenschutzrechtliche Standards berücksichtigt haben wollte[1565], faktisch die Vorhaltung massenhafter Daten voraussetzt.[1566] Er stellte jedoch weder ausdrücklich die Frage, ob diese Datenvorhaltung verfassungs- oder europarechtswidrig sein könnte, noch ging er auf den Umstand ein, dass die Transaktionsdaten aufgrund von Vorschriften anderer Rechtsgebiete ohnehin gespeichert werden.

1563 Übersicht bei *Moser-Knierim,* Vorratsdatenspeicherung, 2014, S. 164 ff.
1564 BT-Drs. 16/9647, S. 3.
1565 BR-Drs. 168/08, S.109.
1566 *Achtelik* in Herzog GWG, 1. Aufl. 2010, KWG § 25c Rn. 25.

Ähnlich knappe Betrachtungen finden sich in der jüngeren Literatur immer wieder hinsichtlich verschiedener Regelungen des Anti-Geldwäscherechts. Diese sind zwar sehr ausdrücklich, lassen aber eine tiefere Auseinandersetzung vermissen.

Von einer *„gesetzlich angeordneten anlasslosen Vorratsdatenspeicherung"* im aktuellen GwG spricht etwa *Heinson*[1567] und zwar in Bezug auf § 6 Abs. 6 GwG (Art. 42 der 4./5. GWRL), wonach die Verpflichteten Vorkehrungen treffen, *„um auf Anfrage der Zentralstelle für Finanztransaktionsuntersuchungen oder auf Anfrage anderer zuständiger Behörden Auskunft darüber zu geben, ob sie während eines Zeitraums von fünf Jahren vor der Anfrage mit bestimmten Personen eine Geschäftsbeziehung unterhalten haben und welcher Art diese Geschäftsbeziehung war. Sie haben sicherzustellen, dass die Informationen sicher und vertraulich an die anfragende Stelle übermittelt werden."*

Dabei übersieht *Heinson* die eigentlich sensiblen Regelungen. § 6 Abs. 6 GwG ist zwar auf den ersten Blick problematisch, da er die Einrichtung heimlicher Zugänge vorschreibt. Zu einer Vorratsdatenspeicherung kommt es aber zuvorderst durch eine umfassende Speicherpflicht bestimmter Daten und die spezifischen Ermächtigungen, auf diese Daten zuzugreifen. Dafür einzurichtende Kanäle ermöglichen dann zwar die Abfrage, sie sind aber nur als Teil eines Vorschriftenkomplexes bedenklich. Dieser Vorschriftenkomplex wird in der Besprechung von *Heinson* nicht ansatzweise ausführlich dargestellt. Darüber hinaus bezieht sich § 6 Abs. 6 GwG (Art. 42 der 4./5. GWRL) nur auf das Bestehen einer Geschäftsbeziehung und deren Eigenart. Es handelt sich also um eine Bestandsdatenabfrage. Diese ist in Deutschland ohnehin automatisiert möglich (s. o.). Ein Zugriffsrecht auf Finanztransaktionsdaten ergibt sich aus dem Wortlaut des § 6 Abs. 6 GwG nicht.

Eine ganz ähnliche Kritik findet sich bei *Krais*. Auch dieser erkannte eine europarechtlich zweifelhafte Vorratsdatenspeicherung[1568] in Art. 42 der 4. GWRL (umgesetzt durch § 6 Abs. 6 GwG). An der Aufbewahrungspflicht für Transaktionsbelege und andere Dokumente selbst aus § 8 GwG scheint er hingegen, wie auch *Heinson*, keine weiteren europa- oder verfassungsrechtlichen Bedenken zu hegen, wobei er aber diese Pflicht auch nicht umfassend für alle Transaktionsbelege, sondern nur für *„Erforderliche"* gelten

1567 *Heinson* in Specht/Mantz (Hrsg.), Hdb. Europ. & Deutsches Datenschutzrecht, 2019, § 14 Rn. 91.

1568 *Krais*, CCZ 2015, 251 (252).

lassen will.[1569] Diese Auslegung dürfte mit Art. 40 der 4./5. GWRL indes unvereinbar sein (s. o. Kap. D. III. 2. d. bb.).

Ausdrücklich bezeichnet auch *Spoerr* in einer aktuellen Kommentierung das allgemein in den Vorschriften, insbesondere aber in § 25h Abs. 2 KWG[1570], zum Ausdruck kommende *„Know-your-Transaction-Prinzip"* als *„umfassende Vorratsdatenspeicherung"*.[1571] Die Aufzeichnungs- und Aufbewahrungspflicht bzw. vergleichbare Vorschriften, auf denen die Anlegung des Datenbestandes für das EDV-Monitoring erst beruht, erwähnt er mit keinem Wort. Auch *Spoerr* stellt damit nur einen einzelnen Aspekt heraus, anstatt die Kombination aus Aufbewahrungs- und Überwachungspflicht als gemeinsamen Komplex zu beschreiben. Eine umfassende Prüfung der Rechtmäßigkeit dieses Komplexes vermisst man ohnehin.

bb. Erklärungsversuche der ausbleibenden Kritik

Darüber, weshalb das GwG seit der Neufassung im Jahr 2008 in Deutschland nicht in besonderer Weise unter dem Stichwort der Vorratsdatenspeicherung diskutiert bzw. überhaupt auf die Vereinbarkeit mit höherem Recht geprüft wurde, lassen sich natürlich nur Vermutungen anstellen. Einmal ist sicher zu beachten, dass § 8 Abs. 1 GwG 2008 eine Aufbewahrung von Transaktionsbelegen weiter von der Ausführung der Sorgfaltspflichten abhängig gemacht hatte. Welche Maßnahmen der Verpflichteten ganz konkret zu den Sorgfaltspflichten zählen, wurde von den Besprechungen aber nicht ausführlich genug betrachtet.

So wurde zwar schnell ein Zusammenhang der für die Banken geltenden Monitoring-Pflicht nach § 25c KWG 2008 und der Überwachungspflicht aus § 3 Abs. 1 Nr. 4 GwG 2008 hergestellt.[1572] Die konsequente Feststellung, dass damit das EDV-Monitoring sämtlicher Kundenbeziehung unter die Sorgfaltspflichten fällt, vermisst man aber in dieser Ausdrücklichkeit.

Mit dieser Erkenntnis hätte es keinen Zweifel mehr geben können, dass auch eine Aufbewahrungspflicht, die nur im Rahmen der Sorgfaltspflichten greift, sämtliche Transaktionsdaten erfasst. Dies musste schon damals unabhängig davon gelten, ob man die Aufbewahrung der Transaktionsdaten

1569 *Ders.,* Geldwäsche, 2018, Rn. 284.
1570 *Spoerr* in BeckOK Datenschutzrecht, Syst. J Rn. 226.
1571 Idem, Syst. J Rn. 153.
1572 Vgl. *Warius* in Herzog GWG, 1. Aufl. 2010, § 3 Rn. 26, § 9 Rn. 55; *Ackermann/Reder*, WM 2009, 158 (164).

als Folge oder Voraussetzung der Sorgfaltspflicht verstehen wollte, denn schon § 8 Abs. 1 GwG 2008 sprach von den „eingeholten" Informationen. Somit sind die Transaktionsdaten auch dann erfasst, wenn man sie nicht als Ergebnis der Überwachungspflicht, sondern als deren Grundlage versteht (s. o. Kap. D. III. 2. d. bb. (1)).

Auf diese Problematik wurde in der Literatur nicht eingegangen. Es bleibt damit im Unklaren, welche Vorstellungen sich die Autoren hinsichtlich des Umfangs der Aufbewahrungspflicht machten. Aber selbst wenn stillschweigend § 8 Abs. 1 GwG 2008 als umfassende Speicherpflicht betrachtet worden wäre, darf bei der Beurteilung der Diskussion nicht vergessen werden, dass es solche Pflichten in anderen Gesetzen schon gab. So wurde etwa bei der Fristenregelung durchaus erkannt, dass diese anfänglich nicht mit den Fristen aus § 257 HGB, § 147 Abs. 1, 3 AO gleichliefen.[1573] Da § 8 Abs. 3 GwG 2008 andere gesetzliche Bestimmungen für unbeschadet erklärte, wurde die geldwäscherechtliche Aufbewahrungspflicht, die jedenfalls hinter der zehnjährigen Frist aus dem Handelsrecht zurückblieb, schlicht für obsolet erklärt.[1574]

Es scheint, als ob die Kommentatoren des Anti-Geldwäscherechts aufgrund bestehender Aufbewahrungspflichten für Buchungsbelege kein Problem erkennen konnten. Schon früh wurde in der Literatur ja erkannt, dass zwar die Speicherung an sich in das Recht auf informationelle Selbstbestimmung eingreift[1575], kritisiert wurde aber von Beginn an nur die Verwendung der Daten, da man das Vorliegen des Datenbestands als gegeben betrachtete. Es wurde ignoriert, dass die geldwäscherechtliche Pflicht aufgrund ihrer Eigenart als Sicherheitsgesetz eine andere Qualität mit sich bringt. Außerdem wurde nicht geprüft, ob es bei der europa- oder verfassungsrechtlichen Bewertung eines Gesetzes überhaupt auf die Frage ankommen darf, ob das Gesetz auch faktische Auswirkungen auf die Menge der zu speichernden Daten mit sich bringt.

1573 *Ackermann/Reder*, WM 2009, 200 (208).

1574 *Warius* in Herzog GWG, 1. Aufl. 2010, § 8 Rn. 19; *Walther* in Schimansky/Bunte/Lwowski (Hrsg.), Bankrechts-Hdb., 5. Auflage 2017, § 42 Rn. 438 jeweils zum GwG 2008, das sich aber hinsichtlich des Fristbeginns nicht vom aktuellen GwG unterscheidet,

1575 *Degen,* Geldwäsche, 2009, S. 200; *Herzog*, WM 1996, 1753 (1757); *ders.*, WM 1999, 1905 (1916).

Eine weitere Rolle dürfte gespielt haben, dass das GwG bis zur Schaffung des § 30 Abs. 3 GwG 2017[1576] noch keine Klausel enthielt, die es der FIU gestattet hätte, heimlich bei den Verpflichteten Informationen einzuholen. Die damals noch beim BKA angesiedelte FIU hatte nach § 10 Abs. 3 GwG 2008 lediglich die allgemeinen Datenerhebungsbefugnisse des BKA. Ein spezieller Zugriff auf den Datenschatz der Verpflichteten war also nicht vorgesehen. Jedenfalls bis zum Jahr 2017 hätte ein Vergleich mit der TK-Vorratsdatenspeicherung also mangels konkreter Zugriffsrechte nicht recht gepasst.

An der allgemeinen Befugnis des BKA zur prinzipiell offenen Datenerhebung gab es grundsätzlich wenig auszusetzen, war der Rückgriff auf Kontoinhaltsdaten durch Sicherheitsbehörden aufgrund bestehender Generalklauseln doch gängige Praxis[1577] und vom BVerfG selbst in einem Ausnahmefall[1578] abgesegnet worden (s. o. Kap. E. I. 1. c. bb.).

6. Kritische Stimmen aus Europa und Vergleich mit der TK-Vorratsdatenspeicherung

Deutlich konkretere Betrachtungen finden sich in der Literatur, die sich unmittelbar mit der europarechtlichen Grundlage des GWG, der GWRL, befasst. Spätestens mit der kommenden Vollharmonisierung durch die geplante EU-GWVO[1579] lassen sich diese Ausführungen unmittelbar auf die deutsche Rechtslage übertragen.

1576 Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen vom 23. Juni 2017 (BGBl. I, S. 1822).

1577 Siehe nur *Beckhusen/Mertens* in Derleder/Knops/Bamberger (Hrsg.), Bank- und Kapitalmarktrecht, Bd. I, 3. Auflage 2017, § 39 Rn. 40 *Kahler,* Kundendaten, 2017, 31 ff.; *F. Jansen,* Bankauskunftsersuchen, 2010, S. 30 ff.; *Reichling*, JR 2011, 12 (16).

1578 BVerfG, NJW 2009, 1405 (1407).

1579 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, 20. Juli 2021, COM(2021) 420 final, 2021/0239 (COD).

a. Kritik Europäischer Datenschutzbehörden

Dass die GWRL Fragen in Bezug auf den Datenschutz und Grundrechte aufwarf, war dem Europäischen Gesetzgeber selbst durchaus bekannt.[1580] Nach Erlass der 3. GWRL war er verstärkter Kritik der europäischen Datenschutzbehörden ausgesetzt.

aa. Stellungnahme der Article 29 Data Protection Working Party

Die *Article 29 Data Protection Working Party* (WP29), Vorläuferin des nach Art. 68 DSGVO eingerichteten Europäischen Datenschutzausschusses (EDPB), setzte sich im Jahr 2011 mit der 3. GWRL auseinander und erließ eine Stellungnahme. [1581] Um eine faire Balance von Datenschutz und Geldwäschebekämpfung zu gewährleisten, machte sie dem europäischen Gesetzgeber insgesamt 44 Vorschläge. Diese Vorschläge befassten sich u. a. auch mit dem Transaktionsmonitoring und den Aufbewahrungspflichten.

Die WP29 war der Meinung, dass sich die Reichweite des Monitorings nicht klar aus der Richtlinie ergeben würde. Insbesondere bei größeren Konzernen sei fraglich, welcher Datenaustausch hierfür notwendig und erlaubt sei. Die Richtlinie ließe sich so interpretieren, dass die vorgesehenen Compliance-Pflichten nur durch ein ausgeprägtes Outsourcing der gesamten Kundendaten eines Konzerns an Dritte mit adäquaten Data-Mining-Technologien erfüllt werden könnten. Genauso gut könnte man aber annehmen, dass in jedem Einzelfall eines Kunden eine individuelle Notwendigkeit vorliegen müsste, weshalb ein gruppenweites Transaktionsmonitoring gar nicht praktikabel wäre.[1582] Die Kritik der WP29 konkret am Transaktionsmonitoring scheint auf diese Problematik des Datenaustauschs innerhalb verschiedener Entitäten eines Konzerns begrenzt.[1583] Aus der Stellungnahme ergibt sich nicht, ob die WP29 an der rechtlichen Zulässigkeit eines umfassenden Transaktionsmonitorings selbst Zweifel hegte.

Konkreter wurde sie bei der Kontrolle der Aufbewahrungspflichten. Hier sei zunächst problematisch, dass die Richtlinie nur eine Minimal- und kei-

1580 *Europäische Kommission,* Commission Staff Working Paper, AML Compliance, SEC(2009) 030 final, 30.06.2009.

1581 *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011.

1582 Idem, Annex Nr. 25, S. 20 f.

1583 Ebenso *Europäische Kommission,* Commission Staff Working Paper, AML Compliance, SEC(2009) 030 final, 30.06.2009, Annex Nr. 7, S. 58 f.

ne Maximalfrist beinhaltete. Dieser Missstand wurde durch Art. 40 Abs. 1 UAbs. 2 der 4. GWRL allerdings behoben, nach der eine Speicherung maximal zehn Jahre lang zulässig ist.

Wichtiger war, dass die WP29 das Risiko einer *„evergreen data retention"* erkannte.[1584] Eine solche sei mit den Grundsätzen der Erforderlichkeit und Datenminimierung nicht zu vereinbaren. Art. 30 der 3. GWRL sei diesbezüglich unklar formuliert. Die Vorschrift gäbe nicht zu erkennen, ob und welche Grenzen für die Speicherung von Daten vorgesehen sei. Eine Auslegung dahingehend, dass Institute aufgrund der Identifikationsvorgänge oder Sorgfaltspflichten gespeicherten Daten ohne klaren Zweck der zukünftigen Verwendung vorhielten, dürfe aber nicht möglich sein. Andernfalls wäre die Vorschrift rechtswidrig. Deshalb sollten die Aufbewahrungspflichten verständlich normiert werden, wobei aber offenbar insbesondere der zeitliche Aspekt der Frist gemeint war. Grundsätzliche Einwände gegen das Vorhalten von Transaktionsdaten zu Zwecken der Geldwäschebekämpfung für eine gewisse Zeit brachten die Datenschützer in der Stellungnahme nicht vor.

Im Übrigen kritisierte die WP29, dass für sämtliche zu speichernde Daten dieselben Regeln galten, anstatt nach der Art der Daten zu differenzieren.[1585] Für die Transaktionsdaten sollte festgestellt werden, dass eine Speicherung zur Geldwäschebekämpfung prinzipiell nicht mehr erlaubt sein könne, wenn sich ein konkreter Verdacht als falsch herausgestellt hat oder die entsprechenden Ermittlungen eingestellt wurden. In diesen Fällen sollten die Daten nicht mehr von der Abteilung für Geldwäschebekämpfung eingesehen werden können, wozu sie entsprechend kodiert werden sollten.[1586]

1584 *Article 29 Data Protection Working Party,* Opinion 14/2011 relating Money Laundering, 13.06.2011, Annex Nr. 27, S. 22.
1585 Idem, Annex Nr. 27-29, S. 21 ff.
1586 Idem, Annex Nr. 31, S. 24.

bb. Stellungnahmen des Europäischen Datenschutzbeauftragten

Auch der Europäische Datenschutzbeauftragte (EDPS) nahm mehrfach zur Entwicklung des Anti-Geldwäscherechts Stellung, erstmals ausführlich zum damals vorgeschlagenen[1587] Erlass der 4. GWRL im Jahr 2013.[1588]

Anders als viele Autoren aus der Rechtswissenschaft wies der EDPS zu Beginn seiner Stellungnahme auf den Umstand hin, dass die Erhebung von Personendaten zu Geldwäschezwecken gleichzeitig auch zu geschäftlichen Zwecken erfolgte.[1589] Auch deshalb würden die datenschutzrechtlichen Anforderungen des Europarechts auch für das Anti-Geldwäscherecht gelten, wenngleich die FATF-Standards auf den Datenschutz keine Rücksicht nähmen.[1590]

Als Schwierigkeiten des Anti-Geldwäscherechts in Bezug auf den Datenschutz erkannte der EDPS *„den Austausch von Informationen innerhalb der Unternehmensgruppe, die Zustimmung der betroffenen Personen, das Aufbewahren von Aufzeichnungen und die rechtlichen Unsicherheiten bezüglich der Verarbeitung von Daten betreffend die Bekämpfung der Geldwäsche/Terrorismusfinanzierung.“*[1591] Der EDPS verzichtete in seiner Stellungnahme zur damals geplanten 4. GWRL allerdings auf eine umfassende europarechtliche Kontrolle des Transaktionsmonitorings und der Aufbewahrung von Transaktionsdaten zu Zwecken der Geldwäschebekämpfung. Eine solche fand sich – jedenfalls ansatzweise – erst in der Stellungnahme[1592] zum Vorschlag[1593] zur 5. GWRL.

Dort erwähnte der EDPS schon zu Beginn die damals neue Rechtsprechung des EuGH zur TK-Vorratsdatenspeicherung im Fall *Digital Rights*

1587 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, 05. Februar 2013, COM(2013) 45 final, 2013/0025 (COD).

1588 *EDPS,* Stellungnahme 4. GeldwäscheRL, 04. Juli 2013.

1589 Idem, Nr. 12, S. 4.

1590 Idem, Nr. 15, S. 4.

1591 Idem, Nr. 19, S. 5.

1592 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017.

1593 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG, 05. Juli 2016, COM(2016) 450 final, 2016/0208 (COD).

Ireland.[1594] Es sei von der Rechtsprechung festgestellt worden, dass die Bekämpfung schwerer Kriminalität und Terrorismus zwar ein legitimes Ziel sei. Für diese Zwecke veranlasste Einschränkungen der Grundrechte auf Privatsphäre und Datenschutz müssten aber verhältnismäßig sein. Durch diese Einleitung zeigte der EDPS erstmals an, dass auch er die Vorschriften der Geldwäschebekämpfung nunmehr durchaus in dem Kontext der Diskussion um die Zulässigkeit einer Vorratsdatenspeicherung verstand. Konsequenterweise beschäftigte er sich dann auch in der Stellungnahme allgemeiner als zuvor mit der Frage, inwiefern das Vorhalten und Erforschen von Finanzdaten für staatliche Akteure verhältnismäßig sein kann.

So sei die Erweiterung der Pflichten etwa auf den Handel mit Kryptowährungen weniger beunruhigend als die vorgeschlagene allgemeine Erweiterung der Zwecke in der 5. GWRL. Diese nannte nicht mehr nur die Ahndung von Geldwäsche und die Terrorismusbekämpfung als Ziel, sondern – wenn auch weniger ausdrücklich – auch die Bekämpfung von Steuerbetrug und Steuerhinterziehung[1595], die bislang nur durch die Aufnahme von Steuerstraftaten als Vortat der Geldwäsche begünstigt werden sollte.[1596] Der Zweck der Richtlinie würde damit nach dem EDPS allgemein auf die Bekämpfung von Finanzkriminalität ausgedehnt.[1597] Dies sei kritisch zu betrachten, da die Verarbeitung von personenbezogenen Daten desto sensibler würde, je weiter der Zweck sei, dem sie diene.[1598]

Im Rahmen der Verhältnismäßigkeit sei sodann zu beachten, dass der EuGH für Eingriffe in das Recht auf Privatheit stets Anhaltspunkte gefordert hatte, die auf ein Verhalten im Zusammenhang mit einer Straftat schließen ließen. Pauschale Eingriffe seien danach unzulässig.[1599] Insofern sei problematisch, dass die Geldwäschebekämpfung nicht ausschließlich mehr einen risikoorientierten Ansatz verfolgte, sondern in Erwägungsgrund 19 auch die *methodische Überwachung einer Kategorie bestehender*

1594 Idem, Nr. 10, S. 6 f.
1595 Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016), S. 2 f.
1596 Vorschlag zur 4. EU-GWRL, 05. Februar 2013, COM(2013) 45 final, S. 5 f.; 4. EU-GWRL (EU) 2015/849, Erwägungsgründe 11, 44.
1597 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 27, S. 9 mit Verweis auf Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016), S. 3.
1598 Idem, Nr. 32, S. 10.
1599 Idem, Nr. 46, S. 13 mit Verweis auf EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 58 = NJW 2014, 2169.

Kunden[1600] forderte. Hierbei wird aber nicht ganz klar, welche Überwachung gemeint sein soll – und zwar weder unmittelbar in Erwägungsgrund 19 des Vorschlags zur 5. GWRL noch in der Stellungnahme des EDPS. Die pauschale Überwachung von Transaktionen war schließlich kein Novum der 5. GWRL, sondern schon seit der 3. GWRL aus 2005 vorgesehen. Offenbar hatte sich der EDPS nicht weiter mit der Frage auseinandergesetzt, wie weit das Transaktionsmonitoring reicht, und welche Daten dafür aufbewahrt werden müssen. Erneut blieb eine grundsätzliche Kritik an der Aufbewahrungspflicht in Verbindung mit der Überwachungspflicht also aus.

Was dem EDPS aber nicht verborgen blieb, war der Vorschlag, den FIUs einen umfassenden Zugang zu den von den Verpflichteten gespeicherten Daten unabhängig vom Vorliegen einer Verdachtsmeldung einzuräumen.[1601] Der Aufgabenbereich der FIUs würde nach Ansicht des Beauftragten damit keinen untersuchungsbezogenen Ansatz mehr verfolgen, sondern wäre schon bei bloßen *Erkenntnissen* eröffnet.[1602] Sie könnten damit „data mining"[1603] betreiben, nicht mehr nur gezielte Untersuchungen. Einen unmittelbaren Vergleich zur TK-Vorratsdatenspeicherung zog der EDPS an dieser Stelle aber nicht.

Stattdessen geriet seine Schlussfolgerung sehr allgemein und wiederholte letztlich nur allgemeine Ausführungen zur Verhältnismäßigkeit staatlicher Eingriffe in das Recht auf Privatsphäre und Datenschutz.[1604] So hätte in dem Vorschlag klargestellt werden sollen, dass alle Datenverarbeitungen und alle Grundrechtseingriffe stets einem genau festgelegten legitimen Zweck dienten, erforderlich und angemessen sind. Außerdem hätte geprüft werden sollen, ob die verfolgten politischen Ziele insgesamt mit dem Zweck zu vereinbaren sind.

Im Mai 2020 veröffentlichte die Europäische Kommission einen Aktionsplan zur Überarbeitung des Anti-Geldwäscherechts,[1605] der im Juli 2021 in

1600 Idem, Nr. 50, S. 13 mit Verweis auf Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016) Erwägungsgrund 19, S. 29.

1601 Vorschlag zur 5. EU-GWRL, 05. Juli 2016, COM(2016), Nr. 11, S. 41, umgesetzt durch Art. 32 Abs. 9 der 5. EU-GWRL.

1602 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 52, S. 14.

1603 Ibid., in der deutschen Übersetzung fälschlich als „Datenminimierung" übersetzt.

1604 Idem, Nr. 66, S. 16 f.

1605 Mitteilung der Kommission zu einem Aktionsplan für eine umfassende Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung, 07. Mai 2020, C(2020) 2800 final.

einem großen Gesetzgebungspaket mündete (s. o. Kap. D. III. 2. a. kk.)[1606]. Sowohl zum Aktionsplan[1607] als auch später zum Gesetzgebungspaket[1608] nahm der EDPS abermals Stellung, wobei nur letztere sich wirklich kritisch mit den Regelungen auseinandersetzte.

Die neuen Vorschriften über die Zugriffsrechte der FIUs seien danach insgesamt exzessiv, ihre Verhältnismäßigkeit fraglich.[1609] Art. 18 des Vorschlags für eine 6. GWRL enthält eine ausführliche Liste an Informationen und Datenbanken, auf die die FIUs Zugriff haben müssen. Hinzu tritt, dass die FIUs bei der einzurichtenden Europäischen Geldwäscheaufsichtsbehörde auch um Informationen aus deren zentralen Register ersuchen dürfen, Art. 11 Abs. 4 der vorgeschlagenen GWVO. Außerdem muss nach Art. 24 des Vorschlags für eine 6. GWRL der Datenaustausch zwischen den FIUs der Mitgliedstaaten gewährleistet werden. Die FIUs haben also einen Zugriff auf weitreichende Informationen, die nicht auf Finanzdaten limitiert sind. Diesen Umstand kritisiert der EDPS weiterhin als „intelligence-based", was angesichts seiner Natur als Verwaltungsbehörde nicht angemessen sein könnte.[1610] Die Zugriffsrechte sollten ausdrücklich dem Verhältnismäßigkeitsgrundsatz unterstellt und an die Notwendigkeit für operative Analysen der FIUs gebunden werden.[1611] Dabei kommentierte der EDPS den Zugriff der FIUs auf Informationen direkt bei den Verpflichteten gemäß der vorgeschlagenen Art. 50 Abs. 1 lit. b) GWVO[1612], Art. 18 Abs. 4 der 6. GWRL nicht mehr unmittelbar.[1613] Die Stellungnahme erwähnt nur die Art. 18 Abs. 1, 2 der 6. GWRL. Aus seinen Schilderungen ergibt sich jedoch, dass der EDPS die umfassenden Zugriffsrechte der FIUs insgesamt

1606 *Europäische Kommission,* Anti-money laundering and countering the financing of terrorism legislative package, https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en, zuletzt aufgerufen am 12.01.2025.

1607 *EDPS,* Stellungnahme Aktionsplan Geldwäsche 05/2020.

1608 *Ders.,* Opinion 12/2021 AML proposals, 22.09.2021.

1609 Idem, Nr. 20 ff, S. 11 .

1610 Idem, Nr. 37, S. 12; zuvor schon *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 53, S. 14; krit. zur Rolle der FIUs auch *Wissenschaftliche Dienste des Bundestags,* Finanzströme, 2019, S. 21; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (249 f.).

1611 *EDPS,* Opinion 12/2021 AML proposals, 22.09.2021, Nr. 30, S. 11.

1612 Erwägungsgrund 79 der EU-GeldwäscheVO stellt klar, dass für Auskunftsersuchen der FIU keine vorherige Meldung erforderlich sein soll.

1613 So noch *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 52, S. 14.

kritisieren wollte, da die Möglichkeit zum Abgleich letztlich einem „data mining" gleichkomme.[1614]

Auch auf die Datenverarbeitung bei den Verpflichteten ging der EDPS ein. Wie bislang wurde aber weder die Rechtmäßigkeit der Aufbewahrungspflicht noch die Rechtmäßigkeit des Kontenmonitorings prinzipiell angezweifelt. Es wurde allerdings verlangt, dass in der Verordnung ausdrücklich bestimmt wird, welche Daten von den Verpflichteten für welche Zwecke bzw. an welcher Stelle der Geldwäschebekämpfung verarbeitet werden.[1615] Außerdem sollte die Verarbeitung persönlicher Daten, die in Verbindung zur sexuellen Orientierung oder ethnischer Abstammung stehen, verboten werden.[1616] Wie genau dies bei der Verarbeitung von Transaktionsdaten erfolgen soll, aus denen sich durchaus Rückschlüsse über diese Datenkategorien ergeben können, bespricht der EDPS allerdings nicht. Er scheint bei der Datenverarbeitung diesbezüglich allein die Identifizierungsmaßnahmen vor Augen gehabt zu haben.

b. Kritik in der Literatur

Ein solcher Ansatz, der die Parallelen des Anti-Geldwäscherechts und der TK-Vorratsdatenspeicherung in den Blick nimmt, wurde in der Europäischen Literatur zur GWRL in den letzten Jahren immer wieder vorgeschlagen. Im Folgenden sollen nur die Beiträge vorgestellt und kritisch kommentiert werden, die die Speicher- und Monitoring-Pflichten konkret anhand der Europäischen Rechtsprechung zur Vorratsdatenspeicherung bewerten. Allgemeine Betrachtungen der Kollision von Privatheit und Geldwäschebekämpfung, die auf eine spezifische Prüfung der einzelnen Pflichten anhand der Rechtsprechung verzichten, bleiben außen vor.[1617]

1614 *Ders.,* Opinion 12/2021 AML proposals, 22.09.2021, Nr. 37, S. 12.
1615 Idem, Nr. 16, S. 9; S. 16.
1616 Ibid.
1617 Etwa *Sciurba,* AML Regimes, 2019, S.88 ff.; *Ioannides,* Money Laundering, 2016, S. 135; *Mitsilegas/Vavoula*, Maastricht J. of EU and Comp. Law 23 (2016), 261 (279 ff.); *Gallant* in Rider (Hrsg.), Int. financial crime, 2015, S. 532.

aa. Böszörmenyi/Schweighofer

Im Jahr 2015, also bald nach Verkündung des wegweisenden EuGH-Urteils in der Sache *Digital Rights Ireland,* untersuchten *Böszörmenyi/Schweighofer*[1618] die Überwachungsmechanismen der sich damals im Gesetzgebungsverfahren befindenden 4. GWRL im Hinblick auf das Europäische Primär- und Menschenrecht. Zunächst stellten sie fest, dass der Vorschlag[1619] zur Richtlinie eine intensivierte Sammlung und Speicherung persönlicher Daten verlangte und nach der Rechtsprechung des EGMR schon dieser Speichervorgang in das Recht auf Privatsphäre aus Art. 8 EMRK eingreift.[1620] Die Nutzung dieser Daten für das laufende Monitoring mithilfe ausgefeilter Software könne man als „dataveillance" bezeichnen. Dieser von *Clarke* geprägte Begriff beschreibe die systematische Nutzung persönlicher Daten zur Ermittlung oder Überwachung bestimmter Handlungen oder Kommunikation einer oder mehrerer Personen[1621] – ein Vorgang, der gemeinhin intensiv und bedrohlich sei.[1622]

Zwischen dem Überwachungsregime der 4. GWRL und der vom EuGH in *Digital Rights Ireland* aufgehobenen Richtlinie über die TK-Vorratsdatenspeicherung[1623] erkannten *Böszörmenyi/Schweighofer* „offensichtliche

1618 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71); krit. zum Transaktionsmonitoring schon *dies.* in Schweighofer/Kummer/Hötzendorfer (Hrsg.), IRIS; Internationales Rechtsinformatik Symposium, Transparenz, 2014, S. 617 (621 f.).

1619 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, 05. Februar 2013, COM(2013) 45 final, 2013/0025 (COD).

1620 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71) mit Verweis auf EGMR, Factsheet – Personal Data Protection, aktuelle Version Januar 2022 https://www.echr.coe.int/Documents/FS_Data_ENG.pdf, zuletzt aufgerufen 12.01.2025; vgl. auch EGMR, Urt. vom 4. Dezember 2008, 350622/04 & 30566/04, Rn. 67 – Marper/Vereinigtes Königreich, EuGRZ 2009, 299; Urt. vom 16. Februar 2000, 27798/95, Rn. 69 – Amann/Schweiz, EMRK-E 2000-II, S. 201

1621 *Clarke* Communications of the ACM 31 (1988), 498 (499).

1622 Idem, (506).

1623 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, Abl. 2006, L 105/54.

Gemeinsamkeiten".[1624] In der Entscheidung hätte der EuGH ebenfalls bemerkt, dass schon die Speicherung persönlicher Daten einen Eingriff in die Grundrechte auf Privatsphäre darstellte.[1625] Dies müsse auch für die geldwäscherechtlichen Aufbewahrungspflichten i. S. d. Art. 39-41[1626] des Vorschlags zur 4. GWRL gelten.[1627] Ebenso sehe die geplante 4. GWRL wie auch die VDS-RL vor, dass staatliche Sicherheitsbehörden auf die gespeicherten Daten zugreifen könnten. Dies geschehe einmal durch die Meldepflichten, würde aber auch durch den vorgeschlagenen Art. 40 der 4. GWRL[1628] gewährleistet. Dieser sah vor, dass die Verpflichteten Kommunikationswege bereitstellten, auf denen sie den Sicherheitsbehörden vertraulich mitteilen würden, ob und welche Geschäftsbeziehung zu einer gewissen Person besteht. Wie auch die Vorratsdatenspeicherung begründe das Anti-Geldwäscherecht in den beschriebenen Maßnahmen daher einen Eingriff in die Privatsphärenrechte aus Art. 7, 8 der EU-GRC, der gerechtfertigt werden müsse.[1629]

Einen eigenen Versuch solch einer Rechtfertigung bzw. Verhältnismäßigkeitsprüfung der Anti-Geldwäschemaßnahmen wagten die Autoren nicht. Sie bewerteten aber in ihrer Schlussfolgerung den Umstand positiv, dass die „*dataveillance*" nicht beim Staat stattfinde, sondern von Privaten ausgeführt werde. Der Staat habe daher nicht unmittelbaren und systematischen Zugriff auf sämtliche Finanzdaten.[1630]

Die Feinheiten der Speicherungspflichten und vor allem der staatlichen Zugriffsrechte wurden in den Ausführungen von *Böszörmenyi/Schweighofer* nicht sauber herausgearbeitet.

So bezeichnen die Autoren neben den Vorschriften über die Meldepflicht auch den späteren Art. 42. der 4. GWRL als Zugriffsvorschrift. Dieser aber sieht nur vor, dass die Verpflichteten bestimmte Kanäle einrichten müssen, um individuelle Bestandsdatenauskünfte vertraulich erteilen zu können.

1624 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71 f.).
1625 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 56 = NJW 2014, 2169.
1626 Art. 39-41 des Vorschlags, COM(2013) 45, wurden zu Art. 40-42 der 4. EU-GWRL.
1627 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (72).
1628 Entspricht Art. 42 der 4. EU-GWRL.
1629 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (72).
1630 Idem, (73).

Die Vorschrift entspricht damit eher dem Regelungsgehalt des § 44 KWG und ist vor dem Hintergrund, dass jedenfalls in Deutschland schon lange eine automatisierte Bestandsdatenauskunft möglich war, nicht weiter bemerkenswert. Art. 42. der 4. GWRL als Bestandteil eines Vorratsdatenspeicherungskomplex in Verbindung mit der Transaktionsüberwachung und -aufzeichnung zu begreifen, geht daher fehl. Dieser Fehler wurde allerdings auch in der deutschsprachigen Literatur begangen (s. o. II. 5. b. aa.).[1631]

Auch die vorgebrachten Meldepflichten eignen sich nicht für eine Gleichsetzung mit den Regeln über die TK-Vorratsdatenspeicherung. Zwar werden hier massenhaft Daten an die FIU geleitet, die dort je nach Praxis sehr lange gespeichert werden (zur deutschen Praxis siehe oben Kap. D. II. 2. c. dd.). Die Datenübermittlung erfolgt aber nicht anlasslos, sondern aufgrund der geldwäscherechtlichen Verdachtsschwelle. Außerdem ist der Staat hier auf das proaktive Mitwirken der Privaten angewiesen.

Die Schlussfolgerung von *Böszörmenyi/Schweighofer* zur 4. GWRL bzw. deren Vorschlag ist somit nur im Ergebnis nachvollziehbar. Aus heutiger Sicht ist die Arbeit relevant, da sie den Blick auf die Aufbewahrungspflichten als Teil einer Vorratsdatenspeicherung geworfen hat.

Dass noch keine kritische Zugriffsnorm genannt wurde, ist verständlich, da die Auseinandersetzung auf der 4. GWRL beruht. Erst später wurde mit Art. 32a Abs. 9 der 5. GWRL eine Norm geschaffen, deren Wortlaut ein Zugriffsrecht der FIUs offen vorsieht.

bb. Milaj/Kaiser

Ebenfalls mit der 4. GWRL beschäftigen sich ein Aufsatz von *Milaj/Kaiser*[1632] und die Dissertation von *Kaiser*[1633], die offenbar die Grundlage für den erstgenannten Beitrag darstellte. Die Arbeiten weisen allein schon aufgrund des unterschiedlichen Umfangs einige Unterschiede auf.

Die Autorinnen verglichen in ihrem Aufsatz wie auch *Böszörmenyi/Schweighofer* das Anti-Geldwäscherecht mit der EuGH-Rechtsprechung zur TK-Vorratsdatenspeicherung seit *Digital Rights Ireland*. Ihre Ausführungen, wie von einer Dissertationsschrift zu erwarten, sind aber

1631 *Heinson* in Specht/Mantz (Hrsg.), Hdb. Europ. & Deutsches Datenschutzrecht, 2019, § 14 Rn. 91; *Krais*, CCZ 2015, 251 (252).
1632 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115.
1633 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 122.

deutlich ausführlicher und wagen sich vor allem auch an eine eigene Prüfung der Verhältnismäßigkeit.

Die Vorschriften der 4. EU-Geldwäschebekämpfung verstehen *Milaj/Kaiser* als umfassende Pflicht zur Überwachung und Speicherung sämtlicher Kontotransaktionen.[1634] Dabei entstünden Sammlungen sensibelster Daten. Kaum ein Datenschatz sei so geeignet zum Erstellen von Persönlichkeitsprofilen wie Transaktionsdaten. Aus den Zahlungen ließen sich nicht nur Bewegungsprofile erstellen, sondern auch persönliche Vorlieben, Interessen, politische Einstellungen oder die Religionszugehörigkeit – etwa durch Spenden, Partei- oder Gewerkschaftsbeiträge.[1635]

Ausgangpunkt der Verhältnismäßigkeitsprüfung des Aufsatzes ist allein die Aufzeichnungs- und Aufbewahrungspflicht bzw. „data retention" aufgrund Art. 40 der 4. GWRL. Die Identifikationspflicht und das Monitoring sämtlicher Transaktionen werden zwar erwähnt, allerding nicht eigenständig auf ihre Vereinbarkeit mit höherrangigem Recht geprüft. Es ist zwar immer wieder von „surveillance" die Rede. Offenbar ist damit aber nicht der eigentliche EDV-Monitoring-Vorgang gemeint, bei dem Transkationen in Echtzeit, also unmittelbar bei der Ausführung, oder im Rahmen periodischer nachträglicher Kontrollen abgeglichen werden (s. o. Kap. D. II. 2. b. aa. (2)), sondern die Aufzeichnung und Aufbewahrung der Transaktionsdaten als solche.[1636] Im Rahmen der Verhältnismäßigkeit spielt deshalb vor allem die Sensibilität bzw. Privatheit der Daten und die Dauer der Aufbewahrung eine Rolle.[1637] Die Untersuchung der Finanzdaten durch die Geldwäscheverpflichteten wird jedoch im Rahmen der Verhältnismäßigkeit als Zweck der Speicherung relevant. So kommen *Milaj/Kaiser* zu dem Ergebnis, dass die überaus lange Aufbewahrung der Finanzdaten zur umfassenden Prüfung sämtlicher Transaktionen genau einen solchen Fall der *ständigen Überwachung*[1638] darstellt, die den EuGH zur Aufhebung der TK-Vorratsdatenspeicherungsrichtlinie veranlasst habe.[1639]

Im Ergebnis stellen sie fest, dass die ausnahmslose Speicherung zwangsweise dazu führt, dass Daten gespeichert werden, die für eine effektive

1634 Idem, S. 96 ff.; *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (122 f.).
1635 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 241 f., 430; *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (122).
1636 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (118, 122 ff.).
1637 Idem, (122 ff.).
1638 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 37 = NJW 2014, 2169.
1639 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115 (124).

Geldwäschebekämpfung mangels Verdachtsmoments völlig irrelevant sind. Die Speicherung sei somit nicht erforderlich und damit unverhältnismäßig.[1640] Auf die Frage, wie der Staat überhaupt auf die gespeicherten Daten zugreifen kann, und wie sich das auf die Frage der Verhältnismäßigkeit der Aufzeichnungs- und Aufbewahrungspflicht auswirkt, geht der Aufsatz nicht ein.

Differenzierter hinsichtlich der verschiedenen in der 4. GWRL angelegten Pflichten geht *Kaiser* in ihrer Dissertation vor. Dort werden zu Beginn der Verhältnismäßigkeitsprüfung die Identifikationspflicht, das EDV-Monitoring, die Meldepflicht, die Aufzeichnungs- und Aufbewahrungspflicht separat als eigenständige Grundrechtseingriffe vorgestellt.[1641] Im Rahmen der Verhältnismäßigkeit werden sie dann aber einheitlich als Komplex geprüft.[1642] Objekt der europarechtlichen Prüfung ist bei *Kaiser* offenbar die 4. GWRL in Gänze.

Dabei kommt sie insgesamt zum selben Ergebnis, das bereits in dem beschriebenen Aufsatz präsentiert wurde. Die Pflichten aus dem Anti-Geldwäscherecht begründeten eine Form der „Massenüberwachung"[1643], da ständig Informationen über den größten Teil der Bevölkerung verarbeitet und gespeichert würden. Das Zusammenspiel der einzelnen Maßnahmen führe im Ergebnis zur Unverhältnismäßigkeit der Richtlinie.

Die Meldepflichten etwa seien aufgrund der niedrigen Verdachtsschwelle extensiv und undurchsichtig.[1644] Ein Schutz besonderer Kategorien persönlicher Daten sei nirgends vorgesehen.[1645] Überhaupt fehle es an Transparenz und damit auch an der Möglichkeit, einen effektiven Rechtsschutz zu erhalten.[1646] Die Fristen der Speicherpflicht seien darüber hinaus deutlich überzogen.[1647]

Prominent werden auch die Zugriffsmöglichkeiten staatlicher Stellen auf die gespeicherten Daten als Aspekte der Verhältnismäßigkeit der Richtlinie besprochen, anstatt als Grundrechtseingriffe eigenständig geprüft zu wer-

1640 Ibid.
1641 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 432 ff.
1642 Idem, S. 451 ff.
1643 Idem, S. 452 ff.
1644 Idem, S. 465 ff.
1645 Idem, S. 467 ff.
1646 Idem, S. 486 ff.
1647 Idem, S. 493 ff.

den. Dabei ging *Kaiser* auf den damals vorliegenden Vorschlag[1648] zur 5. GWRL ein. In diesem war, neben der Einführung des Art. 32 Abs. 9, auch eine Änderung des Art. 33 Abs. 1 lit. b) der 4. GWRL vorgesehen.[1649] Nur letzterer wurde von der *Autorin* als Zugriffsnorm erkannt. Art. 32 Abs. 9 der 5. GWRL blieb unerwähnt.

Nach Art. 33 Abs. 1 lit. b) der 5. GWRL sollten die Verpflichteten „der zentralen Meldestelle auf Verlangen unmittelbar alle erforderlichen Auskünfte zur Verfügung stellen". Die Norm überschneidet sich inhaltlich mit Art. 32 Abs. 9 der 5. GWRL und Art. 32 Abs. 3 S. 4 der 4./5. GWRL, statuiert aber weniger ausdrücklich eine Zugriffsnorm als Art. 32 Abs. 9 der 5. GWRL.

Warum sich *Kaiser* in ihrer Bewertung der Zugriffsmöglichkeit nicht (auch) auf Art. 32 Abs. 9 der 5. GWRL stützte, bleibt unklar. Jedenfalls aber stellte sie fest, dass sich die Möglichkeit einer umfangreichen Ermächtigung der FIUs zu Auskunftsersuchen, unabhängig vom Vorliegen einer Meldepflicht, nachteilig auf die Verhältnismäßigkeit der geldwäscherechtlichen Verpflichtungen auswirkte.[1650] So sei es ein Hauptargument des EuGH in *Digital Rights Ireland* gewesen, dass im Rahmen der EU-VorratsdatenspeicherungsRL keine Voraussetzungen oder Hürden geregelt wurden, unter denen staatliche Sicherheitsbehörden die gespeicherten TK-Verkehrsadern abfragen durften.[1651] Diese Frage war durch Art. 4 der VDS-RL allein den Mitgliedstaaten überlassen worden. Auch die Zugriffrechte der FIUs auf die Informationen der Geldwäscheverpflichteten unterlägen nach der 4./5. GWRL keinen ausdrücklich geregelten Voraussetzungen. Die Aussagen des EuGH könnten also analog auf die Verhältnismäßigkeit der GWRL angewandt werden.[1652]

Kaiser kommt daher zu dem Ergebnis, dass die 4./5. GWRL nicht den Anforderungen des EuGH an die Verhältnismäßigkeit genügen könne.[1653] Durch die Massenüberwachung, die sich aus dem Zusammenwirken der geldwäscherechtlichen Verpflichtungen ergäbe, würden fast sämtliche Bür-

1648 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG, COM(2016) 450 final 2016/0208 (COD).

1649 Beide Vorschläge fanden unverändert Einzug in die Richtlinie.

1650 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 481 ff.

1651 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 61 = NJW 2014, 2169.

1652 *C. Kaiser,* Privacy in Financial Transactions, 2018, S. 483.

1653 Idem, S. 510 ff.

ger der EU unter Generalverdacht gestellt. Die Verhinderung von Geldwäsche und Terrorismusfinanzierung seien zwar sicher legitime Ziele. Sie könnten aber die Maßnahmen aufgrund deren extensiver Ausgestaltung nach den Grundsätzen des EuGH aus *Digital Rights Ireland* und *Tele2Sverige* nicht rechtfertigen.

Die Arbeiten von *Milaj/Kaiser* enthalten den bislang ausführlichsten Vergleich des Europäischen Anti-Geldwäscherechts und der TK-Vorratsdatenspeicherung bzw. der dazu ergangenen Rechtsprechung.

In beiden Schriften wird jedoch übersehen, dass in der GWRL – anders als bei der VDS-RL – verschiedene Pflichten für Private geregelt werden. Letztere enthielt lediglich eine Speicherpflicht bzgl. der TK-Verkehrsdaten sowie die Pflicht der Staaten, Zugriffe ihrer Sicherheitsbehörden auf die gespeicherten Daten zu ermöglichen. Daher konnte der EuGH sinnvollerweise nur eine einzelne Maßnahme prüfen, anhand derer die gesamte Richtlinie letztlich stand oder fiel.[1654]

Die Prüfung der GWRL scheint komplexer. Natürlich hängen die Überwachungs- bzw. Monitoring-Pflicht, die Meldepflicht und die Aufbewahrungspflicht inhaltlich zusammen. Sie wirken sich jedoch unterschiedlich aus und können separat voneinander geprüft werden, wobei sich die Intensität der einzelnen Maßnahmen synergetisch aus deren Wechselwirkung ergibt (s. dazu Kap. B. I. 1. c.).

Wie bereits dargelegt, führt allein das Monitoring noch nicht dazu, dass staatliche Sicherheitsbehörden ohne Weiteres auf anlasslos gespeicherte Daten zugreifen können. Erst durch die Meldung an die FIUs gelangen die Daten an den Staat, wenn die Verpflichteten im Rahmen des Monitorings einen Verdacht erkannt haben. Durch die proaktive Meldung erhalten die Sicherheitsbehörden somit nur einen selektierten Datenschatz (s. o. Kap. D. II. 2. c. ee.). Die Rechtsprechung des EuGH zur TK-Vorratsdatenspeicherung lässt sich auf diesen Teilkomplex der Pflichten also nicht so einfach übertragen, da es hier in sämtlichen Urteilen um den möglichen Zugriff auf anlasslos gespeicherte Daten ging.

Was die Arbeiten im Weiteren außer Acht lassen, sind die Auswirkungen der generellen Zwischenschaltung Privater. Es kann zwar kein Zweifel daran bestehen, dass die staatlich veranlassten Pflichten der Institute und anderer Personen mittelbar in die Rechte derer Kunden eingreifen,

1654 Vgl. EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland), Rn. 32 = NJW 2014, 2169.

es handelt sich also nicht um ein Problem der mittelbaren Drittwirkung (s. o.).[1655] Dennoch ist jedenfalls bei dem Komplex aus Überwachung und Meldung zu beachten, dass letztlich nur Private Daten verarbeiten, bei denen noch kein Verdachtsmoment vorliegt. Dabei handelt es sich um Daten, die den jeweils Verpflichteten aus verschiedenen rechtlichen und faktischen Gründen ohnehin vorliegen. Jedenfalls in dieser Hinsicht könnte man argumentieren, dass die Verpflichteten faktisch nicht zu einer eigenständigen Datensammlung, sondern nur zu einer spezifischen Verarbeitung der ihnen vorliegenden Daten gezwungen werden.

Ein unmittelbarer Vergleich der gesamten Richtlinien ist aufgrund der strukturellen Unterschiede, die die proaktive Einschaltung Privater bzgl. bestimmter Maßnahmen mit sich bringt, jedenfalls nicht angezeigt. Stattdessen sollten die verschiedenen Pflichten einzeln betrachtet und mit der vorhandenen Rechtsprechung abgeglichen werden (dazu unten Kap. G. III. 2.).

cc. Vogel

Der Abgleich der geldwäscherechtlichen Pflichten mit der Rechtsprechung des EuGH zur TK-Vorratsdatenspeicherung wird auch von *Vogel* in einer kritischen Gesamtschau der EU-Geldwäscherichtlinie und insbesondere des GwG bemüht.[1656] Da es in den Urteilen zu *Digital Rights Ireland* und *Tele2Sverige* um Kommunikationsdaten ging, könnten die Entscheidungen zwar nicht unmittelbar auf das Anti-Geldwäscherecht der EU angewandt werden. Aus deren Inhalt ließen sich jedoch die Grenzen der Verhältnismäßigkeit bei der Verarbeitung von Finanzdaten zu Sicherheitszwecken ableiten.[1657]

Hierzu müssten die TK-Verkehrsdaten und Finanzdaten zunächst hinsichtlich ihrer Grundrechtsrelevanz verglichen werden. Dabei könne man leicht annehmen, dass es schon aufgrund der Quantität beachtliche Unterschiede gäbe. Da die moderne Fernkommunikation fast ausschließlich

1655 So schon *Herzog*, WM 1996, 1753 (1757).

1656 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (897 ff.); zur deutschen Rechtslage *ders.* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (246 ff.).

1657 *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (900 f.).

telekommunikativ erfolgt, entstehen zwangsläufig gewaltige Datenmengen. Wie der EuGH auch richtig bemerkt hätte, könne aus den TK-Verkehrsdaten allein aufgrund deren Massen präzise Rückschlüsse über das Privatleben der betroffenen Bürger gewonnen werden.[1658]

Persönliche Finanzdaten entstünden normalerweise in geringerem Umfang. Außerdem könnten Kunden nicht erwarten, dass die Daten so vertraulich behandelt würden wie ihre Telekommunikation, denn sie offenbaren sie in einem geschäftlichen und nicht in einem privaten Verhältnis. Transaktionen und andere wirtschaftliche Verhaltensweisen wären ohne ein gewisses Maß an Öffentlichkeit gar nicht möglich. (Analoge) Banküberweisungen etwa würden zwangsläufig dem verarbeitenden Mitarbeiter zuteilwerden.

Andererseits, meint *Vogel*, müsse beachtet werden, dass auch im laufenden Geschäftsverkehr elektronische Zahlungen immer stärker in den Vordergrund rücken, und zwar sowohl im Offline- als auch insbesondere im Onlinegeschäftsverkehr. Die so getätigten Transaktionen enthielten detaillierte Informationen über sämtliche Umstände des getätigten Geschäfts, aus denen nuanciert Bewegungsprofile, persönliche Verhaltensweisen oder Interessen und somit umfangreiche Persönlichkeitsbilder abgeleitet werden könnten. Da Transaktionsdaten alle Umstände des getätigten Geschäfts offenlegten, seien sie letztlich besser geeignet zur Erstellung von Persönlichkeitsprofilen als TK-Verkehrsdaten. Anders als diese könnten sie zusätzlich auch nicht verschlüsselt werden.[1659]

Mit Transaktionsdaten sei es aber auch noch nicht getan. Die Aufbewahrungspflichten des Anti-Geldwäscherechts wären nicht auf diese limitiert, sondern enthielten sämtliche Informationen, die die Verpflichteten im Rahmen der Sorgfaltspflichten einholten. Je nach Risiko könnten dies auch Social-Media-Analysen oder sonstige persönliche Hintergründe sein. Diese Informationen könnten in Verbindung mit den Transaktionsdaten „extensive Persönlichkeitsprofile" liefern.[1660]

Neben der Daten-Art müssten weiter auch die Umstände der Speicherpflicht untersucht werden, da nach dem EuGH bereits die Speicherpflicht zur späteren Verwendung an sich einen Eingriff in Art. 7, 8 EU-GRC darstellte.[1661] Auch hier aber zeige sich, dass sich das Anti-Geldwäscherecht

1658 Idem, (901).
1659 Idem, (901 f.).
1660 Idem, (902).
1661 Idem, (902 f.).

hinsichtlich der vom EuGH aufgestellten Voraussetzungen eher zulasten der Bürger von der VDS-RL unterscheide. Es würden nicht nur Transaktionsbelege aufbewahrt, sondern Transkationen mittels EDV-Systemen überwacht und auf Auffälligkeiten untersucht. Das Monitoring würde zwar primär zur Durchführung proaktiver Meldungen genutzt. Es bewirke aber dennoch, dass jeder Kunde möglicherweise zum Ziel staatlicher Ermittlung werden könnte, ohne tatsächlich eine Straftat begangen zu haben oder diese vorzubereiten. Die Speicherpflichten des europäischen Anti-Geldwäscherechts müssten daher nach den Standards des EuGH einen Grundrechtseingriff darstellen und könnten an die Voraussetzungen des EuGH an solch einen Eingriff gebunden sein.[1662]

Bei der Bewertung dieses Eingriffes spielten aber verschiedene Aspekte eine Rolle, die vor einer Eins-zu-Eins-Übertragung der Rechtsprechung geklärt werden müssten. Hier nennt *Vogel* zunächst die zuvor besprochene Unterschiedlichkeit von Transaktionsdaten und Telekommunikationsverkehrsdaten. Zwar lesen sich seine Ausführungen so, als ob er offenbar von einer erhöhten Sensibilität gegenüber den TK-Verkehrsdaten ausgeht. Eine ausdrückliche Festlegung erfolgt allerdings nicht. Er stellt lediglich fest, dass es am Ende auf die Möglichkeit der Profilbildung ankommen müsse.[1663] Weiter käme es bei der Bewertung der Speicherpflicht darauf an, welche Konsequenzen aus der Datenverarbeitung folgen – insbesondere, unter welchen Umständen die Daten an die FIUs gemeldet würden, und ob der Bürger gegen die Ausübung der Sorgfaltspflichten einen effektiven Rechtsschutz erlangen könnte.

Da nicht auszuschließen sei, dass die anti-geldwäscherechtliche Aufzeichnungs- und Aufbewahrungspflicht einen ähnlich intensiven Grundrechtseingriff wie die TK-Vorratsdatenspeicherung darstellt, sollten die Gesetzgeber dafür Sorge tragen, dass auf die gespeicherten Daten nur zur Ahndung und Verhinderung schwerer Straftaten zugegriffen werden dürfte.[1664] Ausdrücklich für europarechtswidrig werden die Vorschriften aber nicht erklärt.

Neben der Speicherpflicht untersucht *Vogel* weiter, wie die Datenverarbeitungsbefugnisse der FIUs rechtlich zu bewerten sind.[1665] Diese gingen mittlerweile weit über die Analyse eingehender Verdachtsmeldungen hi-

1662 Idem, (903 f.) .
1663 Idem, (904).
1664 Ibid.
1665 Idem, (904 ff.).

naus. Zwar hätten FIUs mit wenigen Ausnahmen, etwa den Kontobestandsdaten, keinen unmittelbaren Zugriff auf Finanzdaten. Ihnen stünden aber verschiedene Ermächtigungen zum Abfragen solcher Daten bei den Verpflichteten zur Verfügung.[1666]. Ferner könnten die Verpflichteten auf die Auskunftsersuchen hin eigene Untersuchungen vornehmen und so noch mehr Informationen erlangen, die sie dann den FIUs übergeben könnten.[1667]

Diese Umstände in Verbindung mit den verschiedenen Formen des Monitorings führten dazu, dass die Datenanfragen der FIUs letztlich keine bloßen Auskunftsersuchen bzw. Ermittlungen darstellten, sondern eine Überwachung der Kunden.[1668] Daher seien hier die Rechtsprechung des EGMR und des EuGH zu Überwachungsmaßnahmen zu beachten.[1669] Danach sollten insbesondere Ermächtigungsgrundlagen zu Eingriffen, die nicht vom Bestehen einer vorherigen Meldungen oder eines sonstigen Verdachts abhängig sind, von den Gesetzgebern unter spezifische Voraussetzungen gestellt werden.[1670]

Bei *Vogel* findet sich somit eine geteilte Besprechung der Speicherpflichten einerseits und der Ermächtigungsgrundlagen der FIUs andererseits, wobei letztere wiederum im Rahmen der Verhältnismäßigkeit der Speicherpflicht eine Rolle spielen, da die Bewertung der Speicherpflicht davon abhängig sein soll, wie die Daten in der Folge verarbeitet werden können.

Konkret stellt *Vogel* fest, dass es sich beim Anti-Geldwäscherecht letztlich um eine staatlich veranlasste Überwachung der Kunden handle, die zentral von den FIUs gesteuert werde. Auffällig an seiner Kritik ist, dass er es vermeidet, konkrete Normen als europa- oder menschenrechtswidrig zu bezeichnen. Vielmehr stellt er die Anwendbarkeit bestimmter Teile der Rechtsprechung von EuGH und EGMR lediglich in den Raum und macht sie von einer bestimmten Lesart der geldwäscherechtlichen Befugnisse abhängig, ohne sich dabei endgültig festzulegen, ob diese Lesart denn auch zutrifft.

1666 Zu § 30 Abs. 3 GwG: *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 157 (242 ff.).

1667 *Ders.* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (905).

1668 Idem, (906 f.).

1669 Idem, (906 ff.).

1670 Idem, (909) mit Verweis auf EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 119 = NJW 2017, 717; EGMR, Urt. vom 29. Juni 2006, 54934/00, Rn. 97 – Weber and Saravia/Deutschland = NJW 2007, 1433; Urt. v. 27.10.2015, 62498/11, Rn. 134-146 – R.E./Vereinigtes Königreich = NJW 2016, 2013.

Jedenfalls bei der Speicherpflicht drängt sich dann aber doch der Eindruck auf, dass *Vogel* die umfangreichen Speicherpflichten angesichts der darauf aufbauenden Monitorsysteme, Meldepflichten und Zugangsberechtigungen für nicht vereinbar mit den Anforderungen des EuGH hält. Auch die Bewertung der Zugangsrechte der FIUs lässt erkennen, dass er angesichts der fehlenden ausdrücklichen Voraussetzungen eine Unvereinbarkeit der Normen (etwa § 30 Abs. 3 GwG) durchaus für möglich hält.

dd. Betrand/Maxwell/Vamparys

Der zuletzt hier vorzustellende Beitrag zu der Thematik stammt aus dem Jahr 2021 und kam von den Autoren *Betrand/Maxwell/Vamparys*.[1671] In dem Aufsatz wird die Anwendung künstlicher Intelligenz durch die geldwäscherechtlich Verpflichteten aus grundrechtlicher Perspektive untersucht. Dabei stoßen die Autoren auf die Frage, ob die Monitoring-Maßnahmen nach der GWRL, ausgehend von der EuGH Rechtsprechung zur Vorratsdatenspeicherung von TK-Verkehrsdaten[1672] und PNR-Daten[1673], mit den Europäischen Grundrechten auf Privatsphäre in Einklang gebracht werden können. Dies bestimmte sich nach dem Grundsatz der Verhältnismäßigkeit.

Zunächst stellen die Autoren daher den Rechtsrahmen der Verhältnismäßigkeitsprüfung vor. Für sicherheitsrechtliche Maßnahmen folge deren Notwendigkeit nicht nur aus Art. 52 Abs. 1 der EU-GRC und Art. 8 der EMRK, sondern auch aus Art. 11 der Konvention 108[1674] sowie Art. 23 DSGVO und Art. 4 der JI-Richtlinie. Zu unterschiedlichen Ergebnissen würden die verschiedenen Rechtsgrundlagen aber nicht führen, die Verhältnismäßigkeitsprüfung erfolge stattdessen immer nahezu identisch.[1675]

Auf die bisherigen Besprechungen der Verhältnismäßigkeit von Anti-Geldwäschemaßnahmen in der Literatur gehen die Autoren nur kurz ein.

1671 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276.

1672 berücksichtigt auch EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.) = NJW 2021, 531.

1673 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 – PNR Canada = ZD 2018, 23; s.a. jüngst, GA EuGH (Pitruzzella), Schlussantrag v. 27.01.2022 – C-817/19.

1674 *Europarat*, Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981, ETS Nr. 108, (BGBl. 1985 II S. 539).

1675 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (278 f.).

Insbesondere die Arbeit von *Milaj/Kaiser*[1676] (s. o.) weise eine große Ähnlichkeit zu ihrem Ansatz auf. Um sich davon abzugrenzen und eine Lücke zu schließen, legten *Betrand/Maxwell/Vamparys* den Fokus konkret auf die Verhältnismäßigkeit des Einsatzes künstlicher Intelligenz im Rahmen des Transaktionsmonitorings.[1677] Die Speicherpflichten der GWRL spielen in ihrem Aufsatz keine Rolle.

Deutlich intensiver als die Literatur besprechen die Autoren die vorhandene Rechtsprechung. Die Anforderungen an die Verhältnismäßigkeit werden Art. 52 Abs. 1 der EU-GRC entnommen und zunächst anhand der EuGH-Urteile *Digital Rights Ireland* und *Tele2Sverige* in Bezug auf sicherheitsrechtliche Datenverarbeitungen illustriert.[1678] In den Entscheidungen habe der EuGH geklärt, dass das anlasslose Speichern von TK-Verkehrsdaten zu sicherheitsrechtlichen Zwecken grundsätzlich unzulässig sei. Für bestimmte Bereiche oder Zeiträume könnten zwar hiervon Ausnahmen gemacht werden, aber nur, wenn enge Voraussetzungen gegeben seien.[1679] In einem weiteren Fall habe der EuGH allerdings klargestellt, dass nicht jede Form der Vorratsdatenspeicherung illegitim sei. Das universale Vorhalten von Kundendaten sei stattdessen nur dann exzessiv, wenn die entsprechenden Daten auch ein bestimmtes Maß an Sensibilität erreichen.

Besonders relevant für die Bewertung des Transaktionsmonitorings sei weiter das Gutachten des EuGH zum PNR-Abkommen[1680] der EU mit Kanada.[1681] Dieses sah vor, dass Airlines bestimmte Informationen über Passagiere von Flügen zwischen der EU und Kanada an eine kanadische Behörde übermittelten, die dort zur Bekämpfung von Terrorismus auf bestimmte Muster hin analysiert und sodann gespeichert wurden. Der EuGH erklärte in den Gutachten das Abkommen für ungültig, da es u. a. keine ausreichenden Voraussetzungen für den Zugriff auf die übertragenen Daten vorsah und die Speicherung der Daten über den Zeitraum des Aufenthalts in Kanada auch für solche Passagiere erlaubte, bei denen noch nicht fest-

1676 *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115.
1677 Idem, (279 f.).
1678 Idem, (280 ff.)m
1679 Idem, (280) mit Verweis auf EuGH, Urteil v. 21.12.2016, C-203/15, C-698/15 (Tele2 Sverige/Watson ua.), Rn. 9 = NJW 2017, 717.
1680 *Europäisches Parlament,* Agreement between Canada and the European Union on the Transfer and
Processing of Passenger Name Record, 23 June 2014, 2013/0250 (NLE), 12657/5/13 REV 5.
1681 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 – PNR Canada = ZD 2018, 23m

stand, ob von ihnen eine objektive Gefahr ausging. Auch zu der automatischen Analyse äußerte sich der EuGH. Diese sei nur dann verhältnismäßig, wenn, die verwendeten Datenbanken und Kriterien regelmäßig unter Berücksichtigung aktueller Forschung auf ihre Zuverlässigkeit, Aktualität und Diskriminierungsfreiheit untersucht würden.[1682] Hier sahen *Betrand/Maxwell/Vamparys* eine starke Parallele zum (EDV-)Transaktionsmonitoring (s. a. Kap. G. III 2. a. cc (1)).[1683]

Ebenfalls mit systematischer Analyse setzte sich der EuGH in *La Quadrature du Net* auseinander. Dort stellte er fest, dass das Echtzeitmonitoring von TK-Verkehrs- und Standortdaten durch die französische Polizei zur Erkennung von Mustern, die auf terroristische Bedrohungen schließen lassen könnten, einen erheblichen Grundrechtseingriff darstellte. Dieser könne nur legitim sein, wenn für den betreffenden Mitgliedstaat eine akute terroristische Bedrohungslage festgestellt werden könnte.[1684] Hieraus schlossen die Autoren, dass die Verwendung automatisierter Algorithmen zur Erkennung von Straftaten allgemein nicht ohne das Vorliegen bestimmter Voraussetzungen verhältnismäßig sein könne. Das ist wiederum eine Erkenntnis, die sich auf das Transaktionsmonitoring übertragen ließe.[1685]

Aus der Rechtsprechung zur EMRK identifizierten *Betrand/Maxwell/Vamparys* einen weiteren Fall zur Verwendung von Algorithmen im Bereich des Sicherheitsrechts. Im Rahmen des niederländischen SyRI-Programms wurden verschiedene Datenbanken der Sozialbehörden automatisiert auf Muster von Sozialleistungsbetrug hin durchleuchtet. Ein niederländisches Obergericht hielt das Programm mangels Transparenz für unverhältnismäßig i. S. d. Art. 8 Abs. 2 EMRK, obwohl sämtliche positive Treffer von Mitarbeitern händisch überprüft wurden.[1686] Auch dahingehend müsste die Verwendung von Algorithmen beim Transaktionsmonitoring also untersucht werden.[1687]

Ein regelbasiertes Monitoring sei aufgrund der steigenden Zahl von Transaktionen kaum mehr effektiv, da sie eine Vielzahl falschpositiver

1682 Idem, Rn. 174.
1683 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (281 f.).
1684 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Rn. 174 ff. = NJW 2021, 531.
1685 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (282).
1686 Rb. Den Haag - C/09/550982/HA ZA 18/388
1687 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (282 f.).

Meldungen und somit eine große Arbeitslast erzeuge.[1688] Daher setzten einige Institute vermehrt auf künstliche Intelligenz.[1689] Diese würde sehr viel effektiver als Menschen bestimmte Muster erkennen und sehr viel schneller lernen. Problematisch sei jedoch, dass die Systeme zum Lernen eine Grundlage benötigten. An dieser fehle es, da noch immer keine grundsätzlichen Muster bekannt seien, hinter denen regelmäßig tatsächlich kriminelles Verhalten steht.[1690] Das Transaktionsmonitoring beruhe daher überwiegend noch auf einem regelbasierten Ansatz ohne Verwendung maschinellen Lernens.[1691]

Im Rahmen der Verhältnismäßigkeitsprüfung wird das Transaktionsmonitoring dann grundsätzlich und nicht nur im Hinblick auf die Verwendung von Algorithmen untersucht. Zunächst stellen die Autoren fest, dass das Transaktionsmonitoring aufgrund seiner Anlasslosigkeit und Allgemeinheit eine erhebliche Intensität aufweise. Dabei berufen sie sich auf die EuGH-Rechtsprechung zur Vorratsdatenspeicherung von TK-Verkehrs- und PNR-Daten. Hinzu trete, dass bei der Erstellung von Persönlichkeitsprofilen teilweise auf Algorithmen zurückgegriffen würde, jedenfalls aber die Möglichkeit bestehe.[1692]

Der Frage, ob diesem Eingriff ein proportionaler Zweck entgegensteht, wird die Klärung der gesetzlichen Grundlage und deren Bestimmtheit i. S. d. Art. 52 Abs. 1 S. 1 EU-GRC vorangestellt. Insbesondere an der Bestimmtheit haben *Betrand/Maxwell/Vamparys* erhebliche Zweifel, da das Transaktionsmonitoring in der GWRL nicht näher beschrieben werde.[1693]

1688 Idem, (284) mit Verweis auf *IBM,* financial crime AI, 2019, https://web.archive.org/web/20220208195208/https://www.ibm.com/downloads/cas/WKLQKD3W , zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im April 2022); M. *Weber et al.,* AML (preprint), 2018, https://arxiv.org/pdf/1812.00076, zuletzt aufgerufen am 12.01.2025.

1689 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (284 f.) mit Verweis u.a. auf *Canhoto* J. of Business Research 131 (2020), 441; *Accenture,* AML Machine Learning, 2017, https://web.archive.org/web/20220303015059/https://www.accenture.com/_acnmedia/pdf-61/accenture-leveraging-machine-learning-anti-money-laundering-transaction-monitoring.pdf, zuletzt aufgerufen am 12.01.2025 (Original-Link zuletzt aufgerufen im April 2022).

1690 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (285).

1691 Idem, (286) mit Verweis auf *Verhage*, J. of Money Laundering Control 2009, 371; s.a. *Canhoto*, J. of Business Research 131 (2020), 441 (442 mwN.).

1692 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (286).

1693 Idem, (287 f.)

Auch von der Erforderlichkeit der Maßnahme i. S. d. Art. 52 Abs, 1 S. 2 EU-GRC sind die Autoren nicht überzeugt. Schon die finanziellen Kosten des Transaktionsmonitorings würden den Wert der aufgrund gemeldeter Transaktionen konfiszierten Gelder überschreiten.[1694] Ob alternative Systeme weniger einschneidend, aber gleich effektiv sein könnten, müsse besser evaluiert werden.

Zuletzt wird die Angemessenheit nach Art. 52 Abs. 1 S. 2 EU-GRC geprüft. Entscheidend hierfür seien die Maßstäbe des EuGH zur TK-Verkehrs- und Bestandsdatenabfrage. In diesen Entscheidungen zur Verhältnismäßigkeit einer Vorratsdatenspeicherung sei es insbesondere auf die Zugriffsmöglichkeiten der Sicherheitsbehörden angekommen. Aus *Ministerio Fiscal* ergebe sich, dass ein Zugriff auf – im sicherheitsrechtlichen Sinne – anlasslos vorgehaltene Daten nicht grundsätzlich auf schwere Straftaten reduziert werden muss.[1695] Vielmehr ergebe sich aus der EuGH-Rechtsprechung ein Dreistufenkonzept, das zwischen ernsten Gefahren für die nationale Sicherheit, schweren Straftaten und einfachen Straftaten unterscheide (s. dazu oben Kap. C. II. 3.).[1696]

Bei sensiblen Daten wie den Transaktionsdaten wäre eine allgemeine Datenverarbeitung nach den Grundsätzen des EuGH eigentlich nicht möglich. Das führe jedoch zu einem Dilemma. Die Geldwäschebekämpfung basiere auf der Idee, dass sich Risiken nur aus Ungewöhnlichkeiten ableiten ließen. Um Ungewöhnlichkeiten zu erkennen, müsse man aber zwangsläufig alle Transaktionen überwachen, da man sonst ja den Maßstab nicht kenne, aus dem heraus sich Abweichungen erst ergeben.[1697] Dieses Dilemma könne man nur lösen, wenn das Monitoring streng in einen automatisierten Teil und die händische Kontrolle aufgeteilt würde, sodass die allgemeine Überwachung auf den EDV-Prozess beschränkt bleibt. Dieser Prozess müsse von *angemessenen Schutzmaßnahmen* begleitet werden. Einmal müssten die Betroffenen in Kenntnis gesetzt werden, wenn bei ihnen ein „Treffer" erzielt oder gar eine Meldung bei den FIUs vorgelegt wird. Außerdem müssten die Verpflichteten stets erklären können, wie es zu dem Treffer gekommen ist. Zuletzt müsste das System auf seine Rechtskonformität bzw. Effektivität von zuständigen Behörden oder Gerichten kontrolliert

1694 Idem, (288) mit Verweis auf *Sciurba,* AML Regimes, 2019, S. 99.
1695 EuGH, Urteil v. 2.10.2018, C-207/16 (Ministerio Fiscal), Rn. 54 ff. = NJW 2019, 655.
1696 *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276 (289 f.).
1697 Idem, (290).

werden.[1698] Da es derzeit noch an solchen Schutzmaßnahmen fehle, schließen die Autoren damit, dass sich das aktuelle Anti-Geldwäscherecht auch im Rahmen der Angemessenheit als durchaus problematisch darstelle.

Diese Überlegungen zur Verhältnismäßigkeit kranken daran, dass zwischen der allgemeinen Datenverarbeitung durch Vorratsdatenspeicherung und der automatisierten Massenanalyse nicht genau unterschieden wird. Die Vorratsdatenspeicherung zeichnet sich durch zwei Grundrechtseingriffe aus: Speicherung und Zugriff. In *Ministerio Fiscal* etwa betrachtet der EuGH allein das Zugriffsrecht. Zur anlasslosen Speicherung von Bestandsdaten äußert er sich – anders als das BVerfG[1699] – nicht. Zwar ist es richtig, dass der EuGH in den Entscheidungen zur Vorratsdatenspeicherung eigentlich schon die massenhafte Anlegung der Daten und damit die Verarbeitung bei Privaten, die hinter der Massenanalyse zurückbleibt, an Voraussetzungen knüpfen wollte. Die Verhältnismäßigkeit steht aber stets unter der Erkenntnis, dass durch das Vorhalten der Daten letztlich ein staatlicher Zugriff ermöglicht wird. Dieser Umstand ist für das Transaktionsmonitoring nicht unmittelbar zu erkennen, da es allein der proaktiven Meldung von Verdachtsfällen dient. Der staatliche Zugriff ergibt sich erst aus den Aufbewahrungspflichten und den Zugriffsrechten der FIU. Diese Vorschriften werden in dem Beitrag aber an keiner Stelle erwähnt.

Wohl deshalb stellen die Autoren auch nicht nur auf die Rechtsprechung zu den Speicherpflichten ab. Der EuGH hatte sowohl in seinem Gutachten zum PNR-Abkommen[1700] als auch in *La Quadrature du Net*[1701] die automatisierte Datenanalyse und das Vorhalten der verarbeiteten Daten für einen späteren Zugriff als separate Eingriffe behandelt. Lediglich im Rahmen der Verhältnismäßigkeit kommt es dabei zur Interaktion zwischen den einzelnen Maßnahmen. *Betrand/Maxwell/Vamparys* weisen somit auf die passenden Vergleichsobjekte hin, sie beziehen ihre Argumente gegen das Monitoring dann aber primär aus dem allgemeinen Vorbringen gegen anlasslose Speicherpflichten. Die Rechtsprechung des EuGH aus verschieden gelagerten Fällen wird insofern zu pauschal wiedergegeben.

1698 Idem, (290 ff.).

1699 BVerfGE 118, 168 – Kontostammdaten; E 130, 151– Bestandsdatenauskunft I; E 155, 119 – Bestandsdatenauskunft II.

1700 EuGH, Gutachten v. 26.07.2017, Gutachten 1/15 – PNR Canada, Analyse ab Rn. 168 ff.; Speicherung ab Rn. 190 ff. = ZD 2018, 23.

1701 EuGH, Urteil v. 6.10.2020, C-511/18, C-512/18, C-520/18 (La Quadrature du Net ua.), Speicherung ab Rn. 134 ff; Analyse ab Rn. 172 ff. = NJW 2021, 531.

Im Grunde bleibt es bei der Aussage, dass die Voraussetzungen der Vorratsdatenspeicherung zur Unverhältnismäßigkeit des Monitorings führen. Der Unterschied zwischen diesen beiden Maßnahmen wird auf diese Weise verwischt.

c. Zusammenfassung und Stellungnahme

Insbesondere in der europäischen Literatur wird also stark argumentiert, dass die Aufbewahrungspflichten, die Überwachungspflicht samt Transaktionsmonitoring und die Zugriffsrechte der FIU letztlich einen Überwachungskomplex darstellen, der sich an den Voraussetzungen des EuGH zur Vorratsdatenspeicherung messen lassen müsste.[1702]

Übergreifend zeigen sich bei den Besprechungen aber Probleme bei der Übertragung dieser Grundsätze. Anders als die Vorratsdatenspeicherung von TK-Verkehrsdaten besteht das Anti-Geldwäscherecht nicht nur aus einer sicherheitsrechtlichen Speicherpflicht und entsprechenden Zugriffsrechten. Das System basiert primär auf proaktivem Tätigwerden der Verpflichteten zur Überwachung und Meldung. Zwar ist das Monitoring sämtlicher Transaktionen eine intensivere Verarbeitung als das bloße Speichern all dieser Informationen, die automatisierte Analyse mit anschließender Prüfung ist aber auf die Verdachtsmeldung fokussiert. Eine Vorratsdatenspeicherung kann sich erst aus der Pflicht ergeben, die analysierten Daten aufzubewahren – verbunden mit dem Recht der FIUs, anlasslos und geheim darauf zuzugreifen.

Zusammenfassend lässt sich somit sagen, dass die Literatur die Probleme, die sich aus der EuGH-Rechtsprechung zur Vorratsdatenspeicherung für das Anti-Geldwäscherecht ergeben, erkannt und besprochen hat. Die Betrachtungen sind aber in großen Teilen zu undifferenziert geblieben und reflektieren insbesondere nicht die dogmatischen Entwicklungen der Rechtsprechung zum Sicherheitsverfassungsrecht.

Vor deren Hintergrund ist es nicht mehr möglich, die GWRL pauschal für unverhältnismäßig zu erklären, wie es der EuGH mit der VDS-Rl in *Digital Rights Ireland* getan hat (s. o. Kap. C. II. 1. a. aa.). Vielmehr muss

1702 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71 ff.); *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115; *C. Kaiser,* Privacy in Financial Transactions, 2018; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (900 ff.); *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276.

die konkrete gesetzliche Ausgestaltung der jeweiligen Datenverarbeitungsschritte untersucht werden, wobei die Intensität dieser Einzeleingriffe nicht im Rahmen einer isolierten Betrachtung erfolgen kann, sondern in Anbetracht der Wechselwirkungen mit den übrigen Informationseingriffen des Antigeldwäschekomplexes (vgl. Kap. B. I. 1. c.).

7. Ansätze in der Rechtsprechung des BVerfG, EuGH und EGMR

Die Rechtsprechung hat sich bislang nur rudimentär mit der Vereinbarkeit von Anti-Geldwäscherecht und höherrangigem Recht beschäftigt. Eine Verfassungsbeschwerde gegen die verschiedenen Pflichten des Geldwäschegesetzes von mehreren Verpflichteten wies das BVerfG in einem Kammerbeschluss als unzulässig ab. Sie genüge nicht dem Grundsatz der Subsidiarität.[1703] Gegen die geldwäscherechtlichen Pflichten könnten sie mithilfe verwaltungsgerichtlicher negativer Feststellungsklagen vorgehen. Die Voraussetzungen für eine ausnahmsweise mögliche Verfassungsbeschwerde ohne vorherigen fachgerichtlichen Rechtsschutz lägen daher nicht vor, denn über den Verwaltungsrechtsweg könnten die Verpflichteten Rechtsschutz erlangen, ohne zunächst gegen Regeln verstoßen zu müssen, um sodann ein Ordnungswidrigkeiten- oder Strafverfahren zu führen.[1704]

Der fachgerichtliche Rechtsschutz sei den Verpflichteten auch zumutbar. Es stellten sich nicht nur verfassungsrechtliche Fragen, sondern auch ein erheblicher Klärungsbedarf bzgl. den gesetzlichen Vorschriften selbst. So enthalte das GwG eine große Zahl unbestimmter Rechtsbegriffe, deren Bedeutung erst fachgerichtlich geklärt werden müsse.[1705] Außerdem seien etliche Fragen unionsrechtlicher Natur. Auch diese müssten von den Fachgerichten geklärt und eventuell dem EuGH vorgelegt werden.[1706] Eine Vorabentscheidung nach § 90 Abs. 2 BVerfGG käme wegen dieses erheblichen Klärungsbedarfs nicht in Betracht.[1707]

Auf die inhaltlichen Fragen ging das BVerfG quasi nicht ein. Die Überlegung, dass durch die Verpflichtungen auch das Recht der informationellen Selbstbestimmung betroffener Kunden tangiert wird, findet sich in dem Beschluss an keiner Stelle.

1703 BVerfG, NJW 2019, 659.
1704 Iden, (569).
1705 Idem, (660).
1706 Ibid mit Verweis auf BVerfGE 129, 186 (202).
1707 Ibid mit Verweis auf BVerfGE 86, 382 (388).

Auch in der Rechtsprechung des EuGH spielt dieser Aspekt bislang noch eine untergeordnete Rolle. Die bisherigen Urteile zur GWRL befassen sich vorrangig mit Harmonisierungsfragen bzw., inwiefern die Mitgliedstaaten zulasten der Verpflichteten strengere Vorschriften erlassen durften. Die weitergehenden Regeln der nationalen Gesetzgeber wurden aber nicht aufgrund einer etwaigen stärkeren Beeinträchtigung der Kundengrundrechte überprüft, sondern nur als möglicher Verstoß entweder gegen die GWRL selbst oder die europäischen Grundfreiheiten der Verpflichteten.[1708]

Ob die Verpflichtungen nach Maßgabe der Richtlinie selbst gegen höherrangiges Recht verstoßen, wurde vom EuGH bislang nur für Rechtsanwälte geprüft, und zwar in Bezug auf das Recht auf ein faires Verfahren nach Art. 6 Abs 2 EUV und Art, 6 EMRK. Dieses sei allerdings nicht verletzt, da für die Meldepflichten der Rechtsanwälte ausreichende Ausnahmen – etwa für Informationen in Zusammenhang mit rechtlichen Streitigkeiten – geschaffen worden waren.[1709] An der Rechtmäßigkeit der geldwäscherechtlichen Meldepflicht an sich ließ der EuGH keine Bedenken erkennen. Auf die informationelle Selbstbestimmung der betroffenen Mandanten ging der EuGH erst gar nicht ein. Mangels einer vertieften Beschäftigung mit den im Rahmen dieser Arbeit aufgeworfenen Fragen, lassen sich aus den Entscheidungen des EuGH keine entscheidenden Erkenntnisse ziehen.

Der Entscheidung des EuGH zu den Meldepflichten der Rechtsanwälte schloss sich der EGMR im Ergebnis an, stützte seinen Befund aber auf das Recht der Anwälte auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK.[1710] Auf die Rechte der Mandanten stellte der EGMR nicht unmittelbar ab, auch wenn er offenbar von einer Beeinträchtigung dieser ausging.[1711] Mit der Rechtmäßigkeit der geldwäscherechtlichen Aufbewahrungs- und Meldepflichten setzte sich der EGMR ebenfalls nicht auseinander. Auch aus seiner Rechtsprechung lässt sich daher bislang nicht viel mehr schließen, als dass er keine Zweifel an der Vereinbarkeit einer Meldepflicht bzgl. bestimmten Geschäften zur Bekämpfung der Geldwäsche mit der EMRK hegt.

1708 Vgl. EuGH, Urt. v. 10.03.2016, C-235/14 = ZD 2016, 404 (Ls.); Urt. v. 25.4.2013, C-212/11 (Bank Gibraltar) = ZD 2013, 398.
1709 EuGH Urt. v. 26. 6. 2007, C-305/05 (Ordre des barreaux) = NJW 2007, 2387.
1710 EGMR, Urt. v. 6. 12. 2012, 12323/11 – Michaud/Frankreich = NJW 2013, 3423.
1711 Idem, Rn. 114, 123.

8. Zusammenfassung und Stellungnahme

In diesem Kapitel wurde die Entwicklung der Diskussion um das Geldwäscherecht chronologisch dargestellt. Es zeigte sich, dass die Vorschriften des Anti-Geldwäscherechts von Anfang an kritisch begleitet wurden und noch heute die Frage offen gestellt wird, ob sie mit den Grundrechten auf Privatsphäre und Datenschutz in Einklang zu bringen sind.

Der grundsätzliche Ansatz, Private zur Überwachung des Finanzverkehrs und Meldung bestimmter Vorgänge zu verpflichten, um Geldwäsche und Terrorismusfinanzierung zu bekämpfen, wurde zwar von der deutschen Literatur anfangs als illegitime Delegation einer staatlichen Aufgabe kritisiert[1712], ist heute aber weitgehend als eine klassische Compliance-Struktur anerkannt. Jedenfalls an der Legitimität der Meldepflichten können kaum noch Zweifel bestehen, nachdem die Rechtsprechung die Meldepflicht der Rechtsanwälte aufrechterhalten hat.[1713] Diese wurde früher als besonders problematisch bezeichnet.[1714] Man muss also davon ausgehen, dass sich der EuGH und der EGMR auch an den Meldepflichten der Banken und Finanzdienstleister nicht prinzipiell stören.

Schon in den 1990ern wurde aber erkannt, dass die Geldwäschebekämpfung nach Vorstellung des Gesetzgebers und der mit ihr betrauten staatlichen Institutionen letztlich auf eine verfassungsfeindliche Massenüberwachung insb. der Bankkunden herausläuft, da sie nur durch ein umfassendes Monitoring sämtlicher Kundentransaktionen auskommen könne. Hiergegen wurden erhebliche datenschutz- und verfassungsrechtliche Bedenken geäußert. [1715] Diese Kritik wurde im Laufe der 2000er Jahre weiter aufgegriffen – insbesondere, nachdem das Kontenmonitoring auch gesetzlich festgelegt wurde.[1716] Diese Diskussion drang auch zu den Datenschutzbe-

1712 *Löwe-Krahl*, wistra 1994, 121 (125 f.); Oswald Eur. J. of Crime, Criminal Law & Justice 5 (1997), 196 (198).

1713 EuGH Urt. v. 26. 6. 2007, C-305/05 (Ordre des barreaux) = NJW 2007, 2387; EGMR, Urt. v. 6. 12. 2012, 12323/11 – Michaud/Frankreich = NJW 2013, 3423.

1714 Vgl. *Wegner*, NJW 2002, 794 (795 f.) *Wägenbaur*, EuZW 2002, 293 (296); *Hellwig* AnwBl 2002, 144 (146); *Zuck*, NJW 2002, 1397; *Shaugnessy*, Law & Policy in Int. Business 34 (2002), 25 (29 f., 36 f.).

1715 *Dahm*, WM 1996, 1285 (1289 f.); *Herzog*, WM 1996, 1753 (1757 ff.); *ders.*, WM 1999, 1905 (1910 ff.); *V. Lang/A. Schwarz/Kipp,* Geldwäsche, 3. Aufl. 1999, S. 610 ff.; dagegen *Findeisen*, wistra 1997, 121 (127).

1716 Etwa *Jahn*, ZRP 2002, 109 (110 f.) *Herzog/Christmann*, WM 2003, 6 (11 f.); *Herzog* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 47 (72 f.); *Degen,* Geldwäsche, 2009, S. 196 ff.; dagegen *Scherp*, WM 2003, 1254

auftragten vor.[1717] Zweifel wurden aber zunächst nur an der Verpflichtung zum Kontenmonitoring geäußert. Die Aufbewahrungspflichten für Informationen im Zusammenhang mit den Sorgfaltspflichten spielten in der rechtswissenschaftlichen Betrachtung kaum eine Rolle. Zwar hatte *Herzog* früh darauf aufmerksam gemacht, dass schon die Speicherung der Transaktionsdaten in die Rechte der Kunden eingriff. Prinzipielle Zweifel an der Rechtmäßigkeit der Aufbewahrungspflicht ließ er aber nicht erkennen.[1718]

Die europäischen und deutschen Gesetzgeber ließen sich von der Diskussion um das Kontenmonitoring nicht weiter beeindrucken und schrieben die Überwachungspflicht letztlich sogar ausdrücklich in Art. 8 Abs.1 lit. d) der 3. GWRL bzw. in § 3 Abs. 1 Nr. 4 GwG 2008 fest. Da die datenschutzrechtliche Bestimmtheitsproblematik aufgelöst schien, ebbte die deutsche Kritik am Transaktionsmonitoring in den folgenden Jahren ab.[1719]

Dass das Geldwäscherecht bestimmte Parallelen zur Vorratsdatenspeicherung von TK-Verkehrsdaten aufweist, blieb von der deutschen Rechtswissenschaft nicht völlig unbeachtet. Sie verpasste es jedoch, die problematischen Normen des GwG konkret zu identifizieren. So wurden zwar die Zusammenarbeitspflichten von Banken und FIUs und das Transaktionsüberwachungskonzept nebulös mit dem Prinzip der Vorratsdatenspeicherung in Verbindung gebracht.[1720] Eine explizite verfassungs- oder europarechtliche Prüfung der Aufbewahrungspflichten suchte man jedoch vergebens.

Auch vom Europäischen Datenschutzbeauftragten ist offenbar erkannt worden, dass das Anti-Geldwäscherecht an verschiedenen Stellen Parallelen zur Problematik der Vorratsdatenspeicherung aufweist. In den Stellung-

---

(1257 f.); *Findeisen* in Hadding/Hopt/Schimansky (Hrsg.), Bankrechtstag 2003, Basel II, 2004, S. 95.

1717 Krit. der *DSB Berlin,* Jahresbericht, 2000, S. 48 ff.; *ders.,* Jahresbericht, 2005, S. 50 ff.; weniger krit. *DSB Bund,* 19. Tätigkeitsbericht, 2001-2002, S. 67.

1718 *Herzog*, WM 1996, 1753 (1757); s.a. *Degen,* Geldwäsche, 2009, S. 200.

1719 Vgl. *Ackermann/Reder*, WM 2009, 158 (164); *Mülhausen* in Mülhausen/Herzog (Hrsg.), Hdb. Geldwäschebekämpfung, 2006, § 43 Rn. 53; *Achtelik* in Herzog GWG, 1. Aufl. 2010, KWG § 25c Rn. 25; krit noch *Kaetzler*, CCZ 2008, 174 (179 f.) und *Warius* in Herzog GWG, 1. Aufl. 2010, § 9 Rn. 63 aber nur In Bezug auf bestimmte Datenkategorien.

1720 *Heinson* in Specht/Mantz (Hrsg.), Hdb. Europ. & Deutsches Datenschutzrecht, 2019, § 14 Rn. 91; *Spoerr* in BeckOK Datenschutzrecht, Syst. J Rn. 226; *Krais*, CCZ 2015, 251 (252); *Albers* in Zubik/Podkowik/Rybski (Hrsg.), Data Retention, 2021, S. 117 (117, Fn 1) erwähnt ebenfalls die Existenz einer Vorratsdatenspeicherung von Finanzdaten und verweist auf *C. Kaiser,* Privacy in Financial Transactions, 2018.

nahmen zur EU-Geldwäschebekämpfung wird unmittelbar auf die Rechtsprechung aus *Digital Rights Ireland*[1721] Bezug genommen.[1722] Weder die Aufbewahrungspflichten noch das Transaktionsmonitoring wurden vom EDPS aber bislang als unverhältnismäßiger Eingriff in die Grundrechte eingestuft.[1723] Er hat allenfalls die Zugriffsrechte der FIUs kritisiert und angemahnt, dass der Ansatz der FIUs nicht mehr auf konkreten Ermittlungen beruhe, sondern letztlich ein „data mining" darstelle.[1724]

Deutlich offensivere Kritik äußerte die rechtswissenschaftliche Literatur auf europäischer Ebene. Wie auch der EDPS knüpfen einige Autoren an der Rechtsprechung zur Vorratsdatenspeicherung an, gehen aber weiter, indem sie grundlegende Pflichten, Maßnahmen und Rechte der GWRL auf ihre Vereinbarkeit mit Art. 7, 8 der EU-GRC überprüfen.[1725]

Die Beiträge differenzieren aber teilweise nicht sauber zwischen den einzelnen Maßnahmen und offenbaren ein kaum ausreichendes Verständnis des Sicherheitsverfassungsrechts, da sie zu sehr auf eine Rationalitätskontrolle mit absolutem Ausgang drängen, anstatt den Weg der Rechtsprechung einer Prozeduralisierung[1726] konsequent zu Ende zu gehen.

Durch das PNR-Urteil wurden die (unions-)grundrechtlichen Anforderungen an Maßnahmen der Massenüberwachung noch weiter differenziert. Eine umfangreiche Übertragung dieser Prinzipien auf das Anti-Geldwäscherecht hat bislang noch nicht stattgefunden.

1721 EuGH, Urteil v. 8.4.2014, C-293/12, C-594/12 (Digital Rights Ireland) = NJW 2014, 2169.

1722 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 10, S. 6 f.

1723 Vgl. *ders.,* Stellungnahme 4. GeldwäscheRL, 04. Juli 2013; *ders.,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017; *ders.,* Stellungnahme Aktionsplan Geldwäsche 05/2020; *ders.,* Opinion 12/2021 AML proposals, 22.09.2021.

1724 *EDPS,* Stellungnahme 01/2017, 5. GeldwäscheRL, 02.02.2017, Nr. 52, S. 14.

1725 *Böszörmenyi/Schweighofer*, Int. Rev. of Law, Computers & Technology 29 (2015), 63 (71 ff.); *Milaj/C. Kaiser*, Int. Data Privacy Law 7 (2017), 115; *C. Kaiser,* Privacy in Financial Transactions, 2018; *B. Vogel* in Vogel/Maillart (Hrsg.), Anti-Money Laundering Law, 2020, S. 881 (900 ff.); *Bertrand/Maxwell/Vamparys*, Int. Data Privacy Law 2021, 276.

1726 Vgl. *Tzanou/Karyda*, European Public Law 28 (2022), 123 (153 f.).