



Ausarbeitung

Zu möglichen erweiterten Befugnissen der Nachrichtendienste bei der Überwachung von „Finanzströmen“

Zu möglichen erweiterten Befugnissen der Nachrichtendienste bei der Überwachung von „Finanzströmen“

Aktenzeichen: WD 3 - 3000 - 040/19
Abschluss der Arbeit: 7. März 2019
Fachbereich: WD 3: Verfassung und Verwaltung

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

1.	Fragestellung	4
2.	Begriff „Finanzströme“	4
2.1.	Formeller, regulierter Finanzsektor	5
2.2.	Informeller, unregulierter Finanzsektor	5
3.	Derzeitige Befugnisse der Nachrichtendienste	5
3.1.	Finanzströme im formellen Finanzsektor	5
3.1.1.	Kreditinstitute: Kontobewegungen	5
3.1.2.	Bundeszentralamt für Steuern: Kontostammdaten	7
3.1.3.	Finanzbehörden: Gemeinnützigkeit	8
3.1.4.	Finanzbehörden: Sonstige Tatsachen	8
3.1.5.	Zentralstelle für Finanztransaktionsuntersuchungen	9
3.1.5.1.	Grundsatz	9
3.1.5.2.	Verdachtsgrad	10
3.1.5.3.	Relevanz für den BND	10
3.1.5.4.	Übermittlung auf Ersuchen	11
3.1.5.5.	Automatisierter Abruf	11
3.1.5.6.	Indirekter Zugriff auf Polizeidaten	11
3.1.5.7.	Verwertung von Ergebnissen privater Aufklärung	12
3.1.6.	Andere Behörden: Sonstige Tatsachen	13
3.2.	Finanzströme außerhalb des formellen Finanzsektors	14
3.2.1.	Nachrichtendienstliche Mittel	14
3.2.2.	Zentralstelle für Finanztransaktionsuntersuchungen	14
3.2.3.	Zollfahndungsdienst: sonstige Tatsachen	14
3.2.4.	Finanzbehörden: sonstige Tatsachen	15
3.2.5.	Daten anderer öffentlicher Stellen	15
3.3.	BND: Auslandsüberwachung	15
4.	Mögliche erweiterte Befugnisse	16
4.1.	Auskunft über Kontostammdaten (BaFin)	16
4.2.	Direkter Zugriff auf nicht-polizeiliche Dateien	17
4.2.1.	Beispiele bestehenden Direktzugriffs	17
4.2.2.	Beispiele nicht bestehenden Direktzugriffs	18
4.2.3.	Verfassungsrechtliche Zulässigkeit	19
4.2.3.1.	Grundsatz	19
4.2.3.2.	Zentralstelle für Finanztransaktionsuntersuchungen	21
4.3.	Direkter Zugriff auf polizeiliche Dateien	22
4.3.1.	Polizeiliches Informationssystem	22
4.3.2.	Zusätzlicher verfassungsrechtlicher Aspekt: Trennungsprinzip	22
4.4.	Übermittlung von Amts wegen	24
4.5.	Rasterfahndung	25
4.5.1.	Verfassungsrechtliche Grenzen	25
4.5.2.	Widerspruch zur Fluggastdatenkontrolle?	27
4.6.	Überwachen von Datenströmen mit Suchkriterien	28
4.6.1.	Verfassungsrechtliche Grenzen	28
4.6.2.	Widerspruch zu § 25h KWG?	29
4.7.	Steuerbehörden: anlasslose Zugriffsrechte	30
4.7.1.	Wesentliche Zugriffsrechte	30
4.7.2.	Rechtfertigung	32

1. Fragestellung

Es stellt sich die Frage, welche Kompetenzen deutsche Nachrichtendienste haben, um Finanzströme zu überwachen. Ferner stellt sich die Frage, welche Kompetenzen anderen Behörden zur Verfügung stehen, die deutschen Nachrichtendiensten nicht zustehen. Dabei geht es insbesondere um die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die Steuerbehörden und den Zoll. In diesem Zusammenhang ist von Interesse, ob grundsätzliche verfassungsrechtliche Bedenken dagegensprechen, den deutschen Nachrichtendiensten weitere Befugnisse einzuräumen, die anderen Behörden bereits zustehen.

Die Ausarbeitung konzentriert sich auf die drei Nachrichtendienste des Bundes:

- den Bundesnachrichtendienst (BND) als Auslandsnachrichtendienst,
- das Bundesamt für Verfassungsschutz (BfV) als Inlandsnachrichtendienst,
- den Militärischen Abschirmdienst (MAD) als militärischen Nachrichtendienst.

Die 16 Verfassungsschutzbehörden der Länder sind nicht Gegenstand dieser Ausarbeitung.

2. Begriff „Finanzströme“

Der Begriff „Finanzströme“ findet vielfach Verwendung. Seine genaue Bedeutung ist jedoch nicht definiert. Weder der „Brockhaus“ noch der „Duden“ enthalten hierzu einen Eintrag. Einige öffentliche deutsche Stellen befassen sich mit der Bekämpfung „illegaler Finanzströme“. Sie definieren den Begriff aber nicht,¹ sondern allenfalls das Attribut „illegal“.²

Die bei der OECD angesiedelte „Financial Action Task Force“ (FATF, „Arbeitsgruppe für finanzielle Maßnahmen (gegen Geldwäsche)“) hat Richtlinien und Untersuchungen zur Aufspürung verdächtiger finanzieller Transaktionen veröffentlicht.³ Aus diesen lässt sich ableiten, wie sich „Finanzstrom“ umfassend verstehen ließe. Die verschiedenen Erscheinungsformen könnte man hiernach in zwei Hauptkategorien einteilen:

-
- 1 BMZ, Pressemitteilung vom 23.3.2018, Illegale Finanzströme verhindern – Eigeneinnahmen für afrikanische Länder stärken, http://www.bmz.de/de/presse/aktuelleMeldungen/2018/maerz/180321_Illegale-Finanzstroeme-verhindern-Eigeneinnahmen-fuer-afrikanische-Laender-staerken/index.jsp: „illegale Finanzströme wie Korruption, Steuerhinterziehung oder Steuerflucht“ – hierbei handelt es sich nicht um eine Definition, da nur der Grund des Finanzstroms genannt wird, nicht aber, was einen Finanzstrom ausmacht.
 - 2 GIZ, Projektbeschreibung „Illegale Finanzströme weltweit bekämpfen“, <https://www.giz.de/de/weltweit/39748.html>: „Das internationale Engagement für nachhaltige Entwicklung wird zunehmend durch illegale Finanzströme (Illicit Financial Flows, IFF) untergraben. Als illegal bezeichnet man Finanzströme, deren Herkunft, Zweck oder Transfer unrechtmäßig sind. Dies umfasst Erträge aus organisierter Kriminalität, Steuerhinterziehung, Betrug im internationalen Handel, Geldwäsche und Korruption.“
 - 3 <http://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf>.

2.1. Formeller, regulierter Finanzsektor

Hierzu gehören insbesondere die folgenden Finanztransaktionen: Banküberweisungen; Geldtransfers über Zahlungsdienste (nach Zahlungsdiensteaufsichtsgesetz, z. B. „PayPal“, „Western Union“, Mobilfunkzahlungsdienste, etc.); Übertragung regulierter Finanzprodukte (von Kredit- und Finanzdienstleistungsinstituten nach Kreditwesengesetz – KWG, etc.) wie z. B. von Sparverträgen, Versicherungsleistungen; Übertragung von Finanzinstrumenten im Sinne des Wertpapierhandelsgesetzes, z. B. von Fondsanteilen.

2.2. Informeller, unregulierter Finanzsektor

Hierzu gehört die Übertragung von virtuellen Währungen (insoweit noch nicht reguliert),⁴ Wertkarten, Gutscheinen, Edelmetallen oder Edelsteinen.

Ferner gehören hierzu alternative Banksysteme wie z. B. das Verrechnungssystem „Hawala“.⁵ Dieses funktioniert zum Beispiel wie folgt: Person A übergibt an Hawaladar M in Moskau 10.000 Dollar Bargeld. Dieser steht in Beziehung zu Hawaladar L in London, der an Person B dort den Gegenwert bar auszahlt.⁶ Erforderlich ist, dass Person A ihrem Hawaladar M vertraut. Ein zwischen A und B vereinbartes Geheimwort dient zur Authentifizierung von B gegenüber dem Hawaladar L. Über die Zeit gleichen sich Zahlungsbewegungen in beide Richtungen aus („System der zwei Töpfe“).⁷ In Deutschland sind Transaktionen über das Hawala-System genehmigungspflichtig und unterliegen der Kontrolle der BaFin.⁸

3. Derzeitige Befugnisse der Nachrichtendienste

3.1. Finanzströme im formellen Finanzsektor

3.1.1. Kreditinstitute: Kontobewegungen

Die drei deutschen Nachrichtendienste dürfen „im Einzelfall Auskunft einholen bei [...] **Kreditinstituten**, Finanzdienstleistungsinstituten und Finanzunternehmen zu Konten, Konteninhabern

4 Siehe hierzu: FATF (19. Oktober 2018), Regulation of virtual assets, <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html>.

5 Siehe hierzu: FATF (2013), The role of Hawala and other similar service providers in money laundering and terrorist financing, <http://www.fatf-gafi.org/media/fatf/documents/reports/Role-of-hawala-and-similar-in-ml-tf.pdf>.

6 Beispiel nach <https://de.wikipedia.org/wiki/Hawala>.

7 Vgl. BaFin, Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html.

8 Vgl. BaFin, Merkblatt - Hinweise zum Zahlungsdiensteaufsichtsgesetz, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html; zu den strafrechtlichen Risiken siehe: Die Welt (16.06.2017), Wie Kriminelle das muslimische Hawala-System nutzen, <https://www.welt.de/wirtschaft/article165597124/Wie-Kriminelle-das-muslimische-Hawala-System-nutzen.html>.

und sonstigen Berechtigten sowie weiteren am Zahlungsverkehr Beteiligten und zu Geldbewegungen und Geldanlagen, insbesondere über Kontostand und Zahlungsein- und -ausgänge [...]“.⁹

Der Wortlaut umfasst eher nicht die Herausgabe von **Foto-** und Videoaufzeichnungen bankeigener Überwachungssysteme. Darin läge ein (zusätzlicher) Eingriff in das Recht auf informationelle Selbstbestimmung und das Recht am eigenen Bild.¹⁰ Grundsätzlich kann eine Überwachung von Bankbewegungen durch Verfassungsschutzbehörden verfassungsrechtlich gerechtfertigt sein. Das Bundesverfassungsgericht (BVerfG) hat zu einer entsprechenden Bestimmung im Verfassungsschutzgesetz Nordrhein-Westfalen festgestellt:

„Die [...] Erhebung von Kontoinhalten und Kontobewegungen greift in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf **informationelle Selbstbestimmung** ein.

Derartige Kontoinformationen können für den Persönlichkeitsschutz des Betroffenen bedeutsam sein und werden vom Grundrecht geschützt. Nach den gegenwärtigen Gepflogenheiten werden die meisten Zahlungsvorgänge, die über Bargeschäfte des täglichen Lebens hinausgehen, über Konten abgewickelt. Werden Informationen über die Inhalte der Konten einer bestimmten Person gezielt zusammengetragen, ermöglicht dies einen Einblick in die **Vermögensverhältnisse** und die **sozialen Kontakte** des Betroffenen, soweit diese - etwa durch Mitgliedsbeiträge oder Unterhaltsleistungen - eine finanzielle Dimension aufweisen. Manche Konteninhaltsdaten, etwa die Höhe von Zahlungen im Rahmen verbrauchsabhängiger Dauerschuldverhältnisse, können auch weitere Rückschlüsse auf das Verhalten des Betroffenen ermöglichen [...].

Die [...] vorgesehenen Grundrechtseingriffe sind jedoch zur Ermittlung im Hinblick auf [verfassungsfeindliche] Bestrebungen [...] **verfassungsrechtlich gerechtfertigt**. Insbesondere genügt die angegriffene Norm insoweit dem Verhältnismäßigkeitsgrundsatz. [...] Die [...] geregelten Maßnahmen dienen aufgrund der Erweiterung des Anwendungsbereichs der Norm auch zur Aufklärung der Finanzierungswege und der finanziellen Verhältnisse und Verflechtungen im Zusammenhang mit [verfassungsfeindlichen] Bestrebungen [...]. Dies ist ein legitimes Ziel des Verfassungsschutzes [...].“¹¹

9 § 8a Abs. 2 Nr. 2 Bundesverfassungsschutzgesetz (BVerfSchG), Hervorhebung durch Autor; die Vorschriften § 3 Abs. 1 Bundesnachrichtendienstgesetz (BNDG) und § 4a MAD-Gesetz (MADG) verweisen entsprechend auf diese.

10 Mallmann, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG § 8a Rn. 8; a.A. im Ergebnis Droste, Handbuch des Verfassungsschutzrechts, 2007, S. 236.

11 BVerfG, Urteil vom 27. Februar 2008, Az. 1 BvR 370/07 und 1 BvR 595/07, Rn. 314-318 (Hervorhebung durch Autor).

In der Entscheidungsdatenbank „juris“ ist zu § 8a und § 18 BVerfSchG nur eine **Gerichtentscheidung** dokumentiert, die Finanzströme betrifft.¹² Die Redaktion von „juris“ hat zu diesem Urteil folgende Orientierungssätze formuliert:

„1. Das BfV darf im Einzelfall Auskunft einholen bei Kreditinstituten, zu Konten, Konteninhabern und sonstigen Berechtigten und zu Geldbewegungen und Geldanlagen, soweit dies zur Aufklärung von Bestrebungen oder Tätigkeiten erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren vorliegen.

2. Bei der Tatbestandsvoraussetzung tatsächliche Anhaltspunkte für die bezeichneten schwerwiegenden Gefahren handelt es sich um einen unbestimmten Rechtsbegriff, der in vollem Umfang verwaltungsgerichtlicher Nachprüfung unterliegt.

3. Es genügt, dass die von Deutschland aus feststellbaren Hilfen der Hizb Allah als gewaltanwendender Organisation objektiv vorteilhaft sind und sich für diese positiv auswirken.“

3.1.2. Bundeszentralamt für Steuern: Kontostammdaten

Für **Kontostammdaten** besteht ein gesonderter Auskunftsanspruch:¹³

„Soweit dies zur Sammlung und Auswertung von Informationen erforderlich ist und Tatsachen die Annahme rechtfertigen, dass schwerwiegende Gefahren für die in § 3 Absatz 1 genannten Schutzgüter vorliegen, darf das Bundesamt für Verfassungsschutz im Einzelfall das Bundeszentralamt für Steuern ersuchen, bei den Kreditinstituten die in § 93b Absatz 1 der Abgabenordnung [AO] bezeichneten Daten abzurufen. § 93 Absatz 9 der Abgabenordnung findet keine Anwendung.“

Der Auskunftsanspruch wird nur über das Bundeszentralamt für Steuern abgewickelt, **nicht** über die **BaFin** (siehe hierzu unten Abschnitt 4.1). Das Bundeszentralamt für Steuern hat aber Zugriff auf dieselben Daten wie die BaFin.

Nach § 8a Abs. 3 BVerfSchG dürfen sich Auskunftersuchen „nur gegen Personen richten, bei denen

1. tatsächliche Anhaltspunkte dafür vorliegen, dass sie die schwerwiegenden Gefahren nach den Absätzen 2 oder 2a nachdrücklich fördern, oder

2. auf Grund bestimmter Tatsachen anzunehmen ist [...] dass sie die Leistung für eine Person nach Nummer 1 in Anspruch nehmen [...].“

12 VG Berlin, Urteil vom 7. September 2016, Az. 1 K 12.15, verfügbar unter: http://www.gerichtsentcheidungen.berlin-brandenburg.de/jportal/portal/t/279b/bs/10/page/sammlung.phtml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=JURE160016954&doc.part=L&doc.price=0.0#focuspoint.

13 § 8a Abs. 2a BVerfSchG.

Kontostammdaten umfassen im Wesentlichen die **Nummer** eines Kontos bzw. Depots, den Tag der Errichtung und Auflösung sowie Namen, Geburtsdatum und Anschrift des **Inhabers** bzw. Verfügungsberechtigten (vgl. § 93b Abs. 1 AO in Verbindung mit § 24c Abs. 1 KWG). Nicht erfasst sind Angaben über den Inhalt (Guthaben, Belastungen oder Umsätze).¹⁴ Das **BVerfG** hat die Verhältnismäßigkeit der Kontostammdatenabrufe im Wesentlichen gebilligt.¹⁵ Wegen nicht hinreichender Normenklarheit gerügte Bestimmungen hat der Gesetzgeber nach Auffassung der Kommentierung inzwischen in eine **verfassungskonforme Fassung** gebracht.¹⁶

§ 3 BNDG und § 4a MADG verweisen jeweils entsprechend auf § 8a BVerfSchG. Die Behörden können zudem unabhängig vom Abrufverfahren unmittelbar bei den Kreditinstituten Auskünfte einholen (siehe oben 3.1.1).

3.1.3. Finanzbehörden: Gemeinnützigkeit

Ferner können die Nachrichtendienste „die Finanzbehörden um Auskunft ersuchen, ob eine Körperschaft, Personenvereinigung oder Vermögensmasse die Voraussetzungen des § 5 Abs. 1 Nr. 9 des Körperschaftsteuergesetzes [**Gemeinnützigkeit**] erfüllt.“¹⁷ Der Kommentierung zufolge können diesbezügliche „Angaben und tatsächliche Erkenntnisse [...] Aufschluss über Vorliegen, Bedeutung und Umfang verfassungsfeindlicher Bestrebungen geben. Nicht zuletzt bedürfen die VS-Behörden [Verfassungsschutzbehörden] zur Erfüllung ihrer Hauptaufgabe, der Bewertung von Bestrebungen und Tätigkeiten unter dem Aspekt der Verfassungsfeindlichkeit, der Kenntnis **finanzieller Strukturen** der fraglichen organisatorischen Zusammenschlüsse und Verbindungen im Zusammenhang mit ihren steuerrechtlich relevanten organisationsbezogenen Angaben.“¹⁸

3.1.4. Finanzbehörden: Sonstige Tatsachen

Ferner sind die **Steuerbehörden** nach der Abgabenordnung (AO) **verpflichtet**, den Verfassungsschutzbehörden Tatsachen mitzuteilen, „die den Verdacht von Bestrebungen im Sinne des § 4 des Bundesverfassungsschutzgesetzes [BVerfSchG] oder des Zuwiderhandelns gegen den Gedanken der Völkerverständigung begründen [...]“¹⁹ Nach der Kommentierung ermöglichen diese „Durchbrechungen des Steuergeheimnisses [...] unter den angegebenen Bedingungen die Übermittlung steuerrechtlich relevanter Tatsachen und Daten sowohl des Steuerpflichtigen als auch mit ihm wirtschaftlich und finanziell in Kontakt stehender Personen (Informationen über familiäre, berufliche und wirtschaftliche Verhältnisse, Gesellschaftsverhältnisse und betriebsbezogene Informationen inklusive Betriebsgeheimnissen sowie zu Vermögensverwaltern, Verfügungsberechtigten und

14 Mallmann, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG § 8a Rn. 21.

15 BVerfGE 118, 168.

16 Mallmann, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG § 8a Rn. 21.

17 Hervorhebung durch Autor.

18 Bock, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG § 18 Rn. 42.

19 § 51 Abs. 3 S. 3 AO.

Beratern).²⁰ Die Auskunftspflicht der Finanzbehörden soll nicht „von einer eigenen Überprüfung“ durch die angefragte öffentliche Stelle abhängig sein, ob die Voraussetzungen des BVerfSchG gegeben sind.²¹

Im Übrigen können²² Steuerbehörden den Nachrichtendiensten Informationen übermitteln, wenn

„ein zwingendes öffentliches Interesse besteht; ein zwingendes öffentliches Interesse ist namentlich gegeben, wenn [...] die Offenbarung erforderlich ist zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit oder zur Verhütung oder Verfolgung von Verbrechen und vorsätzlichen schweren Vergehen gegen Leib und Leben oder gegen den Staat und seine Einrichtungen [...]“ (§ 30 Abs. 4 Nr. 5 lit. a AO).

3.1.5. Zentralstelle für Finanztransaktionsuntersuchungen

3.1.5.1. Grundsatz

Die Zentralstelle für Finanztransaktionsuntersuchungen „hat die Aufgabe der Erhebung und Analyse von Informationen im Zusammenhang mit **Geldwäsche** oder **Terrorismusfinanzierung** und der Weitergabe dieser Informationen an die zuständigen inländischen öffentlichen Stellen zum Zwecke der Aufklärung, Verhinderung oder Verfolgung solcher Taten“ (§ 28 Abs. 1 S. 1 Geldwäschegesetz – GwG).²³ § 32 Abs. 1 bis 3 GwG regelt die Datenübermittlung an die Nachrichtendienste:

„(1) Meldungen nach § 43 Absatz 1, § 44 [insbesondere von Finanzinstituten und Aufsichtsbehörden zu Geldwäsche und Terrorismusfinanzierung] sind von der Zentralstelle für Finanztransaktionsuntersuchungen unverzüglich an das **Bundesamt für Verfassungsschutz** zu übermitteln, soweit tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung dieser Informationen für die Erfüllung der Aufgaben des Bundesamtes für Verfassungsschutz erforderlich ist.

(2) Stellt die Zentralstelle für Finanztransaktionsuntersuchungen bei der operativen Analyse fest, dass ein Vermögensgegenstand mit Geldwäsche, mit Terrorismusfinanzierung oder mit einer sonstigen Straftat im Zusammenhang steht, übermittelt sie das Ergebnis ihrer Analyse sowie alle sachdienlichen Informationen unverzüglich an die zuständigen Strafverfolgungsbehörden. Die in Satz 1 genannten Informationen sind außerdem an den **Bundesnachrichtendienst** zu übermitteln, soweit tatsächliche Anhaltspunkte vorliegen, dass diese Übermittlung für die Erfüllung der Aufgaben des Bundesnachrichtendienstes erforderlich ist. Im Fall von Absatz 1 übermittelt die Zentralstelle für Finanztransaktionsuntersuchungen außerdem dem

20 Bock, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG § 18 Rn. 41.

21 Bock, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG § 18 Rn. 44.

22 Nach Ermessen, Bock, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, BVerfSchG § 18 Rn. 41.

23 Hervorhebung durch Autor.

Bundesamt für Verfassungsschutz zu der zuvor übermittelten Meldung auch das entsprechende Ergebnis ihrer operativen Analyse sowie alle sachdienlichen Informationen.

(3) Die Zentralstelle für Finanztransaktionsuntersuchungen übermittelt auf **Ersuchen** personenbezogene Daten an die Strafverfolgungsbehörden, das **Bundesamt für Verfassungsschutz**, den **Bundesnachrichtendienst** oder den **Militärischen Abschirmdienst** des Bundesministeriums der Verteidigung, soweit dies erforderlich ist für

1. die Aufklärung von Geldwäsche und Terrorismusfinanzierung oder die Durchführung von diesbezüglichen Strafverfahren oder
2. die Aufklärung sonstiger Gefahren und die Durchführung von anderen, nicht von Nummer 1 erfassten Strafverfahren.“²⁴

3.1.5.2. Verdachtsgrad

Der in Abs. 1 genannte „Verdachtsgrad liegt [...] noch unterhalb des strafprozessualen Anfangsverdachts nach § 152 Abs. 2 iVm § 160 StPO (BT-Drs. 18/11928, S. 40)“.²⁵ Die Kommentierung merkt hierzu an: „Die Konstruktion eines Verdachtsgrades unterhalb dieser zweifelsohne bereits **sehr niedrigen Schwelle** – unterhalb entfernter Indizien auf eine verfolgbare Straftat, aber oberhalb der bloßen Vermutung – ist dabei kaum mehr an Abstraktheit zu überbieten und nicht mehr trennscharf abzugrenzen.“²⁶

3.1.5.3. Relevanz für den BND

Die Kommentierung weist darauf hin, dass es „in der Praxis für die Zentralstelle für Finanztransaktionsuntersuchungen im Detail **nicht einfach zu beurteilen** sein dürfte“, ob die analysierten Finanztransaktionen „für die **Aufgabenerfüllung** des **Bundesnachrichtendienstes**, d.h. die Sammlung und Auswertung erforderlicher Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Abs. 2 S. 1 BNDG), erforderlich sind.“²⁷

24 Hervorhebung durch Autor.

25 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 32 Rn. 9.

26 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 32 Rn. 9 (Hervorhebung durch Autor).

27 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 32 Rn. 15 (Hervorhebung durch Autor).

3.1.5.4. Übermittlung auf Ersuchen

Kritik findet sich an der „Beschränkung in [Abs. 3] Satz 1 ‚auf Ersuchen‘. Damit ist eine **Übermittlung** von Informationen **von Amts wegen** zum Zwecke der Aufklärung von Gefahren oder der Gefahrenabwehr dem Wortlaut zufolge **ausgeschlossen**.“²⁸

3.1.5.5. Automatisierter Abruf

Nach § 32 Abs. 4 S. 1 GwG „sind die Strafverfolgungsbehörden und das **Bundesamt für Verfassungsschutz** berechtigt, die Daten zur Erfüllung ihrer Aufgaben **automatisiert** bei der Zentralstelle für Finanztransaktionsuntersuchungen **abzurufen**, soweit dem keine Übermittlungsbeschränkungen entgegenstehen.“²⁹

Alle Verdachtsmeldungen (auch solche, die die Zentralstelle zunächst noch nicht weitergegeben hat) speichert sie **zusammen mit** den bei **anderen Behörden** erhobenen Informationen.³⁰ Damit hat das Bundesamt für Verfassungsschutz nach § 32 Absatz 4 S. 1 GwG im automatisierten Verfahren Zugriff auf Daten anderer Behörden, die es sonst erst „umständlich“ selbst erheben müsste. Hierzu gehören nach § 30 GwG bestimmte Daten der Finanzbehörden und der Zollverwaltung, sowie „sonstige Informationen aus öffentlichen und nicht öffentlichen Quellen“ im Aufgabenbereich der Zentralstelle.

3.1.5.6. Indirekter Zugriff auf Polizeidaten

Zu den von der Zentralstelle erhobenen Daten gehören nach § 31 Abs. 4 GwG auch solche des polizeilichen Informationssystems INPOL:

„INPOL ist eine **polizeiliche Datenbank**, die als Verbundanwendung für Bundes- und Länderpolizeien kriminalpolizeiliche Daten bereithält. Ein Bestandteil von INPOL ist der sogenannte Kriminalaktennachweis (KAN), der Angaben zu erkennungsdienstlichen Behandlungen, Haftdaten, Strafanzeigen und Beschreibungen auffällig gewordener Personen enthält. Die KAN-Auskunft ermöglicht damit dem Anwender eine erste polizeiliche Beurteilung des Betroffenen und enthält bspw. Hinweise zur Eigensicherung (vgl. auch Bay. Landtag, Drs. 17/9755, S. 2). Informationen zum der Speicherung zugrunde liegenden Sachverhalt beispielsweise in Form einer Sachverhaltsschilderung sind dem KAN-Datenbestand nicht zu entnehmen. Ferner gehören zu INPOL die sog. INPOL-Fall-Anwendungen. Dies sind Fallbearbeitungs- und Analysesysteme, die der Erfassung, Aufbereitung und Darstellung komplexer, verbundrelevanter Sachverhalte dienen [...].“³¹

28 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 32 Rn. 20 (Hervorhebung durch Autor); ausführlich hierzu unten unter 4.4.

29 Hervorhebung durch Autor.

30 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 32 Rn. 26 (Hervorhebung durch Autor); BT-Drs. 18/11928, S. 40.

31 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 31 Rn. 14 (Hervorhebung durch Autor).

Die Zentralstelle erhält diese Daten nach § 31 Abs. 4 GwG durch einen „**Abgleich**“ mit dem INPOL. Abgleich ist „ein Vergleich der [der Zentralstelle gemeldeten] Daten [...] mit bei anderen Stellen gespeicherten Daten, um **weitere Hinweise** auf Geldwäschehandlungen, Terrorismusfinanzierung oder sonstige Straftaten zu erhalten und Zusammenhänge zu anderen Vorgängen herstellen zu können.“³²

Es fällt auf, dass das **Bundesamt für Verfassungsschutz** über den **automatisierten Zugriff** auf Daten der Zentralstelle auch automatisierten Zugriff auf Daten aus **polizeilichen Datenbanken** erhalten könnte. Dies dürfte eine Ausnahme vom Gebot der Trennung von Nachrichtendiensten und Polizei darstellen (zum **Trennungsprinzip** siehe unten 4.3.2).

3.1.5.7. Verwertung von Ergebnissen privater Aufklärung

Hinzuweisen ist noch auf den Umstand, dass die Zentralstelle Daten verwertet, die **Kreditinstitute** in einem Verfahren erhoben haben, die der „Rasterfahndung“ durch das BKA (siehe 4.5) oder der „Überwachung von Datenströmen mit Suchkriterien“ durch den BND (siehe 3.3) ähneln.³³ Das KWG enthält hierzu in § 25h die folgende Rechtsgrundlage:

„Kreditinstitute haben unbeschadet des § 10 Absatz 1 Nummer 5 des Geldwäschegesetzes Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels derer sie in der Lage sind, Geschäftsbeziehungen und einzelne **Transaktionen** im Zahlungsverkehr zu **erkennen**, die auf Grund des öffentlich und im Kreditinstitut verfügbaren Erfahrungswissens über die Methoden der Geldwäsche, der Terrorismusfinanzierung und über die sonstigen strafbaren Handlungen im Sinne von Absatz 1 im Verhältnis zu vergleichbaren Fällen besonders **komplex** oder groß sind, **ungewöhnlich** ablaufen oder **ohne** offensichtlichen wirtschaftlichen oder **rechtmäßigen Zweck** erfolgen. Die Kreditinstitute dürfen personenbezogene Daten verarbeiten, soweit dies zur Erfüllung dieser Pflicht erforderlich ist. Die Bundesanstalt [BaFin] kann Kriterien bestimmen, bei deren Vorliegen Kreditinstitute vom Einsatz von Systemen nach Satz 1 absehen können.“

Auf Grundlage dieser Vorschrift „können sowohl statische (z.B. **Alter**, Nationalität, **Anschrift**, Branche) und dynamische (z.B. Definition eines **Gruppenverhaltens** mit Untersuchung von Abweichungen) Parameter Verwendung finden“.³⁴ Neben einer „**flächendeckenden Überwachung** sämtlicher Kundenkonten und Zahlungsvorgänge kann das System [auf Grundlage des § 25h KWG] auch für die konkrete, anlassbezogene Suche und **Rasterung** von Geschäftsbeziehungen und Transaktionen eingesetzt werden“.³⁵ Die EDV kann auf „politisch exponierte Personen oder Sanktionslisten“ abzielen und „Bundeslagebilder Wirtschaftskriminalität und Korruption des BKA,

32 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 29 Rn. 21 (Hervorhebung durch Autor).

33 Gundelach, NJOZ 2018, 1841 (1846): § 25 Abs. 2 KWG ist „ein dem Mitarbeiterscreening vergleichbares Instrument“, das im „Vergleich zur Rasterfahndung [...] pauschal gegenüber jedem Mitarbeiter statt[findet], ohne dass es eines konkreten Hinweises auf terroristische Aktivitäten des Mitarbeiters bedarf“.

34 Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 25h KWG Rn. 17 (Hervorhebung durch Autor).

35 Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 25h KWG Rn. 17 (Hervorhebung durch Autor).

Jahresberichte, Newsletter und Anhaltspunktepapiere der FIU [...] Lagebilder zur Finanzkriminalität und Geldwäsche der Landeskriminalämter oder Typologiepapiere der FATF und der BaFin“ automatisch auswerten.³⁶ Ferner kann das System ein „**Internet-Screening**“ zur Beschaffung weiterer Informationen einbeziehen.³⁷ Dabei steigt der Kommentierung zufolge in der Praxis „die Bedeutung **selbst lernender Systeme**, die etwa auch in der Lage sind, bestehende Regeln zur Identifizierung von Auffälligkeiten selbst zu modifizieren und manuelle Tätigkeiten zu reduzieren“.³⁸ Einem Teil der Kommentierung erscheint „diese Regelung **verfassungsrechtlich**, insbesondere in Bezug auf die Schranken-Schranken der Verhältnismäßigkeit, durchaus **zweifelhaft**“.³⁹ Dabei wird auch die „**Masse** der faktisch vorzuhaltenden **Daten** und der Einbeziehung von Kunden, die keine ungewöhnlichen oder verdächtigen Transaktionen tätigen“ kritisch hervorgehoben.⁴⁰

3.1.6. Andere Behörden: Sonstige Tatsachen

Insoweit **anderen Behörden** über Finanztransaktionen im formellen Finanzsektor Daten vorliegen, können die Nachrichtendienste auf der Grundlage allgemeiner Rechtsgrundlagen um Übermittlung dieser Daten ersuchen:

„Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie andere Behörden um Übermittlung der zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten ersuchen, wenn sie nicht aus allgemein zugänglichen Quellen oder nur mit übermäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können.“⁴¹

Umgekehrt **unterrichten** die „Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts [...] **von sich** aus das **Bundesamt für Verfassungsschutz** oder die Verfassungsschutzbehörde des Landes“ bei bestimmten Anlässen (§ 18 Abs. 1 S. 1 BVerfSchG). § 18 Abs. 1a und 1b BVerfSchG definiert ferner Unterrichtungspflichten für das Bundesamt für Migration und Flüchtlinge und für „Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen“.

Es existiert ferner eine Vielzahl von Bestimmungen, die **allgemein** für eine **Datenübermittlung** an die Nachrichtendienste in Betracht kommen (z. B. § 32 Bundespolizeigesetz; § 25 Abs. 2 Bundeskriminalamtgesetz).

36 Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 25h KWG Rn. 17 (Hervorhebung durch Autor).

37 Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 25h KWG Rn. 16 (Hervorhebung durch Autor).

38 Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 25h KWG Rn. 17 (Hervorhebung durch Autor).

39 Gundelach, NJOZ 2018, 1841 (1846); nicht problematisiert bei Achtelik, in: Boos/Fischer/Schulte-Mattler, KWG, CRR-VO, 5. Auflage 2016, § 25h KWG, Rn. 16 ff.; Häberle, in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, Werkstand: 222. EL Dezember 2018, § 25h KWG, Rn. 1 ff.

40 Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 25h KWG Rn. 20 (Hervorhebung durch Autor).

41 § 18 Abs. 3 BVerfSchG; für andere Nachrichtendienste: § 23 Abs. 3 BNDG, § 10 Abs. 2 MADG.

Im Übrigen unterrichten sich die **Nachrichtendienste gegenseitig** (siehe insbesondere § 18 Abs. 2 BVerfSchG: BND an BfV; § 24 Abs. 3 BND-Gesetz: BND an MAD; § 20 Abs. 2 S. 2 BVerfSchG: BfV an BND; § 19 Abs. 1 S. 2 BVerfSchG: BfV an MAD; §§ 3, 11 MAD-Gesetz: MAD an BfV und BND).

3.2. Finanzströme außerhalb des formellen Finanzsektors

3.2.1. Nachrichtendienstliche Mittel

Die Überwachung von informellen Finanzströmen, wie die Übergabe von **Bargeld**, erfordert je nach Sachverhalt das gesamte nachrichtendienstliche Instrumentarium. Hierzu gehören: offene Beschaffung von Informationen, Einsatz von verdeckten Ermittlern oder Vertrauensleuten, Observation, Kontrolle des Brief-, Post- und Fernmeldeverkehrs, Abhören des nicht-öffentlich gesprochenen Wortes, Online-Durchsuchung, Ortung von Geräten und Personen und die Zusammenarbeit mit inländischen und ausländischen Behörden.⁴² Z. B. kann es unter Umständen erforderlich sein, alle vorgenannten Mittel anzuwenden, um ein internationales Verrechnungssystem, wie das Hawala-System, zu überwachen. Rechtsprechung zur Anwendung allgemeiner Überwachungsvorschriften auf Finanzströme ist in den Entscheidungsdatenbanken nicht vorhanden.⁴³

3.2.2. Zentralstelle für Finanztransaktionsuntersuchungen

Zu Verdachtsmeldungen sind nicht nur Kredit-, Finanzdienstleistungs- und Zahlungsinstitute verpflichtet („formeller, regulierter Finanzsektor“), sondern auch eine **Vielzahl** anderer **Gewerbe** und **Berufe**: E-Geld-Agenten, Versicherungsunternehmen, Versicherungsvermittler, Kapitalverwaltungsgesellschaften, Rechtsanwälte, Notare, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und Steuerbevollmächtigte, Dienstleister für Gesellschaften und für Treuhandvermögen oder Treuhänder, Immobilienmakler, Veranstalter und Vermittler von Glücksspielen, Güterhändler.⁴⁴ Für den Zugriff der Nachrichtendienste auf diese Verdachtsmeldungen und zu diesen erhobenen Daten der Zentralstelle für Finanztransaktionsuntersuchungen siehe oben Abschnitt 3.1.5.

3.2.3. Zollfahndungsdienst: sonstige Tatsachen

Das Zollfahndungsdienstgesetz sieht in § 23 d Abs. 4 und Abs. 5 die Übermittlung von Daten an die Nachrichtendienste vor:

„(4) Die vom Zollkriminalamt erlangten personenbezogenen Daten dürfen an die **Verfassungsschutzbehörden** des **Bundes** und der Länder sowie an den **Militärischen Abschirmdienst** übermittelt werden, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Sammlung und Auswertung von Informationen über Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die

42 Siehe insbesondere §§ 8-9b und 17-22c BVerfSchG. Für den BND und MAD gelten entsprechende Befugnisse (siehe insbesondere § 3 BNDG und § 4a MADG).

43 Abfrage mit den Suchkriterien „BVerfSchG“ und „Finanz“ oder „Bargeld“ unter Herausnahme von Entscheidungen zu § 8a Abs. 2 Nr. 2 und Abs. 2a und § 18 Abs. 3a.

44 Zu den Einzelheiten siehe § 2 Abs. 1 GwG; Figura, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 2 Rn. 1 ff.

in § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind, oder

2. bestimmte Tatsachen den Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht begründen.

(5) Die vom Zollkriminalamt erlangten personenbezogenen Daten dürfen an den **Bundesnachrichtendienst** übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass diese Daten für die Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Abs. 2 des Gesetzes über den Bundesnachrichtendienst zur Sammlung von Informationen über die in § 5 Abs. 1 Satz 3 Nr. 1 bis 3 des Artikel 10-Gesetzes genannten Gefahrenbereiche erforderlich sind.⁴⁵

Nach Auffassung der Kommentierung ist die Ermächtigung in **Abs. 4** „zu weit gefasst und **verletzt Art. 10 GG**. Insbesondere der in der Gesetzesbegründung angeführte Zweck, gerade terroristische Bestrebungen zu bekämpfen (BT-Drs. 15/3931, 18), schlägt sich im Übermittlungstatbestand nur unvollkommen nieder. Auch nicht-terroristische Gruppierungen können zur Gewalt neigen, zumal der Gewaltbegriff durchaus weit verstanden werden und weniger schwerwiegende Rechtsgutsgefährdungen umfassen kann (vgl. BVerfGE 133, 277 [341 ff.]). Zudem ermöglicht Abs. 4 Übermittlungen weit im Vorfeld konkreter Gefahren und gewährleistet daher nicht durchweg, dass sich aus den Daten wenigstens ein ‚konkreter Ermittlungsansatz‘ ergibt.“⁴⁶ **Abs. 5** hingegen ist nach der gleichen Auffassung bei enger „Auslegung [...] verfassungsrechtlich nicht zu beanstanden.“⁴⁷

3.2.4. Finanzbehörden: sonstige Tatsachen

Für Finanzströme außerhalb des regulierten Finanzsektors können Daten der Finanzbehörden von Belang sein, z. B. zu Eigentumsverhältnissen, Höhe des erklärten Einkommens oder Werbungskosten. Für den Zugriff der Nachrichtendienste auf diese Daten siehe oben Abschnitt 3.1.4.

3.2.5. Daten anderer öffentlicher Stellen

Für Finanzströme außerhalb des regulierten Finanzsektors können Daten anderer öffentlicher Stellen von Belang sein, wie z. B. der Sozial-, Wirtschafts- oder Zollverwaltung. Für den Zugriff der Nachrichtendienste auf diese Daten siehe oben Abschnitt 3.1.6.

3.3. BND: Auslandsüberwachung

Telekommunikation kann Daten zu Finanzströmen im formellen und informellen Finanzsektor übermitteln (z. B. eine Banküberweisung im Internet oder eine Mobilnachricht zu einer Bargeldtransaktion – entweder als unverschlüsselte Datenübertragung oder mit faktisch entschlüsselbarer

45 Hervorhebung durch Autor.

46 Bäcker, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 23d ZFdg Rn. 10 (Hervorhebung durch Autor).

47 Bäcker, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 23d ZFdg Rn. 10.

Verschlüsselung). Für den BND gelten hingegen bei „**rein ausländischen Telekommunikationsverkehren**“⁴⁸ gem. „Abschnitt 2. Ausland-Ausland-Fernmeldeaufklärung“ des BND-Gesetzes erheblich niedrigere Anforderungen.⁴⁹ Mit unterschiedlicher Begründung soll der Grundrechtsstandard bei rein ausländischen Telekommunikationsverkehren „abgesenkt“ sein oder **Grundrechte** nach dem Grundgesetz sollen **nicht gelten**. Dies ist umstritten, wobei „die wohl h. M. [herrschende Meinung] von einer extraterritorialen Grundrechtsgeltung bei Überwachungsmaßnahmen des BND im Ausland“ ausgeht.⁵⁰

4. Mögliche erweiterte Befugnisse

Die Kommentierung beurteilt die Komplexität der Regelungsgrundlagen zur Überwachung von Finanzströmen wie folgt:

„Die Ausweitung der Möglichkeiten für staatliche Informationszugriffe auf Finanzdaten ist mit seinen zahlreichen Regelungsorten im Polizeirecht, Strafverfahrensrecht, im Recht der Nachrichtendienste, im Steuer- und Wirtschaftsverwaltungsrecht und aufgrund einer **kafkaesken Verweisungstechnik** nur noch **schwer überschaubar**. Ob sich in diesem **Geflecht** aus Zuständigkeiten und Befugnissen Wege der Erlangung von Informationen über die finanzielle Privatsphäre von Bürgerinnen und Bürgern noch **rekonstruieren**, geschweige dann effektiv kontrollieren lassen werden, **erscheint fraglich**.“⁵¹

Die nachfolgende Darstellung versucht, innerhalb dieses komplexen Normengeflechts die wesentlichen Befugnisse zu identifizieren, die Nachrichtendiensten derzeit nicht zustehen. Ferner wird der wesentliche verfassungsrechtliche Handlungsspielraum des Gesetzgebers nach dem Grundgesetz umrissen. Aus Völker- und Europarecht sowie der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Europäischen Gerichtshofs können sich weitere Grenzen für den Handlungsspielraum des Gesetzgebers ergeben.⁵² Diese sind nicht Gegenstand dieser Ausarbeitung, finden aber beispielhaft am Rande Erwähnung.

4.1. Auskunft über Kontostammdaten (BaFin)

Das BfV hat bereits Zugriff auf Kontostammdaten über an das **Bundeszentralamt für Steuern** zu richtende Ersuchen. Ein Zugriff über die **BaFin** würde demgegenüber keinen für Außenstehende

48 Dietrich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 2 BNDG Rn. 1 ff.

49 Zu den Einzelheiten siehe Dietrich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 2 BNDG Rn. 1 ff.

50 Dietrich, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Auflage 2019, § 2 BNDG Rn. 1 ff. (Hervorhebung durch Autor); siehe auch Hölscheidt, Jura 2017, 148 (150 ff.).

51 Herzog/Achtelik, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, Einleitung Rn. 160 (Hervorhebung durch Autor); zustimmend Wonka, NJW 2017, 3334.

52 Siehe hierzu nur: Agentur der Europäischen Union für Grundrechte, Überwachung durch Nachrichtendienste: Grundrechtsschutz und Rechtsbehelfe in der Europäischen Union – Teil II (2018), <https://fra.europa.eu/de/publication/2018/uberwachung-durch-nachrichtendienste-grundrechtsschutz-und-rechtsbehelfe-der>; EGMR, National security and European case-law (2013), https://www.echr.coe.int/Documents/Research_report_national_security_ENG.pdf; EGMR, Mass surveillance (2019), https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.

erkennbaren Vorteil bringen. Denkbar wäre gleichwohl ein direkter und automatisierter Zugriff auf die vom BaFin geführte Datei der Kontostammdaten (siehe hierzu sogleich im nächsten Unterabschnitt 4.2).

4.2. Direkter Zugriff auf nicht-polizeiliche Dateien

4.2.1. Beispiele bestehenden Direktzugriffs

Ein direkter Zugriff ist den Nachrichtendiensten ausweislich der Gesetzeslage insbesondere auf folgende Dateien möglich:

- Grundbuchregister (Grundbuchämter), § 133 Abs. 2 Grundbuchordnung: „Die Einrichtung eines automatisierten Abrufverfahrens nach Absatz 1 bedarf der Genehmigung durch die Landesjustizverwaltung. Die Genehmigung darf nur Gerichten, **Behörden**, Notaren, öffentlich bestellten Vermessungsingenieuren, an dem Grundstück dinglich Berechtigten, einer von dinglich Berechtigten beauftragten Person oder Stelle, der Staatsbank Berlin sowie für Zwecke der maschinellen Bearbeitung von Auskunftsanträgen (Absatz 4), nicht jedoch anderen öffentlich-rechtlichen Kreditinstituten erteilt werden.“⁵³
- Gewerberegister (Kommunalverwaltungen), § 14 Abs. 9 Gewerbeordnung: „Darüber hinaus sind Übermittlungen der nach den Absätzen 1 bis 4 erhobenen Daten nur zulässig, soweit die Kenntnis der Daten zur Verfolgung von Straftaten erforderlich ist oder eine besondere Rechtsvorschrift dies vorsieht.“ Eine solche Rechtsvorschrift könnte § 18 BVerfSchG sein. Es besteht die Möglichkeit einer automatisierten Abfrage nach § 14 Abs. 11 Gewerbeordnung.
- Handelsregister (Justiz), § 9 Abs. 1 S. 1 Handelsgesetzbuch (HGB): „Die Einsichtnahme in das Handelsregister sowie in die zum Handelsregister eingereichten Dokumente ist **jedem** zu Informationszwecken gestattet.“⁵⁴
- Melderegister (Bestimmung durch Landesrecht), § 34 Abs. 1 Satz 1 und Abs. 4 Nr. 6-8 Bundesmeldegesetz⁵⁵: „Die Meldebehörde darf einer anderen öffentlichen Stelle [...] im Inland [...] Daten übermitteln, soweit dies zur Erfüllung der in ihrer Zuständigkeit oder in der Zuständigkeit des Empfängers liegenden öffentlichen Aufgaben erforderlich ist. [...] Die Prüfung bei der Meldebehörde, ob die Voraussetzungen [...] vorliegen, entfällt, wenn sie von den folgenden

53 Hervorhebung durch Autor. Siehe auch § 133 Abs. 5 S. 2 GBO: „Unabhängig hiervon ist dem Eigentümer des Grundstücks oder dem Inhaber eines grundstücksgleichen Rechts jederzeit Auskunft aus einem über die Abrufe zu führenden Protokoll zu geben, soweit nicht die Bekanntgabe den Erfolg strafrechtlicher Ermittlungen oder die Aufgabenwahrnehmung einer **Verfassungsschutzbehörde**, des **Bundesnachrichtendienstes** oder des **Militärischen Abschirmdienstes** gefährden würde [...]“

54 Hervorhebung durch Autor. § 156 Abs. 1 Genossenschaftsgesetz und § 5 Abs. 2 Partnerschaftsgesellschaftsgesetz verweisen für das Genossenschafts- bzw. Partnerschaftsregister u.a. auf § 9 HGB. § 79 Abs. 1 und Abs. 3 Satz 1 Bürgerliches Gesetzbuch enthalten eine ähnliche Regelung betreffend das Vereinsregister.

55 Die Datenübermittlung nach dieser Vorschrift kann gemäß § 38 Bundesmeldegesetz in einem automatisierten Abrufverfahren erfolgen.

Behörden um Übermittlung von Daten und Hinweisen [...] ersucht wird: [...] Verfassungsschutzbehörden des Bundes und der Länder, [...] Bundesnachrichtendienst, [...] Militärischer Abschirmdienst, [...].“

- Transparenzregister⁵⁶ (Bundesanzeiger-Verlag als Beliehener des Bundesministeriums der Finanzen), § 23 Abs. 1 Nr. 1 lit. f GwG: „[I]st die Einsichtnahme gestattet [...] den folgenden Behörden, soweit sie zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist: [...] den für Aufklärung, Verhütung und Beseitigung von Gefahren zuständigen Behörden“.
- Zentrales Fahrzeugregister (Kraftfahrtbundesamt), § 36 Abs. 2 lit. d Nr. 3 Straßenverkehrsgesetz: „Die Übermittlung nach § 35 Abs. 1 Nr. 1 bis 5 aus dem Zentralen Fahrzeugregister darf durch Abruf im automatisierten Verfahren erfolgen [...] zur Abwehr von Gefahren für die öffentliche Sicherheit [...] an die Verfassungsschutzbehörden, den Militärischen Abschirmdienst und den Bundesnachrichtendienst zur Erfüllung ihrer durch Gesetz übertragenen Aufgaben“.

Ferner hat das BfV direkten Zugriff auf die Datenbank der Zentralstelle für Finanztransaktionsuntersuchungen, § 32 Abs. 4 GwG:

„In den Fällen des Absatzes 3 Satz 1 Nummer 1 und 2 [1. die Aufklärung von Geldwäsche und Terrorismusfinanzierung oder die Durchführung von diesbezüglichen Strafverfahren oder 2. die Aufklärung sonstiger Gefahren und die Durchführung von anderen, nicht von Nummer 1 erfassten Strafverfahren] sind die Strafverfolgungsbehörden und das Bundesamt für Verfassungsschutz berechtigt, die Daten zur Erfüllung ihrer Aufgaben automatisiert bei der Zentralstelle für Finanztransaktionsuntersuchungen abzurufen, soweit dem keine Übermittlungsbeschränkungen entgegenstehen.“

4.2.2. Beispiele nicht bestehenden Direktzugriffs

Das BfV (wie auch BND und MAD) haben ausweislich der Gesetzeslage keinen automatisierten Zugriff insbesondere auf folgende nicht-polizeiliche Dateien, die direkt oder indirekt Aufschlüsse über Finanztransaktionen geben können:

- Kontostammdaten (BaFin), siehe oben 4.1.
- Luftfahrzeugrolle (Luftfahrtbundesamt), § 64 Abs. 7 Nr. 3 Luftverkehrsgesetz: „[...] Daten dürfen, soweit dies erforderlich ist zur Verfolgung von Straftaten oder zur Abwehr von Gefahren für die öffentliche Sicherheit, vom Luftfahrt-Bundesamt [...] an Behörden [...] im Inland übermittelt werden.“ Ein automatisiertes Abrufverfahren besteht hierfür wohl nicht.

Darüber hinaus bestehen eine Vielzahl interner Datenbanken oder Aktenbestände von Behörden mit Daten, die für die Finanz- und Vermögensverhältnisse relevant sein können, z. B. beim Zoll zu angemeldeten Ein- oder Ausfuhren, bei den für Sozialhilfe zuständigen Behörden, bei den

56 Das Transparenzregister dient nach der Legaldefinition in § 18 Abs. 1 GwG der Erfassung und Zugänglichmachung von Angaben über den wirtschaftlich Berechtigten an einer Gesellschaft oder anderen juristischen Person.

Nachlass- und Familiengerichten oder bei den Baubehörden. Soweit ersichtlich, haben die Nachrichtendienste auf diese internen Datenbanken keinen direkten Zugriff.

Ferner haben BND und MAD – anders als das BfV – keinen automatisierten Zugriff auf die Daten der Zentralstelle für Finanztransaktionsuntersuchungen (siehe oben 4.2.1).

4.2.3. Verfassungsrechtliche Zulässigkeit

Würde der Gesetzgeber den Direktzugriff auf die vorgenannten Fälle (4.2.2) ausweiten, sind für die grundsätzliche verfassungsrechtliche Zulässigkeit die folgenden Aspekte maßgeblich.

4.2.3.1. Grundsatz

Nach ständiger Rechtsprechung des BVerfG gibt es unter den Bedingungen der elektronischen Datenverarbeitung **kein** schlechthin **belangloses** personenbezogenes **Datum** mehr.⁵⁷ Maßgeblich für die Eröffnung des Schutzbereiches der informationellen Selbstbestimmung sei, ob je nach Ziel und Kontext der Datenerhebung sowie durch Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen bestehen können.⁵⁸ Das BVerfG hat den Schutz der Persönlichkeitsrechte insbesondere mit Blick auf die Besonderheiten und Risiken elektronischer Datenverarbeitung zudem auf Gefährdungslagen im Vorfeld konkreter Bedrohungen von Rechtsgütern ausgeweitet:

„Mittels elektronischer Datenverarbeitung sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person unbegrenzt speicherbar und jederzeit und ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Sie können darüber hinaus mit anderen Datensammlungen zusammengefügt werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen [...]. Dadurch können weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch anschließende Eingriffe in seine Verhaltensfreiheit nach sich ziehen können [...]. Eine weitere Besonderheit des Eingriffspotentials von Maßnahmen der elektronischen Datenverarbeitung liegt in der **Menge** der **verarbeitbaren Daten**, die auf konventionellem Wege gar nicht bewältigt werden könnte. Der mit solchen technischen Möglichkeiten einhergehenden **gesteigerten Gefährdungslage** entspricht der hierauf bezogene Grundrechtsschutz [...]“.⁵⁹

57 Vgl. BVerfGE 65, 1 (45); BVerfG, NJW 2007, 2464 (2466); NJW 2008, 1505 (1506 Rn. 66); BVerfG, Beschluss vom 18. Dezember 2018, Az. 1 BvR 142/15, Rn. 37.

58 Vgl. BVerfG NJW 2008, 1505 (1506 Rn. 66); BVerfG, Beschluss vom 18. Dezember 2018, Az. 1 BvR 142/15, Rn. 37.

59 Vgl. BVerfG NJW 2008, 1505 (1506 Rz. 63 f.) (Hervorhebung durch Autor); BVerfG, Beschluss vom 18. Dezember 2018, Az. 1 BvR 142/15, Rn. 37.

Vor diesem Hintergrund sei das Interesse des Einzelnen, dass seine Informationen nicht automatisiert mit der Möglichkeit der Weiterverwertung erfasst werden, auch dann geschützt, wenn diese öffentlich wahrnehmbar sind.⁶⁰

Im Vergleich zu einer nicht-automatisierten Abfrage greift die automatisierte Abfrage wohl etwas intensiver in das Grundrecht auf informationelle Selbstbestimmung ein: Die Missbrauchsgefahr ist bei elektronisch übermittelten und verarbeiteten Daten prinzipiell höher.⁶¹ Allerdings dürfte dieser Eingriff grundsätzlich mit ähnlicher Begründung **gerechtfertigt** sein, wie eine nicht-automatisierte Abfrage (d.h. über ein entsprechend gewichtiges Rechtsgut, wie z. B. die Gefahr eines terroristischen Anschlags). Gleichwohl ist bei der Ausweitung automatisierter Abfragen insgesamt die **Verhältnismäßigkeit** zu beachten. Der automatisierte Zugriff der Nachrichtendienste auf eine übermäßig große Zahl an elektronischen Datenbanken mit einer weiten Vielfalt an Daten könnte den Eindruck eines gegenüber Nachrichtendiensten „**gläsernen Bürgers**“ entstehen lassen. Das BVerfG hat hierzu im Volkszählungsurteil grundlegend ausgeführt:

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.“⁶²

Unter der Annahme, dass die aktuellen Zugriffsrechte verfassungsgemäß sind, dürfte ein Zugriff auf die weiteren unter 4.2.2 genannten Datenbanken (BaFin, Luftfahrtbundesamt, Zentralstelle für Finanztransaktionen) aber wohl keine offensichtlich übermäßige Ausweitung darstellen. Bei der verhältnismäßigen Ausgestaltung der Zugriffsrechte sind insbesondere von Belang, wie genau ein Gesetz den **Verwendungszweck** der Daten definiert,⁶³ welchem **Gemeinwohlbelang** der Datenzugriff dient,⁶⁴ sowie **Transparenz, Rechtsschutz** und **aufsichtliche Kontrolle** über die Datenverarbeitung.⁶⁵

60 Vgl. BVerfG NJW 2008, 1505 (1507 Rz. 64); BVerfG, Beschluss vom 18. Dezember 2018, Az. 1 BvR 142/15, Rn. 37.

61 BVerfG, Beschluss vom 18. Dezember 2018, Az. 1 BvR 142/15, Rn. 37: „Der mit solchen technischen Möglichkeiten einhergehenden gesteigerten Gefährdungslage entspricht der hierauf bezogene Grundrechtsschutz“.

62 BVerfGE 65, 1 (154); siehe auch BVerfG, Beschluss vom 18. Dezember 2018, Az. 1 BvR 142/15, Rn. 37: „Der mit solchen technischen Möglichkeiten einhergehenden gesteigerten Gefährdungslage entspricht der hierauf bezogene Grundrechtsschutz“; siehe auch EuGH, ECLI:EU:C:2016:970, Rn. 100: „Der Umstand, dass die Vorratsspeicherung der Daten vorgenommen wird, ohne dass die Nutzer der elektronischen Kommunikationsdienste darüber informiert werden, ist geeignet, bei den Betroffenen das Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung ist [...]“.

63 Vgl. BVerfG, Urteil vom 24. April 2013, Az. 1 BvR 1215/07, Rn. 140.

64 Vgl. BVerfG, Urteil vom 24. April 2013, Az. 1 BvR 1215/07, Rn. 114.

65 Vgl. BVerfG, Urteil vom 24. April 2013, Az. 1 BvR 1215/07, Rn. 205.

4.2.3.2. Zentralstelle für Finanztransaktionsuntersuchungen

Für einen etwaigen künftigen **automatisierten Zugriff** von **BND** und **MAD** auf die Daten der Zentralstelle für Finanztransaktionsuntersuchungen (zu den aktuellen Grenzen siehe oben 4.2.1) gelten zunächst die vorgenannten Ausführungen (4.2.3.1). Der **Aufgabenbereich** von BND und MAD unterscheidet sich von dem des BfV (siehe nur die weite Definition in § 1 Abs. 2 S. 1 BNDG: „Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus“; etwas enger § 1 MADG). Dies spricht zunächst für eine unterschiedliche Behandlung der Nachrichtendienste. Insoweit jedoch der automatisierte Zugriff von BND und MAD den Schutz gleich gewichtiger Rechtsgüter bezweckt, dürfte ein solcher Zugriff grundsätzlich zu rechtfertigen sein.

Im Hinblick auf die **Zentralstelle für Finanztransaktionsuntersuchungen** ergibt sich ferner die Frage, ob diese funktional eine **polizeiliche Aufgabe** wahrnimmt. In diesem Fall würden die zusätzlichen verfassungsrechtlichen Erwägungen Anwendung finden, die für den Zugriff auf polizeiliche Daten gelten (siehe unten 4.3.2). Für eine polizeiliche Aufgabe spricht die gesetzliche Bezeichnung („Zentrale Meldestelle zur Verhinderung, Aufdeckung und Unterstützung bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung“)⁶⁶ sowie die vormalige Eingliederung in das Bundeskriminalamt. Gleichwohl weist die Kommentierung darauf hin, dass die Zentralstelle seit ihrer Herauslösung⁶⁷ aus dem **Bundeskriminalamt** eine administrative Stelle sei:

„Mit der Umstrukturierung der vormals polizeilich ausgerichteten zentralen Meldestelle zu einer **administrativen** FIU [Financial Intelligence Unit] erhofft sich der Gesetzgeber insbesondere auch eine einfachere Zusammenarbeit im internationalen Kontext, da die Mehrzahl der FIUs weltweit gleichsam administrativ ausgerichtet sind [...].“⁶⁸

Denkbar wäre insoweit, die „präventiven Analysen“ der Zentralstelle als polizeilicher Arbeit **vorgelagerte** Filtertätigkeit anzusehen (ähnlich einer Art Finanz-Nachrichtendienst):

„Konnte im Rahmen der Analyse ein Zusammenhang mit Geldwäsche, Terrorismusfinanzierung oder einer anderen strafbaren Handlung von der Zentralstelle für Finanztransaktionsuntersuchungen nicht festgestellt werden, ist der Fall durch Abstandnahme von weiteren Maßnahmen abzuschließen. Die detaillierte Unterscheidung zwischen der Übermittlung an andere Behörden oder einer Abstandnahme hiervon ist letztlich der ‚**Filterprozess**‘, der den ‚zentralen Mehrwert‘ (u.a. BT-Drs. 18/11928, S. 39) der Zentralstelle für Finanztransaktionsuntersuchungen ausmachen soll [...].“⁶⁹

66 Siehe auch Art. 32 Abs. 1 Richtlinie (EU) 2015/849: „Jeder Mitgliedstaat richtet eine zentrale Meldestelle zur Verhinderung, Aufdeckung und wirksamen Bekämpfung der Geldwäsche und der Terrorismusfinanzierung ein.“

67 <https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Geldwaesche/FIU/fiu.html>.

68 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 27 Rn. 4 (Hervorhebung durch Autor).

69 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 32 Rn. 17 (Hervorhebung durch Autor).

Gleichwohl verbleiben gewisse Zweifel an der rein administrativen Aufgabe der Zentralstelle, da sich ihre Funktion seit der Herauslösung aus dem Bundeskriminalamt wohl nicht wesentlich geändert hat.

4.3. Direkter Zugriff auf polizeiliche Dateien

4.3.1. Polizeiliches Informationssystem

Nach § 31 Abs. 4 GwG ist die Zentralstelle für Finanztransaktionsuntersuchungen

„berechtigt, soweit dies zur Erfüllung ihrer Aufgaben nach § 28 Absatz 1 Satz 2 Nummer 2 erforderlich ist, die in ihrem Informationssystem gespeicherten, personenbezogenen Daten mit den im **polizeilichen Informationssystem** nach § 13 in Verbindung mit § 29 Absatz 1 und 2 des **Bundeskriminalamtgesetzes** [INPOL] enthaltenen, personenbezogenen Daten automatisiert abzugleichen. Wird im Zuge des Abgleichs nach Satz 1 eine Übereinstimmung übermittelter Daten mit im polizeilichen Informationssystem gespeicherten Daten festgestellt, so erhält die Zentralstelle für Finanztransaktionsuntersuchungen automatisiert die Information über das Vorliegen eines Treffers und ist berechtigt, die dazu im polizeilichen Informationssystem vorhandenen Daten automatisiert abzurufen.“⁷⁰

Auf die polizeilichen Vorgangsverwaltungssysteme der **Länderpolizeien** (INPOL-Land) hat die Zentralstelle für Finanztransaktionsuntersuchungen keinen Zugriff. Die Kommentierung führt hierzu aus:

„Seitens der in der Vergangenheit mit der Analyse von Verdachtsmeldungen befassten Ermittlungsdienststellen bei den Landeskriminalämtern (GFGen) wurden insbesondere die Vorgangsverwaltungssysteme als zur Bewertung der mitgeteilten Sachverhalte unerlässlich bezeichnet. U.a. auf diese polizeilichen Vorgangsverwaltungssysteme der Länderpolizeien hat die Zentralstelle für Finanztransaktionsuntersuchungen indessen keinen Zugriff. Es ist mithin **unrichtig**, dass die Zentralstelle für Finanztransaktionsuntersuchungen damit **Zugang** zu allen **wichtigen Dateien** habe, die sie zur Erfüllung ihrer Aufgaben benötigt (so die BReg, BT-Drs. 18/11928, S. 40 [...]).“⁷¹

4.3.2. Zusätzlicher verfassungsrechtlicher Aspekt: Trennungsprinzip

Für einen künftigen direkten Zugriff auf polizeiliche Dateien gelten zunächst die obigen grundsätzlichen Ausführungen (4.2.3.1). Hinzu tritt folgender Aspekt: Das BVerfG hat im Urteil zum Antiterrordateigesetz ein aus dem Grundrecht auf informationelle Selbstbestimmung folgendes **informationelles Trennungsprinzip** bejaht:⁷²

70 Hervorhebung durch Autor.

71 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 31 Rn. 15 (Hervorhebung durch Autor).

72 BVerfG NJW 2013, 1499.

„Die Rechtsordnung unterscheidet [...] zwischen einer **grundsätzlich offen** arbeitenden Polizei, die auf eine operative Aufgabenwahrnehmung hin ausgerichtet und durch detaillierte Rechtsgrundlagen angeleitet ist, und den **grundsätzlich verdeckt** arbeitenden Nachrichtendiensten, die auf die Beobachtung und Aufklärung im Vorfeld zur politischen Information und Beratung beschränkt sind und sich deswegen auf weniger ausdifferenzierte Rechtsgrundlagen stützen können. Eine Geheimpolizei ist nicht vorgesehen.

Regelungen, die den Austausch von Daten der Polizeibehörden und Nachrichtendiensten ermöglichen, unterliegen angesichts dieser Unterschiede gesteigerten verfassungsrechtlichen Anforderungen. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt insoweit ein **informationelles Trennungsprinzip**. Danach dürfen **Daten** zwischen den Nachrichtendiensten und Polizeibehörden **grundsätzlich nicht ausgetauscht** werden. Einschränkungen der Datentrennung sind nur **ausnahmsweise zulässig**. Soweit sie zur operativen Aufgabenwahrnehmung erfolgen, begründen sie einen **besonders schweren Eingriff**. Der Austausch von Daten zwischen den Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss deshalb grundsätzlich einem **herausragenden öffentlichen Interesse** dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt. Dies muss durch hinreichend konkrete und qualifizierte Eingriffsschwellen auf der Grundlage normenklarer gesetzlicher Regelungen gesichert sein; auch die Eingriffsschwellen für die Erlangung der Daten dürfen hierbei nicht unterlaufen werden.“⁷³

Dabei sei es zwar grundsätzlich, aber nicht absolut notwendig, dass Daten nur dann weitergeleitet werden, wenn die abfragende Stelle diese selbst erheben könnte.⁷⁴ Ein Teil der Kommentierung stimmt dem Urteil zu, da es die Antiterrordatei bei Anerkennung der Terrorismusbekämpfung nicht „bis zur Unkenntlichkeit“ beschneide und gleichzeitig „im demokratischen Rechtsstaat unverzichtbare Demarkationslinien“ nachzeichne, die eingehalten werden müssten.⁷⁵ Ein anderer Teil der Literatur kritisiert die Entscheidung als zu weitgehend in die Privatsphäre eingreifend: Es handle sich um einen „stillschweigenden Abschied vom Trennungsgebot“;⁷⁶ das Urteil korrigiere nur die schlimmsten Exzesse der Sicherheitsbehörden, nicht jedoch den Kern des Problems.⁷⁷

Das BVerfG hat unter folgenden Voraussetzungen im konkreten Fall bejaht, dass ein Austausch von Daten zwischen Nachrichtendiensten und Polizeibehörden zulässig ist:

„Erlaubt sind Zugriff und Nutzung der Daten nur zum Schutz besonders gewichtiger Rechtsgüter, das heißt zunächst zum Schutz von **Leib, Leben, Gesundheit** oder Freiheit von Personen. Ersichtlich sind im Kontext dieser Norm unter Gesundheitsbeeinträchtigungen nur schwerwiegende Gesundheitsverletzungen mit dauerhaften Folgen gemeint. Soweit die Vorschrift

73 BVerfG NJW 2013, 1499 (1505 Rn. 122-123); Hervorhebung durch Autor.

74 BVerfG NJW 2013, 1499 (1518 Rn. 226): Das „Kriterium der verfassungsrechtlichen Zulässigkeit einer hypothetischen Neuerhebung der Daten für die Beurteilung einer Weiterleitung bereits erhobener Daten [ist] nicht schematisch abschließend [...] und [schließt] die Berücksichtigung weiterer Gesichtspunkte nicht“ aus; siehe auch Nowroussian, NSTZ 2018, 254 (256).

75 Hörauf, NVwZ 2015, 181; zustimmend auch Löffelmann, GSZ 2018, 85.

76 Arzt, NVwZ 2013, 1328 (1332).

77 Kasiske, NJW-Spezial 2013, 312.

darüber hinaus auch den Schutz von Sachen mit erheblichem Wert vorsieht, stellt der Gesetzgeber klar, dass es nicht um den Schutz des Eigentums oder der Sachwerte als solcher geht, sondern um Sachen, deren Erhaltung im öffentlichen Interesse geboten ist' (§ 5 Abs. 2 Satz 1 ATDG [Antiterrordateigesetz]). Gemeint sind im Zusammenhang mit der Terrorismusabwehr etwa **wesentliche Infrastruktureinrichtungen** oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Auch enthält die Vorschrift hohe Eingriffsschwellen. Es bedarf für die Schutzgüter einer **gegenwärtigen Gefahr**, die sich nicht nur auf tatsächliche Anhaltspunkte stützt, sondern durch bestimmte **Tatsachen** unterlegt sein muss. Dabei sind Zugriff und Nutzung der Daten nur erlaubt, wenn dies **unerlässlich** ist und die Datenübermittlung aufgrund eines Ersuchens nicht rechtzeitig erfolgen kann. Der Zugriff auf die Daten ist überdies verfahrensrechtlich gesichert. Die weitere Verwendung der Daten steht weiterhin unter **Zustimmungsvorbehalt** der jeweils informationsführenden Behörden, über deren Erteilung – wie der Zusammenhang der Norm nahelegt – nach Maßgabe des jeweiligen Fachrechts zu entscheiden ist. Insgesamt sind damit die Anforderungen streng; entsprechend ist die Vorschrift in der bisherigen Praxis auch erst einmal zur Anwendung gekommen. Gegen eine solche Regelung sind verfassungsrechtlich keine Bedenken zu erheben. Sie genügt dem Übermaßverbot und hat auch vor dem informationellen Trennungsprinzip Bestand.⁷⁸

Unter diesen Voraussetzungen ließe sich ein Zugriff der Nachrichtendienste auf polizeiliche Dateien grundsätzlich rechtfertigen.

4.4. Übermittlung von Amts wegen

In § 32 Abs. 2 GwG ist eine Spontanmeldung an alle Nachrichtendienste – mit Ausnahme des **MAD** – vorgesehen (siehe oben 3.1.5). Möglicherweise hat der Gesetzgeber den MAD aufgrund mangelnder praktischer Relevanz ausgenommen. Dazu stünde aber im Widerspruch, dass § 32 Abs. 3 GwG (Ersuchen) den MAD mit aufführt. Verfassungsrechtlich dürfte sich eine Einbeziehung des MAD in § 32 Abs. 2 GwG mit den gleichen Erwägungen rechtfertigen lassen, wie die Einbeziehung des BfV und BND. Denkbar wäre daher, den MAD künftig in die Liste der Nachrichtendienste in § 32 Abs. 2 GwG mit aufzunehmen.

Ferner sollte nach Auffassung der Kommentierung § 32 Abs. 3 Satz 1 GwG dahingehend ausgeweitet werden, dass auch eine Übermittlung von Amts wegen (Spontanmeldung) erfasst wäre:

„Bemerkenswert ist die Beschränkung in Satz 1 ‚auf Ersuchen‘. Damit ist eine Übermittlung von Informationen von Amts wegen zum Zwecke der Aufklärung von Gefahren oder der Gefahrenabwehr dem Wortlaut zufolge ausgeschlossen. Gerade in Fällen, die für die Gefahrenabwehr Bedeutung haben, muss die Zentralstelle für Finanztransaktionsuntersuchungen von sich aus

78 BVerfG NJW 2013, 1499 (1515 Rn. 203); Hervorhebung durch Autor; siehe zum Europarecht auch das Urteil des EuGH, ECLI:EU:C:2016:970, Rn. 119: „Insoweit darf im Zusammenhang mit dem Zweck der Bekämpfung von Straftaten Zugang grundsätzlich nur zu den Daten von Personen gewährt werden, die im Verdacht stehen, eine schwere Straftat zu planen, zu begehen oder begangen zu haben oder auf irgendeine Weise in eine solche Straftat verwickelt zu sein [...]. Allerdings könnte in besonderen Situationen wie etwa solchen, in denen vitale Interessen der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit durch terroristische Aktivitäten bedroht sind, der Zugang zu Daten anderer Personen ebenfalls gewährt werden, wenn es objektive Anhaltspunkte dafür gibt, dass diese Daten in einem konkreten Fall einen wirksamen Beitrag zur Bekämpfung solcher Aktivitäten leisten könnten.“

(von Amts wegen) unverzüglich diese Informationen an die zuständige Polizeidienststelle weiterleiten dürfen. Es **befremdet** in dem Zusammenhang, dass nur in den in Satz 2 genannten Fällen eine Übermittlung von Amts wegen vorgesehen ist (bei Ergänzung des Satzes 1 um ‚von Amts wegen‘ entfielen womöglich die Differenzierungen zwischen Satz 1 und Satz 2). Die entsprechende Norm des Referentenentwurfs des Bundesministeriums der Finanzen (§ 28 Abs. 1 Nr. 6 GwG-RefE) sah noch die Möglichkeit vor, dass die Zentralstelle für Finanztransaktionsuntersuchungen **‚spontan und auf Ersuchen‘** personenbezogene Daten an inländische öffentliche Stellen für die Gefahrenabwehr übermitteln durfte. Ein **redaktionelles Versehen** im Zuge der völligen Neufassung der Normen in diesem Bereich (durch den Gesetzentwurf) ist insofern nicht ausgeschlossen.⁷⁹

Hierbei fällt auch ins Gewicht, dass die Zentralstelle für Finanztransaktionsuntersuchungen **‚von Amts wegen [...] zuständige inländische öffentliche Stellen [informiert], soweit dies erforderlich ist für 1. Besteuerungsverfahren, 2. Verfahren zum Schutz der sozialen Sicherungssysteme oder 3. die Aufgabenwahrnehmung der Aufsichtsbehörden‘** (§ 32 Abs. 3 S. 2 GwG). Damit gelten im Bereich der **Gefahrenabwehr geringere Übermittlungspflichten**, als im Bereich allgemeiner Verwaltung, wie z. B. „Sozialämter“ oder „Jobcenter“.

4.5. Rasterfahndung

4.5.1. Verfassungsrechtliche Grenzen

Die Rasterfahndung ist ein Verfahren der **Massendatenverarbeitung**, bei der automatisiert Informationen aus Fremddatenbeständen mit anderen Datenbeständen abgeglichen werden, um bestimmte Personen zu ermitteln.⁸⁰ Es werden nicht weitere Daten über eine bekannte Person zusammengeführt, sondern es sind im Regelfall die Daten sehr vieler Personen betroffen, um eine bislang **unbekannte Person zu identifizieren**:

„Die praktische Durchführung erfolgt in fünf Schritten. Zunächst wird eine Fahndungs- oder **Ermittlungshypothese** durch die Polizei erstellt. Diese legt bestimmte Merkmale (Rasterkriterien) – wie etwa Geschlecht, Staatsangehörigkeit, Religionszugehörigkeit, Studienfachrichtung – fest, die (mutmaßlich) auf eine gesuchte, bislang nicht identifizierbare Person (oder Personengruppe) zutreffen. Auf dieser Basis übersendet die Polizei entsprechende **Auskunftsersuchen** an die externen datenspeichernden öffentlichen oder nicht-öffentlichen Stellen (etwa an Universitäten, Einwohnermeldeämter oder Telekommunikationsgesellschaften). Diese Stellen **durchsuchen** selbst ihre **Datenbestände** nach den übermittelten Rasterkriterien. Erzielte ‚Treffer‘ werden ausgesondert und in einer Ergebnisdatei gespeichert. Diese Datei wird im Anschluss an die Polizei übermittelt. Die eigentliche Rasterfahndung erfolgt in einem fünften Schritt durch die Polizei selbst. Die übermittelten Dateien werden jeweils in ein spezielles **EDV-Programm** eingespeist, das die verschiedenen polizeifremden Datenbestände automatisiert unter- und miteinander **vergleicht**. Auf diese Weise wird eine **Schnittmenge** von Personen generiert, auf die die vorab gebildeten Rasterkriterien zutreffen (positive Rasterfahndung) oder

79 Barreto da Rosa, in: Herzog, Geldwäschegesetz, 3. Auflage 2018, § 32 Rn. 20 (Hervorhebung durch Autor); siehe schon oben unter 3.1.5.4.

80 Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Kapitel G, Rn. 1058.

gerade nicht zutreffen (negative Rasterfahndung). Die Schnittmenge umfasst in der Regel einen mehr oder weniger großen Kreis von Merkmalsträgern (nur Daten von diesen Personen werden von der Polizei näher untersucht). Aus ihr ist der eigentlich Gesuchte in der Regel durch herkömmliche Ermittlungsarbeit ‚herauszufiltern‘.“⁸¹

§ 48 Abs. 1 Bundeskriminalamtgesetz enthält folgende Rechtsgrundlage für Rasterfahndung:

„Das Bundeskriminalamt kann von öffentlichen oder nichtöffentlichen Stellen die Übermittlung von personenbezogenen Daten von bestimmten Personengruppen zum Zwecke des automatisierten Abgleichs mit anderen Datenbeständen verlangen, soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist, erforderlich ist; eine solche Gefahr liegt in der Regel auch dann vor, wenn konkrete Vorbereitungshandlungen die Annahme rechtfertigen, dass eine Straftat nach § 5 Absatz 1 Satz 2 begangen werden soll. Vom Bundesamt für Verfassungsschutz und von den Verfassungsschutzbehörden der Länder, dem Militärischen Abschirmdienst sowie dem Bundesnachrichtendienst kann die Übermittlung nach Satz 1 nicht verlangt werden.“

Auf Nachrichtendienste dürfte sich diese Befugnis – wenn überhaupt – nur unter **engen Voraussetzungen** übertragen lassen:

„Nach diesen Maßstäben darf eine Rasterfahndung nicht schon im **Vorfeld** einer **konkreten Gefahr** ermöglicht werden, denn sie würde zu vollständig verdachtslos und mit hoher Streubreite erfolgenden Grundrechtseingriffen führen, die Informationen mit intensivem Persönlichkeitsbezug erfassen können.“⁸²

Im Übrigen ist nach Auffassung des BVerfG die Rasterfahndung

„mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) nur vereinbar, wenn eine konkrete Gefahr für **hochrangige Rechtsgüter** wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist. Im Vorfeld der Gefahrenabwehr scheidet eine solche Rasterfahndung aus.

Eine allgemeine Bedrohungslage, wie sie im Hinblick auf terroristische Anschläge seit dem 11. September 2001 durchgehend bestanden hat, oder außenpolitische Spannungslagen reichen für die Anordnung der Rasterfahndung nicht aus. Vorausgesetzt ist vielmehr das Vorliegen weiterer Tatsachen, aus denen sich eine **konkrete Gefahr**, etwa für die Vorbereitung oder Durchführung **terroristischer Anschläge**, ergibt.“⁸³

81 Petri, in: Lisken/Denninger, Handbuch des Polizeirechts, 6. Aufl. 2018, Kapitel G, Rn. 1059 (Nachweise ausgeschlossen).

82 BVerfG, Beschluss vom 4. April 2006, Az. 1 BvR 518/02 (Rasterfahndung), Rn. 138 (Hervorhebung durch Autor).

83 BVerfG, Beschluss vom 4. April 2006, Az. 1 BvR 518/02 (Rasterfahndung), Leitsätze (Hervorhebung durch Autor).

Im Übrigen hat das BVerfG die relativ **geringe Bedeutung** der Rasterfahndung für die Praxis in dem seinem Beschluss zugrunde liegenden Fall unterstrichen:

„Nach Angaben des Bundeskriminalamtes übermittelten die Länder insgesamt 31.988 Datensätze. Diese wurden anschließend mit weiteren, durch das Bundeskriminalamt erhobenen Datenbeständen abgeglichen. [...] Nach Einschätzung des Bundesbeauftragten für den Datenschutz waren in diesen Abgleichsdateien zwischenzeitlich die Daten von 200.000 bis 300.000 Personen gespeichert. [...] Die Rasterfahndung führte, soweit ersichtlich, in keinem Fall dazu, dass ‚Schläfer‘ aufgedeckt worden wären oder gar aufgrund der gewonnenen Erkenntnisse eine Anklage – etwa wegen Mitgliedschaft in einer terroristischen Vereinigung oder wegen Unterstützung einer solchen (vgl. §§ 129a, 129b StGB) – gegen eine der davon erfassten Personen erhoben worden wäre.“⁸⁴

4.5.2. Widerspruch zur Fluggastdatenkontrolle?

Das Fluggastdatengesetz gibt dem BKA weitreichende Befugnisse, Daten bei Flügen aus Deutschland und nach Deutschland zu speichern. Die Kommentierung sieht hierin eine „Art **Rasterfahndung**“:⁸⁵

„Ziel und Mittel des FlugDaG ist die **anlass-** und **verdachtslose Erhebung** und Nutzung eines umfangreichen Katalogs personenbezogener Daten aller Flugreisenden bei Drittstaatenflügen wie auch EU-Flügen zum Zweck der präventiv-polizeilichen Verhütung von Straftaten einerseits und der Verfolgung von Straftaten sowie der Vorsorge für die Verfolgung solcher Straftaten auf der repressiv-polizeilichen Ebene andererseits. [...] Auch wenn jeder Fluggast bei jedem erfassten Flug erneut gespeichert und damit die Zahl der erfassten Personen unter der oben genannten Zahl liegen wird, fallen mit Blick auf die vorgesehene Speicherdauer nach § 13 FlugDaG in fünf Jahren rund **850 Mio. Fluggastdatensätze** an.“⁸⁶

Daher seien die „Grenzen [...] [rechtsstaatliche Mittel] hier überschritten“.⁸⁷ Es ließe sich als Widerspruch ansehen, dass eine Sicherheitsbehörde einerseits **anlasslos** Daten erheben darf, die ganz überwiegend Unbeteiligte betreffen und es ermöglichen, Bewegungsprofile zu erstellen, andererseits Sicherheitsbehörden eine Rasterfahndung nur bei Vorliegen einer konkreten, schweren Gefahr möglich sein soll. Angesichts der klaren, wiederholten Rechtsprechung des BVerfG zur Datenerhebung durch Sicherheitsbehörden⁸⁸ erscheint aber eher unwahrscheinlich, dass dieser

84 BVerfG, Beschluss vom 4. April 2006, Az. 1 BvR 518/02 (Rasterfahndung), Rn. 9-10.

85 Arzt, DÖV 2017, 1023 (Hervorhebung durch Autor).

86 Arzt, DÖV 2017, 1023 (Hervorhebung durch Autor).

87 Arzt, DÖV 2017, 1023 (Hervorhebung durch Autor).

88 Siehe die unter 4.2.3, 4.5.1 und 4.6.1 dargestellte Rechtsprechung.

Widerspruch zugunsten einer künftigen weiteren Kompetenz von Nachrichtendiensten zur Rasterfahndung aufgelöst würde.⁸⁹

4.6. Überwachen von Datenströmen mit Suchkriterien

4.6.1. Verfassungsrechtliche Grenzen

Es wäre denkbar, die Befugnisse des BND für Ausland-Ausland-Fernmeldeaufklärung auf inländische Aufklärung bzw. inländische Kommunikation anzuwenden, z. B. als neue Befugnis des BfV. Das BfV würde dann Kommunikationsströme daraufhin überwachen, ob bestimmte Suchworte auftauchen, wie z. B. das Identitätsmerkmal einer der Terrorismusfinanzierung verdächtigten Person. Eine solche Kompetenz wäre nach der Rechtsprechung des BVerfG grundsätzlich **verfassungswidrig**:

„So ist der Einsatz der Befugnisse des **Bundesnachrichtendienstes**, zur so genannten strategischen Kontrolle **verdachtslos** Fernmeldeverkehre zu überwachen und sie durch Abgleich mit Suchbegriffen auszuwerten, für Zwecke der personenbezogenen Risikoabwehr im Bereich der inneren Sicherheit **in jedem Falle** unverhältnismäßig und damit **verfassungswidrig** [...]“⁹⁰

Das BVerfG stellt daher an die Überwachung der Telekommunikation im Inland (siehe oben 3.2.1) hohe Anforderungen.⁹¹ Es müssten „im Einzelfall **belastbare tatsächliche Anhaltspunkte**“ für eine

89 Siehe die angekündigte Verfassungsbeschwerde gegen das Fluggastdatengesetz, Spiegel online vom 26.7.2017, Europäischer Gerichtshof kippt geplantes Abkommen mit Kanada; EuGH, Gutachten 1/15, Tenor Nr. 3 lit. d: „Das Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen muss, um mit Art. 7, Art. 8 und Art. 52 Abs. 1 der Charta der Grundrechte vereinbar zu sein, die Speicherung von Fluggastdatensätzen **nach der Ausreise** der Fluggäste auf die Daten von Fluggästen **beschränken**, für die **objektive Anhaltspunkte** dafür vorliegen, dass von ihnen eine **Gefahr** im Zusammenhang mit der Bekämpfung des Terrorismus und grenzübergreifender schwerer Kriminalität ausgehen könnte“ (Hervorhebung durch Autor); vgl. auch die Zweifel an der Geeignetheit des Gesetzes: Giemulla/Hoppe, GSZ 2018, 185: „Damit ist es theoretisch möglich, dass keiner der an Bord befindlichen Fluggäste mit seinem tatsächlichen Namen auf der Passagierliste verzeichnet ist.“

90 BVerfG, Beschluss vom 4. April 2006, Az. 1 BvR 518/02 (Rasterfahndung), Rn. 131 (Hervorhebung durch Autor). Siehe auch EuGH, ECLI:EU:C:2016:970, Rn. 105: „Zum anderen sieht eine nationale Regelung wie die im Ausgangsverfahren, die sich allgemein auf alle Teilnehmer und registrierten Nutzer erstreckt und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erfasst, keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel vor. Sie betrifft pauschal sämtliche Personen, die elektronische Kommunikationsdienste nutzen, ohne dass sich diese Personen auch nur mittelbar in einer Lage befinden, die Anlass zur Strafverfolgung geben könnte. Sie gilt also auch für Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit schweren Straftaten stehen könnte. Zudem sieht sie keine Ausnahme vor, so dass sie auch für Personen gilt, deren Kommunikationsvorgänge nach den nationalen Rechtsvorschriften dem Berufsgeheimnis unterliegen [...]“

91 BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a.; mit kritischer Anmerkung Wiemers, NVwZ 2016, 840 (841): „mutet befremdlich an“, „lebensfremd“; „erschließt sich nicht“; Durner, DVBl 2016, 780; Sachs, JuS 2016, 662 (663): „Wenig systematisch“, „überzogene Anforderungen“; Lindner/Unterreitmeier, DÖV 2017, 90: „Es ist an der Zeit für eine dogmatische Neuorientierung, die mit einer tiefgreifenden Analyse des Verhältnisses von Lebens- und Datenschutz einhergeht. Sonst droht das zunehmend von Karlsruhe aus regierte Deutschland zu einer ‚wehrlosen Republik‘ zu werden“; vgl. auch Gärditz, GSZ 2017, 1 (3): „atemberaubende[r] Detailreichtum bundesverfassungsgerichtlicher Angemessenheitskontrolle“; dem Urteil zustimmend z. B. Buchholtz, NVwZ 2016, 906; Übersicht zum Streitstand „Datenschutz versus Sicherheit“ generell: Beaucamp, DVBl 2017, 534.

Gefährdung „von hinreichend **gewichtigen Rechtsgütern**“ bestehen.⁹² Ferner bedürfe es „grundsätzlich einer **vorherigen Kontrolle** durch eine unabhängige Stelle“, deren Regelung der Gesetzgeber „in spezifischer und normenklarer Form mit strengen Anforderungen an Inhalt und Begründung der **gerichtlichen Anordnung** zu verbinden“ habe.⁹³ Dem „Schutz des **Kernbereichs** privater Lebensgestaltung“ müsse der Gesetzgeber sowohl „auf der Ebene der **Datenerhebung**“ durch geeignete Vorkehrungen als auch „auf der Ebene der nachgelagerten **Auswertung** und Verwertung“ durch strikte **Folgenminimierung** Rechnung tragen.⁹⁴ Des Weiteren habe er die „besondere Vertraulichkeit“ zu beachten, die von Verfassungs wegen „gegenüber bestimmten **Berufs-** und anderen **Persongruppen**“ vorausgesetzt wird.⁹⁵ Im Übrigen seien **Benachrichtigungspflichten, Auskunftsrechte, wirksame Sanktionen** bei Rechtsverletzungen, die vollständige **Protokollierung** von Datenerhebungen und **Berichtspflichten** gegenüber Parlament und Öffentlichkeit vorzusehen.⁹⁶ Schließlich bedürfe es einer gesetzlichen „Regelung von **Löschungspflichten**“.⁹⁷

4.6.2. Widerspruch zu § 25h KWG?

Kreditinstitute müssen die Kontobewegungen ihrer Kunden **systematisch** mit **automatisierten Systemen** überwachen (siehe oben 3.1.5.7). Insoweit eine Transaktion hinreichend verdächtig ist, melden Kreditinstitute diese der Zentralstelle (siehe oben 3.1.5.2). Auf diese Meldungen hat das BfV automatisierten Zugriff (siehe oben 3.1.5.5). Es ließe sich als Widerspruch ansehen, dass das BfV einerseits Zugriff auf derartige **anlasslos**, allein über **Suchkriterien** erhobene Daten hat, andererseits selbst aber Datenströme nicht auf Suchkriterien gestützt überwachen darf:⁹⁸

„Damit drängt sich die Frage auf, weshalb ein privatwirtschaftlich agierendes Unternehmen eine Maßnahme sollte vollziehen dürfen, die die Polizei in vergleichbarer Situation nicht ausführen darf, obwohl die Polizei die Maßnahme zur Abwehr einer Gefahr für die Gesellschaft durchführen würde.“

Angesichts der klaren, wiederholten Rechtsprechung des BVerfG zur Datenerhebung durch Sicherheitsbehörden⁹⁹ erscheint wahrscheinlich, dass dieser etwaige Widerspruch wohl nicht zugunsten der Sicherheitsbehörden aufgelöst würde. Ferner spricht für eine unterschiedliche Behandlung unter anderem der Umstand, dass zunächst nur **private Stellen** die Daten verarbeiten. In diesem Sinne hat das BVerfG bei der Vorratsdatenspeicherung zwischen der „Datenbevorratung“ bei

92 BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 104 (Hervorhebung durch Autor).

93 BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 117 ff. (Hervorhebung durch Autor).

94 BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 124 ff. (Hervorhebung durch Autor).

95 BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 131 ff. (Hervorhebung durch Autor).

96 BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 134 ff. (Hervorhebung durch Autor).

97 BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09 u.a., Rn. 144 (Hervorhebung durch Autor).

98 So Gundelach, NJOZ 2018, 1841 (1846) in Bezug auf Mitarbeiterscreening.

99 Siehe die oben unter 4.2.3, 4.5.1 und 4.6.1 dargestellte Rechtsprechung.

Telekommunikationsunternehmen und dem Abruf der Daten durch Sicherheitsbehörden einen wesentlichen Unterschied gesehen:

„Die Datenbevorratung ermöglicht zwar den Abruf, doch führt erst dieser zu konkreten Belastungen. Das Gewicht eines denkbaren Einschüchterungseffekts hängt dann davon ab, unter welchen Voraussetzungen die bevorrateten Daten abgerufen und verwertet werden können. Je weiter die Befugnisse staatlicher Stellen insoweit reichen, desto eher müssen die Bürgerinnen und Bürger befürchten, dass diese Stellen ihr Kommunikationsverhalten überwachen [...].“¹⁰⁰

Der Zentralstelle für Finanztransaktionen (siehe oben 3.1.5.1) und gegebenenfalls den Nachrichtendiensten (siehe oben 3.1.5.4) steht daher nur das sozusagen gefilterte **Ergebnis** dieser Überwachung zur Verfügung, nicht aber die Überwachung selbst.

4.7. Steuerbehörden: anlasslose Zugriffsrechte

4.7.1. Wesentliche Zugriffsrechte

Steuerbehörden haben ähnliche Zugriffsrechte auf Bank- und andere Finanzdaten von Bürgern. Diese Rechte hängen jedoch nicht von ähnlichen Eingriffsschwellen ab, wie bei Polizei und Nachrichtendiensten (z. B. konkrete Gefahr für Leib und Leben). Zum Teil ist für den Zugriff der Steuerbehörden nicht einmal ein Verdacht oder ähnlicher Anlass erforderlich.

Zum Beispiel haben Steuerbehörden die folgenden Rechte oder es bestehen ihnen gegenüber die folgenden Pflichten, ohne dass sie überhaupt den Verdacht einer Steuerhinterziehung geltend machen müssen:

- Offenlegung von Finanzdaten über die Abgabe von **Steuerklärungen**;¹⁰¹
- Offenlegung von Finanzdaten über die Vorlage der **Buchführung**,¹⁰² auch in **elektronischer Form**,¹⁰³
- **Automatisierter Abruf** von **Kontoinformationen**;¹⁰⁴

100 BVerfG, Beschluss vom 8. Juni 2016, 1 BvQ 42/15, Rn. 18.

101 §§ 149 ff. AO.

102 §§ 140 ff. AO.

103 §§ 146 ff. AO.

104 § 93b AO: Der Abruf ist zulässig, z. B. soweit „er erforderlich ist zur Erhebung von bundesgesetzlich geregelten Steuern oder Rückforderungsansprüchen bundesgesetzlich geregelter Steuererstattungen und Steuervergütungen“ (Abs. 7 Nr. 4).

-
- Vorlage von **Kontoauszügen** (z. B. bei einer durch **Zufallsauswahl**¹⁰⁵ möglichen Außenprüfung¹⁰⁶ oder in anderen Fällen);¹⁰⁷
 - Offenlegung von **Rechnungen, Verträgen, Kasseneinzeldaten** oder steuerlich relevanter **e-Post** im Rahmen einer Außenprüfung;¹⁰⁸
 - Anspruch auf **Sammelauskünfte** gegen jedermann, § 93 Abs. 1a S. 1 AO:

„Die Finanzbehörde darf an andere Personen als die Beteiligten Auskunftersuchen über eine ihr noch unbekannt Anzahl von Sachverhalten mit dem Grunde nach bestimmbar, ihr noch nicht bekannten Personen stellen (Sammelauskunftersuchen). Voraussetzung für ein Sammelauskunftersuchen ist, dass ein hinreichender Anlass für die Ermittlungen besteht und andere zumutbare Maßnahmen zur Sachverhaltsaufklärung keinen Erfolg versprechen.“

Die Finanzbehörde ist nicht verpflichtet, zuerst bei dem Beteiligten des Steuerverfahrens den Sachverhalt aufzuklären (§ 93 Abs. 1a S. 2 AO). Ein „Sammelauskunftersuchen [betrifft] eine noch unbekannt Anzahl von Sachverhalten mit noch nicht bekannten Personen, die aber dem Grunde nach bestimmbar sind, zB die Kunden der Auskunftsperson, die ein bestimmtes Auftragsvolumen überschritten haben.“¹⁰⁹ Insoweit lässt sich das Sammelauskunftersuchen als mit einer **Rasterfahndung** vergleichbar ansehen (siehe oben 4.5): Es werden durch den Abgleich von Datenbeständen noch unbekannt Personen ermittelt, die möglicherweise einen Regelverstoß begangen haben.

Im Übrigen ist noch darauf hinzuweisen, dass die Rechtsprechung bei Ermittlungen wegen Steuerhinterziehung verhältnismäßig weite Grenzen für Hausdurchsuchungen zieht. Die Kommentierung bezeichnet diese als **Ausforschungsdurchsuchungen**.¹¹⁰ So hat das BVerfG die Durchsuchung einer Großbank für verfassungsgemäß erachtet wegen des Verdachts der „systematischen Beihilfe zur

105 Intemann, in: Koenig AO, 3. Auflage 2014, § 156 Rn. 51: „Routine- und Anlassprüfung. Die FB ist berechtigt, den zu prüfenden Stpfl. sowohl unter reinen Zufallsgesichtspunkten auszuwählen als auch eine Prüfung aufgrund eines konkreten Anlasses durchzuführen. In beiden Fällen bedarf die Prüfungsanordnung keiner weiteren Begründung (BFH X R 89/89, BStBl. II 1992, 220). Der Hinweis auf § 193 I ist ausreichend, außer eine Begründung ist im Einzelfall zum Verständnis der Prüfungsanordnung erforderlich (BFH X B 210/01, BFH/NV 2003, 3).“

106 Siehe nur Rüsken, in: Klein, AO, 14. Auflage 2018, Rn. 4; Ratschow, in: Klein, AO, 14. Auflage 2018, § 118 Rn. 42, Stichwort „Außenprüfung“.

107 Wünsch, in: Koenig, AO, 3. Auflage 2014, Rn. 2: „Der BFH hatte entschieden, dass für die Besteuerung von Bankkunden das Kreditinstitut auf der Grundlage des § 97 wegen der in Abs. 2 angeordneten Subsidiarität erst dann zur Vorlage von Kontoauszügen aufgefordert werden darf, wenn eine vorherige Auskunft nach § 93 erfolglos geblieben ist, also die Auskunft nicht erteilt wurde, diese unzureichend war oder Bedenken gegen die Richtigkeit bestanden.“

108 Recht + Steuern vom 11. Mai 2015, Steuerprüfung: Darauf darf das Finanzamt zugreifen, <https://www.deutsche-handwerks-zeitung.de/steuerpruefung-darauf-darf-das-finanzamt-zugreifen/150/3098/293452>.

109 Rätke, in: Klein, AO, 14. Auflage 2018, § 93 Rn. 31.

110 Krepold, in: Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 5. Auflage 2017, § 39 Rn. 278.

Steuerhinterziehung“.¹¹¹ Schwarzgelder eines Kunden waren nur mit Angabe einer Kennziffer ohne Namensnennung nach Luxemburg transferiert worden. In der Kladde eines Bankmitarbeiters waren weiteren Bankkunden Kennzeichen zugeordnet. Im Ergebnis hat das BVerfG nach Auffassung der Kommentierung eine „**statistische Plausibilität**“¹¹² für einen Anfangsverdacht ausreichen lassen, um – verbunden mit einem konkreten Verdacht im Einzelfall – Durchsuchungen in großem Ausmaß zu rechtfertigen, und auf dieser Basis den **Verdacht** gegen bislang **unbekannte Personen** in zahlreichen Fällen **erst** einmal zu **begründen**. Hinter dieser Entscheidung soll die in einer früheren Entscheidung des BVerfG¹¹³ geäußerte Auffassung stehen, dass das Bankgeheimnis ein Hindernis für die Gewährung von Gleichheit im steuerlichen Belastungserfolg darstelle. Das BVerfG verlange darüber hinaus vom Gesetzgeber, die Steuerehrlichkeit durch hinreichende, die steuerliche Belastungsgleichheit gewährleistende Kontrollmöglichkeiten abzustützen.¹¹⁴

4.7.2. Rechtfertigung

Verfassungsrechtlich sprechen die folgenden Hinweise des BVerfG dafür, Finanzbehörden anlasslose bzw. niedrigschwellige Zugriffsrechte in Bezug auf Finanzdaten einzuräumen:

„Wird eine Steuer nicht an der Quelle erhoben, hängt ihre Festsetzung vielmehr von der Erklärung des Steuerschuldners ab, werden erhöhte Anforderungen an die Steuerehrlichkeit des Steuerpflichtigen gestellt. Der Gesetzgeber muß die Steuerehrlichkeit deshalb durch hinreichende, die steuerliche Belastungsgleichheit gewährleistende **Kontrollmöglichkeiten** abstützen. Im Veranlagungsverfahren bedarf das Deklarationsprinzip der Ergänzung durch das **Verifikationsprinzip**. [...]

Vielmehr bestätigt die Rechtsprechung des BVerfG zum grundrechtlichen Datenschutz, daß steuerliche Kontrollmitteilungen und **Auskunftspflichten** mit den **Grundrechten** der Banken und der Bankkunden **vereinbar** sind. [...]

Der – auch strafrechtlich sanktionierte – **Steueranspruch** des **Staates** begründet sich aus dem Umstand, daß der Betroffene am staatlichen Leben teilnimmt, ihm insbesondere Schutz, Ordnung und Leistungen der staatlichen Gemeinschaft zugute kommen. Deshalb darf ihm ein Anteil an den finanziellen Lasten zur Aufrechterhaltung des staatlichen Lebens auferlegt werden. Die Bemessung dieses Lastenanteils nach Maßstäben verhältnismäßiger Gleichheit erfordert die Angabe von Daten, die eine solche Gleichheit der Besteuerung ermöglichen. Von hier aus **rechtfertigen** sich – vorbehaltlich ihrer näheren Ausgestaltung anhand der aufgezeigten verfassungsrechtlichen Maßstäbe – **Offenbarungspflichten** der Steuerpflichtigen (vgl. BVerfGE 67, 100 [143] 4). [...]

111 BVerfG, Beschluss vom 23. März 1994, Az. 2 BvR 396/94.

112 Krepold, in: Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 5. Auflage 2017, § 39 Rn. 278.

113 BVerfG, Urteil vom 27. Juni 1991, Az. 2 BvR 1493/89.

114 Krepold, in: Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 5. Auflage 2017, § 39 Rn. 279.

Mit der gesetzlichen Ausgestaltung des **Steuergeheimnisses** hat der Gesetzgeber hinreichende **Sicherheitsvorkehrungen** gegen eine mißbräuchliche Verwendung der erteilten Angaben getroffen.“¹¹⁵

Dem Anspruch des Staates gegen den Bürger auf Abgabe von Steuern entspricht, dass das Steuerungsverfahren ein für den Bürger **mitwirkungspflichtiges** Verwaltungsverfahren ist (siehe nur 4. Teil der AO, Zweiter Abschnitt „Mitwirkungspflichten“). Im Unterschied hierzu besteht **keine** verfassungsrechtliche oder gesetzliche **Offenlegungspflicht** der Bürger über ihre – verfassungskonforme oder verfassungsfeindliche – **Gesinnung** (vgl. Art. 4 GG);¹¹⁶ dementsprechend ist die – ohnehin überwiegend verdeckte – Beobachtung durch Nachrichtendienste kein mitwirkungspflichtiger Vorgang. Die anlasslosen bzw. niedrigschwelligen Zugriffsrechte der Finanzbehörden auf Finanzdaten lassen sich daher nicht auf Nachrichtendienste übertragen.

* * *

115 BVerfG, Urteil vom 27. Juni 1991, Az. 2 BvR 1493/89, Rn. 113, 133, 136, 138 (Hervorhebung durch Autor).

116 Vgl. BVerwG, Urteil vom 15. Dezember 2005, Az. 7 C 20/04: „Die Schutzzerklärung ist voraussetzungsgemäß dazu bestimmt, den Geschäftspartner des Verwenders zur Offenlegung seiner Zugehörigkeit zur Scientology zu zwingen. [...] Für die Herausgabe der Schutzzerklärung fehlt die erforderliche Ermächtigungsgrundlage“ (unter Berufung auf die nach Art. 4 GG geschützte Weltanschauungsfreiheit).