

# Die verfassungsrechtlichen Anforderungen an die Übermittlung personenbezogener Daten an ausländische Nachrichtendienste

Dipl.-Jur. Nils Grimmig, B.A.

Der Autor ist seit September 2025 Rechtsreferendar im Oberlandesgerichtsbezirk Celle. Der Aufsatz basiert auf einem Teil der mit 15 Punkten bewerteten Seminararbeit mit dem Titel „Das Zusammenwirken der Nachrichtendienste des Bundes mit ausländischen Partnerdiensten – rechtliche Möglichkeiten und Grenzen“ im Schwerpunkt Verwaltung an der Leibniz Universität Hannover, die von Prof. Dr. Timo Rademacher, M.Jur. (Oxford) gestellt wurde. Der entsprechende Ausschnitt aus der Seminararbeit wurde für den Zweck der Veröffentlichung in dieser Zeitschrift erheblich überarbeitet und erweitert.

## I. Einführung

Für die Aufgabenerfüllung der Nachrichtendienste – also die Datenerhebung weit vor dem Eintritt einer konkreten Gefahr zur Informationsgewinnung über mögliche Gefährdungslagen<sup>1</sup> – ist es notwendig, die häufig unstrukturiert und ggf. unvollständig erhobenen Daten nicht nur zu filtern, sondern auch und vor allem mit Erkenntnissen anderer Stellen zu verknüpfen.<sup>2</sup> Neben der Kooperation mit inländischen Gefahrenabwehr- und Strafverfolgungsbehörden verstetigt und erhöht sich die Bedeutung des Zusammenwirkens mit ausländischen Nachrichtendiensten aufgrund der zunehmend globalisierten Gefährdungslage,<sup>3</sup> etwa durch internationale Terrorgruppierungen oder hybride Kriegsführung anderer Staaten<sup>4</sup>. Diese internationale Kooperation, die im Kern aus einem Informationsaustausch besteht, ist für die Gewährleistung der inneren und äußeren Sicherheit in Deutschland unerlässlich.<sup>5</sup> Auf einen solchen, weitgehend auf informellen Regeln basierenden, Informationsaustausch lassen sich ausländische Nachrichtendienste indes nur dann nachhaltig ein, wenn die Zusammenarbeit auf Gegenseitigkeit (Prinzip des „*do ut des*“) beruht.<sup>6</sup> Anders gewendet: Um die innere und äußere Sicherheit der Bundesrepublik Deutschland durch Zugang

zu Informationen anderer Nachrichtendienste sicherzustellen, müssen deutsche Nachrichtendienste ihrerseits (ggf. personenbezogene) Informationen an ausländische Partnerdienste übermitteln.

Dafür sieht der Gesetzgeber mittlerweile umfassende Ermächtigungsgrundlagen jeweils für das Bundesamt für Verfassungsschutz und den Militärischen Abschirmdienst in § 25a BVerfSchG (ggf. i.V.m. § 10 S. 1 MADG) sowie den Bundesnachrichtendienst in § 11e BNDG vor. Diese Normen sind häufig in unmittelbarer Reaktion auf entsprechende Entscheidungen des BVerfG<sup>7</sup> im Sicherheits- und Nachrichtendienstrecht geschaffen oder geändert worden, in denen es Anforderungen an die Datenerhebung und -übermittlung durch Nachrichtendienste aufstellt und fortentwickelt hat. Hinsichtlich des Informationsaustausches zwischen inländischen Nachrichtendiensten bzw. Gefahrenabwehrbehörden gibt es zur systematischen Aufbereitung dieser Anforderungen bereits eine umfangreiche Literatur.<sup>8</sup> Wie diese Anforderungen speziell auf die Übermittlung von Daten durch deutsche Nachrichtendienste in das Ausland zu verstehen sind bzw. sich darauf übertragen lassen, ist bislang indes eher seltener Gegenstand der Diskussion.<sup>9</sup>

<sup>1</sup> Vgl. BVerfGE 133, 277 (325); 162, 1 (112).

<sup>2</sup> Vgl. BVerfGE 163, 43 (86).

<sup>3</sup> S. dazu Schmahl in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 8 Rn. 2 ff.

<sup>4</sup> Hierzu lassen sich in jüngerer Vergangenheit vor allem die Gefährdungen durch russische Spionage, Sabotage und Desinformation anführen, vor denen das Bundesamt für Verfassungsschutz (<https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrung-russische-spionage-sabotage-desinformation.html> [Abruf v. 10.09.2025]) ausdrücklich öffentlich warnt.

<sup>5</sup> Vgl. Schöndorf-Haubold, Auf dem Weg zum Sicherheitskooperationsrecht?, in Dietrich/Gärditz/Graulich/Gusy/Warg (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, 3 (4, 9 f.). So waren seit 2010 bei insgesamt 19 vereitelten islamistischen Terroranschlägen in sieben Fällen Hinweise von ausländischen Nachrichtendiensten entscheidend; hinzu kommen unzählige Hinweise, die eine Vereitelung bereits in einem früheren Planungsstadium ermöglichten, vgl. Dahlkamp et al. in: Der Spiegel Nr. 36/2024, 19 (23).

<sup>6</sup> Vgl. Daun, Auge um Auge?, 2011, S. 94 f.; Labasque, The Merits of Informality in Bilateral and Multilateral Cooperation, IJICI 33(3), 492 (493).

<sup>7</sup> Etwa zum ATDG: BVerfGE 133, 277 ff. – ATDG I und BVerfGE 156, 11 ff. – ATDG II; zum BKAG: BVerfGE 141, 220 ff.; zum BNDG: BVerfGE 154, 152 ff.; zum BayVerfSchG: BVerfGE 162, 1 ff.; zum BVerfSchG: BVerfGE 163, 43 ff.

<sup>8</sup> Siehe nur Unterreitmeier, Informationen der Nachrichtendienste: „[...] Schweigen ist Gold“?: Zum Stand der Übermittlungsdogmatik in der Rechtsprechung des BVerfG (Teil 1 und 2), GSZ 2022, 251 ff., GSZ 2023, 34 ff.; Winter, Rahmenbedingungen für eine Kohärenz des Nachrichtendienstrechts, 2022, S. 103 ff., 149 ff. Vgl. insbes. auch zu der Problematik eines informationellen Trennungsprinzips zwischen Nachrichtendiensten und der Polizei: Gusy, Das Trennungsprinzip zwischen Informationen von Nachrichtendiensten und Polizei, GSZ 2021, 141 ff.

<sup>9</sup> Vgl. aber auch etwa Gusy in: Dietrich/Effler, Handbuch des Rechts der Nachrichtendienste, 2017, IV § 2 Rn. 78 ff., Rn. 87 ff.

Dieser Aufsatz soll vor diesem Hintergrund einen Beitrag zur systematischen Erfassung der grundrechtlichen Anforderungen an die Datenübermittlung deutscher Nachrichtendienste an ausländische Partnerdienste leisten und eine Bewertung der derzeitigen Rechtslage ermöglichen. Dazu werden zunächst die Grundlagen der verfassungsrechtlichen Einordnung der Datenübermittlung (siehe II.) dargestellt, um sodann die rechtlichen Grenzen der Datenübermittlung an ausländische Partnerdienste (siehe III.) zu ermitteln. Dies ermöglicht eine kritische Bestandsaufnahme ausgewählter bestehender gesetzlicher Regelungen (siehe IV.). Schlussendlich erfolgt eine Zusammenfassung und ein Ausblick auf die weiteren Rechtsentwicklungen (siehe V.).

## II. Grundlagen der verfassungsrechtlichen Einordnung der Datenübermittlung

Zunächst soll dargestellt werden, welches Recht für die Datenübermittlung an ausländische Nachrichtendienste maßstäblich ist und, ob sich aus diesem das Erfordernis einer gesetzlichen Regelung ergibt.

### 1. Maßstäbliches höherrangiges Recht

Maßgeblich für die gesetzlichen Ermächtigungen zur Übermittlung von personenbezogenen Daten an ausländische Nachrichtendienste ist gem. Art. 20 Abs. 3 Var. 1 GG die verfassungsmäßige Ordnung (sog. Vorrang der Verfassung).<sup>10</sup> Besonders relevant ist in diesem Zusammenhang die Bindung aller staatlichen Gewalt an die Grundrechte. Zwar könnte grundsätzlich auch die europäische Grundrechtecharta neben den deutschen Grundrechten oder anstelle dieser, wenn der fragliche Regelungsbereich vollständig unionsrechtlich determiniert wäre,<sup>11</sup> anwendbar sein. Die Tätigkeit der Nachrichtendienste fällt aber anders als diejenige der Polizeien – trotz fraglos zunehmen-

der Verringerung des funktionellen Abstandes<sup>12</sup> – immer noch unter den Souveränitätsvorbehalt des Art. 4 Abs. 2 S. 3 EUV („nationale Sicherheit“), sodass weder die DSGVO noch die JI-Richtlinie<sup>13</sup> anwendbar sind (vgl. Art. 2 Abs. 2 lit. a DSGVO bzw. Art. 2 Abs. 3 lit. a JI-Richtlinie) und mithin in der Tätigkeit der Nachrichtendienste keine Durchführung des Unionsrechts i.S.d. Art. 51 Abs. 1 S. 1 GrCh zu sehen ist.<sup>14</sup>

Auch die EMRK, die in ihrem Art. 8 Abs. 1 ein – in der Rechtspraxis einem umfassenden Datenschutzgrundrecht angenähertes<sup>15</sup> – Recht auf Achtung des Privatlebens enthält, bleibt hier außer Betracht. Sie ist zwar neben den Grundrechten des Grundgesetzes anwendbar und kann als Auslegungshilfe dienen;<sup>16</sup> es ergeben sich daraus bislang aber keine über das Grundgesetz und die Rechtsprechung des BVerfG hinausgehenden Anforderungen.<sup>17</sup>

### 2. Die Datenübermittlung als Grundrechtseingriff

Einer Datenübermittlung vorangehen muss jeweils stets eine Datenerhebung. Erhebt eine deutsche staatliche Stelle personenbezogene Daten, so stellt dies bzw. die dazu ermächtigende gesetzliche Regelung einen Eingriff mindestens in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG – in speziellen Fällen in Art. 10 Abs. 1 oder Art. 13 Abs. 1 GG<sup>18</sup> – dar.<sup>19</sup> Will ein deutscher Nachrichtendienst nun solchermaßen erhobene Daten an einen ausländischen Partnerdienst übermitteln, liegt darin eine Zweckänderung, die dem Grundsatz der Zweckbindung einmal erhobener Daten widerspricht und damit ihrerseits einen erneuten Grundrechtseingriff bedeutet.<sup>20</sup> Die Datenübermittlung teilt hinsichtlich des betroffenen Grundrechts das Schicksal der Datenerhebung.<sup>21</sup> Aus dem Eingriff in ein Grundrecht folgt zugleich, abzuleiten aus dem Rechtsstaats- bzw. dem Demokratieprinzip (Art. 20 Abs. 2, 3 GG) oder vorgegeben durch die Schran-

<sup>10</sup> Rux in: *Epping/Hillgruber*, BeckOK Grundgesetz, 61. Ed. 15.3.2025, Art. 20 Rn. 165 f.

<sup>11</sup> Vgl. BVerfGE 129, 186 (199); 152, 216 (229 ff.).

<sup>12</sup> Vgl. Bäckers in: *Dietrich et al.* (Fn. 3), § 29 Rn. 15. Diese Entwicklung wird häufig als „Verpolizeichung“ der Nachrichtendienste oder spiegelbildlich auch als „Vernachlässigung“ der Polizei beschrieben, vgl. *Barczak*, Das Recht der Nachrichtendienste: Missstände, Entwicklungen und Perspektiven eines Rechtsgebiets in der Findungsphase, *KritV* 2021, 91 (104), mwN.

<sup>13</sup> Richtlinie (EU) 2016/680, ABl. 2016 L 119, 89 v. 4.5.2016.

<sup>14</sup> Ebenso von *Lewinski* in: *Auernhammer*, DSGVO, 8. Aufl. 2024, Art. 2 Rn. 23; *Schmidt* in: *Taege/Gabel*, DSGVO, 4. Aufl. 2022, Art. 2 Rn. 14; *Zerdlck* in: *Ehmann/Selmayr*, DSGVO, 3. Aufl. 2024, Art. 2 Rn. 8. Anderer Ansicht aber *Bäckers* in: *Wolff/Brink/v. Ungern-Sternberg*, BeckOK Datenschutzrecht, DSGVO, 51. Ed. 1.8.2023, Art. 2 Rn. 9.

<sup>15</sup> Vgl. *van Bernstorff/Asche* in *Dietrich/Eiffler* (Fn. 9), II § 1 Rn. 7 ff.

<sup>16</sup> Ausf. *Schmahl*, Rechtliche Auswirkungen des grundgesetzlichen Prinzips der Völkerrechtsfreundlichkeit auf das Verhältnis zwischen deutscher Rechtsordnung und Europäischer Menschenrechtskonvention, *ZaöRV* 2023, 805 (807 ff.).

<sup>17</sup> Vgl. *Winter* (Fn. 8), S. 351 f.; s. auch *Steiner*, „Big Brother Watch/Centrum för Rättvisa“: Die strategische Fernmeldeaufklärung des Bundesnachrichtendienstes im Spiegel der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte, *GSZ* 2024, 32 (33).

<sup>18</sup> Vgl. *Hecker* in: *Dietrich/Eiffler* (Fn. 9), III § 2 Rn. 19; *Zöller*, Der Rechtsrahmen für die Übermittlung personenbezogener Daten unter Beteiligung der Nachrichtendienste, in: *Dietrich/Gärditz/Graulich/Gusy/Warg* (Hrsg.), *Nachrichtendienste im demokratischen Rechtsstaat*, 2018, 185 (188).

<sup>19</sup> Grundlegend BVerfGE 65, 1 (41 ff.).

<sup>20</sup> Vgl. *Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, 2014, S. 238; *Zöller*, in: *Dietrich et al.* (Fn. 18), 185 (187 ff.).

<sup>21</sup> BVerfGE 154, 152 (266), mwN; stRspr.

kensystematik des jeweiligen Grundrechts, das Erfordernis einer gesetzlichen Regelung (sog. grundrechtlicher Gesetzesvorbehalt).<sup>22</sup>

### III. Rechtliche Anforderungen an Ermächtigungen zur Datenübermittlung an ausländische Partnerdienste

Die rechtlichen Anforderungen an eine solche gesetzliche Regelung ergeben sich aus höherrangigem Recht und, wie zuvor bereits gezeigt, insbesondere aus den Grundrechten des Grundgesetzes. In Abwandlung des – auf das allgemeine Verwaltungsrecht bezogenen – Diktums von Fritz Werner<sup>23</sup> ließe sich also auch formulieren: „Nachrichtendienstrecht ist konkretisiertes Verfassungsrecht“<sup>24</sup>.

#### 1. Normenklarheit und -bestimmtheit

Bezüglich der Ausgestaltung der nach obigen Maßstäben erforderlichen gesetzlichen Grundlagen ist insbesondere der, bei heimlichen Grundrechtseingriffen neben dem Rechtsstaatsprinzip insbesondere aus den jeweils betroffenen Grundrechten herzuleitenden,<sup>25</sup> Grundsatz der Normenklarheit und -bestimmtheit zu beachten. Die Normenklarheit verlangt, dass die Regelung aus sich heraus inhaltlich verständlich ist, sodass die von ihr betroffenen Bürger sich auf mögliche belastende Maßnahmen einstellen können.<sup>26</sup> Verweisungen auf andere Normen sind zwar zulässig, aber nur soweit sie begrenzt bleiben und nicht zu unübersichtlichen Verweisungskaskaden führen.<sup>27</sup> Die Normenbestimmtheit zielt auf steuernde und begrenzende Handlungsmaßstäbe für die Exekutive und die Möglichkeit der wirksamen Kontrolle durch die Gerichte ab und verlangt, dass der Gesetzgeber seine Regelungen so bestimmt fasst, wie es nach der Eigenart des einzuordnenden Lebenssachverhalts mit Rücksicht auf den Normzweck möglich ist.<sup>28</sup>

#### 2. Verfahrensmäßige Anforderungen

Zudem ergeben sich unmittelbar aus dem Verhältnismäßigkeitsgrundsatz<sup>29</sup> Verfahrensanforderungen an die Übermittlung von personenbezogenen Daten.

##### a) Transparenz und individueller Rechtsschutz

Hierbei ist insbesondere die Transparenz der Datenerhebung und -verarbeitung zu nennen, welche zur Entstehung von Vertrauen und Rechtssicherheit und zur Einbindung des Umgangs mit Daten in den demokratischen Diskurs beitragen soll.<sup>30</sup> Dabei sind Pflichten zur Benachrichtigung und Auskunftsrechte für die von informationellen Eingriffen Betroffenen vorzusehen,<sup>31</sup> damit diese eine gerichtliche Rechtmäßigkeitskontrolle erwirken können.<sup>32</sup> Indessen können die Benachrichtigungspflichten und Auskunftsrechte bei heimlichen informationellen Eingriffen von Nachrichtendiensten umfassend eingeschränkt werden, um eine wirksame Aufgabenwahrnehmung zu gewährleisten.<sup>33</sup>

##### b) Rechtskontrolle

Da bei heimlichen informationellen Eingriffen die Grundsätze der Transparenz und individuellen Rechtskontrolle nur eine sehr eingeschränkte Wirkung entfalten, gewinnt das Element der Rechtskontrolle, auch im Sinne einer Ausgleichsfunktion, erheblich an Bedeutung.<sup>34</sup> Insoweit lässt sich zwischen der aufsichtlichen und der justizförmigen Kontrolle unterscheiden, wobei unter ersterer vor allem die Datenschutzbeauftragten des Bundes und der Länder sowie die Fachaufsicht verstanden werden.<sup>35</sup> Neuerdings fällt darunter jedoch auch das administrative Kontrollorgan nach §§ 40 Abs. 2 Nr. 2, 50 ff. BNDG, das als Teil des Unabhängigen Kontrollrates – aufgrund des vom BVerfG hergeleiteten Erfordernisses einer umfassenden und institutionell unabhängigen Kontrolle im Rahmen der Auslands-Fernmeldeaufklärung des BND<sup>36</sup> – errichtet wurde.

<sup>22</sup> Vgl. Grzeszick in: Dürig/Herzog/Scholz, Grundgesetz Kommentar, 97. EL Januar 2022, Art. 20 VI, Rn. 92; Rux in: BeckOK GG (Fn. 10), Art. 20 Rn. 172 ff.

<sup>23</sup> Werner, Verwaltungsrecht als konkretisiertes Verfassungsrecht, DVBl. 1959, 527 ff.

<sup>24</sup> Gusy, Reformperspektiven des Rechts der Nachrichtendienste, in: Dietrich/Gärditz/Graulich/Gusy/Warg (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, 19 (21); s. auch Löffelmann/Zöller, Nachrichtendienstrecht, 2. Aufl. 2025, A. Rn. 85: „angewandtes Verfassungsrecht“.

<sup>25</sup> Etwa für Art. 10 GG, BVerfGE 113, 348 (375); vgl. auch Tanneberger, Die Sicherheitsverfassung, 2014, S. 339.

<sup>26</sup> BVerfGE 156, 11 (45 f.).

<sup>27</sup> BVerfGE 154, 152 (266).

<sup>28</sup> BVerfGE 162, 1 (125).

<sup>29</sup> So BVerfGE 141, 220 (282); krit. zu dieser Verortung Alt, Kompensatorische Kontrolle heimlicher Grundrechtseingriffe, 2024, S. 290 ff.

<sup>30</sup> BVerfGE 141, 220 (282).

<sup>31</sup> BVerfGE 141, 220 (282 f.).

<sup>32</sup> BVerfGE 141, 220 (283 f.).

<sup>33</sup> Vgl. BVerfGE 154, 152 (287 f.).

<sup>34</sup> Vgl. BVerfGE 141, 220 (284).

<sup>35</sup> Vgl. Alt (Fn. 29), S. 236.

<sup>36</sup> BVerfGE 154, 152 (290 ff.).

Justizförmige Kontrolle findet, da individueller Rechtsschutz aufgrund der stark eingeschränkten Benachrichtigungs- und Auskunftsrechte bei heimlichen Maßnahmen kaum zu erlangen ist, insbesondere durch die G 10-Kommission (vgl. § 15 G 10)<sup>37</sup> und das gerichtsähnliche Kontrollorgan des Unabhängigen Kontrollrates nach §§ 40 Abs. 2 Nr. 1, 42 ff. BNDG statt.

### 3. Grundsatz der Verhältnismäßigkeit im engeren Sinne

Für die Verhältnismäßigkeit im engeren Sinne ist eine Abwägung zwischen dem Eingriff und den beeinträchtigten Rechtsgütern auf der einen Seite sowie den zu schützenden Rechtsgütern auf der anderen Seite erforderlich. Für ersteres ist insbesondere die Eingriffsintensität einer hoheitlichen Maßnahme von Bedeutung.<sup>38</sup> Bei nachrichtendienstlichen Maßnahmen können dabei neben der Heimlichkeit der Maßnahme, welche die Eingriffsintensität schon im Ausgangspunkt deutlich erhöht,<sup>39</sup> insbesondere die Dauer oder Streubreite einer Maßnahme, die Schutzbedürftigkeit und der Umfang der erlangten Daten oder auch deren denkbare Verwendung sowie schließlich die Art der betroffenen Grundrechte eine Rolle spielen.<sup>40</sup> Auf der anderen Seite der Abwägung sind die Schutzbedürftigkeit des zu schützenden Rechtsguts, aber insbesondere auch die Höhe der tatbestandlichen Schwellen für den Eingriff zu beachten.<sup>41</sup>

Für die Konkretisierung dieser Abwägungskriterien zieht das BVerfG vor allem den sog. Grundsatz der hypothetischen Datenneuerhebung heran.<sup>42</sup> Dieser wird als Ausprägung des allgemeineren datenschutzrechtlichen Zweckbindungsgrundsatzes verstanden.<sup>43</sup>

#### a) Inhalt des Kriteriums der hypothetischen Datenneuerhebung

Eine Übermittlung personenbezogener Daten an Dritte ist danach nur dann zulässig, wenn ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln auch für den geänderten Zweck erfolgen dürfte.<sup>44</sup> Im Ergebnis orientiert sich danach das Eingriffsgewicht einer Datenübermittlungsregelung an demjenigen der vorangehenden Daten-erhebung.<sup>45</sup> Daraus folgen Anforderungen einerseits an die Wichtigkeit der zu schützenden Rechtsgüter und andererseits an die tatbestandliche Übermittlungsschwelle. Das zu schützende Rechtsgut muss dabei stets besonders gewichtig sein, wozu insbesondere Leib, Leben und Freiheit einer Person sowie der Bestand und die Sicherheit des Bundes oder eines Landes zählen.<sup>46</sup> Die Übermittlungsschwelle demgegenüber differenziert je nachdem, welchen Zweck die Übermittlung erfüllen soll: Erfolgt die Übermittlung zu Zwecken der Gefahrenabwehr oder Strafverfolgung an Behörden mit sog. operativen Zwangsbefugnissen, so muss Voraussetzung einer Übermittlung sein, dass für das o.g. Rechtsgut im ersten Fall wenigstens eine konkretisierte Gefahr<sup>47</sup> und im zweiten Fall bestimmte, einen Verdacht begründende Tatsachen vorliegen.<sup>48</sup> Für die Übermittlung an sonstige Stellen kommt demgegenüber, sofern sie nicht über operative Zwangsbefugnisse verfügen, eine Absenkung dieser Übermittlungsschwellen in Betracht.<sup>49</sup>

#### b) Kritik

Das Kriterium der hypothetischen Datenneuerhebung sieht sich in der Literatur jedoch erheblicher Kritik, insbesondere methodischer Natur, ausgesetzt.<sup>50</sup> So wird die Anknüpfung hinsichtlich der Eingriffsintensität des Ersterhebungsvorgangs als dogmatisch inkonsequent empfunden.

<sup>37</sup> Allerdings hat das BVerfG (NVwZ 2025, 563 [572]) kürzlich festgestellt, dass die G 10-Kommission – bezogen auf die Ermächtigung zur strategischen Inland-Ausland-Fernmeldeaufklärung nach § 5 Abs. 1 S. 3 Nr. 8 G 10 – mangels hauptamtlicher Tätigkeit ihrer Mitglieder und mangels Sicherstellung einer richterlichen Perspektive nicht den verfassungsrechtlichen Anforderungen, die in BVerfGE 154, 152 (290 ff.) entwickelt wurden, entspricht. Das BVerfG (NVwZ 2025, 563 [573]) hat diesbezüglich nicht die Nichtigkeit festgestellt, sondern eine Unvereinbarkeitserklärung mit einer befristeten Fortgeltungsanordnung bis zum 31.12.2026 getroffen. Der Gesetzgeber ist also bis dahin gefordert, die G 10-Kommission nach dem Vorbild des Unabhängigen Kontrollrates umzugestalten.

<sup>38</sup> Löffelmann, Eingriffsintensität und Eingriffsschwelle: Eine Formel für den Gesetzgeber, GSZ 2023, 92 (93).

<sup>39</sup> BVerfGE 120, 378 (402 f.), mwN.

<sup>40</sup> Vgl. Löffelmann, Überwachungsgesamtrechnung und Verhältnismäßigkeitsgrundsatz, 2022, S. 45 f.

<sup>41</sup> Löffelmann (Fn. 38), GSZ 2023, 92 (94).

<sup>42</sup> BVerfGE 163, 43 (89), mwN; stRspr.

<sup>43</sup> BVerfGE 162, 1 (119); s. auch Löffelmann, Die Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung – Schema oder Struktur?, GSZ 2019, 16 (17).

<sup>44</sup> Vgl. BVerfGE 141, 220 (327 f.).

<sup>45</sup> BVerfGE 154, 152 (267).

<sup>46</sup> BVerfGE 163, 43 (92 f.).

<sup>47</sup> BVerfGE 162, 1 (115 f.).

<sup>48</sup> BVerfGE 162, 1 (118).

<sup>49</sup> BVerfGE 162, 1 (120).

<sup>50</sup> Etwa Gitter/Marscholleck, Erster Teil der Reform des Nachrichtendienstrechts: Konzeptioneller Switch mit offenen Praxisfragen, GSZ 2024, 45 (46); Meiertöns, Verfassungsschutzbehörden und Grundrechtseingriffe – Das Urteil des Bundesverfassungsgerichts zum bayerischen Landesverfassungsschutzgesetz, JBÖS 2022/23, 533 (540 f.); Schneider, Die Hypothetische Datenneuerhebung – Begriff ohne Konzept, GSZ 2022, 1 (2 ff.).



Denn wenn die Übermittlung personenbezogener Daten auch nach der Ansicht des BVerfG jeweils einen eigenen neuen Grundrechtseingriff bedeute, so liege eine eigenständige Beurteilung dieses neuen Eingriffs besonders nahe.<sup>51</sup> Demzufolge sollten statt des Vergleichs der Zwecke der Erhebung mit denjenigen der späteren Übermittlung vielmehr nur die Folgen und Verwendungszwecke der Übermittlung betrachtet werden.<sup>52</sup> Dafür spreche – neben der Problematik, dass das Kriterium dann an seine Grenzen komme, wenn es einen korrespondierenden Grundrechtseingriff auf Ebene der Datenerhebung gar nicht gibt (so etwa bei Erhebung von Daten aus allgemein zugänglichen Quellen)<sup>53</sup> – insbesondere, dass nur die Orientierung an der neuen Verwendung sachgerecht die Eingriffsintensität der Datenübermittlung abbilden könne.<sup>54</sup> Denn es seien durchaus Fälle denkbar, in denen der Datenerhebungseingriff keinen schweren Grundrechtseingriff bedeute, die spätere Übermittlung aber sehr wohl – wie etwa wenn diese in das Ausland erfolgt oder mit ihr die unmittelbare Ausübung polizeilicher Zwangsbefugnisse einhergeht.<sup>55</sup>

### c) Bewertung und (modifizierte) Anwendung auf Datenübermittlung in das Ausland

Zwar ist dieser grundlegenden Kritik zuzugeben, dass das Kriterium der hypothetischen Datenneuerhebung – wegen seines Abstellens auf die frühere Erhebungsmaßnahme – bereits im Ausgangspunkt die durch die spätere Übermittlung eintretenden Folgen und Gefährdungen untergewichtet, obwohl hierin der eigentliche (zweite) Grundrechtseingriff liegt. Gleichwohl ist an diesem grundsätzlich festzuhalten. Denn auch das BVerfG nimmt keine schematische Anwendung vor, sondern erlaubt gerade die Berücksichtigung anderer Gesichtspunkte.<sup>56</sup> So interpretiert es den Gedanken der hypothetischen Datenneuerhebung bei Datenübermittlungen durch Nachrichtendienste etwa bereits nicht mehr strikt befugnisbezogen (also mit

Blick auf die Eingriffsintensität der jeweiligen Ersterhebungsmaßnahme), sondern funktional, sodass alle nachrichtendienstlich erhobenen Daten hinsichtlich der Anforderungen an das zu schützende Rechtsgut grundsätzlich gleich behandelt werden.<sup>57</sup>

Zudem haben die Schwierigkeiten bei einer schematisch verstandenen Übertragung des Grundsatzes der hypothetischen Datenneuerhebung auf Übermittlungen in das Ausland zu weiteren Modifikationen durch das BVerfG geführt. So findet das Kriterium auf Datenübermittlungen in das Ausland grundsätzlich ebenfalls Anwendung,<sup>58</sup> sodass jede Übermittlung dem Schutz eines besonders gewichtigen Rechtsguts dienen muss und die entsprechenden Übermittlungsschwellen zu beachten sind. Die konkrete gesetzgeberische Ausgestaltung der Ermächtigungsgrundlagen darf aber hinsichtlich der Beurteilung der für das Empfängerland zu eröffnenden Nutzung der Daten die Besonderheiten der jeweiligen ausländischen Rechtsordnungen und deren Eigenständigkeit berücksichtigen.<sup>59</sup> Denn die deutsche Rechtsordnung trifft hier auf eine andere Rechtsordnung mit unterschiedlichen Abgrenzungslinien, Kategorien und Wertungen, wobei das Grundgesetz diese Andersartigkeit anerkennt und respektiert.<sup>60</sup> So ist etwa das informationelle Trennungsprinzip in dieser Form ein spezifisch deutsches Phänomen und Nachrichtendienste verfügen in vielen anderen Ländern, auch im europäischen Ausland, über polizeiliche Zwangsbefugnisse.<sup>61</sup> Eine Absenkung der strengen Übermittlungsschwellen könnte daher auch bereits dann in Betracht kommen, wenn die jeweilige ausländische Stelle den Ausschluss einer Weiterverarbeitung für Folgemaßnahmen mit unmittelbarer Außenwirkung verbindlich zusagt. Denn die Tatsache, dass Zweckbegrenzungen der Verwendung von Daten in der ausländischen Rechtsordnung nicht völlig identisch zur deutschen Rechtsordnung bestehen, schließt eine Übermittlung jedenfalls nicht von vornherein aus.<sup>62</sup> Insoweit

<sup>51</sup> So Löffelmann (Fn. 43), GSZ 2019, 16 (19); ders. (Fn. 38), GSZ 2023, 92 (96); ders., Hypothetische Datenneuerhebung und konkrete Schutzkategorien – ein kohärentes Datenverarbeitungskonzept für die Sicherheitsbehörden von Bund und Ländern, GSZ 2024, 215 (216); Müller/Schwabenbauer, Datenaustausch zwischen Sicherheitsbehörden: Bestandsaufnahme und Bemerkungen anlässlich der Entscheidungen des Bundesverfassungsgerichts zum Bayerischen Verfassungsschutzgesetz und zum Bundesverfassungsschutzgesetz, GSZ 2023, 1 (6).

<sup>52</sup> Löffelmann, Die Ausland-Ausland-Fernmeldeaufklärung, in: Dietrich/Gärditz/Graulich/Gusy/Warg (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, 33 (41); Meiertöns (Fn. 50), JBÖS 2022/23, 533 (541); Schneider (Fn. 50), GSZ 2022, 1 (4 f.); Unterreitmeier (Fn. 8), GSZ 2022, 251 (256).

<sup>53</sup> Vgl. Löffelmann (Fn. 43), GSZ 2019, 16 (18).

<sup>54</sup> Vgl. Löffelmann (Fn. 51), GSZ 2024, 215 (216).

<sup>55</sup> Vgl. Löffelmann (Fn. 40), S. 50.

<sup>56</sup> BVerfGE 133, 277 (374); 156, 11 (50).

<sup>57</sup> BVerfGE 162, 1 (112); 163, 43 (93); 169, 130 (181 f.). Eine Ausnahme gilt lediglich für die besonders eingriffsintensiven Mittel der Wohnraumüberwachung und Online-Durchsuchung, s. dazu Löffelmann (Fn. 54), GSZ 2024, 215.

<sup>58</sup> Vgl. BVerfGE 141, 220 (341); 154, 152 (273); 162, 1 (121).

<sup>59</sup> Vgl. BVerfGE 162, 1 (122).

<sup>60</sup> BVerfGE 141, 220 (344).

<sup>61</sup> Vgl. Unterreitmeier, Informationen der Nachrichtendienste: „... Schweigen ist Gold“?: Zum Stand der Übermittlungsdogmatik in der Rechtsprechung des BVerfG (Teil 3), GSZ 2023, 81 (83 ff.).

<sup>62</sup> BVerfGE 162, 1 (122).

spiegelt sich hierin auch die grundsätzlich auf Vertrauen, Zuverlässigkeit und Gegenseitigkeit basierende internationale Zusammenarbeit der Nachrichtendienste,<sup>63</sup> deren Regulationssystem weniger auf rechtlicher als auf tatsächlicher Sanktionierung (etwa durch Einschränkung oder gar Aufkündigung der Zusammenarbeit) beruht.

#### 4. Spezielle Anforderungen an Datenübermittlungen in das Ausland

Grundsätzlich ist das Grundgesetz für die Zusammenarbeit deutscher Nachrichtendienste mit ausländischen Partnerdiensten offen, da der verfassungsrechtlich gebotene Schutz der Bürger auch auf einen funktionierenden Informationsaustausch mit ausländischen Stellen angewiesen sein kann.<sup>64</sup> Aufgrund der besonderen Situation, dass in das Ausland übermittelte Daten einem anderen Rechtsregime unterliegen und damit insbesondere den grundgesetzlichen Gewährleistungen entzogen sind,<sup>65</sup> stellt der Verhältnismäßigkeitsgrundsatz aber spezifische Anforderungen an die gesetzliche Regelung von Übermittlungen an ausländische Behörden, die das BVerfG zuvorderst in seinen Entscheidungen zum BKAG<sup>66</sup> und zum BNDG<sup>67</sup> entwickelt hat.

Zunächst muss die Wahrung datenschutzrechtlicher Garantien auch nach der Übermittlung im Wesentlichen gewährleistet sein. Dabei wird durch das Grundgesetz indes auch die Eigenständigkeit der ausländischen Rechtsordnungen respektiert und anerkannt, sodass die Regelungen im Empfängerstaat zur Verarbeitung personenbezogener Daten nicht denjenigen der deutschen Rechtsordnung entsprechen oder gleichwertig sein müssen.<sup>68</sup> Es muss vielmehr ein angemessenes Datenschutzniveau im Empfängerstaat vorliegen, das insbesondere die Beachtung der von den deutschen Diensten mitgeteilten Zweckbindung der übermittelten Daten sowie etwaige Löschungspflichten umfasst.<sup>69</sup> Zudem muss wenigstens im Grundsatz ein Kontrollregime im Empfängerstaat bestehen und eine grundlegende Datensicherheit angenommen werden kön-

nen.<sup>70</sup> Sinn und Zweck dieser Anforderung ist es, dass die grundgesetzlichen Gewährleistungen für den Schutz personenbezogener Daten nicht durch einen Informationsaustausch mit dem Ausland unterlaufen werden.<sup>71</sup>

Weiterhin müssen die elementaren Menschenrechte auch bei der Nutzung seitens des Empfängerstaates gewährleistet sein. Es ist insbesondere sicherzustellen, dass die übermittelten Daten durch den Empfängerstaat nicht genutzt werden, um bestimmte Bevölkerungsgruppen zu verfolgen, Oppositionelle zu unterdrücken oder gar Menschen völkerrechts- oder menschenrechtswidrig zu töten, zu foltern oder ohne rechtsstaatliches Verfahren zu verhaften.<sup>72</sup> Denn der Staat darf keinesfalls seine Hand zu Verletzungen der Menschenwürde reichen.<sup>73</sup>

Schließlich muss durch die Nachrichtendienste des Bundes auch eine Vergewisserung über diese beiden Voraussetzungen – gesetzlich vorgegeben – erfolgen. Es bedarf dabei nicht einer umfassenden Prüfung in jedem Einzelfall, sondern es genügt eine generalisierende Einschätzung der Sach- und Rechtslage im Empfängerstaat; gleichwohl muss diese generalisierende Einschätzung auch durch entgegenstehende Tatsachen erschüttert werden können.<sup>74</sup> Eine verbindliche Zusage der Einhaltung der obigen Voraussetzungen ist zudem grundsätzlich geeignet, etwaige Bedenken auszuräumen, sofern nicht von vornherein erwartet werden muss, dass diese Zusicherung nicht eingehalten wird.<sup>75</sup>

#### 5. Ausnahme für Daten aus allgemein zugänglichen Quellen?

Fraglich ist schließlich, ob eine Ausnahme für solche Daten anzuerkennen ist, die aus allgemein zugänglichen Quellen erhoben wurden. Dies kann jedenfalls nicht bereits daraus hergeleitet werden, dass diese Anforderungen ausdrücklich auf solche Daten beschränkt seien, die mittels nachrichtendienstlicher Mittel erhoben wurden.<sup>76</sup> Denn das BVerfG hat seine diesbezügliche Rechtsprechung nicht auf solchermaßen erhobene Daten beschränkt oder an diese gar ausdrücklich geringere An-

<sup>63</sup> Vgl. Höhner, Das informationelle Verwendungsverbot im Nachrichtendienstrecht, 2024, S. 233 f.; Labasque (Fn. 6), IJICI 33(3), 492 (493 f.).

<sup>64</sup> BVerfGE 154, 152 (279).

<sup>65</sup> Vgl. BVerfGE 154, 152 (273).

<sup>66</sup> BVerfGE 141, 220 ff.

<sup>67</sup> BVerfGE 154, 152 ff.

<sup>68</sup> BVerfGE 141, 220 (344).

<sup>69</sup> BVerfGE 141, 220 (344 f.).

<sup>70</sup> BVerfGE 141, 220 (345).

<sup>71</sup> BVerfGE 154, 152 (274).

<sup>72</sup> BVerfGE 154, 152 (275).

<sup>73</sup> BVerfGE 141, 220 (342).

<sup>74</sup> BVerfGE 154, 152 (275 f.).

<sup>75</sup> Vgl. BVerfGE 140, 317 (350), mwN.

<sup>76</sup> So aber Gitter/Marscholleck (Fn. 50), GSZ 2024, 45 (50) mit Verweis auf BVerfGE 162, 1 (111); ähnlich Friehe, Ausschuss-Drs. 20(4)324 A, S. 10.

forderungen gestellt,<sup>77</sup> sondern sich dazu bisher lediglich nicht geäußert.

Gegen eine solche Ausnahme könnte sprechen, dass Daten, die durch Nachrichtendienste erhoben werden, aufgrund deren breit angelegter Beobachtungstätigkeit generell besonders schutzwürdig sind und daher hinsichtlich der Übermittlung eine Differenzierung nach dem Eingriffsgehalt der Erhebungsmaßnahme ausgeschlossen ist.<sup>78</sup> Eine solche Postulierung der Differenzierung nach Eingriffsgehalt bedingt jedoch bereits sprachlich, dass hinsichtlich der betrachteten Maßnahme zumindest auch ein Eingriff in Grundrechte vorliegt. Bei der Erhebung von Daten aus allgemein zugänglichen Quellen, jedenfalls solange diese nicht systematisch erhoben oder zusammengeführt wurden,<sup>79</sup> fehlt ein solcher jedoch.<sup>80</sup> Daher kann in diesem Fall auf den qualifizierten Rechtsgüterschutz und die besonderen Übermittlungsschwellen, die sich aus dem Kriterium der hypothetischen Datenneuerhebung ergeben,<sup>81</sup> verzichtet werden.

Indes ist damit noch nicht die besondere Gefährdungslage durch eine Übermittlung personenbezogener Daten in das Ausland<sup>82</sup> erfasst. Insbesondere besteht die Gefahr einer Nutzung im Empfängerstaat zu menschenrechtswidrigen Zwecken identisch auch bei personenbezogenen Daten aus allgemein zugänglichen Quellen. Als verfassungsrechtliches Mindestmaß gilt zudem ausnahmslos, dass der Staat nicht die Hand zur Verletzung der Menschenwürde reichen darf.<sup>83</sup> Insoweit kann bei der Übermittlung von Daten aus allgemein zugänglichen Quellen in das Ausland zwar auf die Anforderungen aus dem Kriterium der hypothetischen Datenneuerhebung, nicht aber auf die Vergewisserung über die Wahrung eines angemessenen Datenschutzniveaus und die Gewährleistung der elementaren Menschenrechte verzichtet werden.<sup>84</sup>

#### IV. Kritische Bewertung bestehender gesetzlicher Regelungen

Der Gesetzgeber hat die oben geschilderten Maßgaben des BVerfG an die Übermittlung personenbezogener Daten

in weiten Teilen, teils „nachgerade buchstabengetreu“<sup>85</sup>, umgesetzt. Aus dem Umstand, dass es für die Nachrichtendienste des Bundes jedoch kein einheitliches Regelwerk gibt, sondern jeweils einzelne Gesetze erlassen wurden, folgen stellenweise Kohärenzprobleme bei der Gesetzesanpassung. Zur Verdeutlichung sollen im Folgenden zwei ausgewählte gesetzliche Regelungen kritisch betrachtet werden.

##### 1. Übermittlung personenbezogener Daten aus allgemein zugänglichen Quellen, § 25d Abs. 1 BVerfSchG (i.V.m. § 11 S. 1 MADG), § 10a Abs. 1 BNDG

Zunächst sollen die Ermächtigungsgrundlagen zur Übermittlung personenbezogener Daten, die zuvor aus allgemein zugänglichen Quellen erhoben wurden, betrachtet werden. Dies ermöglicht für das BfV § 25d Abs. 1 BVerfSchG, der gem. § 11 S. 1 MADG auch auf den MAD anwendbar ist. Für den BND regelt dies § 10a Abs. 1 BNDG. Beide Normen erlauben gleichlautend die Übermittlung von personenbezogenen Daten, die aus allgemein zugänglichen Quellen erhoben wurden, bereits bei (bloßer) Erforderlichkeit zur Erfüllung der Aufgaben des Nachrichtendienstes oder der empfangenden Stelle. Weitere Übermittlungsschwellen – etwa in Form einer konkretisierten Gefahr – sind nicht vorgesehen. Wie zuvor bereits gezeigt, ist dies jedoch mit den grundrechtlichen Anforderungen vereinbar, die es ausnahmsweise erlauben bei personenbezogenen Daten, die aus allgemein zugänglichen Quellen erhoben wurden, von dem Erfordernis qualifizierten Rechtsgüterschutzes und von besonderen Eingriffsschwellen im Sinne des Kriteriums der hypothetischen Datenneuerhebung abzusehen, solange sie nicht systematisch erhoben oder zusammengeführt wurden.<sup>86</sup> Folgerichtig hat der Gesetzgeber daher auch die Übermittlung systematisch erhobener oder zusammengeführter Daten im Wege einer Rückausnahme wieder den besonderen Übermittlungsregeln unterworfen (vgl. § 25d Abs. 2 BVerfSchG und § 10a Abs. 2 BNDG). Insoweit begegnen diese Vorschriften hinsichtlich der Datenübermittlung im Inland keinen Bedenken.

<sup>77</sup> BVerfGE 162, 1 (111): „Dabei ist hier [Hervorh. d. Verf.] nur über die Übermittlung von Informationen zu entscheiden, die mit nachrichtendienstlichen Maßnahmen erlangt wurden.“ S. auch Löffelmann, Ausschuss-Drs. 20(4)324 D, S. 11; Zöller, Ausschuss-Drs. 20(4)324 E, S. 15 f.

<sup>78</sup> Vgl. BVerfGE 162, 1 (112).

<sup>79</sup> Vgl. BVerfGE 120, 274 (345); s. auch Löffelmann (Fn. 40), S. 53; Schneider (Fn. 50), GSZ 2022, 1 (5).

<sup>80</sup> Vgl. BVerfGE 120, 274 (344 f.).

<sup>81</sup> S. zu diesen bereits oben III. 3. a).

<sup>82</sup> Siehe nur Löffelmann (Fn. 43), GSZ 2019, 16 (18); ders. (Fn. 40), S. 50; Schluckebier, Sicherheitsgewährleistung zwischen politischer Gestaltung und verfassungsrechtlicher Bindung, in: Dietrich/Gärditz/Graulich/Gusy/Warg (Hrsg.), Reform der Nachrichtendienste zwischen Vergesetzlichung und Internationalisierung, 2019, 3 (13).

<sup>83</sup> So BVerfGE 141, 220 (342).

<sup>84</sup> S. zu diesen bereits unter III. 4.

<sup>85</sup> So pointiert Gärditz, Bundesnachrichtendienst semper reformanda, DVBl. 2021, 905 (906).

<sup>86</sup> Siehe schon III. 5.

Anderes gilt aber für die besondere Gefährdungslage durch eine Übermittlung in das Ausland, bei der, wie gezeigt, ausnahmslos das Erfordernis der Vergewisserung über die Wahrung eines angemessenen Datenschutzniveaus und die Gewährleistung der elementaren Menschenrechte zu verlangen ist.<sup>87</sup> Diese Gefährdungslage wird für § 10a Abs. 1 BNDG noch durch das Übermittlungsverbot des § 9e Abs. 3, 4 BNDG, da diese Norm unterschiedslos für alle Übermittlungsvorschriften im BNDG gilt,<sup>88</sup> berücksichtigt. Für das BfV und den MAD ist ein Übermittlungsverbot für die Gefährdung elementarer Menschenrechte jedoch lediglich in § 25a Abs. 2 S. 2–5 BVerfSchG (i.V.m. § 11 S. 1 MADG) bei der Datenübermittlung an ausländische öffentliche Stellen geregelt. Da § 25d Abs. 1 BVerfSchG jedoch insoweit *lex specialis* ist und der Umkehrschluss aus § 25d Abs. 2 S. 1 BVerfSchG zeigt, dass die Normen der §§ 19 bis 25c BVerfSchG im Falle des § 25d Abs. 1 BVerfSchG nicht gelten sollen, kann auf dieses Übermittlungsverbot nicht zurückgegriffen werden. Mithin ist § 25d Abs. 1 BVerfSchG (i.V.m. § 11 S. 1 MADG) in dieser Hinsicht unverhältnismäßig ausgestaltet und damit verfassungswidrig. *De lege ferenda* sollte die – verfassungsgemäße – Gesetzssystematik des BNDG auf das BVerfSchG übertragen werden.

## 2. Übermittlungsverbote (§ 25a Abs. 2 BVerfSchG, § 9e BNDG)

Schließlich ist noch die konkrete Ausgestaltung der Übermittlungsverbote in § 25a BVerfSchG und § 9e BNDG zu untersuchen. Hier besteht wiederum der Unterschied in der Regelungssystematik, dass § 9e BNDG für alle Übermittlungen nach dem BNDG gilt, wohingegen § 25a Abs. 2 BVerfSchG eine Sonderregelung für die Übermittlung an ausländische öffentliche Stellen darstellt.

§ 9e Abs. 1 S. 1 BNDG formuliert dabei ein Übermittlungsverbot bei – das Allgemeininteresse überwiegenden – schutzwürdigen Interessen der betroffenen Person (Nr. 1), entgegenstehenden überwiegenden Sicherheitsinteressen (Nr. 2) und entgegenstehenden besonderen gesetzlichen Regelungen (Nr. 3). Für Übermittlungen an ausländische öffentliche Stellen wird die Interessenabwägung des § 9e Abs. 1 S. 1 Nr. 1 BNDG durch das Regelbeispiel des § 9e Abs. 3 BNDG und die überwiegenden Sicherheitsinteressen i.S.d. § 9e Abs. 1 S. 1 Nr. 2 BNDG durch das Regelbeispiel des § 9e Abs. 4 BNDG konkretisiert.<sup>89</sup> Für die Abwä-

gung des Individualinteresses mit dem Allgemeininteresse gilt nach § 9e Abs. 3 S. 1 BNDG, den obig dargestellten verfassungsrechtlichen Anforderungen entsprechend, dass eine Übermittlung insbesondere dann zu unterbleiben hat, wenn die Verletzung elementarer rechtsstaatlicher Grundsätzen oder aber erhebliche Menschenrechtsverletzungen in dem ausländischen Staat drohen würden, wobei nach § 9e Abs. 3 S. 2 BNDG auch Zusicherungen der empfangenden Stelle und deren Glaubhaftigkeit zu berücksichtigen sind.

Vergleichbar zu § 9e Abs. 1 S. 1 BNDG regelt auch § 25 Abs. 2 S. 1 Nr. 1–3 BVerfSchG drei Übermittlungsverbote. Problematisch erscheint jedoch die Formulierung des § 25 Abs. 2 S. 2 BVerfSchG,<sup>90</sup> wonach überwiegende schutzwürdige Interessen insbesondere dann entgegenstehen, „[...] wenn Leib, Leben oder Freiheit [Hervorh. d. Verf.] einer Person oder sonstige elementare Menschenrechte gefährdet würden oder Verletzungen von elementaren rechtsstaatlichen Grundsätzen drohen.“ Dass die bloße Gefährdung der Freiheit, also der körperlichen Bewegungsfreiheit,<sup>91</sup> bereits ein Übermittlungsverbot indiziert, bedeutet letzten Endes die grundsätzliche Unzulässigkeit von Datenübermittlungen, die zum Zwecke der Ergreifung von Folgemaßnahmen mit unmittelbarer Außenwirkung erfolgen. Diese Formulierung überrascht zudem vor dem Hintergrund, dass weder im gleichen Gesetz bei inländischen Datenübermittlungen (vgl. § 23 Abs. 1 S. 1 BVerfSchG) noch in der Parallelvorschrift des § 9e Abs. 1 S. 1 Nr. 1, Abs. 3 BNDG eine derart strikte abwägungsleitende Einschränkung gemacht wird. § 23 Abs. 1 S. 1 Nr. 3 i.V.m. § 19 Abs. 3 Nr. 4 BVerfSchG sieht zwar ebenfalls bei Betroffenheit der Freiheit der Person ein Übermittlungsverbot vor; dies jedoch nur bei Vorliegen einer dringenden Gefahr und mit der Möglichkeit der Abwägung, wenn die Übermittlung dem Schutz ebensolcher Schutzgüter anderer Personen dient. § 9e Abs. 1 S. 1 Nr. 1, Abs. 3 BNDG verzichtet demgegenüber völlig auf ein, allein durch die Betroffenheit der Freiheit der Person indiziertes, Übermittlungsverbot, sondern beschränkt sich auf die vom BVerfG für maßgeblich erklärten Voraussetzungen der Vergewisserung über die Wahrung eines angemessenen Datenschutzniveaus und die Gewährleistung der elementaren Menschenrechte. Bereits aus dieser systematischen Gesamtschau folgt, dass die Regelung des § 25a Abs. 2 S. 2 BVerfSchG überdacht und ggf. den Rege-

<sup>87</sup> Siehe schon III. 5.

<sup>88</sup> Vgl. BT-Drs. 20/8627, S. 40.

<sup>89</sup> Vgl. BT-Drs. 20/8627, S. 40 f.

<sup>90</sup> Für einen Hinweis darauf, dass die Formulierung des § 25 Abs. 2 S. 2 BVerfSchG problematisch sein könnte, danke ich herzlich Herrn Prof. Dr. Timo Rademacher, M.Jur. (Oxford).

<sup>91</sup> Vgl. dazu Di Fabio in Dürig/Herzog/Scholz, Grundgesetz Kommentar, 55. EL Mai 2009, Art. 2 Abs. 2 Satz 2, Rn. 22 f.



lungen des § 23 Abs. 1 S. 1 BVerfSchG bzw. § 9e BNDG angepasst werden sollte.

Zudem ist der Anwendungsbereich des Übermittlungsverbotes des § 25a Abs. 2 BVerfSchG nicht eindeutig zu bestimmen. So könnte sich § 25a Abs. 2 BVerfSchG ggf. nur auf Absatz 1 der Vorschrift (Übermittlung ohne Folgemaßnahmen mit unmittelbarer Außenwirkung) – und nicht auch auf Absatz 4 (Verwendung für Maßnahmen mit unmittelbarer Außenwirkung) – beziehen. Dieses Verständnis stützend ließe sich anführen, dass der Gesetzesentwurf ursprünglich einen ausdrücklichen Verweis auf die Belange des § 25a Abs. 2 BVerfSchG in § 25a Abs. 4 S. 3 BVerfSchG-E statuiert hatte, der in den Ausschussberatungen indes gestrichen wurde.<sup>92</sup> Auch die systematische Stellung direkt nach § 25a Abs. 2 BVerfSchG und der augenscheinliche Bezug darauf durch die Wendung „Die [Hervorh. d. Verf.] Übermittlung unterbleibt [...]“ sowie, dass sich § 25a Abs. 4 BVerfSchG dem Wortlaut nach nur auf die „Verwendung“ der – bereits übermittelten – Daten bezieht, sprechen dafür.

Gegen ein solches Verständnis wiederum sprechen aber entscheidend die folgenden Gesichtspunkte: Zunächst soll die Regelung des § 25a Abs. 4 BVerfSchG nach dem Willen des Gesetzgebers sowohl die – erstmalige – Übermittlung als auch die nachträgliche Zustimmung zur Nutzung umfassen.<sup>93</sup> Wenn § 25a Abs. 4 BVerfSchG aber die Übermittlung personenbezogener Daten in das Ausland erlaubt, so ist nach den oben dargestellten Vorgaben des BVerfG zwingend sicherzustellen, dass ein angemessenes Datenschutzniveau und die elementaren Menschenrechte gewahrt werden. Demzufolge wäre die Norm verfassungswidrig, wenn das Übermittlungsverbot des § 25a Abs. 2 BVerfSchG auf diese nicht anwendbar sein sollte. Da hier zwei Auslegungen denkbar erscheinen, aber nur eine der beiden Alternativen mit höherrangigem Recht vereinbar ist, ergibt eine verfassungskonforme Auslegung,<sup>94</sup> dass § 25a Abs. 2 BVerfSchG auch auf Datenübermittlungen nach § 25a Abs. 4 BVerfSchG anzuwenden ist. Dies indes führte nach der aktuellen Rechtslage zu einem indizierten Datenübermittlungsverbot, wenn Maßnahmen mit unmittelbarer Außenwirkung in Form von Einschrän-

kungen der Freiheit der Person drohen. Diese Regelwirkung eines Übermittlungsverbotes erscheint vor dem Hintergrund widersprüchlich, dass § 25a Abs. 4 BVerfSchG eben gerade die Datenübermittlung zur Ergreifung von Maßnahmen mit unmittelbarer Außenwirkung – zumal unter erhöhten Übermittlungsschwellen und dem Erfordernis eines qualifizierten Rechtsgüterschutzes – ermöglichen soll.

Es besteht in § 25a BVerfSchG also Klarstellungsbedarf hinsichtlich des Anwendungsbereiches sowohl von § 25a Abs. 2 BVerfSchG (auch anwendbar auf § 25a Abs. 4 BVerfSchG) als auch von § 25a Abs. 4 BVerfSchG (umfasst auch die Datenübermittlung und nicht nur die Verwendung von bereits nach anderen Ermächtigungsgrundlagen übermittelten Daten). Zudem sollte zur Sicherstellung einer effektiven nachrichtendienstlichen Kooperation das Übermittlungsverbot hinsichtlich der Indizwirkung bereits allein durch bloße Beeinträchtigung der Freiheit der Person (§ 25a Abs. 2 S. 2 BVerfSchG) abgeschwächt werden. In beiderlei Hinsicht bietet sich – wie auch schon oben bei § 25d BVerfSchG – die Übernahme der Regelungssystematik des BNDG an (Ermächtigung zur Datenübermittlung in § 11e BNDG und allgemein für alle Übermittlungen geltendes Verbot in § 9e BNDG).

## V. Zusammenfassung und Ausblick

Zusammenfassend lässt sich eine erhebliche – insoweit im internationalen Vergleich einzigartige<sup>95</sup> – Verrechtlichung der Kooperation von Nachrichtendiensten konstatieren, die vor dem Hintergrund volatiler und zunehmender globaler Gefährdungslagen nicht nur zustimmend kommentiert wird.<sup>96</sup> Andererseits lässt sich die verfassungsgerichtliche Rechtsprechung aber auch als Beitrag zu einer sicherheitsrechtlichen Systembildung, die kohärente Maßstäbe vom Polizei- bis hin zum Nachrichtendienstrecht ermöglicht, verstehen.<sup>97</sup> Zur Verwirklichung dieser verfassungsgerichtlichen Anforderungen hat der Gesetzgeber zwar jedes Fachgesetz einzeln angepasst. Wie oben beispielhaft an § 25a Abs. 2 und § 25d BVerfSchG gezeigt wurde, steht der festgestellten Systembildung auf Verfassungsebene jedoch keine kohärente einheitliche Umset-

<sup>92</sup> Vgl. BT-Drs. 20/8626, S. 10; BT-Drs. 20/9345, S. 11.

<sup>93</sup> Vgl. BT-Drs. 20/8626, S. 31 f.

<sup>94</sup> Dazu etwa Zippelius, Juristische Methodenlehre, 12. Aufl. 2021, S. 44 f.

<sup>95</sup> Vgl. Kahl, Rahmenbedingungen und Notwendigkeiten internationaler Kooperationen von Nachrichtendiensten, in: Dietrich/Gärditz/Graulich/Gusy/Warg (Hrsg.), Nachrichtendienste in vernetzter Sicherheitsarchitektur, 2020, 153 (156).

<sup>96</sup> S. nur Barczak (Fn. 12), KritV 2021, 91 (100); Gärditz, Grundrechtliche Grenzen strategischer Ausland-Ausland-Telekommunikationsaufklärung, Ein Wegweiser durch die BND-Entscheidung des BVerfG, Urteil v. 19.5.2020 – 1 BvR 2835/17, JZ 2020, 825 (834) oder auch Gärditz, Sicherheitsverfassungsrecht und technische Aufklärung durch Nachrichtendienste, EuGrZ 2018, 6 (21 f.), der fordert, „das Sicherheitsrecht graduell zu dekonstitutionalisieren.“

<sup>97</sup> Vgl. Bäcker in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Rn. 184, 188.

zung auf Gesetzesebene gegenüber. Eine solche systematische Überarbeitung des Nachrichtendienstrechts strebt die aktuelle Regierungskoalition aus CDU, CSU und SPD ausweislich des Koalitionsvertrages an.<sup>98</sup> Eine Gelegenheit zur Umsetzung dieses Ziels bietet sich dem Gesetzgeber im Rahmen des – in der vorherigen 20. Legislaturperiode des Deutschen Bundestages bereits anvisierten<sup>99</sup> – zweiten Teils der Reform des Nachrichtendienstrechts.

---

<sup>98</sup> Vgl. CDU/CSU/SPD, Verantwortung für Deutschland, Koalitionsvertrag, S. 83, [https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav\\_2025.pdf](https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf) (Abruf v. 10.09.2025).

<sup>99</sup> Vgl. BT-Drs. 20/8626, S. 1.