

Michael Plöse

## Was Karlsruhe nicht verbietet, macht Berlin nur dreister

Anmerkungen zur Änderung des Antiterrordateigesetzes  
Teil 1: Konsequenzen aus der ATDG-Entscheidung des  
Bundesverfassungsgerichts vom 24. April 2013\*

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 24. April 2013 die Grundstrukturen der als Verbunddatei zwischen den Polizeibehörden des Bundes und der Länder sowie den Geheimdiensten eingerichteten Antiterrordatei (ATD) gebilligt, aber zahlreiche Einzelregelungen für mit dem Grundgesetz unvereinbar erklärt und grundlegende Nachbesserungen verlangt. Dazu wurde dem Gesetzgeber eine Übergangsfrist bis zum 31. Dezember 2014 gesetzt, um damit ausdrücklich Gelegenheit zu geben, die „Bestimmungen anderer Gesetze, die den angegriffenen Vorschriften ähnlich sind,“ zu überarbeiten.<sup>1</sup> Das am 1. Januar 2015 in Kraft getretene Gesetz zur Änderung des Antiterrordateigesetzes und anderer Gesetze vom 18. Dezember 2014 (BGBl. I S. 2318) ändert neben dem ATDG zugleich das Rechtsextremismusedateigesetz (RED-G) und das Aufenthaltsgesetz. Es ist jedoch alles andere als eine grundlegende Revision der Übermittlungsbestimmungen für die informationelle Zusammenarbeit von Polizeien, Staatsanwaltschaften und Geheimdiensten. Vielmehr werden nun standardmäßig Befugnisse zum Data-Mining und damit zur gemeinsamen Datennutzung und -erzeugung eingeführt. Michael Plöse stellt im ersten Teil seines Beitrags die maßgeblichen Entscheidungskriterien vor, auf die das BVerfG sein Urteil über die Verfassungsmäßigkeit eines Datenaustauschs zwischen Geheimdiensten und der Polizei gestützt hat. Vor dem Hintergrund der vielfältigen juristischen Kommentare zu der Entscheidung fragt er nach den Konsequenzen, die das Urteil für die Neugestaltung einer informationellen Zusammenarbeit von Sicherheitsorganen aufgestellt hat. Der zweite Teil (in der nächsten Ausgabe) widmet sich der Analyse, warum die ATDG-Novelle in wesentlichen Teilen mit der Sicherheitsverfassung des Grundgesetzes unvereinbar ist.

\* Ich danke Marie Melior, Sven Lüders, Jörg Pohle und Eric Töpfer für wichtige Hinweise und kritische Anmerkungen, Prof. Clemens Arzt und Prof. Rosemarie Will für viele erhellende Gespräche zur Konstruktion und rechtlichen Beurteilung der Verbunddateien.

## Konzeptionelles Vorspiel

„Die Frage nach denkbaren Wertkonflikten zwischen Datenverarbeitung und Menschenrechten“ stellt sich nicht erst seit der begrifflichen Neuprägung der gigantisch angewachsenen und aus allen denkbaren Quellen stammenden Datenmengen als „Big Data“, die privaten und öffentlichen Stellen bei ausreichender Rechenqualität die Erstellung umfassender Persönlichkeitsprofile erlaubt. Schon zu Beginn der elektronischen Datenverarbeitung hatte sich das Verhältnis von Individuum und datenverarbeitender Organisation grundlegend verändert; insbesondere dort, wo die Auswertung von Daten operative Eingriffsbefugnisse des Staates auslösen kann: „Infolge des Zuwachses an bisher nicht gekannter Schnelligkeit, Genauigkeit und Aktualität der mehrdimensional beliebig verknüpfbaren Informationen hat sich die polizeiliche Informationsverarbeitung sprunghaft zu völlig neuen Dimensionen der Effizienz fortbewegt.“ Dabei fänden sich die Möglichkeiten von Angriffen auf die Menschenwürde bereits in den Strukturen der Informationstechnologie angelegt. Diese lade geradezu dazu ein, „die örtlich und sachlich gezogenen Grenzen ihrer Anwendung aufzuheben, die Enge und Isoliertheit von Ressorts aufzulösen, innerstaatliche und nationale Grenzen zu überwinden und Wissen in immer größer werdenden Speichern zu sammeln. Die Grenzenlosigkeit der Informationsverarbeitung würde es gestatten, das Individuum auf seinem gesamten Lebensweg zu begleiten, von ihm laufend Momentaufnahmen, Ganzbilder und Profile seiner Persönlichkeit zu liefern, es in allen Lebensbereichen, Lebensformen, Lebensäußerungen zu registrieren, zu beobachten, zu überwachen und die so gewonnenen Daten ohne die Gnade des Vergessens ständig präsent zu halten. Die Gefahren des 'großen Bruders' sind nicht mehr bloß Literatur. Sie sind nach dem heutigen Stand der Technik real.“

Das erklärte nicht etwa ein Whistleblower über die Ausspähprogramme des US-amerikanischen Geheimdienstes NSA, der damit das Ausmaß der geheimdienstlichen Überwachung offenbaren wollte, sondern im Jahre 1980 der Präsident des Bundeskriminalamtes Horst Herold in einem Vortrag vor den Vereinten Nationen.<sup>2</sup> Offenbar wollte er durch seine kritische Reflexion und vorausschauende Beschränkung der maßgeblich von ihm eingeführten Technik deren Akzeptanz in der Bevölkerung erhöhen und das Bild einer verantwortungsbewussten Informationspolizei abgeben. An Data-Mining, PRISM, XKeyscore und TEMPORA war damals freilich nicht gedacht, die bedrohliche Elektronik der Datenverarbeitung bewegte sich auf dem Niveau von Lochkarten und Magnetbändern, verbunden durch ein ca. 60.000 km langes Leitungsnetz, das täglich gerade einmal zwei Millionen Transaktionen ermöglichte.<sup>3</sup> Dennoch schien die von anderer Seite<sup>4</sup> noch viel präziser beschriebene Bedrohung durch asymmetrische Informationshierarchien hinreichend klar, um rechtliche Konsequenzen zu ziehen.

So seien zwischen den einzelnen Funktionen staatlichen Handelns, das sich mit den Menschen befasst, Schranken nötig, referierte Herold weiter, die einen Datenverbund, d.h. die Zusammenfassung mehrerer oder aller staatlichen Bereiche zu einer wechselseitig abfragbaren Einheit aller Informationssysteme, verhindern. „Die Grundgedanken der Gewaltenteilung, die das kontinentale Rechtsdenken entwickelt hat, müssen

für die elektronische Datenverarbeitung zu einer wechselseitigen Abschottung und informatorischen Begrenzung der jeweiligen Behörden auf ihre spezifische Aufgabenstellung, also zur Informationsgewaltenteilung, fortentwickelt werden.“<sup>5</sup>

Angesichts so weitsichtiger Einsichten sollte es eigentlich keinen Unterschied machen, dass das BVerfG mit seiner Entscheidung über die Verfassungsmäßigkeit der Antiterrordatei den Enthüllungen von Edward Snowden zum „Überwachungs-GAU“<sup>6</sup> der international operierenden Geheimdienste gut zwei Monate zuvorkam. Spannend ist die Frage dennoch, wie das BVerfG in der Sache entschieden hätte, wenn es sich noch ein weiteres Jahr Zeit genommen und das ganze Ausmaß der Überwachungsrealität ebenso wie den Evaluationsbericht der Bundesregierung zur ATD<sup>7</sup> in seinen Entscheidungshorizont ernsthaft einbezogen hätte.<sup>8</sup> Vor dem Hintergrund dessen, was wir heute über die (nicht nur) technischen Möglichkeiten des Data-Mining als gesetzlichen Anwendungsfall gehorteter Datenmacht wissen, hätte den Richter\_innen in Karlsruhe die Unterkomplexität der empirischen Grundlagen ihres verfassungsrechtlichen Analyserahmens deutlich klarer vor Augen stehen müssen.

## 1. Was bleibt vom Trennungsgebot?

Was statt dessen geschah, ist bekannt und wurde auch schon trefflich kommentiert.<sup>9</sup> Das BVerfG hat in seiner für Sicherheitsgesetze mittlerweile eingeübten 'Ja-jedoch-Walterschrift-Rechtsprechung'<sup>10</sup> die ATD in ihren Grundstrukturen für verfassungskonform gehalten (Rn. 105 ff.), jedoch wegen der Schwere der damit verbundenen Grundrechtseingriffe eine Vielzahl von Einzelregelungen für unvereinbar mit dem Bestimmtheitsgebot und/oder dem Übermaßverbot erklärt (Rn. 138 ff.). Der sozialdemokratische RAF-Jäger Herold hat nie ein Hehl daraus gemacht hat, dass er eine informationelle Zusammenarbeit von Polizei und Geheimdiensten im konkreten Fall für sinnvoll hält. Dabei ging er jedoch nicht so weit, wie dies im Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus gefordert wird. Darin wurde als Konsequenz aus der Ignoranz der deutschen Sicherheitsbehörden in Sachen NSU-Terror u.a. die Schlussfolgerung gezogen, das Problem mangelnder Zusammenarbeit zwischen Verfassungsschutz- und Polizeibehörden liege an einer gegenseitigen „Kopfsperre“, die es „zu Gunsten eines gemeinsamen Verständnisses von Verantwortung für die Sicherheit“ zu überwinden gälte.<sup>11</sup>

Auch der Entscheidung des BVerfG ist eine deutliche „Grundskepsis“<sup>12</sup> zu entnehmen, die jedenfalls „einen allgemeinen Austausch personenbezogener Daten aller Sicherheitsbehörden oder den Abbau jeglicher Informationsgrenzen zwischen ihnen“, die „den Grundsatz der Zweckbindung als solchen unterlaufen“ würden, von vornherein für unzulässig erklärt (Rn. 106). Dennoch bleibt die Frage, wie viel Trennungsgebot eine freiheitlich-demokratische<sup>13</sup> „Informationsgewaltenteilung“<sup>14</sup> voraussetzt und ob ein aus den Grundrechten, namentlich dem Grundrecht auf informationelle Selbstbestimmung, abgeleitetes informationelles Trennungsprinzip hierfür genügt.

Das BVerfG schwieg zu der – eigentlich entscheidenden – Frage über das Bestehen, die Reichweite und die verfassungsrechtliche Verankerung eines objektiv-rechtlichen

Trennungsgebots zwischen Polizei und Geheimdiensten.<sup>15</sup> Statt dessen meinte es, diese Frage durch die Proklamation eines grundrechtlichen Trennungsprinzips (Rn. 123) umgehen zu können. Begründet wurde dieses Prinzip mit der spezifischen grundrechtlichen Gefährdungslage, die sich aus einem ungehinderten Informationsaustausch zwischen den mit Zwangsbefugnissen ausgestatteten Polizei- und Strafverfolgungsbehörden einerseits und den ohne jeden konkreten Verdacht zur (auch) verdeckten Informationserhebung berechtigten Geheimdiensten andererseits ergebe. Dieser 'Ausfallschritt' wurde zu Recht als „verpasste Chance“<sup>16</sup> bezeichnet.

Mit zunehmendem Abstand scheint sich jedoch die Aufmerksamkeit vom Ergebnis der Entscheidung und deren Stellschrauben zu den Prämissen hin zu verschieben, in denen vorsichtige, aber durchaus ausbaufähige Töne mitschwingen,<sup>17</sup> kurz gesagt: Da ist Musik drin. Ein Rhythmus freilich, der im Bundesinnenministerium geflissentlich überhört und im Bundestag nicht gespielt wurde (dazu mehr im zweiten Teil).

Zunächst zu den Stellschrauben: Um dem Datenaustausch zwischen Polizeibehörden und Geheimdiensten, wie er sich in der Antiterrordatei (bzw. in der Rechtsextremismusdatei auf der Grundlage des RED-G) als einem „Zweckänderungsautomaten“<sup>18</sup> vollzieht, nicht schon auf kompetenzrechtlicher Ebene den Garaus zu machen – denn nichts anderes würde ein strenges Verständnis des Trennungsgebots im Sinne eines (nur) durch gesetzlich geregelte Einzelfälle durchbrochenen Kooperationsverbots bewirken –, ging das BVerfG im Gleichschritt mit der Gesetzesbegründung<sup>19</sup> davon aus, dass das ATDG über die Zugriffskompetenz im Eilfall (§ 5 Abs. 2 und § 6 Abs. 2 ATDG) hinaus selbst keine Befugnisse für eine unmittelbare Datenübermittlung enthält (Rn. 125). Im Kern sei die ATD vielmehr auf eine bloße „Informationsanbahnung“ beschränkt, die den beteiligten Behörden die Suche nach Datenbeständen erleichtern solle, ohne die Anforderungen einer einzelfallbezogenen Prüfung der Übermittlungsvoraussetzungen sowohl durch die anfragende (= abrufende) als auch die datenbesitzende (= verantwortliche) Stelle nach den Vorgaben des „Fachrechts“ entbehrlich zu machen (Rn. 125 f.).

Damit wird der zuvor festgestellte Grundrechtseingriff von erheblichem (Rn. 110) – im Eilfall (Rn. 129) und im Falle der zweckfremden Weiterverwendung für operative Aufgaben sogar von besonders schwerem (Rn. 123) – Gewicht auf ein Maß reduziert, das ihn gegenüber einem herausragenden öffentlichen Interesse generell abwägbar macht (Rn. 123, 129 ff.). Sind die Schutzgüter nur bedeutend genug, woran das BVerfG im Hinblick auf die Verhinderung terroristischer Gewalttaten – als „gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes“ gerichtete „Angriffe“ (Rn. 133) – keinen Zweifel lässt, kann diese Abwägbarkeit des grundrechtlichen Zweckbindungsgebots von Daten schnell zu dessen Wegwägbarkeit beitragen.<sup>20</sup> Um dies zu verhindern, setzt das BVerfG dieser Stellschraube eine Prämisse voraus und zieht mit dem *obiter dictum* ausgesprochenen Verboten eines „allgemeinen Austausch[s] personenbezogener Daten aller Sicherheitsbehörden“ sowie eines „Abbau[s] jeglicher Informationsgrenzen zwischen ihnen“ eine rote Linie als letzte Schranke.<sup>21</sup>

Das ist nicht trivial, denn das BVerfG würde ein solches gesetzgeberisches Ziel von vornherein als nicht legitim erachten: Es ist mit dem Grundsatz der Zweckbindung jeglicher Datenverarbeitung unvereinbar, welchen Karlsruhe selbst im Angesicht der

Herausforderungen des internationalen Terrorismus gegen die Idee eines 'Feindstrafrechts' verteidigt (Rn. 133). Eine generelle Verschmelzung von präventiven, repressiven und nachrichtendienstlichen Sicherheitsbehörden ist dem Gesetzgeber damit von Verfassung wegen untersagt, egal ob er eine solche nun bewusst regeln wollte oder sie sich durch das Zusammenwirken von Einzelgesetzen ergibt.

Die Schaffung von Einrichtungen, die kompetenziell dem nationalsozialistischen Reichssicherheitshauptamt oder der Staatssicherheit in der DDR gleichkommen, ist damit ebenso ausgeschlossen, wie die bis 1978 übliche Praxis der polizeilich-justiziell-geheimdienstlichen Zusammenarbeit unter der Regie der Alliierten Kontrollmächte auf der Grundlage der Unkeler Richtlinien vom 8. Oktober 1954 in Westdeutschland.<sup>22</sup> Vor diesem Hintergrund wirft Fremuth die Frage auf,<sup>23</sup> ob das BVerfG mit dem explizit formulierten 'grundrechtlich-materiellen'<sup>24</sup> „informationellen Trennungsprinzip“ nicht implizit ein zumindest auch funktionales (und damit staatsorganisatorisch-formales) Trennungsgebot voraussetzt.

So sehr also den Kritik\_innen darin zuzustimmen ist, dass das BVerfG erneut eine klare Äußerung zur verfassungsmäßigen Verankerung eines organisatorischen Trennungsgebotes vermieden hat, obwohl ein formaler Verstoß explizit gerügt wurde,<sup>25</sup> so ernst gilt es das BVerfG darin zu nehmen, dass es den im Urteil beschriebenen einfachgesetzlichen Aufbau des Sicherheitsrechts, in dem „eine Geheimpolizei [...] nicht vorgesehen“ ist (Rn. 122), zur Voraussetzung und Grundlage seiner Bewertungen gemacht hat. Damit hat es das einfachgesetzlich weitgehend praktizierte Trennungsprinzip zwischen Polizei und Geheimdiensten zugleich als grundlegende Umsetzung des grundrechtlich geforderten informationellen Trennungsprinzips vorausgesetzt, unter dessen – fachrechtlich allerdings im Einzelnen ungeprüft gebliebenen<sup>26</sup> – Bedingungen sich die ATD in ihren Grundstrukturen erst als verfassungskonform erweist. Von daher ist an das Bild zu erinnern, welches das BVerfG in seiner Entscheidung zur Rasterfahndung nach 9/11 gebraucht hatte: „Die Balance zwischen Freiheit und Sicherheit darf vom Gesetzgeber neu justiert, die Gewichte dürfen jedoch von ihm nicht grundlegend verschoben werden.“<sup>27</sup>

Das BVerfG hat das informationelle Trennungsprinzip als eine besondere materielle Ausprägung des Verhältnismäßigkeitsgrundsatzes im Rahmen von Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG gefasst. Die zu Art. 10 und 13 GG entwickelte Grundrechtsdogmatik<sup>28</sup> wird damit auf den Zweckbindungsgrundsatz des Grundrechts auf informationelle Selbstbestimmung und den Bereich des Informationsaustauschs zwischen Behörden übertragen. Für die Frage, wie die Sicherheitsarchitektur auszugestalten sei, hält das derart konstruierte Trennungsprinzip zwar keine streng formale Antwort bereit. Dafür hat die grundrechtlich-materielle Antwort nicht nur auf Bundesebene Bedeutung,<sup>29</sup> sondern wirkt generell für das Verhältnis der Zusammenarbeit von operativen Sicherheitsbehörden und Geheimdiensten sowohl in und zwischen den einzelnen Bundesländern sowie gegenüber Bundesbehörden als auch in Bezug auf die Datenübermittlung an ausländische oder private Stellen.

Ob es sich bei dem informationellen Trennungsprinzip am Ende dann nur um eine konkretisierte Wiederholung des bereits seit dem Volkszählungsurteil mit Verfassungsrang ausgestatteten Zweckentfremdungsverbots von Daten handelt, wie es Rosemarie Will enttäuscht herausstellte,<sup>30</sup> oder um eine grundrechtlich-materielle Unter-

mauerung des unausgesprochen objektiv-rechtlich vorausgesetzten funktionalen Trennungsgebots, ist am Ende vielleicht gar nicht so entscheidend. Damit es überhaupt Substanz erhält, müssen die vom BVerfG aufgestellten Prämissen ernst genommen und konsequent angewendet werden – was freilich auch für das Gericht selbst gilt.

## 2. Weitere Prämissen für die Novellierung sicherheitsrechtlicher Übermittlungsvorschriften

### a) Schwere des Grundrechtseingriffs

Im Hinblick auf die Schwere des Grundrechtseingriffs setzte das BVerfG mit seiner Entscheidung den schon seit dem Volkszählungsurteil von 1983 eingeschlagenen, u.a. im Rasterfahndungsbeschluss von 2006 konturierten Weg fort. Danach gibt es unter den Bedingungen der automatisierten Datenverarbeitung keine „belanglosen“ Daten mehr, entscheidend sind vielmehr ihre Nutzbarkeit und Verwendungsmöglichkeiten. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab.<sup>31</sup> Mit dem Fortschreiten der technischen Möglichkeiten geht daher eine gesteigerte Gefährdungslage einher, welcher ein entsprechender Grundrechtsschutz gegenüberstehen muss.<sup>32</sup> Dieser bestimmt sich im Rahmen einer „Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang“ nach der Intensität des behördlichen Interesses an den betroffenen Daten.<sup>33</sup> Dementsprechend stellte das BVerfG bereits im Falle der Rasterfahndung klar, dass sich das Gewicht „informationsbezogener Grundrechtseingriffe“ auch danach richte, welche Nachteile den Betroffenen aufgrund der Eingriffe drohen oder von diesen nicht grundlos befürchtet werden könnten („Gefühl des Überwachtwerdens“):<sup>34</sup> Dabei kann es sich um staatliche Ermittlungsmaßnahmen, Einschränkungen der Handlungsfreiheit oder stigmatisierende/diskriminierende Auswirkungen der Befugnisse handeln.

Bei der Übermittlung personenbezogener Daten zwischen Sicherheitsbehörden mit völlig unterschiedlichen Aufgaben und (Vollzugs-)Kompetenzen geht das BVerfG insoweit konsequent von einem „erheblichen Eingriffsgewicht“ aus (Rn. 110 ff.), das im Fall der ATD nur deswegen abgesenkt sei, weil diese die eigentliche Datenübermittlung nicht vorwegnehme, sondern – zumindest dort, wo sie als reine Indexdatei funktioniert – nur vorbereite (s.o.). Wo aber – wie im Eilfall oder bei der merkmalsbezogenen Recherche in den erweiterten Grunddaten durch die insoweit auch für unzulässig erklärte „Inverssuche“ – tatsächlich eine Datenübermittlung zwischen Polizeibehörden und Geheimdiensten unter Durchbrechung des informationellen Trennungsprinzips stattfindet, die Daten mit „nachrichtendienstlichen Mitteln“ gewonnen wurden und die Betroffenen damit der möglichen Gefahr weiterer operativer (= mit Zwang durchsetzbarer) Anschlussmaßnahmen ausgesetzt werden, stellt dies einen „beson-

ders schweren Eingriff“ dar, der nur auf der Grundlage normenklarer gesetzlicher Regelungen und zum Schutze „herausragender öffentlicher Interessen“ gerechtfertigt werden kann (Rn. 123).

Das Eingriffsgewicht mag bei der Übermittlung von Erkenntnissen aus offen zugänglichen Quellen geringer sein. Allerdings stellt auch das Anlegen teilweise sehr umfangreicher Dossiers über Einzelpersonen und deren Bewertung selbst im Vorfeld kriminalisierter Handlungen ein spezifisches Mittel nachrichtendienstlicher Tätigkeit dar, das den Polizeibehörden verwehrt ist. Entsprechend dürfen Daten zwischen Polizei- und Strafverfolgungsbehörden einerseits sowie Geheimdiensten andererseits „grundsätzlich nicht ausgetauscht werden“. Eine Übermittlung geheimdienstlicher Erkenntnisse ist daher „nur ausnahmsweise zulässig“. Dabei dürfen die behördenspezifischen Eingriffsschwellen für die Erlangung von Daten (nach den jeweiligen Polizeigesetzen oder der StPO) nicht unterlaufen werden (Prinzip des hypothetischen Erdatzeingriffs, s. Rn. 123).

#### b) Keine Umgehung der fachgesetzlichen Anforderungen durch Datenübermittlung

Das BVerfG überträgt die hohen Anforderungen, die es eigentlich für die Zweckänderung von mittels Eingriffen in Art. 10 GG erhobenen Daten entwickelt hat, auch auf übermittlungsbedingte Eingriffe in das Recht auf informationelle Selbstbestimmung. Folglich bestimmt es (Rn. 114.), dass die „verfassungsrechtlichen Voraussetzungen für die Erhebung, Speicherung und Verarbeitung von Daten [...] nicht dadurch unterlaufen werden [dürfen], dass Behörden, für die aufgrund ihrer Aufgabenstellung weniger strenge Anforderungen gelten, Daten im Wege der Übermittlung an Behörden weiterleiten, die ihrerseits strengeren Anforderungen unterliegen.“ Hierbei stellt das BVerfG wiederum maßgeblich auf die unterschiedlichen Aufgaben und Kompetenzen der beteiligten Behörden ab, die wegen ihrer Intensität für eine mögliche Grundrechtsbeschränkung unterschiedlichen Anforderungen (sog. Eingriffsschwellen) unterliegen.

Dieser Gedanke lässt sich freilich auch in anderer Richtung fortentwickeln, insbesondere mit Blick auf den bekannt gewordenen Datenaustausch zwischen den Geheimdiensten des Bundes und ausländischen Stellen. So stellt sich die Frage nach der Zulässigkeit einer Weiterverwendung von Erkenntnissen ausländischer Stellen, die mit Mitteln erhoben wurden, die deutschen Stellen generell (z.B. durch Folter) oder jedenfalls unter den konkreten Bedingungen des Einzelfalls versagt sind (z.B. wegen eines Verstoßes gegen die Menschenwürde).<sup>35</sup> Angesichts der Tatsache, dass fast 90 Prozent der in der ATD erfassten Personen im Ausland leben (14.213 von insgesamt 16.180 Personen zum Stand August 2012, vgl. Rn. 68) und überwiegend vom BND eingegeben wurden (ca. 46 Prozent),<sup>36</sup> der in einer Vielzahl der von ihm verarbeiteten Daten wohl kaum über die konkreten Umstände der Datenerhebung informiert sein dürfte, wirft dieses Kriterium die Frage auf, wie viele der eingegebenen Datensätze selbst nach Bereinigung der ATD in Folge des Karlsruher Diktums von 2013<sup>37</sup> rechtsstaatlichen Erhebungsgrundsätzen entsprechen.

### c) Ziel der Datei als Rechtfertigungsmaßstab des Grundrechtseingriffs

Das BVerfG hat es für gerechtfertigt angesehen, „zur Effektivität der Aufklärung und Bekämpfung des internationalen Terrorismus“ auch jenseits von Einzelübermittlungsvorschriften eine „sie koordinierende Verbunddatei zur Informationsanbahnung“ (Rn. 132) zu schaffen.<sup>38</sup> Dabei stellte es maßgeblich auf die Schwere der „Straftaten mit dem Gepräge des Terrorismus“ ab, die „zur Verbreitung von Angst und Schrecken“ verübt würden, auf eine „Destabilisierung des Gemeinwesens“ zielten und sich hierzu „in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter“ bedienten (Rn. 133). Sollen solche „Angriffe“ nicht als Krieg oder jenseits der Verfassung in einem die Grundrechte suspendierenden Ausnahmezustand abgewehrt werden, müsse der Maßstab des verfassungsrechtlich Zulässigen großzügiger sein, d.h. die Grenzen der Verfassung weiter gezogen und also – mit den Worten des Gerichts – „der Terrorismusbekämpfung im rechtsstaatlichen Rahmen der Verhältnismäßigkeitsabwägung ein erhebliches Gewicht“ beigemessen werden.<sup>39</sup>

Unter Zugrundelegung dieser Maßstäbe hat Nikolas Gazeas in seiner Dissertation<sup>40</sup> nachgeholt, was das BVerfG schuldig geblieben ist: Er hat einen Großteil der fachgesetzlichen Übermittlungsvorschriften zwischen Geheimdiensten sowie Polizei- und Ermittlungsbehörden (z.B. §§ 17 ff. BVerfSchG, §§ 8 ff. BNDG, §§ 10 ff. MADG, § 474 Abs. 2 Satz 2, § 477 Abs. 1 Satz 3 Nr. 2 StPO) auf ihre Verfassungsmäßigkeit hin geprüft und insbesondere im Hinblick auf die dort in Bezug genommenen Straftatenkataloge vielfachen Anlass zu Beanstandungen gehabt.<sup>41</sup> Zunächst erscheint fraglich, ob die darin aufgelisteten, nach §§ 100a Abs. 2 und 100c Abs. 2 StPO jedenfalls als „schwere Straftaten“ klassifizierten Delikte tatsächlich in jedem Fall als „Straftaten mit dem Gepräge des Terrorismus“ die Schwelle zu einem herausragenden öffentlichen Interesse erreichen. Weiterhin gilt es, sie im Hinblick auf die Zulässigkeit ihrer Aufnahme in einer gemeinsamen Verbunddatei von Polizei und Geheimdiensten am Maßstab des verfassungsrechtlichen Übermaßverbots zu messen. Neben der Frage nach einer hinreichenden Wahrscheinlichkeit des Schadenseintritts bzw. der persönlichen Nähe des Betroffenen zum Gefahrenzusammenhang ist hierfür das Gewicht der jeweils bedrohten Rechtsgüter von Bedeutung.<sup>42</sup> Als besonders schwerwiegend sind im präventiven wie repressiven Zusammenhang die unmittelbaren Bedrohungen von Leib, Leben oder Freiheit sowie die Integrität herausragender Einrichtungen des Gemeinwesens (insbesondere der Infrastruktur) anerkannt;<sup>43</sup> also genau die Fälle, in denen nach § 5 Abs. 2 ATDG auch im Eilfall unter Umgehung der fachgesetzlichen Übermittlungsvorschriften ein Direktzugriff auf die erweiterten Grunddaten der ATD zulässig wäre.

Auch wenn dieser Maßstab als Zulässigkeitskriterium für die Aufnahme jeglicher Information in der ATD zu streng sein mag, so lässt sich doch festhalten, dass ein „herausragendes öffentliches Interesse“ nur dann angenommen werden kann, wenn es im konkreten Tat- oder Gefahrenzusammenhang jedenfalls um den Schutz von Leib, Leben, Freiheit oder den Bestand des Staates geht – tatbestandlich um einen Eilfall ohne Eile eben.<sup>44</sup>

Ein näherer Blick auf die Straftatenkataloge, die nach § 20 Abs. 1 Satz 2 BVerfSchG, also nach der „fachgesetzlichen Übermittlungsvorschrift“ des Bundesamtes für Ver-



fassungsschutz (BfV), über die §§ 74a und 120 des Gerichtsverfassungsgesetzes (GVG) auf bestimmte Staatsschutzdelikte im Strafgesetzbuch verweisen und eine Übermittlung entsprechender Erkenntnisse durch das BfV an Staatsanwaltschaft und Polizei von Amts wegen (also nicht erst auf Anforderung) vorsehen, nährt nicht nur im Einzelfall erhebliche Zweifel am Bestehen eines „herausragenden öffentlichen Interesses“ an der Übermittlungspflicht: Warum sollte bspw. der konkrete Verdacht der Verbreitung von Propaganda verfassungswidriger Organisationen (§ 20 Abs. 1 Satz 2 BVerfSchG i.V.m. § 74a Abs. 1 Nr. 2 GVG i.V.m. § 86 StGB) oder einer politischen Verdächtigung (§ 20 Abs. 1 Satz 2 BVerfSchG i.V.m. § 74a Abs. 1 Nr. 6 GVG i.V.m. § 241a Abs. 1–3 StGB) eine Speicherung in der ATD<sup>45</sup> rechtfertigen können?<sup>46</sup> Von einem Verstoß gegen das Übermaßverbot ist dementsprechend wohl auch in den Fällen der §§ 89b, 97Abs. 2, 241a Abs. 1–3 StGB, § 20 Abs. 1 Nr. 1–4 VereinsG, §§ 17 Abs. 4 und 5, § 18 Abs. 1–6 AWG auszugehen.<sup>47</sup> Wenn aber die Übermittlung solcher Informationen auf der Grundlage der fachgesetzlichen Vorschriften als unverhältnismäßig ausscheidet, weil es hierfür von vornherein an einem herausragenden öffentlichen Interesse fehlt, kann eine Speicherung der Daten in der ATD nicht in Betracht kommen. Denn in diesen Fällen liefe letztlich auch die Informationsanbahnung ins Leere. **Was aber nicht übermittelt werden darf, ist auch nicht erforderlich und darf daher nicht gespeichert werden.**

Zwar ist vor einer Aufnahme von Daten noch die Erforderlichkeit von deren Kenntnis „für die Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland“ gem. § 2 ATDG zu prüfen und würden auch offene oder minder schwere Straftatbestände nach den Anforderungen des BVerfG vor ihrer Erfassung im Einzelfall durch eine tatbestandliche Einengung „in einer dem Verhältnismäßigkeitsgrundsatz genügenden Weise“ auf die „gegen terroristische Straftaten gewendete Zielrichtung der Antiterrordatei“ aussortiert werden können (Rn. 151). Dadurch würde sich aber kein anderes Bild ergeben. Denn entweder haben die anlassgebenden Handlungen eine strafbarkeitsbegründende Nähe zum Terrorismus oder die Schwere einer Leib, Leben oder Freiheit gefährdenden Gewalttat – dann stellt das an sich unzureichende Anlassdelikt nur einen „mitwirklichen“ Straftatbestand dar –, so dass es genügen würde, nur die verfassungsrechtlich unstrittigen Straftatbestände zu erfassen, oder die Speicherung hat zu unterbleiben, weil sie schon nach § 2 ATDG nicht erforderlich ist oder jedenfalls unverhältnismäßig wäre.

In diesem Lichte erscheint auch die konzeptionell weitgehend identisch aufgebaute RED in ihrem gegenwärtigen Umfang weitgehend unzulässig. In jedem Fall steht hier eine genauere Prüfung aus. Es kann nicht davon ausgegangen werden, dass „die im Rahmen der gesetzlichen Evaluation [der ATD] noch offen gebliebenen verfassungsrechtlichen Fragen durch die Entscheidung des BVerfG vom 24. April 2013 abschließend geklärt“ worden sind – wie dies in der Begründung des Entwurfs zur Neufassung des RED-G behauptet wird, um dessen Entfristung zu rechtfertigen.<sup>48</sup>

*Der Beitrag wird fortgesetzt im nächsten Heft.*

**MICHAEL PLÖSE** studierte Rechtswissenschaft und Sozialwissenschaften an der Humboldt-Universität zu Berlin, war dort im arbeitskreis kritischer juristinnen und juristen (akj-berlin) aktiv. Seit 2007 Lehrbeauftragter für Staats- und Verwaltungsrecht an der Juristischen Fakultät der HUB, seit 2010 auch an der Hochschule für Wirtschaft und Recht Berlin (Fachbereich 5 – Polizei und Sicherheitsmanagement). Er promoviert mit einem Stipendium der Hans-Böckler-Stiftung bei Prof. Rosemarie Will zur „Sicherheitsrechtsprechung des BVerfG vor und nach dem 11. September 2001“. Kontakt: ploese@rewi.hu-berlin.de

## Anmerkungen:

- 1 BVerfG, Urteil vom 24. April 2013, Az. 1 BvR 1215/07, zitiert nach [http://www.bundesverfassungsgericht.de/entscheidungen/rs20130424\\_1bvr121507.html](http://www.bundesverfassungsgericht.de/entscheidungen/rs20130424_1bvr121507.html), Rn. 232, von dort auch die nachfolgend nicht näher bezeichneten Randnummern = Absatznummern.
- 2 *Horst Herold*, Polizeiliche Datenverarbeitung und Menschenrechte, *Recht und Politik*, S. 79 ff. (80 f.).
- 3 *Hans Magnus Enzensberger*, Geheimnisse der deutschen Demokratie, in: *Kursbuch 56, Unser Rechtsstaat*, 1979, S. 11.
- 4 *Wilhelm Steinmüller* u.a., Grundfragen des Datenschutzes, Technischer Bericht zum Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. VI/3826, Anlage 1, 1971; *ders.*, Der aufhaltsame Aufstieg des Geheimbereichs. Vom Verfassungsstaat zum Sicherheitsstaat, in: *Kursbuch 56*, 1979, S. 169 ff.
- 5 *Herold*, a.a.O. (Anm. 2), S. 81.
- 6 *Martin Kutscha*, Offene Fragen zum Überwachungs-GAU, in: *Vorgänge 204, 4/2013*, S. 89; *Wolf-Dieter Narr*, Wer schützt die Innere Sicherheit? Der Untersuchungsausschuss und die Geheimdienste, *Bürgerrechte & Polizei/CILIP 105* (Mai 2014), S. 3–9 sowie in der selben Ausgabe: *Ben Hayes*, Der bloßgestellte Überwachungsstaat. Der NSA-Skandal und die globale Gegenwehr, S. 44–54.
- 7 BT-Drs. 17/12665 vom 07.03.2013.
- 8 Zur hypothetischen Geschichtsschreibung im Datenschutzrecht sowie der generellen Beschränktheit dieser Methode: *Kai von Lewinski*, Zufall und Notwendigkeit bei der Entstehung des Datenschutzrechts, in: *Andrea Knaut/ Jörg Pohle*, *Foundationes I: Geschichte und Theorie des Datenschutzes*, Münster 2013, S. 13 ff.
- 9 Vgl. nur *Rosemarie Will*, Das Bundesverfassungsgericht und die Anti-Terror-Datei, *vorgänge 201/202* (1/2-2013), S. 102; *Klaus Ferdinand Gärditz*, Urteilsanmerkungen, *JZ 12/2013*, S. 633; *Clemens Arzt*, Antiterrordatei verfassungsgemäß – Trennungsgebot tot?, *NVwZ 2013*, S. 1328; *Thomas Petri*, Anmerkungen zum Urteil vom 24.4.2013, *ZD 2013*, S. 348.
- 10 Treffender noch beschreiben *Alexander Klose* und *Hubert Rottleuthner*, Gesicherte Freiheit, *PROKLA 152* (2008), S. 377 (395) den Gesamtprozess als „Springprozeession“, bei der die Sicherheitspolitiker\_innen parlamentarisch mit neuen Sicherheitsgesetzen „ins verfassungsrechtliche Niemandsland“ vorpreschen, um anschließend in einer Weise von Karlsruhe zurückgepiffen zu werden, die zunächst nur einzelne Punkte betrifft und „den Gesetzgeber zugleich darüber belehr[t], wie er es in Zukunft 'besser' machen kann“, wodurch sich das BVerfG für die Zukunft unnötig selbst binde. So könne dann das „verfassungsrechtlich (gerade noch) 'Mögliche' [...] mit Verweis auf den Karlsruher Segen problemlos 'umgesetzt' werden.“
- 11 Bundesministerium des Innern und Ständige Konferenz der Innenminister und -senatoren der Länder (Hg.): Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus. Zusammenfas-

- sung der Empfehlungen vom 30.04.2013, S. 3; kritisch dazu *Eric Töpfer*, Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei, Policy Paper des Deutschen Instituts für Menschenrechte, Juni 2013, S. 8; *Narr*, a.a.O. (Anm. 6), S. 6 f.
- 12 *Michael Lysander Fremuth*, Wächst zusammen, was zusammengehört? Das Trennungsgebot zwischen Polizeibehörden und Nachrichtendiensten im Lichte der Reform der deutschen Sicherheitsarchitektur, *Archiv öffentlichen Rechts (AöR)* 139 (2014), S. 32–79 (61).
- 13 Zur Verteidigung des Begriffs vgl. *Martin Kutscha*, a.a.O. (Anm. 6), S. 93 mit Verweis auf Art. 18 und 21 Abs. 2 GG sowie die abgewandelte Formel im Urteil des BVerfG zur Vorratsdatenspeicherung, BVerfGE 125, 260 (324), wonach das Gebot, „dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf,“ zur „verfassungsrechtlichen Identität der Bundesrepublik Deutschland“ gehöre.
- 14 Das BVerfG spricht im Volkszählungsurteil selbst von „informationeller Gewaltenteilung“, BVerfGE 65, 1 (69); zu den Konsequenzen *Bernhard Schlink*, *Datenschutz und Amtshilfe*, NVwZ 1986, 249–256.
- 15 Vgl. dazu *Fremuth*, a.a.O. (Anm. 12), S. 35 ff.; weitere Nachweise auch bei *Rosemarie Will*, Der automatisierte Datenaustausch zwischen Polizei und Nachrichtendiensten im Urteil des Bundesverfassungsgerichts zum Antiterrordateigesetz, in: *Jakob Nolte/ Ralf Poscher/ Henner Wolter* (Hrsg.), *Die Verfassung als Aufgabe von Wissenschaft, Praxis und Öffentlichkeit*, Freundesgabe für Bernhard Schlink zum 70. Geburtstag, Heidelberg 2014, S. 429–445 (433), Fn. 17–19.
- 16 *Will*, a.a.O. (Fn. 15), S. 445; vergleichbar *Arzt*, a.a.O. (Anm. 9), S. 1332.
- 17 So jedenfalls die Interpretation bei *Fremuth*, a.a.O. (Anm. 15), S. 37 ff. und 56 ff.
- 18 *Will*, a.a.O. (Fn. 15), S. 429 ff.
- 19 BT-Drs. 16/2950, S. 15; ähnlich auch BT-Drs. 17/8672; kritisch *Thomas Petri*, Die Antiterrordatei, Prototyp für verfassungswidrig ausgestaltete Verbunddateien?, *ZD* 1/2013, S. 3 (5).
- 20 Ähnliche Bedenken bei *R. Will*, a.a.O. (Anm. 9), S. 107.
- 21 Rn. 106; gegen ein Leerlaufen der Angemessenheitsprüfung auch schon im Urteil vom 4. April 2006 (Az. 1 BvR 518/02, Rasterfahndung, BVerfGE 115, 320 (359)): „Aber auch im Rahmen der Abwägung nach Maßgabe des Grundsatzes der Verhältnismäßigkeit im engeren Sinne dürfen staatliche Schutzpflichten nicht dazu führen, dass das Verbot unangemessener Grundrechtseingriffe unter Berufung auf grundrechtliche Schutzpflichten leer läuft, so dass in der Folge allenfalls ungeeignete oder unnötige Eingriffe abgewehrt werden könnten.“
- 22 Dazu *Christoph Gröpl*, *Die Nachrichtendienste im Regelwerk der deutschen Sicherheitsverwaltung*, Berlin 1993, S. 258; *Mark A. Zöller*, *Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten*, Heidelberg 2002, S. 309; *Josef Foschepoth*, *Überwachtes Deutschland*, Göttingen 2012, S. 139.
- 23 A.a.O. (Anm. 12), S. 41 f., 47 f.
- 24 So die treffende Formulierung bei *Gärditz*, a.a.O. (Anm. 9), S. 634.
- 25 *R. Will*, *Vorgänge* 2013, Heft 201/202, S. 102; *C. Arzt*, NVwZ 20/2013, S. 1329.
- 26 Offenbar stößt das BVerfG hier an die Grenzen seiner eigenen Rechtsprechung (z.B. BVerfGE 65, 1 (45); 115, 320 (343 und 351)), die eigentlich eine prozesshafte Analyse des Zusammenwirkens von Datenerhebungs- und -verwertungsnormen geboten hätte; womit es sich indes den Vorwurf gefallen lassen muss, die prognostizierte grundrechtliche Gefährdungslage unter Laborbedingungen festgestellt zu haben, von deren Kontaminationsfreiheit es sich vor Operationsbeginn nicht überzeugt hat.
- 27 BVerfGE 115, 320 (360).
- 28 Stichwort: Hypothetischer Ersatzeingriff; vgl. *Gärditz*, a.a.O. (Anm. 9), S. 635; ausführlich bei *Nikolas Gazeas*, *Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden*, Berlin 2014, S. 232 f.; das ist insoweit nur konsequent, als das BVerfG die im Volkszählungsurteil zu Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entwickelten Maßgaben zunächst auf Art. 10 GG übertragen hatte, vgl. 100, 313 (359); 110, 33 (53).

- 29 Auf diese Einschränkung eines formalen Trennungsgebots verweist *Gärditz*, a.a.O. (Anm. 9), S. 634 (m.w.N.), soweit dieses allein aus den Kompetenzbestimmungen des Staatsorganisationsrechts für den Bund, insbesondere aus Art. 73 Nr. 9a, 10 und 87 Abs. 1 Satz 2 GG, abgeleitet würde. Soweit es jedoch objektiv-rechtlich aus dem Rechtsstaatsprinzip heraus begründet wird, spielt diese Einschränkung freilich keine Rolle; so bspw. bei *Christoph Gusy*, Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, VVDStRL 63 (2004), Berlin 2004, S. 151 ff. (184).
- 30 A.a.O. (Anm. 15), S. 444; noch als undifferenzierte Gleichsetzung mit dem Zweckbindungsgrundsatz, in: *vorgänge*, a.a.O. (Anm. 9), S. 108.
- 31 BVerfGE 65, 1 (45).
- 32 BVerfGE 65, 1 (42); 113, 29 (45 f.); 115, 320 (342).
- 33 BVerfGE 115, 320 (343).
- 34 BVerfGE 100, 313 (376); 107, 299 (320, 328); 115, 320 (351, 354 f.).
- 35 Vgl. *Töpfer*, a.a.O. (Anm. 11), S. 18 sowie die entsprechenden Nachfragen von Bundesverfassungsrichter *Reinhard Geier* an den Präsidenten des Bundesamtes für Verfassungsschutz *Hans-Georg Maaßen* während der Mündlichen Verhandlung am 6.11.2012, wiedergegeben bei *M. Plöse*, Im Datenbackstudio mit Innenminister Friedrich. Das Bundesverfassungsgericht verhandelt über die Antiterrordatei, telepolis vom 08.11.2012: <http://www.heise.de/tp/artikel/37/37967/3.html> (08.11.2014).
- 36 Evaluationsbericht, BT-Drs. 17/12665, S. 5.
- 37 Entsprechend des Tenors: (1.b) Eingrenzung des zu erfassenden Personenkreises auf willentliche Förderer von Aktivitäten, die den Terrorismus unterstützen (§ 2 Satz 1 Nr. 1 b ATDG), (1.e) Streichung der Befürworter von „rechtswidriger Gewalt“ aus dem nach § 2 Satz 1 Nr. 2 zu erfassenden Personenkreis sowie (1.a) Neuordnung der Speicherung der Daten aller Kontaktpersonen nach § 2 Satz 1 Nr. 3 ATDG durch ihre Zuordnung zu den erweiterten Grunddaten von Hauptpersonen nach dem Vorbild von § 3 Abs. 1 Nr. 1 lit. b oo ATDG und deren verdeckte Speicherung (BVerfG, Rn. 165); vgl. die Gesamtübersicht bei *Töpfer*, a.a.O. (Anm. 11), S. 17.
- 38 Eine Koordination von Einzelübermittlungsvorschriften leisten jedoch weder die ATD noch das ATDG.
- 39 Rn. 133 mit Verweis auf BVerfGE 115, 320 (357 f.), wobei sich das BVerfG dort selbstverständlich nicht zu einer Verschiebung der Grenzen des verfassungsrechtlich Zulässigen äußert, sondern den wenig dialektischen Eindruck aufrechtzuerhalten versucht, auch bei einer Gewichteverlagerung in der Verhältnismäßigkeitsabwägung bliebe der verfassungsrechtliche Rahmen des Grundrechtsschutzes unverändert; zur Dialektik der Vorstellung von einem Diesseits und Jenseits der Verfassung vgl. *Steffen Augsberg*, Denken vom Ausnahmezustand her. Über die Unzulässigkeit der anormalen Konstruktion und Destruktion des Normativen, in: ders. u.v.a. (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit, Tagungsband zur 48. Assistententagung Öffentliches Recht, Baden-Baden 2009, S. 17–39.
- 40 *Nikolas Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, Berlin 2014, S. 305 ff.
- 41 Bspw. verweist § 20 Abs. 1 Satz 2 Halbsatz 1 BVerfSchG auf §§ 74a und 120 GVG. Zu den Anforderungen des Gebots der Normenklarheit und Bestimmtheit bei der Verwendung von Verweisungsketten in Polizeigesetzen vgl. das Urteil des Thüringer Verfassungsgerichtshofs vom 21. November 2012 - VerfGH 19/09 -, S. 33 f., 39 und 41 der im Internet abrufbaren Beschlussausfertigung mit Verweis auf BVerfGE 120, 274 (315 ff.); 118, 168 (186 ff.); 110, 33 (52 ff.).
- 42 BVerfGE 115, 320 (361 f.).
- 43 BVerfGE 115, 320 (346).
- 44 In Rn. 151 nimmt die Senatsmehrheit zum Gewaltbegriff von § 2 Nr. 2 ATDG insoweit auch eine verfassungskonforme Reduktion im Lichte der „Zielrichtung der ATD“ dahingehend vor, „dass er nur Gewalt umfasst, die unmittelbar gegen Leib und Leben gerichtet oder durch den Einsatz gemeingefährlicher Mittel geprägt ist.“

- 45 Eine Speicherung in der RED, die hier wohl näher läge, scheidet wegen deren Erfordernis eines unmittelbaren Bezugs zu rechtsextremistisch begründeter Gewalt nach § 2 RED-G wohl eher aus.
- 46 Gazeas geht daher a.a.O. (Anm. 40), S. 327 f. auch konsequent von einem Verstoß gegen das Übermaßverbot aus, das er freilich auch auf § 86a StGB (Verwendung von Kennzeichen verfassungswidriger Organisationen) bezieht, der von § 74a Abs. 1 GVG gar nicht erfasst wird und folglich auch keine Übermittlungspflicht begründet. Eine knappe Auflistung weiterer Verstöße finden sich auch in seinem Thesenpapier zum Fachgespräch der Grünen-Bundestagsfraktion am 4. April 2014 im Deutschen Bundestag, Reader: Polizei | Nachrichtendienste. Trennungsgebot wahren – Bürgerrechte schützen, April 2014, S. 11 (abrufbar im Internet: [http://www.gruene-bundestag.de/uploads/tx\\_ttproducts/datasheet/18-10-Reader-PolizeiNachrichtendienste-web\\_01.pdf](http://www.gruene-bundestag.de/uploads/tx_ttproducts/datasheet/18-10-Reader-PolizeiNachrichtendienste-web_01.pdf)).
- 47 Gazeas, a.a.O. (Anm. 40), S. 13.
- 48 BT-Drs. 18/1565, S. 21 f., zumal die Evaluation der RED noch nicht einmal abgeschlossen ist.