

Deutscher Bundestag
Finanzausschuss

Prof. Dr. Klaus F. Gärditz
Lehrstuhl für Öffentliches Recht

Postanschrift:
Adenauerallee 24-42
53113 Bonn
Tel.: 0228/73-9176
Email: gaerditz@jura.uni-bonn.de

22. November 2019

Geszentwurf der Bundesregierung

Entwurf eines Gesetzes zur Neustrukturierung des Zollfahndungsdienstgesetzes (BT-Drs. 19/12088)

Anhörung des Finanzausschusses am 25. November 2019

Inhalt

I. Hintergrund	2
II. Gesetzgebungskompetenz	2
III. Einzelregelungen.....	3
1. Zollkriminalamt als Sicherheitsbehörde	3
2. Datenverarbeitung	4
a) Allgemeine Anforderungen.....	4
b) Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen	5
c) Datenverwendung zur Identifikation	6
3. Schutz Zeugnisverweigerungs- und Auskunftsberechtigter	6
4. Übermittlungshindernisse.....	8

5. DNA-Identifizierungsmuster von Mitarbeiterinnen und Mitarbeitern.....	9
6. Einsatz von V-Leuten und Verdeckten Ermittlern	9
7. Schutz des Kernbereichs privater Lebensgestaltung	10
8. Reform der Telefonüberwachung	11
IV. Resümee	12

I. Hintergrund

Der Regelungsentwurf des Zollfahndungsdienstgesetzes (ZfdG-E) überträgt – wie bereits im Rahmen der letzten Novellierung des BKAG – die Anforderungen an Eingriffsermächtigungen, die das BVerfG in seiner Entscheidung zum BKAG vom April 2016 formuliert hat, auf den Bereich der Zollfahndung. Zudem war die Richtlinie der EU über die Datenverarbeitung im Bereich von Polizei und Strafverfolgung (RL 2016/680)¹ umzusetzen. Diese Richtlinie, die von der DGSVO nicht erfasste Bereiche der Hoheitstätigkeit erfasst, hat einen funktional definierten Anwendungsbereich. Sie enthält ausweislich Art. 1 Bestimmungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Die Richtlinie richtet sich allgemein an staatliche Stellen (Art. 3 Nr. 7 RL 2016/680), die diese Aufgaben erfüllen, also auch an die Behörden der Zollfahndung. Die meisten der dortigen Anforderungen erfüllte das – nicht unbedingt datenschutzrechtliche unterdeterminierte – deutsche Sicherheitsrecht schon bislang, so auch das ZfdG. Insoweit war der unionsrechtliche Anpassungsbedarf vergleichsweise gering.

Der vorliegende Gesetzentwurf behandelt das Zollkriminalamt (ZKA) konsequent als eine Sicherheitsbehörde des Bundes neben Bundespolizei, BKA, BfV, BSI und BND. In seiner Doppelfunktion als Gefahrenabwehr- und Strafverfolgungsbehörde (vgl. § 52 ZfdG-E) mit Zentralstellenfunktion entspricht das ZKA strukturell und verwaltungsorganisationsrechtlich in vielen Facetten dem BKA. Daher ist folgerichtig, dem ZKA auch analoge Befugnisse zuzuweisen, über die das BKA bereits verfügt. Die vorliegende Novelle gleicht insoweit vor allem die Befugnisse des ZKA dem novellierten BKAG an.

II. Gesetzgebungskompetenz

Der Bund verfügt über eine entsprechende Gesetzgebungskompetenz. Im Kern beruht diese auf Art. 73 Abs. 1 Nr. 5 GG, die auch präventiv-polizeiliche Maßnahmen erfasst.² Soweit das ZKA zugleich zur Aufklärung von Straftaten tätig wird, sichert Art. 74 Abs. 1 Nr. 1 GG die Kompetenz des

¹ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119, S. 89)

² BVerfGE 110, 33 (48).

Bundes flankierend ab. Nicht einschlägig – aber insoweit auch nicht erforderlich – ist die in der Entwurfsbegründung genannte³ Gesetzgebungskompetenz aus Art. 73 Abs. 1 Nr. 10 GG für die internationale Verbrechensbekämpfung, denn diese ist – insoweit in der Regelungsstruktur atypisch – explizit an das Bundeskriminalpolizeiamt gebunden, ermöglicht also eine Zuweisung von Aufgaben an andere und eine Ermächtigung von anderen Behörden nicht. Datenschutzregelungen sind Annex zur jeweiligen Sachgesetzgebungskompetenz.⁴ Die *Verwaltungskompetenz*, die Aufgaben dem ZKA als Bundesoberbehörde zu übertragen, folgt nicht aus Art. 108 Abs. 5 Satz 1 GG. Da es nicht um Finanzverwaltungsvorfahren als solche geht, sondern aus Art. 87 Abs. 3 GG.⁵

III. Einzelregelungen

Im Rahmen der Neufassung des ZfdG werden die meisten Bestimmungen des bislang geltenden Rechts, die sich bewährt haben, fortgeführt. Einige Regelungsansätze sind jedoch neu und tragen den verfassungs- sowie unionsrechtlichen Anforderungen Rechnung. Mehrere Regelungen enthalten im Detail kleinere Anpassungen an die Semantik oder Systematik des Unionsrechts. So führt beispielsweise § 12 Abs. 1 Nr. 2 ZfdG-E die Kategorie der Kontaktpersonen nach Art. 6 lit. d RL 2016/680 ein. § 22 Abs. 1 ZfdG setzt das Gleichbehandlungsgebot nach Art. 9 Abs. 4 RL 2016/680 um. Insoweit bestand grundsätzlich kein Umsetzungsspielraum, es ging vielmehr um notwendige Anpassungen. Die nachfolgende Stellungnahme konzentriert sich daher auf neue und verfassungsrechtlich relevante Regelungen.

1. Zollkriminalamt als Sicherheitsbehörde

§ 3 Abs. 7 Satz 1 Nr. 3 ZfdG-E enthält eine erweiterte Aufgabenzuweisung. Das ZKA verkehrt hier nach als Zentralstelle mit den für den Staatsschutz zuständigen Stellen. Dies stärkt die Funktion des ZKA als Sicherheitsbehörde. Das Amt wird hierdurch in die „Bekämpfung des Terrorismus und des Extremismus“ einbezogen.⁶ Insoweit wird klargestellt, dass auch das ZKA in den Datenaustausch mit anderen Sicherheitsbehörden integriert wird, was im Übrigen sektorspezifisch im Rahmen der Antiterrordatei schon bislang der Fall war (§ 1 Abs. 1 ATDG). Es ist sinnvoll, das sicherheitsbehördliche Aufgabenprofil klar zu regeln und damit die Bedeutung der Zollfahndung für den Schutz der inneren Sicherheit gegenüber grenzüberschreitenden Gefährdungen hervorzuheben. Möglicherweise sollte jedoch an die Stelle des – im Bundesrecht im Übrigen grundsätzlich nicht gebräuchlichen – Begriff des Staatsschutzes eine Benennung der beteiligten Behörden erfolgen (Vorbild § 1 Abs. 1 ATDG). Die amtliche Begründung führt hier lediglich die einschlägigen Polizeibehörden des Bundes und der Länder an,⁷ jedoch erfasst der materielle Staatsschutz auch andere Behörden, jedenfalls den Generalbundesanwalt (vgl. Art. 96 Abs. 5 Nr. 5 GG) sowie die Nachrichtendienste des Bundes und der Länder.

³ BT-Drs. 19/12088, S. 77.

⁴ BT-Drs. 19/12088, S. 77.

⁵ BVerfGE 110, 33 (47 f.).

⁶ BT-Drs. 19/12088, S. 14.

⁷ BT-Drs. 19/12088, S. 14.

2. Datenverarbeitung

Das BVerfG hat in seiner Entscheidung vom 20. April 2016⁸ die Anforderungen an die Datennutzung konsolidiert und präzisiert. Dem trägt der Entwurf des ZfdG nunmehr Rechnung.

a) Allgemeine Anforderungen

Der Gesetzgeber kann nach der Rechtsprechung eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus als weitere Nutzung im Rahmen der ursprünglichen Zwecke dieser Daten erlauben. Er kann sich insoweit auf die der Datenerhebung zugrundeliegenden Rechtfertigungsgründe stützen und unterliegt damit nicht den – qualifizierten – verfassungsrechtlichen Anforderungen an eine Zweckänderung. Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung, die zuständige Stellen und Zweck der Datenerhebung konkret festlegt. „Eine weitere Nutzung innerhalb der ursprünglichen Zwecksetzung kommt damit nur seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter in Betracht wie für die Datenerhebung maßgeblich: Ist diese nur zum Schutz bestimmter Rechtsgüter oder zur Verhütung bestimmter Straftaten erlaubt, so begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine zulässige Zweckänderung eine weitergehende Nutzung erlaubt“.⁹

Dementsprechend kommt es nach dem BVerfG für die Wahrung der Zweckbindung letztlich darauf an, dass die erhebungsberechtigte Behörde die Daten „im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt, wie es die jeweilige Datenerhebungsvorschrift erlaubt“. Diese – nicht allzu hoch angesiedelten – Anforderungen sind erforderlich, aber grundsätzlich auch ausreichend, um eine weitere Nutzung der Daten im Rahmen der Zweckbindung als verhältnismäßig zu rechtfertigen.¹⁰ An diese Vorgaben schließt die Neufassung des ZfdG an, indem es im allgemeinen Teil vor die Klammer gezogen eine Generalklausel stellt, die die Reichweite der Zweckbindung allgemein festschreibt. Das ZKA kann nach § 8 Abs. 2 ZfdG-E – vergleichbar § 12 Abs. 2 BKAG – personenbezogene Daten, die es selbst erhoben hat, weiterverarbeiten (1.) zur Erfüllung derselben Aufgabe und (2.) zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten, wie es die jeweilige Erhebungsvorschrift erlaubt. Eine im Rahmen der Verhältnismäßigkeit grundsätzlich zulässige Zweckänderung – sprich: eine Nutzung zu gemessen hieran anderen Zwecken als denen der Erhebung – setzt eine spezifische Ermächtigung voraus, was § 8 Abs. 3 Satz 1 ZfdG-E klarstellt. Höhere Anforderungen sind nach der Rechtsprechung des BVerfG lediglich an die Zweckänderung bei einer Nutzung von Daten, die aus besonders eingriffsintensiven Maßnahmen stammen, zu stellen, die nur unter qualifizierten Voraussetzungen zulässig sein sollen (dazu sogleich). Dies wird durch § 8 Abs. 3 Satz 2 ZfdG-E klargestellt.

Letztlich sind die Regelungen in § 8 Abs. 2-3 ZfdG-E *rein deklaratorisch*, erfüllen aber insoweit eine sachgerechte Bündelungsfunktion, weil hier die allgemeinen Prinzipien hinter den im Einzelnen ausdifferenzierten Spezialeingriffsermächtigungen transparent gemacht werden. Eine solche Generalklausel

⁸ BVerfGE 140, 220 ff.

⁹ BVerfGE 140, 220 (324 f.).

¹⁰ BVerfGE 140, 220 (325).

ist verfassungsrechtlich ausreichend, weil sich die einzelnen Anforderungen an die Datenerhebung aus den jeweiligen besonderen Ermächtigungsgrundlagen des Gesetzes ergeben, die dann auch die Reichweite der Datennutzung determinieren sowie die hinreichende Bestimmtheit von Inhalt und Grenzen legaler Datennutzung sicherstellen. Konkretisierungen finden sich z. B. in § 26 Abs. 4 ZfdG-E.

b) Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen

Für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen hat das BVerfG qualifizierte Anforderungen entwickelt. Entsprechend dem Gedanken des hypothetischen Ersatzeingriffs,¹¹ der im Kern ein Umgehungsverbot ist,¹² kommt es darauf an, ob die entsprechenden Daten nach verfassungsrechtlichen Maßstäben fiktiv auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften.¹³ Solche eingriffsintensiven Maßnahmen im Sinne der Rechtsprechung des BVerfG sind im Rahmen des vorliegenden Gesetzes Datenerhebungen nach

- § 47 ZfdG-E bzw. § 62 ZfdG-E (Datenerhebungen mit besonderen technischen Mitteln, längerfristige Observation, Einsatz von V-Leuten und Verdeckten Ermittlern zur Gefahrenabwehr bzw. als Sicherungs- und Schutzmaßnahmen);
- § 72 ZfdG-E (Überwachung von Telekommunikation, Brief- und Postverkehr);
- § 77 ZfdG-E (Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten) und
- § 78 ZfdG-E (Identifizierung und Lokalisierung von Mobilfunkkarten und Telekommunikationsendgeräten).

Konsequenterweise unterwirft daher die ausführliche Regelung zur Datenverarbeitung in § 27 ZfdG-E die Weiterverarbeitung von Daten, die aus solchen Eingriffen erlangt wurden, zu *anderen* als in der jeweiligen Erhebungsvorschrift genannten Zwecken den strikten Anforderungen einer hypothetischen Datenneuerhebung, indem entsprechend hohe Hürden errichtet werden, unter denen dann aber auch eine Primärerhebung zulässig wäre. Insoweit handelt es sich jeweils um vergleichbar gewichtige Rechtsgüter und im Übrigen auch um eine abstrakt vergleichbare Schutzrichtung. Insoweit trägt die Neuregelung den Anforderungen des BVerfG vollumfänglich Rechnung.¹⁴ Auch das Kriterium der drohenden Gefahr (§ 27 Abs. 1 Satz 1 Nr. 2 b ZfdG-E) ist verfassungskonform, sofern eine hinreichende Konkretisierung des Schutzgutes erfolgt,¹⁵ was hier der Fall ist. Besondere gesetzliche Bestimmungen, die die Weiterverarbeitung von personenbezogenen Daten ausdrücklich erlauben, bleiben nach § 27 Abs. 1 Satz 2 ZfdG-E unberührt; die wichtigste Spezialregelung findet sich in der Übermittlungsbestimmung des § 76 ZfdG-E.¹⁶

¹¹ Vgl. §§ 161 Abs. 2, 477 Abs. 2 Satz 2 StPO; BFHE 215, 12 Rn. 94; BGHSt 58, 32 Rn. 30; 62, 123 Rn. 38; BGH, Urt. v. 12.12.1996 – 4 StR 499/96, NStZ 1997, 294; Böse, Wirtschaftsaufsicht und Strafverfolgung, 2005, S. 312 f.; Kelnhofer, Hypothetische Ermittlungsverläufe im System der Beweisverbote, 1994, S. 177 ff.; Schnarr, Die Verwendung präventiv erhobener Daten zu repressiven Zwecken, StraFo 1998, 217 ff.; Veltien, Verkehrsdaten in der Strafverfolgung, in: FS Gerhard Fezer, 2008, S. 89 (92 f.).

¹² Vgl. BVerfGE 130, 1 (34).

¹³ BVerfGE 141, 220 (327 f.).

¹⁴ BT-Drs. 19/12088, S. 97.

¹⁵ Vgl. BVerfGE 141, 220 (272).

¹⁶ Vgl. BT-Drs. 19/12088, S. 115.

c) Datenverwendung zur Identifikation

Eine Ergänzung stellt die Verwendung von Personendaten zur Identifikation nach § 27 Abs. 2 ZfdG-E dar. Diese (§ 12 Abs. 4 BKAG vergleichbare) Regelung, die an enge Voraussetzungen gebunden ist, soll vornehmlich Identitätsverwechslungen verhindern,¹⁷ schützt also nicht nur öffentliche Ermittlungsinteressen, sondern letztlich auch Rechte unbeteiligter Dritter. Verfassungsrechtlich ist die Regelung unbedenklich. Selbst wenn es um Daten gehen sollte, die im Zusammenhang mit schwerwiegenden Grundrechtseingriffen gewonnen wurden, sind nur *Personendaten* (§ 11 Abs. 2 Nr. 1 lit. a bzw. § 31 Abs. 2 Nr. 1 lit. a ZfdG-E) betroffen, aus denen sich über die Identifikation hinaus keine weiteren grundrechtsrelevanten Schlüsse ziehen lassen. Auf die bloße Identifikation lassen sich auch die qualifizierten Anforderungen, die das BVerfG an Zweckänderungen angelegt hat, nach Sinn und Zweck nicht übertragen.

3. Schutz Zeugnisverweigerungs- und Auskunftsberechtigter

§ 9 Abs. 3 Satz 1 ZfdG-E erklärt die Bestimmungen über Zeugnis- und Auskunftsverweigerungsrechte nach den §§ 52-55 StPO auf Auskunftsverweigerungen gegenüber der Zollfahndung für entsprechend anwendbar. Eine Ausnahme enthält § 9 Abs. 3 Satz 2 ZfdG-E, soweit die Auskunft zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist. Eine Rückausnahme hiervon sieht wiederum Satz 3 für bestimmte Berufsgeheimnisträger nach § 53 Abs. 1 Satz 1 Nr. 1-3, 4 StPO vor (vereinfacht: Geistliche, Verteidiger, Rechtsberater, Ärzte, Apotheker, Psychotherapeuten, Parlamentarier).

a) Verfassungsrechtliche Bewertung

Die Gefahr einer zwangsweisen Instrumentalisierung des Beschuldigten/Betroffenen gegen sich selbst lässt sich indes durch Beweistransferverbote in andere Verfahren ausschalten, sodass es nicht notwendigerweise eines universellen Auskunftsverweigerungsrechts auch in nichtstrafrechtlichen Verfahren bedarf. Die Rücksichtnahme auf die Subjektstellung des Zeugen und seine Grundrechte begründet keinen generellen Anspruch, „vor Konflikten und Beeinträchtigungen bewahrt zu werden, die aus seiner Zeugnispflicht herrühren können [...]“. Diese müssen vielmehr in einem der Bedeutung des beeinträchtigten Grundrechts angemessenen Verhältnis zu dem mit der Zeugnispflicht verfolgten Ziel stehen.¹⁸ Richtigerweise ist der Anwendungsbereich des Nemo-tenetur-Grundsatzes zudem auf das Strafverfahren zu beschränken und von verfahrensübergreifenden informationellen Abwehrrechten freizuhalten.¹⁹ Auch das BVerfG hat zutreffend einem absoluten Schutz der Freiheit vor Zwang zur Selbstbelastung jenseits von Strafverfahren eine Absage erteilt. In der Gemeinschuldnerentscheidung²⁰ stellt das Gericht maßgeblich auf die zentrale und unentbehrliche Informantenrolle des Gemeinschuldners ab, die zu einer Auskunftspflicht führe. Grundrechte bildeten – so das Gericht mit Recht – keinen lückenlosen Schutz gegen Selbstbezeichnung; vielmehr sei der Persönlichkeitsschutz im Rahmen des Zumutbaren einer Relativierung zum Schutz anderer verfassungsrechtlicher Güter zugänglich. Der Auskunftspflichtige müsse aber davor bewahrt werden, dass eine in einem anderen (z. B. administrativen) Verfahren

¹⁷ BT-Drs. 19/12088, S. 97.

¹⁸ BVerfG-K, Beschl. v. 25. 1. 2007, 2 BvR 26/07, NJW 2007, 1865 (1867), Rn. 16.

¹⁹ Böse, Wirtschaftsaufsicht und Strafverfolgung, 2005, S. 149 ff., 181 ff., 198 f.

²⁰ BVerfGE 56, 37 (48 ff.).

erzwungene Auskunft in einem Strafverfahren gegen ihn verwertet würde. Dem trägt hier § 9 Abs. 3 Satz 5 ZfdG angemessene Rechnung. Dieser stellt klar, dass verpflichtende Auskünfte nur zu dem in Satz 2 genannten Zweck – sprich: zur Abwehr schwerwiegender Gefahren – verwendet werden dürfen. Eine strafprozessuale Verwertung schließt dies aus.²¹ Insoweit wirkt § 9 Abs. 3 Satz 5 ZfdG zugleich als gesetzliches Beweisverwertungsverbot.

b) Rechtspolitische Kritik

Stellt sich die Begrenzung des Auskunftsverweigerungsrechts mithin als verfassungskonform dar, stellt sich *rechtspolitisch* allerdings die Frage, ob die Rückausnahmen nach § 9 Abs. 3 Satz 3 ZfdG nicht zu weit gefasst sind. Dass etwa die Vertraulichkeit des Arzt-Patienten- oder des Rechtsberatungsverhältnisses höher gewichtet wird als Leib und Leben Gefährdeter, vermag nicht einzuleuchten. Unter den erfassten Berufsgeheimnisträgern kommt allein den Verteidigern nach § 53 Abs. 1 Satz 1 Nr. 2 StPO ein besonders qualifizierter Schutz zu, weil diese die in der Menschenwürde wurzelnde Subjektstellung der Beschuldigten im Strafprozess zu wahren haben.²² Insoweit besteht aber bereits durch das Verwertungsverbot des § 9 Abs. 3 Satz 5 ZfdG hinreichender Schutz. Dass beispielsweise eine Apothekerin auch dann keine Auskünfte über die Beratung ihrer Kunden erteilen muss, wenn die Information zur Abwehr einer Gefahr für Leib und Leben benötigt wird, überzeugt nicht, zumal wenn man mögliche Schutzpflichten des Staates für die bedrohten Rechtsgüter mitberücksichtigt.

Ebenfalls zu weitgehend erscheint das Verwertungsverbot nach § 9 Abs. 3 Satz 5 ZfdG, sofern die potentiell zu erlangenden Informationen einen Beschuldigten im Strafverfahren *entlasten* können. Die strafprozessuale Verwertung zugunsten Beschuldigter generell auszuschließen, dürfte sich als unangemessene Beschränkung des – gerade auch Angeklagte schützenden – Auftrags der Strafgerichte erweisen, die materielle Wahrheit zu ermitteln²³. Nicht zuletzt das BVerfG hat mit Recht einseitigen Beweisverwertungsverboten einen Riegel vorgeschoben, weil auch den Belangen einer funktionstüchtigen Strafrechtspflege und einer möglichst vollständigen Wahrheitsermittlung im Strafprozess angemessene Rechnung zu tragen sei.²⁴ Dies muss gerade für die Verwertung von Erkenntnissen aus rechtmäßigen Maßnahmen der Gefahrenabwehr gelten, weil diese dazu dienen, konkret bedrohte Rechtsgüter gegen Beeinträchtigungen zu schützen.

Insgesamt empfiehlt es sich nicht, die dem Strafprozess und seiner hohen Formalisierung Rechnung tragenden §§ 52 ff. StPO unmodifiziert auf Maßnahmen der Gefahrenabwehr zu übertragen, weil im letzteren Fall das bedrohte Schutzgut (anders als bei der retrospektiven Straftataufklärung) noch gerettet werden kann und daher hier dem Gesetzgeber wesentlich weitere Gestaltungsspielräume zukommen.²⁵ Auch das BVerfG geht im präventiv-polizeilichen Bereich nicht von der Notwendigkeit eines strikten Schutzes von Vertrauensverhältnissen aus, sondern akzeptiert die Möglichkeit, diesen nach Maßgabe von Güterabwägungen zu relativieren, wenn hinreichend gewichtige Gemeinwohlbelange auf

²¹ BT-Drs. 19/12088, S. 88.

²² BVerfGE 109, 279 (318 f., 322); 129, 208 (263 ff.).

²³ Hierzu BVerfGE 133, 168 (199); 140, 317 (344).

²⁴ BVerfGE 130, 1 (26 f.).

²⁵ Eingehend *Würtenberger/Schenke*, Der Schutz von Amts- und Berufsgeheimnis im Recht der polizeilichen Informationserhebung, JZ 1999, 548 ff. Siehe vertiefend hierzu auch *Shirvani*, Präventiv-polizeiliche Datenerhebung und der Schutz besonderer Vertrauensverhältnisse, ZG 2011, 45 ff.

dem Spiel stehen.²⁶ Das BVerfG hat die Privilegierung der Strafverteidiger gegenüber anderen Rechtsbeiständen auch nur insoweit für verfassungswidrig erachtet, als diese Differenzierung im Rahmen von Gefahrenabwehrmaßnahmen nicht plausibel war,²⁷ hat aber keine allgemeinen Anforderungen an das Schutzniveau im präventiv-polizeilichen Bereich formuliert. Die damit bestehenden Gestaltungsmöglichkeiten sollte der Gesetzgeber nutzen. Es würde daher nahe liegen, Auskunftsverweigerungsrechte im Bereich der Gefahrenabwehr grundsätzlich unter dem Abwägungsvorbehalt mit höherrangigen Interessen der Gefahrenabwehr zu stellen und nur einen Kernbereich der persönlichen Lebensgestaltung absolut zu schützen. Das *nemo tenetur*-Prinzip lässt sich durch strafprozessuale Verwertungsverbote angemessen sichern.

Entsprechendes gilt dann auch für den zu umfassenden und undifferenzierten Schutz Zeugnisverweigerungsberechtigter nach § 82 ZfdG-E. Namentlich der nach Abs. 1 vermittelte absolute Schutz ist nicht gerechtfertigt. Wenn es namentlich um die Abwehr von konkreten Gefahren für Leben, Gesundheit oder Freiheit geht, kann z. B. das Vertrauensverhältnis des Störers zu einem Arzt oder Anwalt keinen absoluten Vorrang beanspruchen.²⁸ Sachgerechter wäre es, wie im Rahmen Kollateralbetroffener nach Abs. 2 den Schutz von Vertrauensverhältnissen grundsätzlich unter Abwägungsvorbehalt zu stellen, jedenfalls wenn es um den Schutz hochrangiger Rechtsgüter oder institutioneller Bestandsinteressen des Staates geht.

4. Übermittlungshindernisse

Die §§ 22, 23 ZfdG erlauben auch die Datenübermittlung an Behörden eines anderen EU-Mitgliedstaats sowie im internationalen Bereich. Dies ist notwendig, weil sich eine sicherheitsbehördliche Aufgabenerfüllung – zumal im grenzüberschreitenden Portfolio des ZKA – nicht sinnvoll ohne europäische und internationale Zusammenarbeit verwirklichen lässt. Auch in anderen Regelungsbereichen des Sicherheitsrechts wurde daher die europäische und internationale Kooperation zunehmend verrechtlicht sowie institutionell grundiert (Vgl. § 26 BNDG, §§ 22b, 22c BVerfSchG, §§ 3, 26, 27BKAG), was einerseits eine Ermächtigungsfunktion erfüllt, andererseits aber Kooperation auch in rechtsstaatliche Bahnen lenkt.

Das BVerfG hat mit Recht einen angemessenen Schutz rechtsstaatlicher Standards sowie gesetzliche Kooperationsschranken gefordert, falls im Empfängerstaat Menschenrechtsverletzungen zu besorgen sind. „Zwingend auszuschließen“ sei jedenfalls die Datenübermittlung an Staaten, „wenn zu befürchten ist, dass elementare rechtsstaatliche Grundsätze verletzt werden [...]. Keinesfalls darf der Staat seine Hand zu Verletzungen der Menschenwürde reichen“.²⁹ Dies ist mit Blick auf die nach Art. 23 Abs. 1 Satz 3 i. V. mit Art. 79 Abs. 3 GG unverfügbaren Mindestanforderungen, die aus der Menschenwürde und dem Rechtsstaatsprinzip folgen, im Konfliktfalls sogar gegen unionsrechtliche Verpflichtungen

²⁶ BVerfGE 141, 220 (318 f.).

²⁷ BVerfGE 141, 220 (319).

²⁸ Droht beispielsweise die illegale Ausfuhr von Dual-Use-Gütern oder Kriegswaffen, die im Zielgebiet den Tod von unzähligen Menschen verursachen können, und konsultiert der Exporteur hierbei einen Rechtsanwalt, dann ist es verfassungsrechtlich sicherlich nicht geboten, das Vertrauensverhältnis mit absolutem Schutz zu armieren und hierdurch eine Vielzahl von Opfern in Kauf zu nehmen.

²⁹ BVerfGE 141, 220 (342).

aufrechtzuerhalten.³⁰ Entsprechendes anerkennt im Übrigen Art. 38 Abs. 2 RL 2016/680 eher general-klauselartig hinsichtlich einer Übermittlung an Drittstaaten.

Diesen Anforderungen trägt § 24 ZfdG Rechnung. Abs. 1 enthält hierbei eine Konkretisierung der Verhältnismäßigkeit, der Datenübermittlungen im Inland, innerhalb der EU sowie an Drittstaaten generell unterliegen. Da insoweit alle Übermittlungen gleichbehandelt werden, steht die Regelung mit Art. 9 Abs. 4 RL 2016/680 in Einklang. § 24 Abs. 2 ZfdG-E enthält Übermittlungsbeschränkungen, die nur für Übermittlungen in EU-Mitgliedstaaten (§ 22 ZfdG-E) oder Drittstaaten (§ 23 ZfdG-E) gelten. In Bezug auf Drittstaaten liegen diese Beschränkungen im Rahmen der Art. 35 ff. (namentlich der Art. 37, 38) RL 2016/680. In Bezug auf EU-Mitgliedstaaten liegt insoweit allerdings eine nicht-äquivalente Beschränkung vor, die Art. 9 Abs. 4 RL 2016/680 eigentlich ausschließt. Hierbei ist indes zu beachten, dass die Übermittlungshindernisse entweder – aus anderem Grund – auch im Inland unterbleiben würde (Gefährdung wesentlicher Sicherheitsinteressen von Bund und Ländern oder von Leib, Leben und Freiheit nach Nr. 1-2; Verletzung geltenden Rechts Nr. 4) oder es um Gefahren geht, die überhaupt erst in einem grenzüberschreitenden Zusammenhang entstehen können, etwa Beeinträchtigungen wesentlicher Sicherheitsinteressen von Bund und Ländern dadurch, dass eine geheimhaltungsbedürftige Information nicht mehr beherrscht werden kann. Richtigerweise schließt Art. 9 Abs. 4 RL 2016/680 solche Vorbehalte zugunsten staatlicher Integritätsinteressen – auch im Lichte von Art. 4 Abs. 2 EUV – nicht aus. Der Schutz der menschenrechtlichen Mindestanforderungen bei Übermittlungen in EU- oder Drittstaaten gewährleistet schließlich § 24 Abs. 2 Nr. 5 ZfdG.³¹

5. DNA-Identifizierungsmuster von Mitarbeiterinnen und Mitarbeitern

§ 17 ZfdG enthält eine Bestimmung, wonach das ZKA von Mitarbeiterinnen und Mitarbeiter, die mit Aufgaben der Spurensicherung betraut sind, DNA-Identifizierungsmustern zur Erkennung von DNA-Trugspuren nehmen und speichern kann. Die Bestimmung entspricht der Parallelnorm in § 24 BKAG. Die Norm ist eine Reaktion auf einen spektakulären Ermittlungsfehler („Phantom von Heilbronn“),³² der dadurch aufgetreten ist, dass identische DNA-Spuren an verschiedensten Tatorten verschiedenster – miteinander nicht im Zusammenhang stehender – Taten gefunden wurden, die letztlich bereits in den zur Probenentnahme verwendeten Wattestäbchen vorhanden waren und von einer Mitarbeiterin der Herstellung stammten. Zwar greift eine entsprechende Verpflichtung in das Allgemeine Persönlichkeitsrecht (Art. 1 Abs. 1 i. V. mit Art. 2 Abs. 1 GG) ein. Der Eingriff ist jedoch zu rechtfertigen, namentlich verhältnismäßig, weil die Verwendung der Daten strikt begrenzt wird und ausschließlich der Vermeidung von – ggf. fatalen – Ermittlungsfehlern dient, die ein besonderes Risiko in den labornahen Ermittlungsbereichen betrifft.

6. Einsatz von V-Leuten und Verdeckten Ermittlern

§ 47 Abs. 2 ZfdG regelt besondere – eingriffsintensive – Datenerhebungen zur heimlichen Überwachung neu und passt diese den Anforderungen der verfassungsgerichtlichen Rechtsprechung an. Er-

³⁰ Vgl. BVerfGE 140, 317 (347).

³¹ Vgl. BT-Drs. 19/12088, S. 95.

³² BT-Drs. 19/12088, S. 90 f.

möglicht wird auch der als unerlässlich für die Ermittlungsarbeit bewertete³³ Einsatz von V-Leuten und Verdeckten Ermittlern (§ 47 Abs. 2 Nr. 3-4 ZfdG-E). Dies folgt einem allgemeinen Trend zur Verrechtlichung (vgl. §§ 9a, 9b BVerfSchG³⁴). Die Voraussetzungen des Einsatzes sind hinreichend genau geregelt und genügen sowohl den rechtsstaatlichen Bestimmtheitsanforderungen als auch den verfassungsrechtlich gemessen an der potentiellen Eingriffsintensität gebotenen rechtsstaatlichen Eingriffsschwellen.

- Zu begrüßen ist, dass hierbei die Handlungsmöglichkeiten *Verdeckter Ermittler* – in Konkordanz zu § 45 Abs. 6 BKAG – in § 47 Abs. 3 ZfdG-E konkreter geregelt werden, weil insoweit hierüber lange Zeit Rechtsunsicherheit bestand. Nunmehr werden Handlungsbefugnisse und Einsatzgrenzen genauer festgelegt, wobei die Norm zugleich der lebensweltlichen Vielfalt möglicher Einsatzstrategien Rechnung trägt und auf unnötige Detailfestlegungen verzichtet.
- Eine nähere Umschreibung des Einsatzes der *Vertrauenspersonen* bedurfte es hingegen nicht, weil es sich hierbei um Private handelt, die durch ihre Anwerbung weder mit Hoheitsbefugnissen ausgestattet werden noch Sonderrechte erhalten. Für den mit V-Personen einhergehenden schlichten Informationsabfluss reicht die Ermächtigungsgrundlage des § 47 Abs. 2 Nr. 3 ZfdG-E vollständig aus.

Die richterliche Anordnung nach § 48 ZfdG-E entspricht den vom BVerfG formulierten Anforderungen,³⁵ Grundrechtsschutz durch Verfahren mittels einer präventiven Kontrolle durch eine unabhängige Stelle sicherzustellen.

7. Schutz des Kernbereichs privater Lebensgestaltung

Durchgängig wird bei heimlichen Überwachungsmaßnahmen der Schutz des Kernbereichs der privater Lebensgestaltung gewährleistet, durch § 49 ZfdG-E für besondere Datenerhebungen, durch § 73 ZfdG-E für die Überwachung der Telekommunikation sowie des Brief- und Postverkehrs. Dieser Kernbereichsschutz soll sicherstellen, dass Maßnahmen durch ihre potentielle Eindringtiefe in die Privatsphäre nicht die Menschenwürde (Art. 1 Abs. 1 GG) verletzen,³⁶ und wurde in der Rechtsprechung des BVerfG ausgeformt.³⁷ Hierzu gehört nach der Rechtsprechung die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, namentlich im Rahmen der nichtöffentlichen Kommunikation mit Personen des höchstpersönlichen Vertrauens.³⁸ Aufgrund der potentiellen Vielgestaltigkeit und Situationsabhängigkeit des zu schützenden Kernbereichs ist es trotz der Eingriffsintensität zulässig, entsprechende Auffangvorschriften – wie auch hier – als Generalklausel auszugestalten. Da sich ungeachtet aller

³³ BT-Drs. 19/12088, S. 102.

³⁴ Vgl. zur dortigen Novelle *Bergemann*, Die Freiheit im Kopf? – Neue Befugnisse für die Nachrichtendienste, NVwZ 2015, 1705 ff.; *Marschollock*, Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, NJW 2015, 3611 ff.

³⁵ BVerfGE 141, 220 (275).

³⁶ Zur Struktur vertiefend *Barrot*, Der Kernbereich privater Lebensgestaltung, 2012; *Dammann*, Der Kernbereich der privaten Lebensgestaltung, 2011; *Reichert*, Der Schutz des Kernbereichs privater Lebensgestaltung in den Polizeigesetzen des Bundes und der Länder, 2015; *Warntjen*, Heimliche Zwangsmaßnahmen und der Kernbereich privater Lebensgestaltung, 2007.

³⁷ BVerfGE 109, 279 (280f., 325ff.); 113, 248 (389 ff.); 120, 274 (335 ff.); 129, 208 (245 ff.); 130, 1 (2); 141, 220 (276 ff.).

³⁸ BVerfGE 141, 220 (276).

Sorgfalt bei der Strukturierung einer Überwachungsmaßnahmen „Zufallstreffer“ innerhalb des Kernbereichs nicht ausschließen lassen, sind Verwertungsverbot und Löschungspflicht konsequent. Dass die Prüfung, ob ein entsprechender Sachverhalt betroffen ist, bereits die Kenntnisnahme durch eine mit der Sichtung betraute Person einschließen wird, ist unvermeidbar und im Interesse des prozeduralen Menschenwürdeschutzes aufgrund des hohen Ranges der durch den Eingriff zu schützenden Rechtsgüter hinzunehmen.³⁹ Der besonderen Sensibilität wird insoweit dadurch Rechnung getragen, dass die Auswertung in Zweifelsfällen einem unabhängigen Richter anvertraut wird (§ 49 Abs. 1 Sätze 3-5 bzw. § 73 Abs. 1 Sätze 3-5 ZfdG-E). Bei Gefahr in Verzug ist ausnahmsweise eine Verwertung auf Anordnung der Leitung des ZKA vorläufig möglich, die gerichtliche Kontrolle aber nachzuholen (§ 49 Abs. 2 bzw. § 72 Abs. 2 ZfdG-E). Möglicherweise wäre es sinnvoll, an dieser Stelle klarzustellen, dass sich der zuständige Richter ungeachtet der extremen Sensibilität zur Auswertung auch sachverständiger Hilfspersonen bedienen kann, wenn dies für eine wirksame Kontrolle erforderlich ist, etwa zur technischen Aufbereitung oder sprachlichen Unterstützung, soweit eine Aufbereitung der Daten durch das ZKA noch nicht hinreichend erscheint. Bei Löschungen erfolgt eine Dokumentation, die die gebotene Datenschutzkontrolle (§ 84 ZfdG) ermöglicht, aber die mit dem Eingriff einhergehende Rechtsgutsbeeinträchtigung nicht unnötig perpetuiert (§ 49 Abs. 1 Sätze 6-7 bzw. § 73 Abs. 1 Sätze 6-7 ZfdG). Insgesamt schlägt der Entwurf eine verfassungskonforme Regelung vor, die den Leitplanken der Rechtsprechung des BVerfG folgt.

8. Reform der Telefonüberwachung

Die Eingriffsschwellen der präventiven Telefonüberwachung im Rahmen des § 72 Abs. 1 ZfdG wurden den Anforderungen der Rechtsprechung des BVerfG⁴⁰ angepasst. Hiernach bedarf es bei Maßnahmen zur Straftatenverhütung „zumindest einer auf bestimmte Tatsachen und nicht allein auf allgemeine Erfahrungssätze gestützten Prognose, die auf eine konkrete Gefahr bezogen ist. Grundsätzlich gehört hierzu, dass insoweit ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist“.⁴¹ Dem tragen die differenzierten Schwellen des § 72 Abs. 1 Nr. 1 und Nr. 2 ZfdG Rechnung.

§ 72 Abs. 3 ZfdG-E führt die Möglichkeit einer *Quellen-TKÜ* ein, die angesichts der Fortentwicklung der Kommunikationstechniken – nicht zuletzt der Verschlüsselung – für die praktische Ermittlungsarbeit oftmals unverzichtbar geworden ist. Eine Quellen-TKÜ führt letztlich keine inhaltlich neue Überwachung ein, sondern versucht vielmehr lediglich durch einen anderen ermittlungstechnischen Ansatz mit der technischen Entwicklung Schritt zu halten und die bisherige Option einer Telefonüberwachung überhaupt noch praktisch aufrechtzuerhalten. Das sah auch das BVerfG in seiner Entscheidung zu einer entsprechenden Regelung des BKAG so: „Die Vorschrift hat damit lediglich die Aufgabe, den technischen Entwicklungen der Informationstechnik zu folgen und – ohne Zugriff auf weitere inhaltliche Informationen des informationstechnischen Systems – eine Telekommunikationsüberwachung auch dort zu ermöglichen, wo dies mittels der alten Überwachungstechnik nicht mehr möglich ist. Von daher ist sie nicht am Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informations-

³⁹ Vgl. BVerfGE 113, 348 (392).

⁴⁰ Vgl. BVerfGE 141, 220 (272 f., 290 f.).

⁴¹ BVerfGE 141, 220 (291).

technischer Systeme, sondern an Art. 10 Abs. 1 GG zu messen“.⁴² Das Gericht hat diese Erweiterung aufgrund des unmittelbaren Zugriffs auf die Endgeräte zwar als schwerwiegenden Eingriff bewertet, aber eine Rechtfertigung bei entsprechender Wertigkeit der Schutzgüter für möglich erachtet, solange eine Maßnahme an Eingriffsschwellen der Gefahrenabwehr gebunden bleibt.⁴³ Diesem Erfordernis wird im Rahmen des § 72 Abs. 3 ZfdG-E aber schon dadurch Rechnung getragen, dass die in Abs. 1 erfassten Maßnahmen entsprechende Eingriffsschwellen ganz allgemein – also auch für die traditionelle TKÜ – vorsehen. Auch die Erstreckung auf Nachrichtensmittler im Rahmen des § 72 Abs. 4 ZfdG-E⁴⁴ ist gemessen an der Rechtsprechung des BVerfG⁴⁵ zulässig.

Ergänzende – verfassungskonforme – Eingriffsermächtigungen enthalten die §§ 77, 78 ZfdG-E betreffend die Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten und die Identifizierung und Lokalisierung von Mobilfunkkarten und Telekommunikationsendgeräten.

Im Übrigen schreiben die Regelungen bei der früheren Rechtslage fort und sind unproblematisch. Teilweise geht es um niederschwellige Eingriffe wie die Bestandsdatenauskunft (§ 10, 30 ZfdG), die mit Blick auf die geringe Eingriffsintensität einerseits und die Notwendigkeit für eine angemessene Aufgabenerfüllung der Zollfahndung auch verhältnismäßig ist.

IV. Resümee

Insgesamt stellt der Gesetzentwurf eine ausgewogene Neuregelung dar, die das Recht der Zollfahndung sowie in Sonderheit die Ermächtigungen des ZKA in Einklang mit den verfassungs- und unionsrechtlichen Anforderungen hält, zugleich aber auch punktuell fortentwickelt. Zu begrüßen ist hierbei die weitgehende Parallelführung zu den Befugnissen des BKA, weil das ZKA – obgleich weniger prominent – letztlich eine Sicherheitsbehörde des Bundes mit vergleichbarem Aufgabenprofil ist. Die parallele Ausgestaltung der Eingriffsbefugnisse hat zudem den Vorteil, dass die – in aller Regel im Bereich heimlicher Überwachungsmaßnahmen gegenstandsbedingt spärliche – Rechtsprechung zu einzelnen Regelungen Erkenntnisse liefern wird, die auch die rechtssichere Interpretation paralleler Bestimmungen erleichtern. Die Novelle trägt so zur Kohärenz des Sicherheitsrechts des Bundes wesentlich bei.

(Prof. Dr. Klaus F. Gärditz)

⁴² BVerfGE 141, 220 (309).

⁴³ BVerfGE 141, 220 (310 ff.).

⁴⁴ Hierzu BT-Drs. 19/12088, S. 113.

⁴⁵ BVerfGE 141, 220 (311 f.).