ALLGEMEINE BEITRÄGE

Aufgaben und Befugnisse des Bundeskriminalamts im digitalen Rechtsraum – Das Gesetz zur Neugestaltung des BKAG im Jahr 2017

von Prof. Dr. Kurt Graulich[*]

Abstract
Das Gesetz über das Bundeskriminalamt ist im Jahr 2017 umfassend neugestaltet worden. Es gibt wenige Bereiche von Gefahrenabwehr oder Strafverfolgung, in denen es nicht um die Erhebung oder Verarbeitung personenbezogener Daten geht. Ihr Milieu ist der digitale Raum, der als Rechtsraum begriffen werden muss. Inhaltlich finden sich die Auswirkungen der Digitalisierung des gesellschaftlichen Lebens, die daran knüpfenden polizeilichen Maßnahmen und – ihnen auf dem Fuß folgend – eine grundlegende Veränderung des Datenschutzes en gros und en detail in der Novellierung des BKAG. Die Neufassung verhilft dem Gesetz zu einer Ausstattung mit sämtlichen derzeit bekannten polizeirechtlichen Typen von Aufgabenzuweisungen und Befugnisnormen. Durch die Rechtsprechung des Bundesverfassungsgerichts ist die „hypothetische Datenneuerhebung" zum Kriterium des subjektiven Datenschutzes im Sicherheitsrecht geworden und hat im novellierten BKAG seinen vielfältigen Ausdruck gefunden. Der objektive Datenschutz hat sich in zahlreichen neuen institutionellen Konstruktionen niedergeschlagen, deren nutzbringende Auswirkungen auf den einzelnen Rechtsbetroffenen sich allerdings noch erweisen müssen. Sämtliche seither mit Buchstabenzusätzen versehen gewesene Normen sind nunmehr in die Nummerierung des Paragraphenwerks einbezogen worden und verhelfen dem Gesetz dadurch zu einem geschlossenen Aussehen. Die Novellierung macht rechtspolitisch die Forderungen nach einem neuen „Musterentwurf für ein einheitliches Polizeigesetz" überflüssig, denn das vorliegende BKAG ist dieses Muster.

I. Anlass und Ziel der Novellierung des BKAG

Zum Ende der 18. Wahlperiode ist das Bundeskriminalamt (BKA) von einer umfassenden gesetzlichen Neuregelung betroffen worden. Das Gesetz zur Neugestaltung des Bundeskriminalamtsgesetzes (BKAG) vom 8.6.2017[1] wurde notwendig durch das Urteil des *Bundesverfassungsgerichts* (*BVerfG*) vom 20.4.2016[2] sowie angestoßen durch die Ergebnisse des NSU-Untersuchungsausschusses im deutschen Bundestag[3] und hat mit seinem Art. 1 bereits äußerlich dem bislang von nachträglichen Einfügungen geprägten Flickenteppich von Regelungen zu einem geschlossenen Aussehen verholfen: trotz der nur eingeschränkten Gesetzgebungskompetenz liegt damit erstmals ein vollständiges Polizeigesetz des Bundes mit praktisch sämtlichen modernen polizeirechtlichen Befugnistypen vor.[4] Es dient außerdem der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 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.[5]

Mit der Neufassung des BKAG hat der Gesetzgeber nach eigenem Bekunden drei Ziele verfolgt, nämlich erstens die Stärkung des Datenschutzes, zweitens die Harmonisierung zur Verbesserung des Informationsflusses zwischen den Polizeibehörden in Europa und drittens die Modernisierung des BKA als Zentralstelle, u.a. nach dem Vorbild Europols.[6] Das novellierte BKAG tritt im Wesentlichen am 25.5.2018 in Kraft.[7] Dabei waren zwei rechtliche Maßgaben und eine sachliche Grenze zu beachten: Rechtlich war der Umsetzungsspielraum zum einen beschränkt, weil das *BVerfG* in seinem Urteil vom 20.4.2016 hinsichtlich der mit dem Grundgesetz für unvereinbar erklärten Vorschriften[8] eine Fortgeltung bis zu einer Neuregelung, längstens jedoch bis zum 30.6.2018 angeordnet hatte. [9] Zum anderen ist bis Mai 2018 die Richtlinie (EU) 2016/680 vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung

* Der Verfasser ist Richter am BVerwG a.D. und Honorarprofessor an der Humboldt-Universität zu Berlin.
1 BGBl. I 2017 S. 1354
2 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09 u. 1 BvR 1140/09, BVerfGE 141, 220.
3 BT-Drs. 18/11163, S. 76.
4 A.a.O., S. 1.
5 ABl. L 119 vom 4.5.2016, S. 89.
6 BT-Drs. 18/11163, S. 1.
7 Art. 13 des Gesetzes zur Neustrukturierung des Bundeskriminalamtsgesetzes vom 8.6.2017, BGBl. I 2017, S. 1354.
8 Vgl. *Graulich*, Anm. zu *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09, KriPoZ 2016, 75.
9 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 355 ff.

von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr umzusetzen.

Sachlich wäre eine kürzere Frist angesichts des erheblichen Erfüllungsaufwandes von einigen hundert Millionen Euro und der notwendigen personellen Verstärkungen kaum realistisch gewesen. Die Umsetzung der Vorgaben aus dem Urteil des *BVerfG* zieht eine grundlegende Neustrukturierung der bestehenden IT-Architektur des BKA, insbesondere des polizeilichen Informationssystems INPOL, nach sich. Demzufolge muss der Grundsatz der hypothetischen Datenneuerhebung als zentrales Element des Urteils des *BVerfG* effektiv und effizient in der IT-Architektur umsetzbar sein. Die Bundesregierung geht dafür von einer insgesamt fünfjährigen Aufbauphase aus.[10] Mit der verfassungsgerichtlichen Zeitvorgabe wiederum koinzidiert die Möglichkeit der vollständigen Umsetzung der Empfehlung Nr. 7 des NSU-Untersuchungsausschusses für den Bereich der Polizei innerhalb des Informationssystems des BKA und des polizeilichen Informationsverbundes zwischen den Polizeien des Bundes und der Länder. Als Lehre aus der Aufdeckung der NSU-Mordserie im November 2011 hat der Deutsche Bundestag nämlich u.a. gefordert, dass die informationstechnischen Grundlagen für die notwendige Vernetzung aller an einer Ermittlung beteiligten Dienststellen jederzeit sofort verfügbar sein müssten. Die Interoperabilität der Datensysteme müsse zügig erreicht werden.[11]

II. Inhalte der Novelle

1. Zu den Aufgaben

Die Aufgabenbeschreibung für das BKA ist vor allem[12] in den §§ 2 bis 8 BKAG enthalten.[13] Aus verfassungsrechtlichen Gründen kann dies nicht – wie in den Polizeigesetzen der Länder üblich – durch eine Generalklausel geschehen, denn die Zuständigkeit des Bundes im Polizeirecht ist auf die vom Grundgesetz zugestandenen Materien begrenzt. Dies führt zum charakteristischen Aufbau des BKAG, wonach jeder Aufgabenbeschreibung auch ein besonderer Abschnitt mit Befugnissen zugeordnet ist.[14] Als legislativen Antrieb für die vorliegende Reform benennt der Bundesgesetzgeber nicht nur seine mit der Ausfüllung des Zentralstellenbegriffs verbundene Gesetzgebungs- und Einrichtungskompetenz, sondern mindestens gleichgewichtig den grundrechtlichen Gestaltungsauftrag durch das Urteil des *BVerfG*. Die Novelle hat also eine organisationsrechtliche und grundrechtliche Seite. Nachfolgend sollen die Änderungen betrachtet werden und nicht die bereits vorhanden Regelungen.

Die Zentralstellenfunktion des BKA ist verfassungsrechtlich vorgegeben[15] und wird als polizeiliche Aufgabe einfachgesetzlich in § 2 BKAG aufgenommen. Die Hauptziele der Gesetzesnovelle schlagen sich dort in mehreren Änderungen nieder. Die bestehende IT-Architektur des BKA, insbesondere das polizeiliche Informationssystem INPOL, ist nach Ansicht des Gesetzgebers für die Umsetzung der Vorgaben aus dem Urteil des *BVerfG* vom 20.4.2016 nicht ausgelegt und daher grundlegend neu zu strukturieren.[16] Dieser Reformbedarf setzt sich aus normativen, administrativen und operativen Teilen zusammen, die deshalb vom Gesetzgeber nur teilweise gestaltet werden können. Einen wesentlichen Aspekt der Modernisierungsbestrebung stellt die Bereitstellung eines einheitlichen Verbundsystems mit zentraler Datenhaltung im BKA dar, um die verfassungsrechtlichen Vorgaben auch für die anderen Polizeien des Bundes und die der Länder effektiv erfüllen zu können; dafür steht in § 2 Abs. 3 BKAG nunmehr, dass das BKA einen „einheitlichen polizeilichen Datenverbund“ erhält.

Die einzelnen normativen Anteile der Zentralstellenreform beschränken sich nicht auf § 2 BKAG, sondern sind im novellierten BKAG verteilt. Dies gilt insbesondere für die Kennzeichnungsregelung in § 14 BKAG, die elementare Voraussetzung für das vom *BVerfG* geforderte Kriterium der „hypothetischen Datenneuerhebung“ bei der Weiterverwendung von Daten nach § 12 BKAG ist. Der Datenbesitz und damit die Verantwortung für die Daten verbleibt weiterhin bei den entsprechenden Polizeien des Bundes und der Länder (§ 29 Abs. 5 S. 1 BKAG). Die Harmonisierung und Standardisierung der Informationsverarbeitung verlangt zukünftig eine Zentralstelle, die eine einheitliche Informationstechnik zur Verfügung stellt, Prozesse koordiniert und Diskussionsprozesse moderiert. Hierzu soll das BKA mit seiner bereits originär definierten Position als Zentralstelle ertüchtigt werden (§ 29 Abs. 1 S. 2 BKAG). Das Verbundsystem muss nach § 29 Abs. 2 S. 1 BKAG die Anforderungen von § 13 Abs. 2 BKAG erfüllen.

Durch eine textliche Erweiterung von § 3 Abs. 1 BKAG wird klargestellt, dass das BKA die nationale Stelle für Europol ist. Dies ist bislang lediglich in § 1 des Gesetzes zur Umsetzung des Beschlusses des Rates 2009/371/JI vom 6.4.2009 zur Errichtung des Europäischen Polizeiamtsgeregelt gewesen.

Bei der Kompetenz des BKA zur Strafverfolgung unternimmt der Gesetzgeber durch Änderungen von § 4 BKAG eine sinnvolle Angleichung an die bereits bestehende Kompetenz des GBA und bündelt somit die

---

10 BT-Drs. 18/11163, S. 3.
11 BT-Drs. 17/14600, S. 862.
12 Das Fluggastdatengesetz vom 6.6.2018, BGBl. I 2016, S. 1484, begründet in § 1 eine weitere Aufgabe als Fluggastdaten-Zentralstelle.
13 § 2 Zentralstelle, § 3 Internationale Zusammenarbeit, § 4 Strafverfolgung, § 5 Abwehr von Gefahren des internationalen Terrorismus, § 6 Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamtes, § 7 Zeugenschutz, § 8 Sicherung des Bundeskriminalamtes, behördlicher Eigenschutz.
14 Abschnitt 3 Zentralstelle, Abschnitt 4 Befugnisse im Rahmen der Strafverfolgung, Abschnitt 5 Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus, Abschnitt 6 Befugnisse zum Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamtes, Abschnitt 7 Zeugenschutz, Abschnitt 8 Befugnisse zur Sicherung des Bundeskriminalamtes und zum behördlichen Eigenschutz.
15 Art. 73 Abs. 1 Nr. 10 lit. a und Art. 87 Abs. 1 S. 2 GG.
16 BT-Drs. 18/11163, S. 2.

Fähigkeiten des Bundes in einem bestimmten Bereich der Strafverfolgung. Durch die Einfügung der neuen Regelung in § 4 Abs. 1 Nr. 6 BKAG wird für das BKA eine originäre Ermittlungskompetenz im Bereich der Spionagebekämpfung und damit eng zusammenhängender Delikte geschaffen. Die Strafverfolgungszuständigkeit für die im zweiten Abschnitt des Strafgesetzbuchs geregelten Straftaten Landesverrat und Gefährdung der äußeren Sicherheit (§§ 94 bis 100a StGB) liegt nicht bei den Staatsanwaltschaften der Länder, sondern gemäß § 142a Abs. 1 S. 1 i.V.m. § 120 Abs. 1 Nr. 3 GVG beim Generalbundesanwalt.[17] Durch eine leichte Umformulierung von § 5 Abs. 1 S. 2 BKAG[18] wird der Begriff „Gefahren des internationalen Terrorismus" als Gefahren der Verwirklichung von Straftaten definiert. Darin liegt nicht nur eine Präzisierung, sondern auch eine signifikante Verschränkung der Schutzbereiche von Strafrecht und Gefahrenabwehrrecht.

Die Aufgabe des Schutzes der Bundesorgane bzw. Verfassungsorgane des Bundes teilen sich Bundespolizei (§ 5 BPolG) und BKA (§ 6 BKAG). Dabei ist die Aufgabe der Bundespolizei eher räumlich und diejenige des BKA eher persönlich ausgerichtet; Details werden im Einzelfall durch Absprachen geregelt.[19] Durch eine marginale Änderung in § 6 BKAG wird die Aufgabe des BKA für den Personenschutz auf den Schutz von Hilfsorganen des Deutschen Bundestages erweitert, sofern der Präsident des Deutschen Bundestages darum ersucht.

Während die Möglichkeiten strafprozessualen Zeugenschutzes durch das ZSHG bundeseinheitlich geregelt sind,[20] stützen sich die Maßnahmen des polizeilichen Zeugenschutzes grundsätzlich auf das Gefahrenabwehrrecht der Länder, insbesondere die Generalermächtigungen der Polizeigesetze. Nur das BKAG enthielt bis zum Erlass des ZSHG in § 6 BKAG a.F. eine besondere Aufgabenzuweisung für den Zeugenschutz zzgl. der Befugnisnorm in § 29 BKAG a.F.[21] Diese Kompetenz ist nunmehr leicht ausgebaut worden. Nach § 7 Abs. 1 BKAG wird die Zuständigkeit des BKA für Zeugenschutzmaßnahmen auf alle Bereiche erstreckt, in denen es nach § 4 Abs. 1 BKAG originär für die Strafverfolgung zuständig ist. Und nach dem neuen § 7 Abs. 3 S. 1 BKAG nimmt das BKA seine Aufgabe als Zentralstelle für die internationale Zusammenarbeit auch auf dem Gebiet des Zeugenschutzes wahr. In der Praxis häufen sich insbesondere aufgrund der vertieften europäischen Zusammenarbeit ausländische Ersuchen an das BKA, dort geschützte Personen aus Gefährdungsgründen nach Deutschland umzusiedeln, um den Schutz dieser Personen sicherzustellen.[22]

2. Zur Verarbeitung personenbezogener Daten im polizeilichen Verfahren

Das novellierte BKAG enthält in „Abschnitt 2 „Allgemeine Befugnisse zur Datenverarbeitung" übergreifende Regelungen betreffend Datenerhebung, Weiterverarbeitung von Daten sowie die Datenübermittlung. Darin berücksichtigt es die Quintessenz der Maßgaben aus dem Urteil des *BVerfG* vom 20.4.2016. Das Herzstück sind die Vorschriften über die Zweckbindung sowie den Grundsatz der hypothetischen Datenneuerhebung für besonders eingriffsintensive Maßnahmen (§ 12 BKAG), das Informationssystem des BKA zur Erfüllung der in den §§ 2 bis 8 BKAG genannten Aufgaben (§ 13 BKAG) und die Kennzeichnung von personenbezogenen Daten mit den notwendigen Zusatzinformationen für den Fall der Übermittlung (§ 14 BKAG).

a) Der Grundsatz der hypothetischen Datenneuerhebung und die Datenkennzeichnung

Vor den datenschutzrechtlichen Neuregelungen im BKAG steht die verfassungsrechtliche Grundannahme, dass Anforderungen an die Nutzung und Übermittlung staatlich erhobener personenbezogener Daten sich nach den Grundsätzen der Zweckbindung und Zweckänderung richten.[23] Das Zusammenwirken des Zweckbindungsgrundsatzes mit dem Kriterium der hypothetischen Datenneuerhebung im Falle der Zweckänderung wird im neuen § 12 BKAG als allgemeines Modell beschrieben, das bei jeder Verarbeitung personenbezogener Daten durch das BKA – unabhängig von der jeweiligen Eingriffsintensität der ursprünglichen Erhebungsmaßnahme – zu beachten ist.[24] Den zugrundeliegenden Erwägungen des *BVerfG* folgen die Regelungen im neuen BKAG eng wie sich an vier Normierungen zeigen lässt:

(1) Zunächst sind Inhalt und Wirkung der Zweckbindung zu ermessen. Die Reichweite der Zweckbindung richtet sich nach der jeweiligen Ermächtigung für die Datenerhebung; die Datenerhebung bezieht ihren Zweck zunächst aus dem jeweiligen Ermittlungsverfahren. Der Gesetzgeber kann eine Datennutzung über das für die Datenerhebung maßgebende Verfahren hinaus im Rahmen der ursprünglichen Zwecke dieser Daten erlauben (weitere Nutzung). Dies setzt voraus, dass es sich um eine Verwendung der Daten durch dieselbe Behörde zur Wahrnehmung derselben Aufgabe und zum Schutz derselben Rechtsgüter handelt. Normiert wird der so verstandene Grundsatz der Zweckbindung in § 12 Abs. 1 S. 1 BKAG. Damit wird klargestellt, dass die Verarbeitung von personenbezogenen Daten zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verfolgung

17 BT-Drs. 18/11163, S. 88.
18 Vormals § 4a Abs. 1 S. 2 BKAG.
19 *Graulich*, in: Schenke/Graulich/Ruthig, BPolG (2014), § 5 Rn. 1.
20 Zeugenschutz-Harmonisierungsgesetz (ZSHG) vom 11.12.2001 (BGBl. I, S. 3510), das durch Art. 2 Abs. 12 des Gesetzes vom 19.2.2007 (BGBl. I 2007, S. 122) geändert worden ist.
21 *Graulich*, in: Schenke/Graulich/Ruthig, BPolG, § 6 Rn. 4.
22 BT-Drs. 18/11163, S. 89.
23 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 276.
24 BT-Drs. 18/11163, S. 92.

oder Verhütung derselben Straftaten durch das Bundeskriminalamt nicht den verfassungsrechtlichen Anforderungen an eine Zweckänderung unterliegt.[25]

(2) Allerdings kann der Gesetzgeber nach der Rechtsprechung des *BVerfG* darüber hinaus eine Nutzung der Daten auch zu anderen Zwecken als denen der ursprünglichen Datenerhebung erlauben (Zweckänderung).[26] Die Verhältnismäßigkeitsanforderungen für eine solche Zweckänderung orientieren sich am Grundsatz der hypothetischen Datenneuerhebung. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Diesen Zusammenhang normiert § 12 Abs. 2 BKAG.

(3) Mit dem Kriterium der hypothetischen Datenneuerhebung hat das B*VerfG* dem Gesetzgeber auch ein Mittel gegeben, an dem Problem der unterschiedlichen Eingriffsschwellen im Sicherheitsrecht vorbeizukommen. Als neu zu rechtfertigender Eingriff bedarf danach auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt.[27] Damit hatte das *BVerfG* das Problem der unterschiedlichen Eingriffsschwellen bei Nachrichtendiensten, Gefahrenabwehr und Strafverfolgung und ihre Auswirkungen im Falle der Weitergabe von Daten ausgeklammert: Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Die diesbezüglichen Anforderungen bestimmen unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst, nicht aber auch für die weitere Nutzung der erhobenen Daten.[28]

Die Abstrahierung von der Eingriffsschwellen-Thematik hat allerdings das *BVerfG* selbst in seinem Urteil bei besonders schweren Grundrechtseingriffen eingeschränkt. Für Daten aus Wohnraumüberwachungen oder einem Zugriff auf informationstechnische Systeme reicht der Blickwinkel der hypothetischen Datenneuerhebung nicht aus, vielmehr müssen zusätzlich für jede weitere Nutzung auch die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sein.[29] Diese gesteigerten gesetzlichen Voraussetzungen beim Dateneingriff regelt § 12 Abs. 3 S. 1 BKAG. Danach muss für die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder technischer Mittel in informationstechnischen Systemen erlangt wurden, gilt § 12 Abs. 2 S. 1 Nr. 2 lit. b BKAG mit der Maßgabe entsprechend, dass im Einzelfall eine dringende Gefahr oder eine Gefahrenlage im Sinne des § 49 Abs. 1 S. 2 BKAG vorliegen.

(4) Verfassungsrechtlich beanstandet hatte das *BVerfG* außerdem, dass Daten aus optischen Wohnraumüberwachungen von einer Übermittlung an die Strafverfolgungsbehörden nicht ausgeschlossen wurden. Art. 13 Abs. 3 GG erlaubt für die Strafverfolgung nur den Einsatz der akustischen Wohnraumüberwachung. Dies dürfe durch eine Übermittlung von Daten aus einer präventiv angeordneten optischen Wohnraumüberwachung nicht unterlaufen werden.[30] Dem trägt § 12 Abs. 2 S. 2 BKAG nun durch eine entsprechende Einschränkung Rechnung.

Notwendig Voraussetzung für die praktische Umsetzung des Schutzkonzepts aus § 12 BKAG ist die Kennzeichnung der personenbezogenen Daten bei ihrer Erhebung (§ 14 BKAG). Die Grundregel dazu bestand zwar schon in der Vergangenheit jedenfalls verfassungsrechtlich, war aber nur rudimentär in § 9a Abs. 2, § 10 Abs. 4 S. 2, § 20v und § 33 BKAG normiert.[31] Nun hat das Urteil des *BVerfG* detaillierte Regeln für die Kennzeichnung unabweisbar gemacht, weil es sonst an der elementaren Voraussetzung für die Bestimmung des Erhebungszwecks und somit auch der Beurteilung der Zweckänderung bei der hypothetischen Datenneuerhebung fehlen würde.[32] § 14 Abs. 1 S. 1 BKAG sieht dementsprechend vor, dass personenbezogene Daten durch Angabe des Mittels der Erhebung der Daten einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden (Nr. 1), bei Personen, zu denen Grunddaten angelegt wurden, durch die Angabe der Kategorie nach §§ 18, 19 (Nr. 2), durch die Angabe der Rechtsgüter, deren Schutz die Erhebung dient oder Straftaten, deren Verfolgung oder Verhütung die Erhebung dient (Nr. 3), und durch die Angabe der Stelle, die sie erhoben hat, sofern nicht das BKA die Daten erhoben hat (Nr. 4), zu kennzeichnen sind. Diese umfassende Kennzeichnung, die nach § 29 BKAG auch für den Informationsverbund gilt, schafft die Voraussetzung für eine konsistente Anwendung des Grundsatzes der hypothetischen Datenneuerhebung.[33]

b) Das System von Datenverarbeitung und Datenschutz

Nach § 13 Abs. 1 BKAG betreibt das BKA ein Informationssystem zur Erfüllung der in den §§ 2 bis 8 BKAG genannten Aufgaben. Nach § 28 Abs. 1 BKAG stellt das BKA als Zentralstelle für den polizeilichen

25 A.a.O., S. 92.
26 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 284.
27 A.a.O., Rn. 287.
28 A.a.O., Rn. 289.
29 A.a.O., Rn. 279.
30 A.a.O., Rn. 317.
31 *Graulich*, in: Schenke/Graulich/Ruthig, BKAG (2014), § 7 Rn. 4 m.w.N.
32 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 285.
33 BT-Drs. 18/11163, S. 96.

Informationsverbund ein einheitliches Informationssystem zur Verfügung. Das BKA ist nach § 28 Abs. 3 BKAG selbst Teilnehmer am Informationsverbund. Nach § 13 Abs. 3 BKAG erfolgt die Teilnahme am polizeilichen Informationsverbund technisch mit dem Informationssystem. § 15 BKAG regelt ausgeklügelt die Zugriffsberechtigungen auf personenbezogene Daten und schützt sie dadurch verfahrenstechnisch.

Mit § 16 BKAG werden die bislang an verschiedenen Stellen im BKAG geregelten Befugnisse zur Datenweiterverarbeitung in einer zentralen Norm neu systematisiert. Danach ist das BKA berechtigt, Daten, die im Zusammenhang mit der Erfüllung einer bestimmten gesetzlichen Aufgabe anfallen, auch für die Erfüllung einer anderen Aufgabe zu nutzen. Nach § 13 Abs. 4 BKAG i.V.m. Abs. 1 BKAG ist das BKA verpflichtet, die im Rahmen seiner Aufgaben nach den §§ 3 bis 6 BKAG gewonnenen Informationen der Zentralstelle zu übermitteln. Als wichtigste Aussage zum Datenschutz wird man § 16 Abs. 1 S. 1 BKAG zu verstehen haben, wonach das BKA „personenbezogene Daten nach Maßgabe des § 12 BKAG im Informationssystem weiterverarbeiten kann“, d.h. unter Beachtung des Kriteriums der hypothetischen Datenneuerhebung. Die Vorschrift stellt klar, dass bei der Verarbeitung personenbezogener Daten stets der in § 12 BKAG geregelte Grundsatz der hypothetischen Datenneuerhebung beachtet werden muss. Durch Ergänzung des letzten Halbsatzes wird verdeutlicht, dass speziellere Weiterverarbeitungsbefugnisse der Norm vorgehen.[34]

Der neue § 17 BKAG entspricht weitestgehend dem bisherigen § 9a BKAG und regelt die gemeinsamen projektbezogenen Dateien; punktuelle Erweiterungen auszuwertender Deliktsbereiche sollen vor allem die Erkenntnisse aus dem nachrichtendienstlichen Bereich bei der Polizeiarbeit[35] besser nutzbar machen.[36]

c) Datenübermittlung

Die Anforderungen an die weitere Nutzung und Übermittlung staatlich erhobener Daten richten sich nach den Grundsätzen der Zweckbindung und Zweckänderung. Erlaubt der Gesetzgeber die Nutzung von Daten über den konkreten Anlass und rechtfertigenden Grund einer Datenerhebung hinaus, muss er hierfür eine eigene Rechtsgrundlage schaffen.[37] Dies ist bei Datenübermittlungen der Fall. Dabei ist der Grundsatz der Verhältnismäßigkeit zu beachten. Die Verhältnismäßigkeitsanforderungen für eine darin liegende Zweckänderung orientieren sich – wie auch in anderen Fällen – am Grundsatz der hypothetischen Datenneuerhebung.[38]

Dementsprechend begründet – anstelle des seitherigen § 10 BKAG – nunmehr § 25 BKAG die Befugnis des BKA zur Datenübermittlung im innerstaatlichen Bereich, knüpft sie aber durch Verweis auf § 12 Abs. 2 bis 4 BKAG an das Kriterium der hypothetischen Datenneuerhebung. Entscheidend für eine Datenübermittlung an sonstige öffentliche Stellen ist demnach, dass neben konkreten Ermittlungsansätzen für die Aufdeckung von Straftaten oder Gefahren für Rechtsgüter zugleich auch Erkenntnisse zu einer Gefährdung von mindestens gleichwertigen Rechtsgütern vorliegen, die zur Erfüllung der Aufgabe der jeweiligen Behörde bedeutsam sein können.[39] Für die Datenübermittlung an die Verfassungsschutzbehörden des Bundes und der Länder, an den Bundesnachrichtendienst sowie an den Militärischen Abschirmdienst ist es notwendig, dass in Anwendung des Grundsatzes der hypothetischen Datenneuerhebung neben konkreten Ermittlungsansätzen für die Aufdeckung von Straftaten oder Gefahren für hochrangige Rechtsgüter zugleich auch konkrete Erkenntnisse zu einer Gefährdung hochrangiger Rechtsgüter erkennbar sind, die für die Lagebeurteilung nach Maßgabe der Aufgaben der jeweiligen Behörde bedeutsam sein können.[40]

Der neue § 26 BKAG regelt die Datenübermittlung an Mitgliedstaaten der Europäischen Union, die im bisherigen § 14a BKAG geregelt war und stellt sie mit den Datenübermittlungen im Inland gleich. Durch den Verweis auf die Regelungen des § 25 BKAG gilt der in § 12 BKAG verankerte Grundsatz der hypothetischen Datenneuerhebung auch für die innereuropäische Datenübermittlung[41]. Der Regelfall von Übermittlungen nach § 26 Abs. 1 S. 1 Nr. 1 BKAG stellen Übermittlungen an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union dar. Als solche können insbesondere jene Stellen gelten, die von diesem Staat gemäß Art. 2 Buchst. a des Rahmenbeschlusses 2006/960/JI des Rates vom 18.12.2006[42] über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union[43] benannt wurden.

Die Übermittlung von personenbezogenen Daten an öffentliche Stellen anderer Staaten stellt eine Zweckänderung dar. Sie ist insoweit nach den allgemeinen Grundsätzen jeweils an den Grundrechten zu messen, in die bei der Datenerhebung eingegriffen wurde.[44] Die Grenzen der inländischen Datenerhebung und -verarbeitung des GG dürfen durch einen Austausch zwischen den Sicherheitsbehörden nicht in ihrer Substanz unterlaufen werden. Der Gesetzgeber hat daher dafür Sorge zu tragen, dass dieser Grundrechtsschutz

---

34 A.a.O., S. 97.
35 *Graulich,* in: Schenke/Graulich/Ruthig, BKAG, § 9a Rn. 3.
36 BT-Drs. 18/11163, S. 96 ff.
37 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 277.
38 A.a.O., Rn. 287.
39 BT-Drs. 18/11163, S. 104.
40 A.a.O., unter Hinw. auf *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 320.
41 BT-Drs. 18/11163, S. 105.
42 *Graulich*, in: Schenke/Graulich/Ruthig, BKAG, § 14a Rn. 10.
43 ABl. L386 v. 29.12.2006, S.89, L75 v. 15.3.2007, S.26.
44 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 324.

nicht ausgehöhlt wird.[45] Zwingend auszuschließen ist zudem jedenfalls die Datenübermittlung an Staaten, wenn zu befürchten ist, dass elementare rechtsstaatliche Grundsätze verletzt werden.[46] Demnach muss ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten sein. Zwar müssen im Zielstaat insbesondere nicht die formellen und institutionellen Sicherungen vorhanden sein. Geboten ist jedoch die Gewährleistung eines angemessenen materiellen datenschutzrechtlichen Niveaus für den Umgang mit den übermittelten Daten im Empfängerstaat.[47]

Diese Anforderungen werden von den §§ 27 und 28 BKAG umgesetzt, die an die Stelle der seitherigen §§ 14 und 27 BKAG getreten sind. Grundsätzlich ist die Einführung des Kriteriums der hypothetischen Datenneuerhebung in § 27 Abs. 1 BKAG. Durch die in § 27 Abs. 6 BKAG vorgesehene entsprechende Geltung des § 75 Abs. 2 BDSG unterbleibt die Übermittlung, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den personenbezogenen Daten bei den Dienststellen der Stationierungsstreitkräfte nicht hinreichend gesichert ist. Der neue § 27 Abs. 8 BKAG enthält eine Befugnis zur Datenübermittlung an zwischen- und überstaatliche Stellen, die nicht mit Aufgaben der Verhütung oder Verfolgung von Straftaten befasst sind. Diese Regelung vervollständigt die auf die Verarbeitung beim BKA anwendbare Befugnis aus § 81 BDSG, in eng umgrenzten Fällen für die Aufgabenerfüllung Daten an nicht für die Strafverfolgung zuständige Stellen in Drittstaaten zu übermitteln.[48]

Der neue § 28 Abs. 3 BKAG verpflichtet das BKA, für den polizeilichen Informationsaustausch und Rechtshilfeverkehr eine Aufstellung über die Einhaltung der elementaren rechtsstaatlichen Grundsätze und Menschenrechtsstandards sowie das Datenschutzniveau in den jeweiligen Drittstaaten zu erstellen.[49] Hierbei hat das BKA insbesondere die jeweiligen Erkenntnisse der Bundesregierung und die Angemessenheitsbeschlüsse der Europäischen Kommission gemäß Art. 36 der oben genannten Richtlinie zu berücksichtigen. Diese Aufstellung ist regelmäßig zu aktualisieren.[50]

3. Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus

Die Abwehr von Gefahren des internationalen Terrorismus als Aufgabe ist spät in das Pflichtenheft des BKA gelangt und dennoch kann der für die zugehörigen Befugnisse einschlägige Abschnitt 5 typologisch als der reichhaltigste Teil dieses Polizeigesetzes angesehen werden, der sämtliche derzeit bekannten Standardbefugnisse enthält. Davon seien einige in den Blick genommen.

a) Besondere Mittel der Datenerhebung

Nicht neu, aber infolge des Urteils des *BVerfG* vom 20.4.2016 vollständig überarbeitet worden ist die – vormals in § 20g BKAG[51] – enthaltene Vorschrift des § 45 BKAG über die besonderen Mittel der Datenerhebung. Eingriffsrechtlich handelt es sich um einen der Kernbereiche heimlicher polizeilicher Mittel, die das *BVerfG* zu seiner umfassenden Konzeption des Verhältnismäßigkeitsgrundsatzes geführt hat. Die Neuregelung ist nicht nur vom Textumfang her, d.h. nach Absätzen und Zeichen fast zweimal so groß wie die Vorgängervorschrift. Sie hat auch die materiellen und formellen Eingriffsschwellen im Falle ihrer Anwendung deutlich erhöht.

Langfristige Observation (§ 45 Abs. 2 Nr. 1), das Abhören oder Aufzeichnen des außerhalb von Wohnungen nicht öffentlich gesprochenen Wortes (§ 45 Abs. 2 Nr. 2 lit. b), der langfristige Einsatz technischer Mittel für Observationszwecke (§ 45 Abs. 2 Nr. 3), der Einsatz von Vertrauensperson (§ 45 Abs. 2 Nr. 4) und der Einsatz von verdeckten Ermittlern (§ 45 Abs. 2 Nr. 5) bedürfen zukünftig der richterlichen Anordnung. Der Gesetzentwurf bezieht wegen der mit der langfristigen Observation vergleichbaren Eingriffsschwere auch die Anfertigung von Bildaufnahmen oder -aufzeichnungen von Personen, die sich außerhalb von Wohnungen befinden (§ 45 Abs. 2 Nr. 2 lit. a), ein, insoweit durchgehend länger als 24 Stunden oder an mehr als zwei Tagen Bildaufzeichnungen bestimmter Personen angefertigt werden sollen.[52]

b) Wohnraumüberwachung

Die besonderen Bestimmungen über den Einsatz technischer Mittel in oder aus Wohnungen ist von § 20h zu § 46 BKAG geworden und unter dem Einfluss des Urteils des *BVerfG* auf der Eingriffs- und Kontrollseite völlig neugestaltet worden. Die Beobachtung von Kontakt- und Begleitpersonen ist infolge des Verdikts des *BVerfG* bei Wohnraumüberwachungen als unverhältnismäßig erkannt worden, und die Angemessenheit solcher Überwachungsmaßnahmen wird nur dann als gewahrt angesehen, wenn sie sich von vornherein ausschließlich auf Gespräche der Gefahrenverantwortlichen beziehen (§ 46 Abs. 1 und 2 BKAG). Der neue § 46 Abs. 7 BKAG entspricht dem bisherigen § 20h Abs. 5 S. 6 bis 9 BKAG.[53] Durch die Einfügung von S. 1 wird bestimmt, dass die Aufzeichnungen aus Wohnraumüberwachungen unverzüglich dem anordnenden Gericht vorzulegen sind. Die Neufassung des S. 6 und die Einfügung der S. 7 und 8 dienen der Umsetzung des Urteils des *BVerfG* vom 20.4.2016 zur Aufbewahrungsfrist der Löschungsprotokolle zwecks effektiver Ausübung der Betroffenenrechte und einer

45 A.a.O., Rn. 327.
46 A.a.O., Rn. 328 unter Hinweis auf *BVerfG*, Urt. v. 24.6.2003 – 2 BvR 685/03, BVerfGE 108, 129 (136 f.); siehe auch *BVerfG*, Urt. v. 15.12.2015 – 2 BvR 2735/14, Rn. 62 m.w.N.
47 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220, Rn. 333 und 335 unter Hinweis auf *EuGH*, Urt. v. 6.10.2015 – C-362/14.
48 BT-Drs. 18/11163, S. 107.
49 *Ruthig*, in: Schenke/Graulich/Ruthig, BKAG, § 27 Rn. 16.
50 BT-Drs. 18/11163, S. 108.
51 Vgl. *Schenke*, in: Schenke/Graulich/Ruthig, BKAG, § 20g Rn. 1 ff.
52 BT-Drs. 18/11163, S. 114.
53 Vgl. *Schenke*, in: Schenke/Graulich/Ruthig, BKAG, § 20h Rn. 36 ff.

wirksamen Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.[54]

c) Verdeckter Eingriff in informationstechnische Systeme

Eines der invasivsten Aufklärungsmittel ist der „Verdeckte Eingriff in informationstechnische Systeme", früher in § 20k BKAG[55] und nunmehr in § 49 BKAG geregelt. Damit ist gesetzgebungsgeschichtlich die polizeirechtliche Regelung im BKAG der strafverfahrensrechtlichen in der StPO vorausgeeilt; dafür wird die neu eingeführte entsprechende Regelung des § 100b StPO aber auch gleich mit dem richtigen Namen bezeichnet, nämlich „Online-Durchsuchung".[56] Als Online-Durchsuchung wird der verdeckte staatliche Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze mittels einer Überwachungssoftware bezeichnet. Das *BVerfG* hatte das Rechtsinstitut selbst unbeanstandet gelassen, aber an den Voraussetzungen und Verfahrensregeln Fehler festgestellt. Daraus wird u.a. in § 49 Abs. 1 BKAG die Konsequenz gezogen und die Gefahrenlage ausdrücklich umschrieben, die im Vorfeld einer konkreten Gefahr einen Eingriff in informationstechnische Systeme rechtfertigt. § 49 Abs. 7 BKAG setzt die vom *BVerfG* geforderte Voraussetzung[57] um, dass für die Sichtung von Informationen aus verdeckten Eingriffen in informationstechnischen Systemen eine unabhängige Stelle vorzusehen ist und eine Beschränkung auf Zweifelsfälle verfassungsrechtlich nicht möglich ist. Durch die Neuregelung wird sichergestellt, dass die Informationen aus verdeckten Eingriffen in informationstechnische Systeme unverzüglich dem anordnenden Gericht vorzulegen sind. Die Neufassung des letzten Satzes und die Einfügung eines weiteren Satzes dienen der Umsetzung des Urteils des *BVerfG* vom 20.4.2016 zur Aufbewahrungsfrist der Löschungsprotokolle zwecks effektiver Ausübung der Betroffenenrechte und einer wirksamen Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.[58]

d) Telekommunikationsüberwachung – auch an der Quelle

Die nunmehr in § 51 BKAG geregelte präventive Telekommunikationsüberwachung tritt an die Stelle von § 20l BKAG.[59] In § 51 Abs. 1 BKAG wird nun präziser umrissen, wann eine Gefahrenlage im Vorfeld einer konkreten Gefahr einen Eingriff in informationstechnische Systeme rechtfertigt. Die Befugnis umfasst auch weiterhin die sog. Quellen-TKÜ.[60] Bei der Quellen-Telekommunikationsüberwachung wird – wie bei der Online-Durchsuchung – ein fremdes informationstechnisches System infiltriert, um mit einer eigens für diesen Zweck entwickelten Überwachungssoftware die Kommunikation zwischen den Beteiligten überwachen und aufzeichnen zu können. Dies geschieht aus technischen Gründen, weil die Kommunikation nach dem geltenden Recht zwar im öffentlichen Telekommunikationsnetz ausgeleitet werden könnte, den Ermittlungsbehörden dann aber nur in verschlüsselter Form vorliegen würde. Die Entschlüsselung ist entweder extrem zeitaufwändig oder sogar gänzlich ausgeschlossen. Die Maßnahme ist nach der Rechtsprechung des *BVerfG* grundsätzlich zulässig.[61] Das Strafverfahrensrecht hat mit dem neu eingeführten § 100a StPO inzwischen mit dem Polizeirecht gleichgezogen.

e) Aufenthaltsverbot und Kontaktverbot

Durch die neu aufgenommene Vorschrift in § 56 BKAG erhält das BKA die Befugnis, zur Abwehr von Gefahren sowie zur Verhütung von Straftaten nach § 5 Abs. 1 S. 2 Personen zu untersagen, sich an bestimmten Orten aufzuhalten, bestimmte Orte zu verlassen (Aufenthaltsverbot) oder Kontakt mit bestimmten Personen zu haben (Kontaktverbot). Diese Verbote ergänzen den in § 54 BKAG geregelten „klassischen" Platzverweis, der nur eine vorübergehende Entfernung einer Person von einem bestimmten Ort zum Ziel hat. Vergleichbare Regelungen finden sich in nahezu allen Landespolizeigesetzen sowie auch in § 68b Abs. 1 S. 1 Nr. 1 und 2 StGB.[62] Die Aufnahme der Vorschrift in den Instrumentenkasten des BKAG überrascht insofern etwas, als das BKA im Unterschied zu den Polizeien der Länder und der Bundespolizei nicht ausgesprochen in der Fläche präsent ist, wo ggfs. die Befolgung solcher Maßnahmen allein zu kontrollieren ist.

f) Elektronische Aufenthaltsüberwachung

Die freiheitlichen Rechtsordnungen tragen schwer am Umgang mit terroristischen Gefährdern. Selbst nach einem verübten Anschlag gelingt es nicht ohne weiteres, den äußeren und inneren Weg eines Attentäters zum Ursprung seines Verhaltens zurückzuverfolgen und wenigstens zurückblickend rechtlich zu analysieren. Umso schwerer tun sich – im Vorhinein – die drei großen Sicherheitsbereiche mit dem Einsatz ihrer In-

54 BT-Drs. 18/11163, S. 117.
55 Vgl. *Schenke*, in: Schenke/Graulich/Ruthig, BKAG, § 20k Rn. 1 ff.
56 Die Regelungen der § 100a StPO über die Quellen-TKÜ und § 100b StPO über die Online-Durchsuchung wurden am 15.5.2017 in einer Spätphase des Gesetzgebungsverfahrens durch eine „Formulierungshilfe" der Bundesregierung für einen Änderungsantrag der Fraktionen CDU/CSU und SPD zu dem Gesetzentwurf der Bundesregierung zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze – Drucksache 18/11272 – eingefügt (Ausschussdrucksache 18(6)334). Diese Vorgehensweise hat berechtigte Kritik erfahren.
57 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 224.
58 BT-Drs. 18/11163, S. 118.
59 Vgl. *Schenke*, in: Schenke/Graulich/Ruthig, BKAG, § 20l Rn. 1 ff.
60 *Schenke*, in: Schenke/Graulich/Ruthig, BKAG, § 20l Rn. 26.
61 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 1 ff.
62 BT-Drs. 18/11163, S. 121.

strumente: Wann liegen für eine terroristische Gesinnung bei einem Menschen tatsächliche Anhaltspunkte vor (Nachrichtendienste), wann besteht eine konkrete Gefahr (Gefahrenabwehr), und wann besteht ein Anfangsverdacht (Strafverfolgung)? Durch den neu eingefügten § 56 BKAG zur elektronischen Aufenthaltsüberwachung erhält das BKA im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus die Befugnis, den Aufenthaltsort von Personen, von denen die Gefahr der Begehung einer terroristischen Straftat i.S.v. § 5 Abs. 1 S. 2 BKAG ausgeht, elektronisch zu überwachen. Dazu kann das BKA auf entsprechende richterliche Anordnung eine Person dazu verpflichten, ständig ein für die elektronische Überwachung des Aufenthaltsortes geeignetes technisches Mitteln („elektronische Fußfessel") in betriebsbereitem Zustand am Körper bei sich zu führen.[63] Es handelt sich um einen weiteren Versuch, mit präventiv-polizeilichen Mitteln den Einsatz des Strafrechts hinauszuschieben. Denn im Falle des Misserfolgs des neuen Instruments werden die Bemühungen sich auf eine Ausweitung des präventiven Strafrechts richten. Dann wird der Richter voraussichtlich nicht mehr um seine Zustimmung zur Fußfessel, sondern zur Vorbeugehaft ersucht werden.

g) Schutz der Träger von Berufsgeheimnissen

Den Trägern von Berufsgeheimnissen kommt aus gutem Grund ein besonderer Schutz zu, weil an ihnen die Achtung der Rechtsgüter ihrer Patienten und Klienten hängt, sie aber auch selbst bei ihrer Tätigkeit nicht unverhältnismäßig von staatlichen Eingriffen betroffen werden dürfen. Das *BVerfG* hatte die Unterscheidung zwischen Strafverteidigern und den in anderen Mandatsverhältnissen tätigen Rechtsanwälten als Abgrenzungskriterium für einen unterschiedlichen Schutz als verfassungsrechtlich nicht tragfähig erachtet.[64] Der neue § 62 Abs. 1 S. 7 BKAG trägt diesem Umstand Rechnung und bezieht sämtliche Rechtsanwälte und Kammerrechtsbeistände in den Schutzbereich ein.

4. Datenschutzaufsicht

Das Datenschutzrecht befindet sich, ausgelöst durch Richtlinien der Europäischen Union, im Umbruch. Abschnitt 9 des novellierten BKAG enthält Regelungen zum Datenschutz und zur Datensicherheit, welche die entsprechenden auf die Datenverarbeitung beim BKA anwendbaren Regelungen, die im zukünftigen BDSG enthalten sind, ergänzen, etwa um Besonderheiten der Struktur der Datenverarbeitung beim BKA und die verteilte datenschutzrechtliche Verantwortung im polizeilichen Informationsverbund abbilden zu können. Zentraler Standort der Umsetzung der Richtlinie (EU) 2016/680 ist aber das BDSG.[65] Auswirkungen ergeben sich allerdings auch aus dem Urteil des *BVerfG* vom 20.4.2016. Zu den umfangreichen Neuregelungen, die hier nur ansatzweise behandelt werden können, gehört § 69 Abs. 1 BKAG, der die Anforderungen aus dem vorgenannten Urteil des *BVerfG*[66] im Hinblick auf die aufsichtliche Kontrolle der Wahrnehmung der Verarbeitungsbefugnisse des BKA unternimmt. Es handelt sich insbesondere um die Übernahme von Anforderungen, die das Urteil an die Wirksamkeit der aufsichtlichen Kontrolle stellt. Die Regelung sieht dementsprechend vor, dass die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Kontrollen im Hinblick auf die Verarbeitung bei Maßnahmen nach Abschnitt 5 BKAG, das sind Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus, nach § 34 BKAG (Einsatz technischer Mittel zur Eigensicherung), nach § 64 BKAG (besondere Mittel der Datenerhebung bei Nutzung der Befugnisse zum Schutz von Mitgliedern der Verfassungsorgane) und zu Datenübermittlungen an Drittstaaten auf der Grundlage des § 27 BKAG durchführt. Damit wird – organisationssoziologisch – eine Institutionenkonkurrenz um den Datenschutz bestärkt, deren Auswirkungen vor allem die öffentliche Diskussion befeuern wird. Abzuwarten bleibt, inwieweit auch der Individualrechtsschutz von den Ergebnissen profitieren wird, denn die Maßnahmen nach § 69 Abs. 2 BKAG schließen nicht die Löschung personenbezogener Daten ein und setzen außerdem voraus, dass ein erheblicher Verstoß in Rede stehen muss.

5. Berichtspflicht gegenüber dem Deutschen Bundestag

In § 88 BKAG werden in Umsetzung der im Urteil des *BVerfG* vom 20.4.2016 enthaltenen Anforderungen turnusmäßige Berichtspflichten des BKA über die Wahrnehmung der in Abschnitt 5 (Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus) sowie in den §§ 34 und 64 BKAG enthaltenen Befugnisse eingeführt. Berichte des BKA gegenüber Parlament und Öffentlichkeit sind nach dem *BVerfG* erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Datenerhebung, einschließlich der Handhabung der Benachrichtigungspflichten und Löschungspflichten, zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen.[67]

III. Annex: Ein Wechsel vom vertikalen zum horizontalen Datenschutzkonzept?

Wie bereits erwähnt handelt es sich bei der Novellierung des BKAG und seiner Implementierung um normative, administrative und operative Teile; dies drückt sich in dem immensen Kostenrahmen aus, den die Begründung des Entwurfs Regierungskoalitionen beschreibt, aber auch in der nur annähernd ersichtlichen Kombination von sächlichen und personellen Umsteuerungen in der Verarbeitung von Daten des BKA

63 A.a.O., S. 122.
64 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 257.
65 BT-Drs. 18/11163, S. 129.
66 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 140f., 266, 340 und 354.
67 A.a.O., Rn. 143.

selbst sowie solcher der von ihm verkörperten Zentralstelle. In diesem Zusammenhang hat der Text des Koalitionsentwurfs ein Verständnisproblem ausgelöst, von dem nicht klar ist, inwieweit es sich auf die Normebene auswirkt. An mehreren Stellen seiner Begründung ist von einem Wechsel des bisherigen „vertikalen Datenschutzkonzepts" zu einem „horizontalen" die Rede.[68] Diese Kategorien finden sich weder im Normtext selbst noch wird deutlich gemacht, in welchen Normen sich die Umsteuerung manifestiere. Erläuternd wird ausgeführt, bislang werde der Datenschutz in der IT-Architektur des BKA vertikal durch die Speicherung der Daten in vielen Dateien, welche den Aufgabenzuschnitt der jeweiligen Organisationseinheiten abbilden, umgesetzt. Dies führe dazu, dass die gleichen personenbezogenen Daten in vielen verschiedenen Dateien mehrfach gespeichert seien, wenn sie für das jeweilige Aufgabengebiet des betreffenden Fachreferats des BKA erforderlich seien.[69] Zur rechtlichen Begründung für den insinuierten Systemwechsel werden zwei gesonderte Anstöße miteinander verknüpft, deren Dynamik in Bezug auf den Datenschutz aber gegenläufig ist.

Zum ersten wird ausgeführt, das bisherige System zum Schutz der personenbezogenen Daten habe das *BVerfG* in seinem Urteil vom 20.4.2016[70] für verfassungsrechtlich nicht ausreichend erachtet und es durch ein horizontal wirkendes Datenschutzkonzept, welches durch den Grundsatz der hypothetischen Datenneuerhebung bestimmt und geprägt sei, ersetzt. Es habe ausgeführt,[71] dass der Grundsatz der hypothetischen Datenneuerhebung dem Umstand Rechnung trage, „dass sich die Generierung von Wissen – nicht zuletzt auch, wenn es um das Verstehen terroristischer Strukturen gehe – nicht vollständig auf die Addition von je getrennten, nach Rechtskriterien formell ein- oder ausblendbaren Einzeldaten reduzieren lasse. In den dargelegten Grenzen erkenne das die Rechtsordnung an.[72] Diese Erwägungen zeigen in die Richtung einer Verminderung des Datengebrauchs.

Allerdings befasst sich[73] die zitierte Stelle des Urteils des *BVerfG* allein mit der Verwendung von Spurenansätzen durch die Daten erhebende Behörde und nicht mit Zweckänderungen und der hypothetischen Datenneuerhebung.[74] Die Ausführungen dazu beginnen im Urteil erst im späteren Text der Entscheidungsgründe.[75] Die vom Koalitionsentwurf bezogenen Ausführungen des *BVerfG*[76] können damit nicht – wie beabsichtigt – zur Fundierung des vorgeblich neuen Systems herangezogen werden.

Zum zweiten wird ausgeführt, ein horizontales Datenschutzkonzept, welches für den Zugriff auf Daten nicht auf die Zugehörigkeit zu einer Organisationseinheit abstelle, sondern sich auf die Bindung an die für die Datenerhebung maßgebliche Aufgabe und die Anforderungen des Rechtsgüterschutzes konzentriere,[77] biete schließlich die Möglichkeit der vollständigen Umsetzung der Empfehlung Nr. 7 für den Bereich der Polizei des NSU-Untersuchungsausschusses[78] innerhalb des Informationssystems des BKA und des polizeilichen Informationsverbundes zwischen den Polizeien des Bundes und der Länder.[79] Als Lehre aus der Aufdeckung der NSU-Mordserie im November 2011 habe der Deutsche Bundestag als Empfehlung in der o.g. Nr. 7 gefordert, die informationstechnischen Grundlagen für die notwendige Vernetzung aller an einer Ermittlung beteiligten Dienststellen müssten jederzeit sofort verfügbar sein. Der Koalitionsentwurf folgert daraus, in einem sich strikt an dem Grundsatz der hypothetischen Datenneuerhebung orientierenden zukünftigen Informations- und Verbundsystem könnten insbesondere phänomenübergreifende Abfrage- und Recherchemöglichkeiten auf der Grundlage eines einheitlichen technischen Austauschstandards (XPolizei) geschaffen werden, um die Aussagekraft der Auswerteergebnisse der polizeilichen Ermittlungsarbeit zu optimieren. Durch den Austausch von Personen-, Fall- und Sachdaten werde eine effektive Kriminalitätsbekämpfung durch die Polizeien des Bundes und der Länder sichergestellt (z.B. zur Aufklärung nicht nur länder-, sondern auch phänomenübergreifender Tat-/Täter- bzw. Tat-/Tat-Zusammenhänge).[80] Diese Erwägungen zeigen eher in die Richtung eines umfangreicheren Datengebrauchs.

Es fällt nicht leicht, sich ein Datenschutzkonzept vorzustellen, welches gleichzeitig den beiden gegenläufigen Zielen entweder einer Einschränkung oder einer Ausweitung des Gebrauchs personenbezogener Daten dienen könnte. Woraus besteht also das sog. horizontale Datenschutzkonzept und was ist sein normativer Kern im novellierten BKAG?

Der Bundesrat hat in seiner Stellungnahme zum Koalitionsentwurf genau diesen Punkt aufgegriffen und zur Prüfungsbitte zugespitzt, ob das „horizontal wirkende Datenschutzkonzept "die Vorgaben des *BVerfG* in ausreichender Weise umsetzt und die Neustrukturierung des Datenverbunds beziehungsweise der IT-Architektur den verfassungsrechtlichen Anforderungen hinreichend gerecht werde. Die Prüfungsbitte bezog sich auch auf die Neustrukturierung der IT-Architektur einschließlich der Schaffung eines Datenver-

---

68 z.B. BT-Drs. 18/11163, S. 75 u. 98.
69 A.a.O., S. 75.
70 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, BVerfGE 141, 220.
71 A.a.o., Rn. 281.
72 BT-Drs. 18/11163, S. 75.
73 Worauf der Bundesrat in seiner Stellungnahme zum Gesetzesentwurf zutreffend hinweist (BT-Drs. 18/11658, S. 1).
74 *BVerfG*, Urt. v. 20.4.2016 – 1 BvR 966/09, Rn. 281 sowie auch Rn. 280.
75 A.a.O., ab Rn. 284 bzw. Rn. 287.
76 A.a.O., Rn. 281.
77 Aus dem Zusammenhang heraus ist damit wohl der Grundsatz der hypothetischen Datenneuerhebung gemeint.
78 2. Untersuchungsausschusses nach Art. 4 GG – BT-Drs. 17/14600, S. 862.
79 BT-Drs. 18/11163, S. 76.
80 A.a.O., S. 76.

bundsystems, in welchem die Dateien in einer Zentralstelle zusammengeführt werden sollen.[81] Die Bundesregierung hat zugesagt, der Prüfbitte im weiteren Gesetzgebungsverfahren zu entsprechen.[82] Diese Spur verliert sich. Möglicherweise hat sich der Begründungsteil des Entwurfs mit dem wiederholten Gebrauch der Begriffe „vertikales Datenschutzkonzept" und „horizontales Datenschutzkonzept" aber auch nur etwas zu weit exponiert und reduziert sich Angelegenheit schlicht auf die Einstellung des zentralen Kriteriums der hypothetischen Datenneuerhebung in den Gesetzestext. Es wäre hilfreich gewesen, wenn die aufgeworfenen Zweifel im Gesetzgebungsverfahren tatsächlich ausgeräumt worden wären.

[81] A.a.O., S. 1.

[82] A.a.O., S. 10.