Digitalisierte Verwaltung Vernetztes E-Government

Herausgegeben von
Priv.-Doz. Dr. Margrit Seckelmann

Bearbeitet von

Prof. Dr. Marion Albers, Prof. Dr. Nadja Braun Binder,
Dr. Alfred G. Debus, Dr. Wolfgang Denkhaus,
Prof. Dr. Daniela Heinemann, Manuel J. Heinemann,
Dr. Thorsten Hennrich, Priv.-Doz. Dr. Tobias Herbst,
Melanie Horster, Prof. Dr. Constanze Janda,
Dr. Markus Kaulartz, Kai-Niklas Knüppel,
Prof. Dr. Dieter Kugelmann, Prof. Dr. Kai von Lewinski,
Prof. Dr. Jörn von Lucke, Prof. Dr. Andreas Mann,
Prof. Dr. Veith Mehde, Manuel Misgeld,
Prof. Dr. Ralf Müller-Terpitz, Dr. Conrad Neumann,
Priv.-Doz. Dr. Jakob Julius Nolte, Prof. Eike Richter,
Prof. Dr. Utz Schliesky, Dr. Sönke E. Schulz,
Dr. Stephan Schwarz, Priv.-Doz. Dr. Margrit Seckelmann,
Prof. Dr. Thorsten Siegel, Prof. Dr. Christoph Sorge,
Dr. Mike Weber, Maria Wilhelm, Markus Wojtczak

Begründet von

Prof. Dr. Frank Bieler und Prof. Dr. Gunnar Schwarting

2., völlig neu bearbeitete Auflage

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Weitere Informationen zu diesem Titel finden Sie im Internet unter ESV.info/978-3-503-18139-1

- 1. Auflage 2007
- 2. Auflage 2019

Gedrucktes Werk: ISBN 978-3-503-18139-1
eBook: ISBN 978-3-503-18140-7

Alle Rechte vorbehalten
© Erich Schmidt Verlag GmbH & Co. KG, Berlin 2019
www.ESV.info

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Gesetzt aus der 9/11 Stempel Garamond

Satz: multitext, Berlin
Druck und Bindung: Hubert & Co., Göttingen

Sicherheitsbehördliche Vernetzung und Datenschutz

Marion Albers

A. Einleitung

Die Vernetzung der Sicherheitsbehörden gehört zu den zentralen Bausteinen und Zielen der modernen Sicherheitsarchitektur: Den Netzwerken im Bereich des Terrorismus oder der organisierten Kriminalität soll „ein Netzwerk der Sicherheitsbehörden entgegengestellt“ werden.¹ Das ist auch, aber es ist mehr als ein Schlagwort. Die Paradigmata der „Vernetzung“, der „Netze“ oder der „Netzwerke“ beziehen sich angesichts der föderalen Strukturen und der Aufgabenteilung zwischen verschiedenen Polizei- und Verfassungsschutzbehörden zum einen auf Organisations-, Verfahrens- und Informations- oder Wissensmanagementmuster auf nationaler Ebene.² Zum anderen nutzt man sie, um bestimmte europäische Verbund- und Zusammenarbeitsformen zu erfassen und zu beschreiben, z.B. Netzwerke zum institutionalisierten Erfahrungsaustausch oder Daten- und Informationsnetze.³ Sie liefern dabei, sofern man den jeweiligen Rahmen und die Bezugspunkte präzisiert, hilfreiche Denkmuster in empirischen und sozialwissenschaftlichen, aber auch in rechtlichen Zusammenhängen. Die „Digitalisierung“ und der damit einhergehende Umbau der Verwaltung sowie der Verwaltung/Umwelt-Beziehungen⁴, der nicht zuletzt die Sicherheitsbehörden erfasst⁵, treiben solche Denkmuster voran. Umgekehrt erschließen sie sich erst dadurch mit ihren Potenzialen. Netzwerke erschöpfen sich allerdings nicht in digitalisierten Formen.

- 1 S. z.B. die Ausführungen unter https://www.protokoll-inland.de/DE/Themen/Sicherheit/Terrorismusbekämpfung/Sicherheitsbehoerden/sicherheitsbehoerden_node.html (abgerufen 30. 03. 2018); außerdem *Otto Schily*, Netzwerke des Terrors – Netzwerke gegen den Terror, in: Bundeskriminalamt (Hrsg.), *Netzwerke des Terrors – Netzwerke gegen den Terror*, München, 2005, S. 5–14, 7 ff. Zur Netzwerkstruktur des Terrorismus vgl. *Marion Albers/Lena Groth*, Globales Recht und Terrorismusfinanzierungsbekämpfung: Zur Einführung, in: dies. (Hrsg.), *Globales Recht und Terrorismusfinanzierungsbekämpfung*, Baden-Baden 2015, S. 9–35, 11.
- 2 Vgl. *Schily* (Fn. 1), S. 9 ff., unter Aspekten der Verzahnung von Aufgaben, der Organisationsstrukturen, der Koordination operativer Maßnahmen sowie der Gewinnung, des Austauschs und der Auswertung von Daten.
- 3 S. näher Rn. 6.
- 4 Übergreifend dazu *Bundesregierung*, „Digitale Verwaltung 2020“, hrsg. vom Bundesministerium des Innern, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/2014/regierungsprogramm-digitale-verwaltung-2020.pdf?__blob=publicationFile&v=3. S. außerdem die Ausführungen und das Maßnahmenbündel in: *Bundesregierung*, *Digitale Agenda 2014 bis 2017*, Berlin 2014; *Bundesregierung*, *Legislaturbericht Digitale Agenda 2014 bis 2017*, Berlin 2017; beide abrufbar unter https://www.digitaleagenda.de/Webs/DA/DE/Home/home_node.html. Außerdem übergreifend der Beitrag von *Denkhaus* im vorliegenden Handbuch (Kapitel 1), Rn. 1 ff.

(Fußnote 5 auf Seite 510)

Im Gegenteil kann eine weit getriebene Technisierung und Verdichtung sicherheitsbehördlicher Kooperation neue Interaktionsnetzwerke erfordern, wie die Institutionalisierung der Gemeinsamen Abwehrzentren deutlich macht. Dass die Vernetzung der Sicherheitsbehörden in der Praxis noch Ziel und nicht allein Befund ist, zeigt der Terroranschlag vom Breitscheidplatz, in dessen Vorfeld es eine Reihe von Fehlentscheidungen und -einschätzungen im Gemeinsamen Terrorabwehrzentrum (GTAZ) gegeben und die Vernetzung der verschiedenen Behörden defizitär funktioniert hat.⁶

- 2 Die Digitalisierung, Technisierung und Vernetzung werfen übergreifend und im Feld der Sicherheitsbehörden eine Fülle von Rechtsfragen auf. Datenschutzperspektiven sind davon nur ein Teil, allerdings ein wichtiger Teil. Es handelt sich um eine den gesamten Umgang mit Daten, Informationen und Wissen überlagernde Perspektive aus Sicht eines spezifischen (Persönlichkeits-)Schutzbedarfs. In dieser Weise muss Datenschutz als Teilelement des Umgangs mit Daten, Informationen und Wissen im Kontext übergreifender Ansätze der Wissensgenerierung und des Wissensmanagements, die sich wiederum in den Rahmen exekutiver Aufgabewahrnehmung einbetten, begriffen werden. Datenschutzregelungen erfordern eine Koordination mit den sachlichen Kompetenzen der involvierten Behörden oder Akteure, mit den Verfahrensregelungen, mit den Organisationsmustern und mit anderweitigen Informationsregelungen, z. B. denjenigen auf Dokumentenzugang.⁷ Sie selbst sind notwendig vielschichtig und fächern sich in mehrere Stränge mit verschiedenen (Teil-)Schutzzielen auf⁸. Ein angemessenes Verständnis der Schutzgüter oder der normativ geschützten Datenschutzinteressen, der Regelungserfordernisse und der Funktionen von Datenschutzregelungen ist umso wichtiger, als der Datenschutz aufgrund sowohl der Europäisierung als auch des Fortschritts der Digitalisierung und des Internets weiterentwickelt werden muss. Das Thema der mit der Digitalisierung in neuer Weise ermöglichten Vernetzung von Behörden und weiteren Akteuren macht diese und weitere Herausforderungen besonders anschaulich.

5 Dazu noch Rn. 8 ff. Übergreifend s. auch den Beitrag von *Seckelmann* im vorliegenden Handbuch (Kapitel 1), Rn. 1 ff. S. außerdem die Beiträge in: *Thomas-Gabriel Rüdiger/Petra Saskia Bayerl* (Hrsg.), *Digitale Polizeiarbeit. Herausforderungen und Chancen*, Wiesbaden, 2018.

6 Eine Chronik des Behördenhandelns mit Stand Februar 2017 ist abrufbar unter: http://www.bmjv.de/SharedDocs/Artikel/DE/2017/01162017_Chronologie.html (abgerufen 30.03.2018). S. auch die Kleine Anfrage der Abgeordneten *Mihalic* u.a., BT-Drs. 18/10812, und die Antwort der *Bundesregierung* BT-Drs. 18/11027.

7 S. näher *Marion Albers*, *Umgang mit personenbezogenen Informationen und Daten*, in: *Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle* (Hrsg.), *Grundlagen des Verwaltungsrechts*, Bd. 2, 2. Aufl., München 2012, § 22, Rn. 92 ff.

8 Hierzu *Marion Albers*, *Informationelle Selbstbestimmung*, Baden-Baden 2005, S. 454 ff. S. außerdem zum europäischen Datenschutzgrundrecht *Nikolaus Marsch*, *Das europäische Datenschutzgrundrecht*. Grundlagen – Dimensionen – Verflechtungen, Tübingen 2018; *Jörn Reinhardt*, *Konturen des europäischen Datenschutzgrundrechts*. Zu Gehalt und horizontaler Wirkung von Art. 8 GRCh, AöR 142 (2017), S. 528–564, 529 ff.

B. Grundlagen: Vernetzung und Digitalisierung

I. Vernetzung, Netze und Netzwerke als konkretisierungsbedürftige Paradigmata

Wenn man komplexe Verbund- und Zusammenarbeitsformen als Vernetzung, als Netze oder als Netzwerke erfasst, arbeitet man im Ausgangspunkt mit eher unscharfen Begriffen. Charakteristisch ist deren metaphorischer Gehalt. Gerade deswegen greift man aber sowohl in alltagssprachlichen Zusammenhängen als auch in verschiedenen wissenschaftlichen Disziplinen gerne auf sie zurück. Ihr jeweiliger Sinn divergiert dabei allerdings ebenso wie die Verwendungskontexte. Der Begriff der „Vernetzung“ bezeichnet für sich genommen nicht mehr als eine Verknüpfung zweier oder mehrerer Einheiten unter bestimmten Aspekten. Etwas weiter gehend bietet das Paradigma der „Netzwerke“ ein anschauliches Bild: man vergegenwärtigt sich eine Konstruktion, die sich auf elementarer Ebene aus Verbindungslinien und Knoten und auf übergeordneter Ebene aus Maschen als spezifischer Struktur zusammensetzt.⁹ Das Bild ermöglicht und erzwingt es, dass man sich von einer punktuell-isolierenden Betrachtung löst, Kontexte mitdenkt und den Blick für die Vielfältigkeit von (Wechsel-)Beziehungen öffnet. In Abgrenzung gegen pyramidische Formen hat man zudem mit einem im Ansatz heterarchischen Arrangement und mit funktional gestaltbaren, beweglichen Verbindungen zu tun. Das bedeutet nicht, dass die jeweiligen Elemente deswegen notwendig vollständig gleichwertige Positionen innehätten¹⁰ oder Teile komplexerer Netzwerke nicht auch hierarchische Strukturmuster aufweisen könnten. Nähere Aussagen, die die Kategorien der Vernetzung oder der Netzwerke erst verständlich und ertragreich machen, setzen eine Präzisierung des theoretischen Zugriffs und der Erkenntnisinteressen, des Begriffsrahmens und der Abgrenzungskriterien im Hinblick auf andere Paradigmata sowie der jeweils relevanten Bezugsebenen und Bezugspunkte voraus.

In empirischen oder theoretischen sozialwissenschaftlichen Untersuchungen spielt das Netzwerkparadigma eine wachsende Rolle. Zu deren gemeinsamen Ausgangsannahmen gehört, dass Netzwerke als relativ stabile Arrangements eingeordnet werden, die sich sowohl gegen Marktmechanismen als auch gegen hierarchische Formen abgrenzen lassen.¹¹ Meist geht es um ein strukturell verdichtetes Beziehungsgeflecht zwischen mehreren Akteuren, das durch spezifische Mechanismen der Koordination von (Teil-)Handlungen oder der Informations-

9 Vgl. *Dorothea Jansen*, Einführung in die Netzwerkanalyse, 3. Aufl., Wiesbaden 2006, S. 13. Zur Relevanz von Metaphern und Bildern im Recht s. *Sigrid Boysen/Ferry Bühning/Claudio Franzius/Tobias Herbst/Matthias Kötter/Anita Krentz/Kai von Lewinski/Florian Meinel/Jakob Nolte/Sabrina Schönrock*, Netzwerke im Öffentlichen Recht, in: dies. (Hrsg.), Netzwerke, Baden-Baden 2007, S. 289–300, 291 f.

10 Im Gegenteil interessieren sich Netzwerkanalysen gerade für hegemoniale Positionen oder für die unterschiedliche Dichte von Verbindungen.

11 Grundlegend hierzu *Walter W. Powell*, Weder Markt noch Hierarchie: Netzwerkartige Organisationsformen, in *Patrick Kenis/Volker Schneider* (Hrsg.), Organisation und Netzwerk, Frankfurt 1996, S. 213–271.

und Wissensgenerierung, durch mehr oder weniger reziproke Beiträge der Beteiligten und durch die sich herausbildenden netzwerkspezifischen Erwartungs- und Handlungsmuster gekennzeichnet ist.¹² Abgesehen von solchen Gemeinsamkeiten sind die theoretische Rahmung und die gewählten Bezugspunkte konkreter Analysen unterschiedlich. Das betrifft etwa die Fragen, ob Personen oder Organisationen als Netzwerkknoten oder „Adressen“¹³ gewählt oder ob Handlungskoordinationen oder der Austausch von Daten und Wissensgenerierungsmuster in den Blick genommen werden. Keineswegs alle, aber einige der sozialwissenschaftlichen Ansätze grenzen Netzwerke gegen funktionssystemische Differenzierungen und Rollen¹⁴ oder gegen Strukturmuster „formaler“ Organisationen oder Verfahren ab.¹⁵ Netzwerke zeichnen sich dann dadurch aus, dass relevante Kommunikationen nicht allein in den vorgegebenen Formen stattfinden, sondern auch in darüber hinausgehenden, formale Formen gegebenenfalls überspielenden „informellen“ Beziehungsgeflechten, die sich über Vertrauen oder persönliche Bekanntschaft stabilisieren.

- 5 In rechtlichen Analysen muss man unterscheiden, ob Vernetzung, Netze oder Netzwerke allein als Kategorien empirischer oder sozialwissenschaftlicher Untersuchungen oder ob sie als Rechtskategorien begriffen werden sollen.¹⁶ Rechtliche Überlegungen, die empirische oder sozialwissenschaftliche Studien zur „Vernetzung“ von Behörden oder zu institutionellen „Netzwerken“ als Grundlage heranziehen, sind im jeweils zu begründenden Ausgangspunkt unproblematisch und können je nach Erkenntnisinteresse hilfreich sein. Entsprechende Beobachtungs- und Beschreibungsperspektiven können auf der normativen Ebene erstens das Verständnis komplexer und miteinander verzahnter Regelungen erleichtern. Das gilt etwa im Bereich des Datenaustauschs: während das hier häufig verwendete Bild der (Daten-)„Ströme“ unverändert bleibende Komponenten nahelegt, macht

12 Vgl. etwa *Karl-Heinz Ladeur*, Der Staat der „Gesellschaft der Netzwerke“. Zur Notwendigkeit der Fortentwicklung des Paradigmas des „Gewährleistungsstaates“, Der Staat 2009, S. 163–192, 175; „Als Netzwerk sollten in einer rechts- und sozialwissenschaftlichen Perspektive primär nicht-hierarchische Beziehungen zwischen privaten oder öffentlichen Akteuren, Ressourcen und Entscheidungen verstanden werden, deren Selbstkoordination emergente, nicht unabhängig vom Prozess ihrer Hervorbringung denkbare Regeln, Handlungsmuster und Erwartungen erzeugen kann.“

13 *Michael Bommes/Veronika Tacke*, Das Allgemeine und das Besondere des Netzwerkes, in: dies. (Hrsg.), Netzwerke in der funktional differenzierten Gesellschaft, Wiesbaden, 2011, S. 25–50, 28, 30 ff.

14 *Boris Holzer*, Die Differenzierung von Netzwerk, Interaktion und Gesellschaft, in: Bommes/Tacke (Fn. 13), S. 51–66, 59 ff.

15 S. z.T. als Überblick *Dorothea Jansen/Andreas Wald*, Netzwerke, in: Arthur Benz/Susanne Lütz/Uwe Schimank/Georg Simonis (Hrsg.), Handbuch Governance, Wiesbaden 2007, S. 93–105; dies., Netzwerktheorien, ebd., S. 188–199. S. auch mit anderer Akzentuierung aus systemtheoretischer Perspektive *Bommes/Tacke* (Fn. 13), S. 34 ff.

16 Empirische Beschreibungen, sozialwissenschaftlich-theoretische Ansätze oder rechtsdogmatische Konzeptionen können aufeinander bezogen, dürfen aber nicht vermengt werden (was nicht selten vorkommt). S. dazu auch *Eberhard Schmidt-Aßmann*, Verwaltungsrechtliche Dogmatik, Tübingen 2013, S. 139 f., 163.

das Bild eines „Netzes“ deutlicher, dass es darum geht zu begreifen, welche wie veränderten Daten an welche Stellen in welche neuen Kontexte gelangen und mit welchen Folgen zu Informationen und Wissen umgewandelt werden. Zweitens könnte man beispielsweise evaluieren, ob rechtliche Regelungen sachgerecht funktionieren oder angesichts anders stabilisierter Kommunikationsmuster ins Leere laufen, denen man dann entweder entgegenkommen oder entgegenwirken müsste. Drittens ließen sich sozialwissenschaftliche Überlegungen zu Funktionsweisen oder Strukturen von Behördennetzen oder zu Netzwerken nutzen, damit rechtliche Regelungen passend gestaltet werden. Auch dies kann gerade im Bereich des Datenschutzes oder im Hinblick auf „Sicherheitsnetzwerke“ staatlicher und privater Akteure, die sich aus den über traditionelle dogmatische Denkmuster erzeugten Perspektiven nur verkürzt erschließen, weiterführend sein. Netze oder Netzwerke werden dabei nicht zu Rechtsbegriffen, solange es bei eigenständigen rechtlichen Kategorien bleibt, mit denen man Organisation, Verfahren oder Daten- und Informationsverarbeitungen erfasst.

Ob und inwiefern Netze oder Netzwerke „(organisations-)rechtsunspecifische 6 Kennzeichnungen komplexer Verflechtungsphänomene“¹⁷ sind oder als rechtsdogmatisch verankerte und folgenreiche, gegen etablierte Figuren abgrenzbare Rechtskategorien eingestuft werden können, ist umstritten. Koordinations- und Kooperationsformen, die man durchaus treffend so begreifen kann, haben sich allerdings inzwischen vor allem in europäischen Zusammenhängen in bestimmtem Umfang rechtlich etabliert, etwa im Telekommunikationsrecht, im Umweltrecht, im Lebensmittelrecht oder im Sicherheitsrecht.¹⁸ Sie sind über Institutionalisierung-, Rahmen- und Verfahrens- oder auch Rechtsfolgenbestimmungen verankert, ohne dass jedoch sämtliche rechtlichen Bausteine darauf eingestellt und abgestimmt wären. Dass man ihre Rechtsprobleme deswegen zumindest teilweise mit anderweitigen rechtlichen Figuren abarbeiten muss, mag den Streit über ihre rechtliche Einordbarkeit erklären. Schon um den Blick für die teilweise eigenständigen Rechtsprobleme zu schärfen, ist eine Unterscheidung zwischen „Netzen“,

17 So *Matthias Jestaedt*, Grundbegriffe des Verwaltungsorganisationsrechts, in: Wolfgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band I, 2. Aufl., München 2012, § 14, Rn. 18.

18 S. mit Beispielen *Christoph Möllers*, Netzwerk als Kategorie des Organisationsrechts, in: Janbernd Oebbecke (Hrs.), Nicht-normative Steuerung in dezentralen Systemen, Stuttgart, 2005, S. 285–302, 290 ff.; *Karl-Heinz Ladeur*, Was leistet die Netzwerkanalyse für die Verwaltungswissenschaft?, in: Veith Mehde/Ulrich Ramsauer/Margrit Seckelmann (Hrsg.), Staat, Verwaltung, Information, FS Bull, Berlin 2011, S. 639–657, 651 f.; *Katrin Schoppa*, Europol im Verbund der europäischen Sicherheitsagenturen, Baden-Baden 2013, S. 328 ff.; *Manuel Patrick Schwind*, Netzwerke im europäischen Verwaltungsrechts, Tübingen 2017, S. 151 ff. S. auch *Nikolaos Simantiras*, Netzwerke im europäischen Verwaltungsverbund, Tübingen 2016, S. 26 ff., der Netzwerke allerdings als rein deskriptive Kategorie und dann funktional als Verwaltungskooperation begriff, die mit einer Kombination aus Verwaltungsorganisations-, Verfahrens- und materiellem Recht erschlossen werden kann. Vgl. außerdem in internationalen Zusammenhängen *Lena Groth*, Globales Finanzmarktrecht gegen Terrorismusfinanzierung, Baden-Baden 2016, S. 79 ff.

die zwar durch Vernetzung, aber nicht zumindest auch durch Charakteristika wie eine mehr oder weniger weit reichende Informalität gekennzeichnet sind¹⁹, und „Netzwerken“ sinnvoll.²⁰ Auch eine Typenbildung – z.B. in Netze oder Netzwerke zum institutionalisierten Erfahrungsaustausch²¹, dem Datenaustausch und der Wissensgenerierung dienende oder vollzugsunterstützende, -beeinflussende oder -gestaltende Informationsnetze oder -netzwerke²², Regulierungs-, Planungs- oder Vollzugsnetze oder -netzwerke²³, Behördennetzwerke im Bürgerinteresse²⁴ – ist trotz mancher Überschneidungen weiterführend. Von den Feldern her ist das europäische Sicherheitsrecht eines der Referenzgebiete vor allem für Informationsnetze oder -netzwerke²⁵, die man partiell mit einem sich herausbildenden Netz- oder Netzwerkrecht²⁶ erfassen kann und muss. Für das nationale Sicherheitsrecht gilt dagegen bislang, dass Vernetzung, Netze und Netzwerke noch nicht als Rechtsbegriffe etabliert und in rechtsdogmatischen Zusammenhängen andere Kategorien maßgeblich sind.

- 7 Im nationalen Sicherheitsrecht können diese Kategorien gegenwärtig als Grundlage der Beschreibung tatsächlicher Phänomene nützlich sein. Darüber hinaus sind die Anfänge eines europäischen Netz- und Netzwerkrechts für produktive Überlegungen und für Strukturierungen hilfreich. Man sollte die durch koopera-

19 Nähere Überlegungen erfordern eine weitere Präzisierung, weil die Differenz formell/informell von den Bezugspunkten abhängt und sich im übergreifenden Kontext relativieren kann, s. zutr. Möllers (Fn. 18), S. 297 f.

20 Markus A. Glaser, Internationale Verwaltungsbeziehungen, Tübingen 2010, S. 272 f.

21 Zum Typus Bettina Schöndorf-Haubold, Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen et al. (Fn. 9), S. 149–171, 156 f.

22 Schwind (Fn. 18), S. 167 ff.; s.a. Schöndorf-Haubold (Fn. 21), S. 158 ff., hier ohne die notwendige Unterscheidung zwischen Vernetzung, Netzen und Netzwerken.

23 Schwind (Fn. 18), S. 241 ff.; Wolfgang Kahl, Europäische Behördenkooperationen – Typen und Formen von Verbundsystemen und Netzwerkstrukturen, in: Michael Holoubek/Michael Lang (Hrsg.), Verfahren der Zusammenarbeit von Verwaltungsbehörden in Europa, Wien 2012, S. 15–46, 35 ff.

24 Schwind (Fn. 18), S. 155 ff.

25 S. etwa Schoppa (Fn. 18), S. 103 ff., 333 ff.; Schwind (Fn. 18), S. 184 ff.; Hartmut Aden, Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem, dms 2014, S. 55–73, 63 ff. Übergreifender zu europäischen Entwicklungen Bettina Schöndorf-Haubold, Das Recht der Zivilen Sicherheit an der Schnittstelle von nationaler, europäischer und internationaler Zuständigkeit, in: Christoph Gusy/Dieter Kugelmann/Thomas Würtenberger (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin/Heidelberg 2015, S. 691–718, Rn. 3 ff.; zur polizeilichen Zusammenarbeit auf der Ebene der EU etwa Dieter Kugelmann, Europäische Polizeiliche Kooperation, in: Martin Böse (Hrsg.) Europäisches Strafrecht mit polizeilicher Zusammenarbeit, Enzyklopädie Europarecht Bd. 9, Baden-Baden 2013, S. 631–678; zu weiteren grenzüberschreitenden bilateralen Zusammenarbeitsformen s. auch Marion Albers, Datenverarbeitung und Datenschutz als Aufgabe der grenzüberschreitenden Verwaltungskooperation. Am Beispiel der grenzüberschreitenden polizeilichen Zusammenarbeit, in: Uwe Kischel/Hinnerk Wißmann (Hrsg.), Grenzüberschreitende Verwaltungsaufgaben, Stuttgart u.a. 2017, S. 59–77.

26 Frühzeitige Anfangsüberlegungen dazu bei Schöndorf-Haubold (Fn. 21), S. 168 ff. Vgl. weiter Schoppa (Fn. 18), S. 334 ff.; Schwind (Fn. 18), S. 295 ff.

tions- oder informationsrechtliche Regelungen (faktisch) entstehenden Behörden „netze“ gegen Arrangements wie die als „Netzwerke“ beschreibbaren Gemeinsamen Abwehrzentren²⁷ abgrenzen. Auch Typisierungen etwa in Netzwerke zwecks institutionalisierten Erfahrungsaustauschs, Informationsnetze oder Informationsnetzwerke zwecks Wissensgenerierung oder unmittelbarer Vollzugsunterstützung oder Koordinations- und Planungsnetzwerke sind sinnvoll. „Vernetzung“ beschreibt als Grundelement die Verknüpfung sicherheitsbehördlicher Einheiten unter einem bestimmten Aspekt (Handlungskoordination, arbeitsteilige Verfahren, Datenaustausch) vor dem Hintergrund komplexerer und mitzudenkender Arrangements.

II. Digitalisierung sicherheitsbehördlicher Arbeit

Ebenso wie „Vernetzung“ und „Netzwerke“ ist die „Digitalisierung“ mittlerweile ein Schlagwort, aber eben auch mehr als das. Die ursprünglich primär informationstechnische Bedeutung bezeichnet die Umwandlung von Objekten analogen Formats in digitale und hier regelmäßig binäre Werte (vor allem 1 und 0 als Dualsystem). Die damit verbundene Technikentwicklung hat von der Datenverarbeitung durch Rechner über die Integration von rechnergestützter Datenverarbeitung (Computertechnik) und Datenübertragung (Nachrichtentechnik) bis hin zum Internet als einem Set untereinander verknüpfter, im Grundsatz dezentral organisierter, aber nach bestimmten Standards und einheitlichen (Meta-)Protokollfamilien arbeitender Netze und Rechner geführt. Das Internet ist kein Medium, sondern eher eine vielschichtige Infrastruktur. Man teilt seine Geschichte in verschiedene Phasen ein, ohne dass die Entwicklungsschritte im Sinne einer linearen und bruchlosen Evolution verstanden werden könnten. Das ab Anfang der 2000er Jahre beginnende Web 2.0 hat vor allem mit den Sozialen Netzwerken die heutige Gesellschaft und auch die Arbeit der Sicherheitsbehörden bereits deutlich verändert.²⁸ Mit den nächsten Schritten steht ein noch weiter reichender Wandel an. Das Web 3.0, das „semantische Web“, zielt darauf, mittels komplexer Programmarchitekturen und Metadatenzuordnungen, maschinenunterstützten Lernens und künstlicher Intelligenz „Bedeutungen“ von Daten in kontextualen Bezügen zu erfassen. Nahezu parallel dazu verläuft die Entwicklung des Web 4.0, der internetvermittelten Vernetzung der Dinge. Unter technischen Aspekten beschreibt das „Internet der Dinge“²⁹ die Vernetzung unterschiedlichster physischer Objekte mit dem Internet und darüber vermittelt auch untereinan-

27 Vgl. hierzu auch *Alisa Sommerfeld*, Verwaltungsnetzwerke am Beispiel des Gemeinsamen Terrorismusabwehrzentrums des Bundes und der Länder (GTAZ), Berlin 2015, insb. S. 226 ff.

28 Ausf. *Seckelmann* (Fn. 5), Rn. 3, 6 ff.

29 Der Begriff „Internet of Things“ (IoT) wird auf *Kevin Ashton* zurückgeführt, der damit die Vision eines gerade hinsichtlich der Datenverarbeitung relativ autonom operierenden Systems vernetzter Rechner und Dinge bezeichnete: *That „Internet of Things“ Thing*, RFID Journal 1999, <http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf> (abgerufen 31.03.2018).

der mit Hilfe einer Reihe ergänzender (und auch außerhalb des Internets einsatzfähiger³⁰) Techniken und Instrumente, etwa der RFID-Technik, speziellen Sensortechniken, Chiptechniken oder Energieversorgungstechniken. Nicht selten sollen Techniken und Internetprozesse dabei im Hintergrund wirken, möglichst unauffällig in Handlungsabläufe integriert werden, allgegenwärtig und gleichzeitig unsichtbar sein.³¹ Welches Veränderungspotenzial das Internet der Dinge birgt, erschließt sich, wenn man die wachsenden Speicher-, Verarbeitungs- und Auswertungsfunktionalitäten im Zusammenhang mit Cloud Computing, Big Data Analytics-Methoden oder künstlicher Intelligenz hinzunimmt.³² Die Zukunftsszenarien des „Internet of Bodies“ prognostizieren angesichts der Konvergenz von Bio-, Gen-, Neuro- und Informationstechniken, dass Implantate von smart lenses über memory chips bis hin zu brain-to-brain-interfaces den Körper technisieren und die Menschen darüber „unmittelbar“ mit dem Internet vernetzen werden. In Abgrenzung zur Sicht in den Anfangsjahren des Internet, die es wie einen eigenständigen Raum konzipierte, den „Cyberspace“ als „virtuelle“ in Abgrenzung zur „wirklichen“ Realität³³, redet man heute von der „onlife“³⁴-Welt. Vor diesem Hintergrund ist „Digitalisierung“ zu einem Bündelungsbegriff geworden, der weit über die ursprünglich informationstechnische Bedeutung hinaus auf den gesellschaftlichen, kulturellen oder ökonomischen Wandel zielt, der durch das binäre digitale Format, die dadurch erreichten Datenverarbeitungsmöglichkeiten, die Konvergenz und das Zusammenspiel verschiedenster Techniken, umfassende Vernetzungen und die neue Rolle von Daten, Informationen und Wissen entsteht.

- 9 Entsprechend weit reichen die Folgen der „Digitalisierung“, die unter anderem die Möglichkeiten sicherheitsbehördlicher Ermittlungen, interne Organisationsstrukturen, die Vernetzung von Sicherheitsbehörden, aber auch die Außenkommunikation und gesellschaftliche Erwartungen an die sicherheitsbehördliche Arbeit³⁵ betreffen.³⁶ Bei den Ermittlungsmöglichkeiten kann das Internet mit seinen

30 Dieses breite, auch internetunabhängige Einsatzspektrum wird meist mit dem Begriff „ubiquitous computing“ oder „pervasive computing“ beschrieben.

31 S. dazu – mit Hinweisen auf daraus resultierende Probleme, insbesondere Privatheitsrisiken – das White Paper des Forums „Privatheit und selbstbestimmtes Leben in der digitalen Welt“, Das versteckte Internet: Zu Hause – Im Auto – Am Körper, 2015.

32 S. zum Überblick, auch über verschiedene Einsatzfelder, die Beiträge in: *Nilanjan Dey/Aboul Ella Hassanien/Cbintan Bhatt/Amira S. Ashour/Suresh Chandra Satapathy* (Eds.), *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, Cham 2018.

33 Frühzeitig kritisch dazu *Stefan Münker*, Was heißt eigentlich: „Virtuelle Realität“? Ein philosophischer Kommentar zum neuesten Versuch der Verdopplung der Welt, in: ders./Alexander Roesler (Hrsg.), *Mythos Internet*, Frankfurt am Main 1997, S. 108–127, bes. 115 ff.

34 Etwa *Mireille Hildebrandt*, *Smart Technologies and the End(s) of Law*, Cheltenham 2016, S. 1 ff.

35 S. zutr. *Seckelmann* (Fn. 5), Rn. 1 f.

36 S. auch die Beiträge in: *Thomas-Gabriel Rüdiger/Petra Saskia Bayerl* (Hrsg.), *Digitale Polizeiarbeit. Herausforderungen und Chancen*, Wiesbaden 2018.

verschiedenen Schichten und über Dienste, die technisch ausgereifte Verschlüsselungen der Internetkommunikationen anbieten, zwar sicherheitsbehördliche Ermittlungen erschweren oder sogar vor unüberwindbare Hindernisse stellen. Ganz überwiegend eröffnet es jedoch mit der Verdattung der Kommunikation im Internet weit reichende Überwachungsmöglichkeiten. Von zunehmender Bedeutung ist dabei der staatliche Zugriff auf Daten, die Private gespeichert haben und freiwillig oder unfreiwillig herausgeben. Denn übergreifend betrachtet sammeln Private Daten unter den Bedingungen der Digitalisierung und des Internets weitaus umfassender (und unkontrollierter) als der Staat. Zudem können die Sicherheitsbehörden den Ertrag bestimmter Ermittlungsmethoden erheblich verbessern, etwa im Falle einer Öffentlichkeitsfahndung (auch) in sozialen Netzwerken³⁷ oder „smarter“ Videoüberwachung.³⁸ Unter den Bedingungen der Digitalisierung reicht es nicht, sich auf einzelne Ermittlungsmethoden und punktuelle Datenerhebungseingriffe zu konzentrieren. Man muss immer auch Datenverknüpfungen, Datenauswertungsformen, Datenübermittlungen und Datenverbände, Datenkreisläufe und Datenverarbeitungsprogramme als vorweggenommene Entscheidungs- und Bewertungsverfahren mitbedenken. Was den Umgang mit Daten angeht, liegt die Zukunft der sicherheitsbehördlicher Arbeit im Übrigen nicht allein in Tools zur prädiktiven Beschreibung von potentiellen Gefahrensituationen und potentiellen Tätern anhand von Algorithmen („predictive policing“).³⁹ Sie liegt auch im Einsatz ausgefeilter automatischer Auswertungsprogramme⁴⁰, schon damit Sicherheitsbehörden nicht „in Daten ertrinken“⁴¹. Außerdem liegt sie in einer effektiven Vernetzung der Sicherheitsbehörden, wie sie durch die Digitalisierung grundsätzlich ermöglicht wird.

37 Hierzu *Seckelmann* (Fn. 5), Rn. 1 f.

38 Dazu *Marion Albers*, Zukunftsszenarien polizeilicher Überwachung, in: Heinrich-Böll-Stiftung Sachsen/Johannes Lichdi (Hrsg.), *Digitale Schwellen. Privatheit und Freiheit in der digitalen Welt*, Dresden 2015, S. 135–147, 143; *Cornelius Held*, *Intelligente Videoüberwachung. Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz*, Berlin 2014, S. 15 ff.

39 *Albers* (Fn. 38), S. 141 ff.; *Timo Rademacher*, *Predictive Policing im deutschen Polizeirecht*, AöR 142 (2017), S. 366–416; vgl. auch zu den Erfordernissen und Schwierigkeiten der Ausarbeitung treffender formaler Modelle *Mohammad A. Tayebi/Uwe Glässer*, *Social Network Analysis in Predictive Policing – Concept, Method and Models*, Cham 2016.

40 Zu der in diesem Rahmen dringend nötigen Unterscheidung von Daten, Informationen und Wissen und zu den Möglichkeiten und Grenzen den Beitrag von *Weber* im vorliegenden Handbuch (Kapitel 4). Übergreifender zu Schwierigkeiten etwa *Rita Haverkamp*, *Die Prognose von terroristischen Anschlägen: Grenzen wissenschaftlicher Erkenntnisse und der Versuch zur Entwicklung eines Präventionsmodells*, ZStW 2011, S. 92–109, 100 ff. S. außerdem den Überblick bei *Matthias Bäcker*, *Big Data und Sicherheitsrecht*, in: Wolfgang Hoffmann-Riem (Hrsg.) *Big Data – Regulative Herausforderungen*, Baden-Baden 2018, S. 167–172.

41 *Schulte-Lob*, *Sicherheitsbehörden ertrinken in Daten – WDR Interview mit Jan-Philipp Albrecht*, 10.06.2016 (<http://www1.wdr.de/radio/wdr5/sendungen/morgenecho/eu-parlament-datenaustausch-terror-100.html>, abgerufen 11.03.2017).

- 10 Das Schlagwort „Digitalisierung“ ist allerdings auch trügerisch. Es scheint eine mehr oder weniger problemlose Realisierbarkeit prinzipiell eröffneter Möglichkeiten zu versprechen. Wie voraussetzungsvoll viele technisch grundsätzlich mögliche Anwendungen sind und dass sie nie allein von technischen Grundlagen abhängen, haben mehr als 50 Jahre sozialwissenschaftliche Technikforschung und Technikfolgenabschätzungen jedoch klargestellt. Bei der sicherheitsbehördlichen „Vernetzung“ geht es nicht nur um Interoperabilität, um rechtlichen Gestaltungsbedarf oder um rechtliche Hindernisse. Es geht immer auch um komplexe sozio-technische Zusammenhänge. Das zeigt sich bei der Vernetzung europäischer Informationssysteme⁴² ebenso wie auf nationaler Ebene.

C. Datenschutz vor neuen Herausforderungen

- 11 Aus rechtlicher Perspektive ist der sicherheitsbehördliche Umgang mit Informationen und Daten durch Datenschutzanforderungen gebunden. Diese sind wiederum stark durch das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG, das Telekommunikationsgeheimnis aus Art. 10 GG und durch die einschlägigen Entscheidungen des Bundesverfassungsgerichts geprägt worden, zuletzt namentlich durch die Entscheidung des BVerfG zum BKA-Gesetz.⁴³ Ebenso wie die Datenschutz-Grundverordnung⁴⁴ führt die Richtlinie zu Polizei und Strafjustiz⁴⁵, die neben grenzüberschreitenden auch rein innerstaatliche Datenverarbeitungen in Datenbanken, elektronischen Vorgangsbearbeitungssystemen oder strukturierten Akten erfasst, zu einem Europäisierungsschub.⁴⁶ Allerdings fallen die Nachrichtendienste nicht unter diese Vorgaben. Die Richtlinie setzt Mindeststandards unter anderem für die Festlegung von Gegenstand und Zwecken der Datenverarbeitung, für die Erforderlichkeit, für Zweckänderungen, für die Verarbeitung sensibler Daten, für die kategoriale Differenzierung in Anspruch genommener Personen, für automatisierte Einzelent-

42 Hierzu *Eric Töpfer*, Verheddert im Netz der DNA-Datenbanken. Prüm und die Mythen der Interoperabilität, in: Michael Plöse/Thomas Fritsche/Michael Kuhn/Sven Lüders, „Worüber reden wir eigentlich?“, Festgabe für Rosemarie Will, Berlin, 2016, S. 809–826.

43 BVerfG, Urteil v. 20.04.2016, 1 BvR 966/09 und 1140/09 = BVerfGE 141, 220 *BKA-Gesetz*; NJW 2016, 1781.

44 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1. Hierzu den Beitrag von *Herbst* im vorliegenden Handbuch (Kapitel 16), Rn. 2, 8 ff.

45 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 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. 2016 L 119/89.

46 Hierzu *Kugelmann* im vorliegenden Handbuch (Kapitel 18), Rn. 2, 8 ff., s. insbes. auch Rn. 15: „Der eigenständig bestimmte Anwendungsbereich der Richtlinie verdrängt die Datenschutz-Grundverordnung.“

scheidungen und Profilingmaßnahmen, für Datenübermittlungen vor allem an Drittstaaten und internationale Organisationen, für Informationsrechte betroffener Personen und für die Befugnisse der Datenschutzaufsichtsbehörden.⁴⁷

Über die Vorgabe sekundärrechtlicher Maßstäbe hinaus führt die Richtlinie zu Polizei und Strafjustiz im Zusammenwirken mit der Datenschutz-Grundverordnung, auf der die Richtlinie partiell aufbaut, zur Einschlägigkeit der Unionsgrundrechte, zu einer Zuständigkeit des Europäischen Gerichtshofs und zu einer aufgewerteten Rolle der Fachgerichte. Wie weit Art. 51 Abs. 1 GRCh reicht, nach der die Mitgliedstaaten an die Unionsgrundrechte gebunden sind, soweit sie Unionsrecht „durchführen“, ist zwischen BVerfG und EuGH umstritten. Das BVerfG vertritt, wie es in der Entscheidung zum Antiterrordatei-Gesetz bekräftigt hat, die Position, dass der nationale Gesetzgeber „in Durchführung des Rechts der Union“ handelt, sofern es sich bei dem nationalen Umsetzungsgesetz um einen vollständig unionsrechtlich determinierten Rechtsakt handelt. Sofern jedoch ein Gestaltungsspielraum besteht und im Umsetzungsgesetz eigene Einschätzungen und Abwägungsergebnisse des nationalen Gesetzgebers zum Tragen kommen, hält es nicht die Unionsgrundrechte, sondern allein die nationalen Grundrechte für anwendbar.⁴⁸ Der EuGH vertritt dagegen weiter reichende Perspektiven: Mitgliedstaatliche Maßnahmen unterliegen den Bindungen an die Unionsgrundrechte dann, wenn sie sich im Sinne im Anwendungsbereich des Unionsrechts bewegen, und ob der notwendige Zusammenhang zwischen einem Unionsrechtsakt und nationalen Maßnahmen gegeben ist, ist nach einem Kriterienbündel zu bestimmen.⁴⁹ Zudem erfolgt auch die Ausfüllung von Umsetzungs- und Gestaltungsspielräumen, wie sie Richtlinien enthalten, aus Sicht des EuGH in Durchführung des Rechts der Union und ist an die Unionsgrundrechte gebunden.⁵⁰ Neben den danach immer einschlägigen Unionsgrundrechten kommt aus Sicht des EuGH eine Anwendung nationaler Schutzstandards in Betracht, „sofern durch diese Anwendung weder das Schutzniveau der Charta, wie sie vom Gerichtshof ausgelegt wird, noch der Vorrang, die Einheit und die Wirksamkeit des

47 Näher *Kugelman* (Fn. 46), Rn. 8 ff.; *Matthias Bäcker*, Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hermann Hill/Dieter Kugelman/Mario Martini (Hrsg.), Perspektiven der digitalen Lebenswelt, Baden-Baden 2017, S. 63–88, 68 ff.; *Robert Weinhold/Paul C. Johannes*, Europäischer Datenschutz in Strafverfolgung und Gefahrenabwehr – Die neue Datenschutz-Richtlinie im Bereich Polizei und Justiz sowie deren Konsequenzen für deutsche Gesetzgebung und Praxis, DVBl 2016, S. 1501–1506.

48 BVerfG, Urteil v. 24.04.2013, 1 BvR 1215/07 = BVerfGE 133, 277 – *Antiterrordatei-Gesetz*, Rn. 88 ff. Zusammenfassend *Gabriele Britz*, Grundrechtsschutz durch das Bundesverfassungsgericht und den Europäischen Gerichtshof, EuGRZ 2015, S. 275–281 m.w.N.

49 Weit gefasst noch EuGH, Urt. v. 26.02.2013 = *Akerberg Fransson*, Rs. C-617/10, Rn. 16 ff.; enger dann die Folgerechtsprechung, etwa EuGH, Urt. v. 6.03.2014, Rs. C-206/13, Rn. 20 ff.; Urt. v. 10.07.2014, Rs. C-198/13, Rn. 34 ff.

50 Vgl. EuGH (GK), Urt. v. 21.12.2011, Rs. C-411/10 u.a., Rn. 77 ff.; EuGH, Urt. v. 21.12.2016 = *Tele Sverige AB* u.a., C-203/15 und C-698/15, Rn. 82 ff.

Unionsrechts beeinträchtigt werden“.⁵¹ In der Literatur wird teilweise aus Art. 53 GRCh als Schutzniveaunklausel gefolgert, dass im Rahmen von Gestaltungsspielräumen eine „doppelte Grundrechtsbindung“ sowohl an die Unionsgrundrechte als auch an die nationalen Grundrechte bestehe und dann im Sinne der Meistbegünstigung der höhere Grundrechtsstandard gelte.⁵² Teilweise gelangt man zu einer Bindung sowohl an die Unionsgrundrechte als auch an die nationalen Grundrechte, indem man die determinierten Gesichtspunkte und den Determinationsgrad aufschlüsselt und danach differenziert.⁵³ Der Streit um die Anwendbarkeit der Unions- und/oder der nationalen Grundrechte ist sowohl im Anwendungsbereich der Datenschutz-Grundverordnung, soweit sie Öffnungsklauseln und Spielräume enthält, als auch im Anwendungsbereich der Richtlinie für Polizei und Strafjustiz von auch praktisch großer Relevanz.

- 13 Gleichgültig, wie man sich hier positioniert: in mehr oder weniger weit reichendem Umfang werden die nationalen Grundrechte und die Rechtsprechung des BVerfG durch die unionalen Grundrechte und die Rechtsprechung des EuGH abgelöst. Das BVerfG hat den Schutzbereich des für den Datenschutz bislang zentralen Rechts auf informationelle Selbstbestimmung weit reichend, aber zugleich inhaltlich blass bestimmt, die Vorgaben des Telekommunikationsgeheimnisses und der Unverletzlichkeit der Wohnung weitgehend parallelisiert und ergänzend weitere fallspezifisch einschlägige Freiheitsgrundrechte herangezogen. Nicht eine inhaltliche Konkretisierung der Schutzgüter – anders formuliert: der mit Blick auf die Grundrechtsgewährleistung begründbaren Datenschutzinteressen –, sondern vor allem das Übermaßverbot ist wesentlicher Anker fein ziselierter Maßstäbe, und auch die wichtigen Figuren der Zweckfestlegung und Zweckbindung werden normativ zu rudimentär verankert.⁵⁴ Der EuGH hat bislang vor allem Art. 7 und Art. 8 GrCh als relevante Grundrechte hervorgehoben, aber teilweise auch auf anderweitige Freiheitsgewährleistungen zurückgegriffen, insbesondere auf die Meinungsfreiheit.⁵⁵ Art. 8 GrCh schützt das Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten. Vom Normtext her handelt es sich um eine offene Formulierung, die eine relative Ausgestaltungsbedürftigkeit impliziert. Maßstäbe und Dogmatik dieses Grundrechts sind auf unionaler Ebene noch nicht ausgefeilt. Aber schon aus rechtsdogmatischen Gründen verbietet sich ein schlichter „Transfer“ des Rechts auf informationelle Selbstbe-

51 EuGH, Urt. v. 26. 02. 2013 = *Akerberg Fransson*, Rs. C-617/10, Rn. 29.

52 Vgl. dazu mit weiter gehenden Ausführungen *Claudio Franzius*, Grundrechtsschutz in Europa, ZaöRV 2015, S. 383–412, 394 ff.

53 S. etwa *Christoph Ohler*, Grundrechtliche Bindungen der Mitgliedstaaten nach Art. 51 GRCh, NVwZ 2013, S. 1433–1438, 1437 f.

54 Kritisch und mit Nachweisen aus der Rspr. *Marion Albers*, Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in: Michael Friedewald/Jörn Lamla/Alexander Roßnagel (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, S. 11–31, 17 ff.

55 S. die Entscheidungen zur Vorratsdatenspeicherung, EuGH, Urt. v. 8. 04. 2014 = *Digital Rights Ireland* u. a., C-293/12 u. C-594/12., Rn. 23 ff.; Urt. v. 21. 12. 2016 = *Tele Sverige AB* u. a., C-203/15 und C-698/15, Rn. 93 ff.

stimmung auf die unionsrechtliche Ebene, wie er in der Literatur gelegentlich umstandslos erfolgt. Die zunehmende Diskussion über die inhaltlichen Aussagen des Art. 8 GrCh zeigt, dass das „Grundrecht auf Datenschutz“ gerade mit seiner offenen Formulierung eine Chance bietet, vielschichtige und mehrdimensionale Maßgaben zu entwickeln.⁵⁶ Weitere Grundrechte treten hinzu.

Die Europäisierung trifft mit zahlreichen neuen Herausforderungen in der Sache zusammen, vor denen der Datenschutz aufgrund der Entwicklungen des Internets und der Digitalisierung steht. Zu den zentralen Problemen gehört, wann genau Daten personenbezogen sind und inwieweit das für den Schutz entscheidende Kriterium der Personenbezogenheit überhaupt noch passt.⁵⁷ Keineswegs alle Konstellationen, aber etwa Verarbeitungsformen im Big-Data-Kontext oder Re-Identifikationsmöglichkeiten aufgrund der Zugänglichkeit und Verknüpfbarkeit von Daten werfen teilweise kaum lösbare Probleme der Abgrenzbarkeit personenbezogener und nicht-personenbezogener Daten auf.⁵⁸ Gerade deswegen wird man die Schutzgüter oder die rechtlich schutzwürdigen Datenschutzinteressen, die im Recht auf informationelle Selbstbestimmung blass geblieben sind, schärfen müssen. Das gilt zudem, weil neue Diskussionen um Schutzerfordernisse und Schutzkonzeptionen hinzukommen. Angesichts des Internets der Dinge gibt es zum Beispiel zunehmende Debatten um ein Eigentum an generierten Daten.⁵⁹ Der Einsatz komplexer und lernender Algorithmen im Internet oder in anderweitigen Zusammenhängen der Verarbeitung großer Datenmengen hat Diskussionen über deren Regulierung und etwaige Rechtsansprüche ausgelöst. So sollen die „Transparenz“, die „Neutralität“ oder die „Richtigkeit“ von Algorithmen oder erwartbarer Ergebnisse deren Einsatzes gewährleistet werden.⁶⁰ Die künftig wichtigeren europäischen Debatten sind außerdem breitgefächert und inhaltsreich,

56 Zu diesem Erfordernis s. die Nw. in Fn. 8.

57 Personenbezogen sind dabei auch Daten, die mit Hilfe von Datenverknüpfungen oder Zusatzwissen auf Personen bezichbar sind. S. die Legaldefinition in Art. 4 Ziff. 1 und Erwägungsgrund 26 der Datenschutz-Grundverordnung v. 4.05.2016, ABl. EU L 119/1.

58 Aus der Rechtsprechung etwa zur Personenbezogenheit dynamischer IP-Adressen s. EuGH, Urt. v. 19.10.2016, C-582/14, Rn. 32 ff., zur Personenbezogenheit von Prüferanmerkungen in einer berufsbezogenen Prüfung EuGH, Urt. v. 20.12.2017, C-434/16, Rn. 27 ff.; jeweils abrufbar unter curia.europa.eu. Übergreifender *Martin Sebastian Haase*, Datenschutzrechtliche Fragen des Personenbezugs, Tübingen 2015, insb. S. 338 ff.; *Nadya Purtova*, The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation, and Technology 2018, DOI:10.1080/17579961.2018.1452176. Vgl. außerdem zur US-amerikanischen Debatte *Paul M. Schwartz/Daniel J. Solove*, The PII-Problem: Privacy and a New Concept of Personally Identifiable Information, *New York University Law Review* 86 (2011), S. 1814–1894, 1815 ff.

59 Dazu differenziert und kritisch *Lothar Determann*, No One Owns Data, *Hastings Law Journal* Vol. 70 (2018), i.E.

60 Aus der breiten Debatte s. *Wolfgang Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, *AöR* 2017, S. 1–42, 2 ff.; *Mario Martini*, Algorithmen als Herausforderung für die Rechtsordnung, *JZ* 2017, S. 1017–1025, 1017 ff.

was etwa die Schutzerfordernisse hinsichtlich der mit dem Internet und der Digitalisierung ermöglichten Massenüberwachung angeht.⁶¹ Angesichts dessen, dass das europäische Sicherheitsrecht ein Referenzgebiet für die „informationelle Vernetzung“ unterschiedlicher Akteure und für den Datenaustausch und der Wissensgenerierung dienende oder vollzugsunterstützende, -beeinflussende oder -gestaltende Informationsnetze oder -netzwerke⁶² ist, sind darüber hinaus Diskussionen zu erwarten, wie ein vernetzungs- oder netzwerkgerichtetes Datenschutzrecht zu gestalten ist. Zu den wichtigen Fragen zählt, auf welchen wie erhobenen und verarbeiteten Datengrundlagen welche Informationen und welches Wissen, hier etwa Verdachtsmuster, mit welchen Folgen oder Freiheitskosten gerade in den vernetzten Zusammenhängen entstehen und wie man dies schutzgütergerecht reguliert. Antworten setzen die Ausarbeitung übergreifender Kontexte voraus, unter anderem die Analyse der sachlichen Aufgaben und Befugnisse der vernetzten Behörden oder Akteure. Vor dem Hintergrund des Bildes der Informationsnetze oder -netzwerke wird darüber hinaus deutlich, wie vielschichtig und vielfältig datenschutzrechtliche Vorgaben sein müssen.

D. Informationelle Vernetzung der Sicherheitsbehörden

- 15 Im deutschen föderalistischen System stößt die Vernetzung der Sicherheitsbehörden schon deshalb auf Probleme, weil vor dem Hintergrund der Länderorganisationskompetenz eigene Infrastruktur- und Softwaresysteme angeschafft und aufgebaut wurden.⁶³ Die verschiedenen Systeme, Verfahren oder Dateiformate sind nur eingeschränkt kompatibel und nur begrenzt über Schnittstellen verbunden. Teilweise müssen verbundrelevante Daten mehrfach in unterschiedliche Systeme eingegeben werden, damit sie allen an einem Verbund Beteiligten zur Verfügung stehen. Vor diesem Hintergrund hat die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK) auf ihrer Tagung im November 2016 die „Saarbrücker Agenda zur Digitalisierung der Inneren Sicherheit“ beschlossen.⁶⁴ Sie zielt auf den Aufbau einer gemeinsamen, modernen und einheitlichen Informationsarchitektur für die Polizeien des Bundes und der Länder. Die Polizistinnen und Polizisten sollen nach Maßgabe der rechtlichen Rahmenbedingungen jederzeit und überall Zugriff auf diejenigen Informationen

61 Exemplarisch *Maria Tzanou*, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford/Portland 2017.

62 Oben Rn. 6.

63 Zur „zersplitterten IT-Landschaft“ und daraus resultierenden Problemen *Bundesministerium des Innern*, *Polizei 2020 – White Paper*, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.pdf?__blob=publicationFile&v=1, S. 1. S. auch etwa *Aden* (Fn. 25), S. 61, 63.

64 *Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit* v. 30. 11. 2016, <https://www.medien-service.sachsen.de/medien/medienobjekte.download/110307>.

haben, die sie benötigen, um ihre Aufgaben zu erfüllen. Erreicht werden soll eine digitale, medienbruchfreie Vernetzung der Polizei mit ihren nationalen und internationalen Partnern.⁶⁵ Die Saarbrücker Agenda gehört zu den Grundlagen des Programms Polizei 2020.⁶⁶

Rechtliche Rahmenbedingungen für die informationelle Vernetzung der Sicherheitsbehörden reichen von Kooperations- und Zusammenarbeitsregelungen über Datenschutzbestimmungen bis hin zu allgemeinen Vorgaben für technische Standards⁶⁷ und Vorschriften zur IT-Sicherheit. Die Aspekte sind in bestimmten Umfang miteinander verbunden und insoweit zu koordinieren. Für den Austausch personenbezogener Daten finden sich Rahmenbedingungen vor allem in der Richtlinie zu Polizei und Justiz, in den allgemeinen Datenschutzgesetzen und in den bereichsspezifischen Fachgesetzen von Bund und Ländern. Neben allgemein relevanten Maßgaben etwa zum Systemdatenschutz, zum Datenschutz durch Technik, zu Informationsrechten oder zu Berichtigungspflichten gelten für den Datenaustausch vor allem Vorgaben, die in Gestalt einer Phasenregulierung die Übermittlung, Bereitstellung oder Dateneingabe auf Seiten der einen Stelle und den Empfang oder Abruf und die Weiterverwendung der Daten auf Seiten der anderen Stelle regeln. Dieses „Doppeltürmodell“ mit der Beteiligung zweier Stellen führt dazu, dass zwei Kontexte und Regelungskomplexe miteinander koordiniert werden müssen, dies ggf. im Bund-Länder-Verhältnis.⁶⁸ Zudem sind Weiterleitung und Empfang nicht isoliert, sondern ihrerseits als Elemente vorangegangener bzw. nachfolgender Datenverarbeitungsprozesse zu betrachten.⁶⁹ Beispielsweise erschließt sich die Bedeutung des Datenempfangs, auch hinsichtlich seiner Eingriffsintensität, erst mit Blick darauf, wie lange Daten bei der empfangenden Stelle gespeichert, wie sie verknüpft und wie sie verwendet werden dürfen. Das wiederum wirkt darauf ein, wie die Datenweiterleitungs- und die Datenempfangsbefugnisse auszugestalten sind. Die einzelnen Regelungselemente solcher Befugnisse kann man funktional aufschlüsseln. Im Wesentlichen geht es um Elemente, die sich auf den Verwendungszweck und die Zweckbindung beziehen, um das Tatbestands-

65 S. für die europäische Ebene auch die Vorschläge der Europäischen Kommission vom 12. 12. 2017 für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen, hinsichtlich Grenzen und Visa: COM (2017) 793 final, hinsichtlich polizeiliche und justizielle Zusammenarbeit, Asyl und Migration: COM (2017) 794 final.

66 Fn. 63.

67 Vgl. hierzu übergreifend *Ivo Appel*, Technische Standards und Software: Ermöglichung oder Präjudizierung von Entscheidung und Zusammenarbeit, in: Hermann Hill/Utz Schliesky (Hrsg.), Herausforderung e-Government, Baden-Baden 2009, S. 113–130.

68 *Marion Albers*, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001, S. 334 f.; *Nikolaos Gazeas*, Übermittlung nachrichtendienstlicher Erkenntnisse an Strafverfolgungsbehörden, Berlin 2014, S. 228 f., 501 ff.

69 BVerfG, Urteil v. 24. 04. 2013, 1 BvR 1215/07 = BVerfGE 133, 277 – *Antiterrordatci-Gesetz*, Rn. 111.

merkmal der Erforderlichkeit, um gegenstandsbezogene Tatbestandsvoraussetzungen, die Art oder Aussagegehalte der relevanten Daten oder Informationen konkretisieren, um Weiterleitungs- oder Empfangsschwellen, die sich beispielsweise an einem eingegrenzten Kreis geschützter Rechtsgüter orientieren oder besondere Prognoseanforderungen stellen, um Tatbestandsvoraussetzungen zur differenzierten Inanspruchnahme bestimmter Personen (Zielpersonen, Kontakt- und Begleitpersonen), um bestimmte Schutzvorkehrungen und um Verantwortlichkeitsverteilungsregeln.⁷⁰ Im Näheren hängt die Ausgestaltung der Regelungen und der einzelnen Regelungselemente unter anderem von den Rollen und Funktionen der beteiligten Behörden, sei es im Verhältnis Bund – Land, sei es im Verhältnis Polizeien – Nachrichtendienste⁷¹, und von den Formen der Vernetzung ab.

I. Datenübermittlung und Datenempfang

- 17 Traditionelles Kernelement der informationellen Vernetzung zwischen den beteiligten Sicherheitsbehörden sind Regelungen zur gegenseitigen Übermittlung und zum Empfang von Daten. Die einschlägigen Vorschriften stellen häufig eine Mischung von Zusammenarbeits- und Datenschutzvorgaben dar, denn der in einer einheitlichen Vorschrift geregelte Gegenstand einer Übermittlung betrifft nicht nur personenbezogene, sondern sämtliche Daten. Man kann die Vorschriften zunächst danach systematisieren, ob die Übermittlung zur Erfüllung eigener Aufgaben oder zur Erfüllung von Aufgaben der empfangenden Stelle, ob sie aus eigener Veranlassung oder auf Ersuchen und ob sie obligatorisch oder fakultativ erfolgt. Die Übermittlung von Informationen einschließlich personenbezogener Daten von den Polizeien an die Nachrichtendienste ist unter bestimmten Voraussetzungen obligatorisch.⁷² Die Datenübermittlung von den Nachrichtendiensten an die Polizeien ist dagegen regelmäßig als fakultative Befugnis⁷³ und namentlich in Fällen der Verhinderung oder Verfolgung von Staatsschutzdelikten als Pflicht⁷⁴ ausgestaltet. Die informationelle Zusammenarbeit zwischen den Polizeien untereinander⁷⁵ und zwischen den verschiedenen Nachrichtendiensten untereinander⁷⁶ gestaltet sich nach den jeweiligen Regelungen eng. Die Übermittlungsschwellen, die dem Datenschutz Rechnung tragen sollen, sind in den eigentlichen Ermächtigungen regelmäßig niedrig. Es gibt aber „hinter die Klammer“ gestellte Übermitt-

70 S. für eine Aufschlüsselung der Regelungselemente auch *Marion Albers*, Datenschutzbestimmungen der Polizei- und Nachrichtendienstgesetze des Bundes, in: Heinrich Amadeus Wolff/Stefan Brink (Hrsg.), *Datenschutzrecht*, Beck'scher Online-Kommentar, 25. Edition, München, Stand 5/2018, Rn. 62.

71 Zum hierfür hergeleiteten „informationellen Trennungsprinzip“ s. BVerfG, Urteil v. 24.04.2013, 1 BvR 1215/07 = BVerfGE 133, 277 – *Antiterrordatei-Gesetz*, Rn. 123.

72 S. §§ 18 Abs. 1 BVerfSchG, 23 Abs. 2 BNDG.

73 Etwa §§ 19 Abs. 1 BVerfSchG, 24 Abs. 1 BNDG.

74 Vgl. §§ 20 Abs. 1 BVerfSchG, 24 Abs. 3 BNDG, 11 Abs. 2 MAIDG. Ausf. dazu im Hinblick auf Übermittlungen an die Strafverfolgungsbehörden *Gazeas* (Fn. 68), S. 291 ff.

75 Vgl. exemplarisch § 32 Abs. 1 BPoIG.

76 Exemplarisch § 20 Abs. 1 S. 2 BVerfSchG.

lungsverbote in Gestalt von Abwägungsklauseln.⁷⁷ Die datenempfangende Stelle muss obligatorisch prüfen, ob die Daten für die Erfüllung ihrer Aufgaben überhaupt erforderlich sind.⁷⁸ Im Übrigen gibt es neben der allgemeinen Zweckbindung⁷⁹ im Falle der Erhebung personenbezogener Daten mittels besonders eingriffsintensiver Methoden eingengte Zweckbindungen. Die engere Zweckbindung ist im Falle von Datenübermittlungen zu beachten, der datenempfangenden Stelle aufzugeben und bestimmt insofern auch den weiteren Verarbeitungsprozess.⁸⁰

Datenübermittlung und Datenempfang werden in diesen Regelungen nur scheinbar aus einer eher punktuellen Perspektive betrachtet. Es handelt sich um Grundelemente der Vernetzung der Sicherheitsbehörden. Sie sind im Hinblick auf vorangehende und nachfolgende Verarbeitungsprozesse und zudem im Kontext zu erfassen. In der Praxis spielen sie neben automatisierten zentralen Dateien mit einer Vielzahl angeschlossener Stellen eine große Rolle, weil diese Dateien aus einer Reihe rechtlicher Gründe engeren rechtlichen Grenzen unterliegen. So sind etwa die Antiterror- und die Rechtsextremismusdatei im Grundsatz auf eine Kontakt- und Informationsanbahnung zugeschnitten; im Trefferfall erfolgt ein Datenaustausch in einem konkreten Komplex nach Maßgabe der grundlegenden Datenübermittlungs- und -empfangsbestimmungen.⁸¹

II. Zentraldateien und Verbunddateien

Eines der wichtigsten Elemente der Vernetzung der Sicherheitsbehörden sind Zentraldateien und vor allem Verbunddateien für den elektronischen Datenverbund zwischen Bund und Ländern.⁸² Solche Dateien werden vom Bundeskriminalamt, vom Zollkriminalamt und vom Bundesamt für Verfassungsschutz in Ausübung ihrer Zentralstellenfunktion geführt. Zu den Verbunddateien zählen das Informationssystem der Polizei INPOL⁸³, das Zollfahndungsinformationssystem INZOLL und das nachrichtendienstliche Informationssystem NADIS. Die an dem jeweiligen Verbundsystem beteiligten Stellen des Bundes und der Länder

77 S. etwa § 33 Abs. 3 BPolG oder §§ 23 BVerfSchG, 31 BNDG, 12 MADG. Danach unterbleibt eine Übermittlung u.a. dann, wenn für die übermittelnde Stelle erkennbar ist, dass unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen oder besondere Pflichten zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen bestehen.

78 Zu dieser Prüfpflicht s. exemplarisch § 25 BVerfSchG.

79 S. etwa § 33 Abs. 6 BPolG.

80 S. etwa §§ 25 Abs. 1 i.V.m. 12 Abs. 3 BKAG, 19 Abs. 1 BVerfSchG, 24 Abs. 1 S. 3 BNDG.

81 Dazu noch Rn. 22 ff.

82 S. zu den verschiedenen Dateiformen Kurt Graulich, in: Wolf-Rüdiger Schenke/Kurt Graulich/Josef Rutbig (Hrsg.), *Sicherheitsrecht des Bundes*, München 2014, BKAG § 8 Rn. 5 ff.

83 Zur Entwicklung und zum Aufbau von INPOL Anicee Abbühl, *Der Aufgabenwandel des Bundeskriminalamts*, Stuttgart u.a. 2010, S. 148 ff.

pflügen in einer vielfältig, partiell gestuft gestalteter Form selbst Daten ein und können Daten nach Maßgabe von Berechtigungen auch unmittelbar abrufen.

Die gegenwärtige Ausgestaltung ist allerdings verbesserungsbedürftig. Nimmt man INPOL als Beispiel, enthält es unterschiedliche Datenbanken, so für die polizeiliche Fahndung, für allgemeine Auskunftszwecke oder verbundrelevante Daten aus den Fallbearbeitungssystemen, die in beispielsweise nach Deliktstypen strukturierten Dateien gespeichert werden. Da sich Datenbestände in voneinander isolierten Silos befinden und keine übergreifende Verknüpfung zwischen den unterschiedlichen Datenbanken besteht, können bestimmte Verbindungen zwischen eingespeisten Daten nicht systemunterstützt ermittelt werden. Zudem mangelt es, und dies ist eine interessante Information, an einem mit den rechtlichen Anforderungen abgestimmten Zugriffsberechtigungskonzept. Nicht zuletzt führen die unterschiedlichen IT-Systeme der Polizeien in Bund und Ländern zu Schnittstellenproblemen mit der Folge, dass manche Daten manuell in das Verbundsystem eingegeben werden muss(t)en oder eine Eingabe dann eben unterbleibt.⁸⁴

- 19 Künftig soll die Architektur dieses Verbundsystems im Anschluss an die Saarbrücker Agenda fundamental umgestaltet werden.⁸⁵ Es bleibt bei einem Verbundsystem mit einer Verantwortlichkeitsverteilung auf das Bundeskriminalamt als Zentralstelle und die datenverantwortlichen Stellen der Polizeien des Bundes und der Länder. Allerdings soll es ein neu konzeptioniertes „Datenhaus“ beim Bundeskriminalamt geben. Beim Umbau sollen bisherige Innovationsschritte integriert werden. Dazu gehören die Einrichtung des Polizeilichen Informations- und Analyseverbundes (PIAV), das einen bruchlosen Datenaustausch zur Aufklärung länder- und phänomen- oder dateiübergreifender tat- und personenbezogener Zusammenhänge ermöglichen soll, und die Entwicklung eines einheitlichen Fallbearbeitungssystems. Weitere Komponenten sind das Zugriffs- und Rechtekonzept und Schritte zur Sicherstellung der Interoperabilitätsvoraussetzungen etwa hinsichtlich des Datenmodells oder Austauschformats. Das „Datenhaus“ zeichnet sich dadurch aus, dass verbundrelevante Daten in einem einheitlichen System nur einmal nach den gleichen Regeln erfasst und durch die Nutzung zentraler Dienste einheitlich verarbeitet werden. Die Zentralstellenfunktion des Bundeskriminalamts schließt dabei ein, dass es den Polizeien von Bund und Ländern Anwendungen und Dienste bereitstellt, die zentral unter Einbeziehung der Anforderungen von Bund und Ländern entwickelt werden. In der Sache soll das Informationssystem eine leichtere Eingabe, über funktionale Module und Dienste eine ertragreichere Recherche und vor allem eine bessere verfahrens- und dateiübergreifende Verknüpfung von Daten zur Herstellung von Zusammenhängen ermöglichen. Der Datenzugriff soll über ein Berechtigungsmanagement gesteuert werden, das sich in Abstimmung mit rechtlichen Anforderungen aufgaben-, rollen- und kontextbezogen gestaltet. Ziel ist es, der Polizei im Sinne des „Grund-

84 Zur Problembeschreibung s. *BMI, Polizei 2020* (Fn. 64), S. 5 ff. Zur Beschreibung des Inpol-Systems s. auch *Graulich* (Fn. 82), BKAG § 11 Rn. 3 ff.

85 Zum Folgenden *BMI, Polizei 2020* (Fn. 64), S. 6 ff.

satzes der Verfügbarkeit“ die für die polizeiliche Arbeit erforderlichen Daten zu jeder Zeit an jedem Ort nach Maßgabe der rechtlichen Anforderungen zur Verfügung zu stellen. Im Übrigen soll auch eine bessere Basis für den unionalen und internationalen Datenaustausch geschaffen werden.

Die Grundlage für den Umbau des Verbundsystems soll das neue BKAG liefern. Es wurde mit Blick auf das Urteil des BVerfG zum bisherigen BKA-Gesetz⁸⁶ und zwecks Umsetzung der Richtlinie zu Polizei und Strafjustiz⁸⁷ novelliert. Danach ist das Bundeskriminalamt Zentralstelle für den polizeilichen Informationsverbund zwischen Bund und Ländern und stellt zu diesem Zweck ein einheitliches Verbundsystem zur Verfügung. Es selbst nimmt mit seinem eigenen Informationssystem an diesem Verbund teil. Teilnahmeberechtigt sind außerdem u.a. die Landeskriminalämter, sonstige Polizeibehörden der Länder, die Bundespolizei und das Zollkriminalamt. Mit Blick auf die Grundfunktionen des Verbundsystems, etwa Unterstützung bei polizeilichen Ermittlungen, bei der polizeilichen Informationsverdichtung oder bei strategischen Analysen⁸⁸, stellen die teilnehmenden Behörden einander verbundrelevante⁸⁹ Daten zum Abruf und zur Verarbeitung zur Verfügung.⁹⁰ Das Bundeskriminalamt hat durch organisatorische und technische Maßnahmen sicherzustellen, dass Eingaben von und Zugriffe auf Daten im polizeilichen Informationsverbund nur möglich sind, soweit die jeweiligen Behörden hierzu berechtigt sind.⁹¹ Die dafür unter anderem geltenden Maßgaben werden mit einem Verweis auf eine entsprechende Geltung zentraler für die Datenweiterverarbeitung des BKA geltenden Regelungen verankert.⁹² Danach greifen insbesondere der „Grundsatz der hypothetischen Datenenerhebung“⁹³, die dafür nötigen Kennzeichnungspflichten⁹⁴, die Bindung an die Erforderlichkeit der Kenntnis der Daten für mehr oder weniger konkretisierte Aufgaben und Pflichten⁹⁵ sowie sachlich oder personell mehr oder weniger differenzierte Schwellen für die Datenverarbeitung. Neben der Abstimmung mit den Vorgaben, die das BKAG selbst enthält, ist eine Koordination mit den für die jeweiligen beteiligten Stellen geltenden Rechtsgrundlagen erforderlich.⁹⁶

Vom Ausgangspunkt einer besseren Vernetzung der Sicherheitsbehörden, bei der zugleich Datenschutzanforderungen gewährleistet sind, ist die Verbesserung der Architektur des Informationsverbundes notwendig. Die Ausgestaltung der neuen

86 BVerfG, Urteil v. 20.04.2016, 1 BvR 966/09 und 1140/09 = BVerfGE 141, 220 *BKA-Gesetz*.

87 Oben Rn. 11.

88 §§ 29 Abs. 2 i.V.m. 13 Abs. 2 BKAG.

89 § 30 BKAG.

90 § 29 Abs. 2 S. 2 BKAG.

91 § 29 Abs. 4 S. 1 BKAG.

92 § 29 Abs. 4 S. 2 BKAG.

93 § 29 Abs. 4 S. 2 i.V.m. § 12 Abs. 2 – 5 BKAG.

94 § 29 Abs. 4 S. 2 i.V.m. § 14 BKAG.

95 Etwa § 29 Abs. 4 S. 2 i.V.m. § 15 Abs. 1 Nr. 2 BKAG.

96 Vgl. oben Rn. 16.

Regelungen des BKAG ist jedoch nicht in jeder Hinsicht gelungen. Das liegt nicht zuletzt daran, dass der Gesetzgeber verfassungsrechtliche Vorgaben als Orientierung gewählt hat, die aus dem BKA-Urteil des Bundesverfassungsgerichts herauskristallisiert worden sind. Unabhängig davon, ob die gesetzgeberische Deutung immer passt, sind manche der vom Bundesverfassungsgericht abgesteckten Maßgaben missverständlich. Das betrifft gerade die zentralen Ausführungen, die der Neugestaltung des polizeilichen Informationsverbundes zu Grunde gelegt werden. Jedenfalls nicht als generelle Grundlinie für jedwede anderweitige Nutzung missverstehen darf man die verfassungsgerichtlichen Ausführungen zur Rolle einer Datenerhebungsermächtigung für Zweckfestlegung, Zweckbindung und eine sich in diesem Rahmen haltende weitere Nutzung.⁹⁷ Der Gesetzgeber scheint sie im Sinne einer mittels der Erhebungsermächtigung ggf. weit gespannten einheitlichen Zweckfestlegung zu deuten. Richtig ist, dass die immer abstrakten, typisierenden oder auch verschiedene Fallkonstellationen bündelnden gesetzlichen Erhebungsermächtigungen einen Rahmen für die Festlegung der Verwendungszwecke setzen, die die zuständige Behörde verfahrensbezogen oder auch im Hinblick auf einen konkreten Aufgabenkomplex vorzunehmen hat.⁹⁸ Nur ein solches Verständnis trägt den Anforderungen des Art. 4 Abs. 1 lit. b, c oder e der Richtlinie zu Polizei und Strafjustiz Rechnung. Müsste die jeweilige Erhebungsermächtigung als solche abschließend die Zweckfestlegung liefern, gelangte man entweder zu kontraproduktiven Bestimmtheits- und Präzisierungserfordernissen hinsichtlich des Gesetzes oder zu Ergebnissen, die mit datenschutzrechtlichen Anforderungen, wie sie über Zweckfestlegung, Zweckbindung und (geregelte) Zweckänderungsmöglichkeiten gewährleistet werden sollen, unvereinbar wären. Das macht

97 Entscheidend sind die Ausführungen in BVerfG, Urteil v. 20.04.2016, 1 BvR 966/09 und 1140/09 = BVerfGE 141, 220 *BKA-Gesetz*, Rn. 278 f.: „Der Gesetzgeber kann 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 verfassungsrechtlichen Anforderungen an eine Zweckänderung. Die zulässige Reichweite solcher Nutzungen richtet sich nach der Ermächtigung für die Datenerhebung. Die jeweilige Eingriffsgrundlage bestimmt Behörde, Zweck und Bedingungen der Datenerhebung und definiert damit die erlaubte Verwendung. Die Zweckbindung der auf ihrer Grundlage gewonnenen Informationen beschränkt sich folglich nicht allein auf eine Bindung an bestimmte, abstrakt definierte Behördenaufgaben, sondern bestimmt sich nach der Reichweite der Erhebungszwecke in der für die jeweilige Datenerhebung maßgeblichen Ermächtigungsgrundlage. 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.“

98 Ausführlich zu den Bausteinen der Zweckfestlegung, Zweckbindung und Zweckänderungsmöglichkeiten, insbes. auch zu ihren Funktionen, ihrer Ausgestaltung und ihrer Konkretisierung *Marion Albers* (Fn. 8), S. 497 ff.

ein Blick auf die oft weit und bündelnd formulierten sicherheitsbehördlichen Erhebungsermächtigungen schnell klar.⁹⁹ Auch das „Kriterium der hypothetischen Datenenerhebung“¹⁰⁰ ist im Urteil des BVerfG nicht in einer Weise formuliert, dass es als Grundsatz zentrale Datenschutzerfordernisse erfüllen und als Grundlage für die Ausarbeitung von Berechtigungen in einem automatisierten Datenaustauschverbund ausreichen könnte. Die unterschiedlichen Funktionen des Bundesverfassungsgerichts, seiner Verfahren und seiner Entscheidungen einerseits und der Gesetzgebung andererseits werden verkannt, wenn man meint, Urteile des Bundesverfassungsgerichts ließen sich gleichsam 1:1 umsetzen. Das ambitionierte Projekt einer Neukonzeption der Architektur des polizeilichen Verbundsystems wird daher noch einige Arbeit und gesetzgeberische Nacharbeit erfordern.

III. Gemeinsame Dateien von Polizeien und Nachrichtendiensten

Ein weiteres Element der informationellen Vernetzung der Sicherheitsbehörden ist die Möglichkeit einer befristeten projektbezogenen Führung gemeinsamer Dateien zwischen Polizeien und Nachrichtendiensten. Entsprechende Rechtsgrundlagen in den Fachgesetzen ermächtigen das Bundeskriminalamt, das Bundesamt für Verfassungsschutz oder den Bundesnachrichtendienst zur Errichtung einer solchen Datei und benennen beteiligte Behörden.¹⁰¹ Darüber hinaus sehen spezielle Gesetze die Errichtung gemeinsamer Dateien in bestimmten Sachbereichen vor. Die jeweils beteiligten Behörden sind dann verpflichtet, bereits erhobene Daten, die automatisiert verarbeitet werden dürfen, unter bestimmten Voraussetzungen in der gemeinsamen Datei zu speichern.¹⁰² Grundsätzlich sollen automatisierte zentrale gemeinsame Dateien den Informationsaustausch zwischen den jeweils beteiligten Behörden effektivieren und die Datenlage zu bestimmten Personen, Objekten oder Sachverhalten verdichten, indem Erkenntnisse, über die eine der beteiligten Behörden verfügt, eingegeben werden, zu einem neuen Bild beitragen und für alle beteiligten Behörden zugänglich sind.¹⁰³ Je nach Ausgestaltung der Gemeinsamen Datei machen sie einen Datenaustausch nach den allgemeinen Datenübermittlungs- und Datenempfangsregelungen aber nicht überflüssig. Treffer in der Datei können vielmehr einen solchen Austausch erfordern und auslösen. Das gilt vor allem, wenn die Funktion und Ausgestaltung der Verbunddatei sich im Prinzip auf eine Kontakt- und Informationsanbahnung beschränken. Paradigmatisch hierfür sind die gemeinsame standardisierte zentrale Antiterrordatei mit der Regelung im Antiterrordateigesetz (ATDG) und die gemeinsame

⁹⁹ Zu den vielfältigen Problemen der neuen Regelungen des BKAG s. auch *Matthias Bäcker*, Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz. *VerfBlog* 2017/6/08, DOI: 10.17176/20170608-215340.

¹⁰⁰ BVerfG, Urteil v. 20.04.2016, 1 BvR 966/09 und 1140/09 = BVerfGE 141, 220 *BKA-Gesetz*, Rn. 287.

¹⁰¹ §§ 17 BKAG, 22a BVerfSchG, 25 BNDG.

¹⁰² Vgl. zur Speicherpflicht § 2 ATDG, § 2 RED-G.

¹⁰³ Vgl. die Begründung zum Gesetzentwurf der Bundesregierung zum Gemeinsame-Dateien-Gesetz v. 16.10.2006, BT-Drs. 16/2950, S. 1, 12 f.

standardisierte zentrale Datei zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus mit der Regelung im RED-G.¹⁰⁴

- 23 Zweck der informationellen Vernetzung der Sicherheitsbehörden, die an der beim Bundeskriminalamt geführten Antiterror- und Rechtsextremismusdatei jeweils beteiligt sind, ist die Erfüllung der jeweiligen gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland bzw. zur Aufklärung oder Bekämpfung des gewaltbezogenen Rechtsextremismus.¹⁰⁵ Neben allgemeinen Bausteinen zur Realisierung des Datenschutzes – Auskunftsansprüche, Berichtigungs- und Löschungspflichten, Protokollierungspflichten, Regelungen zur datenschutzrechtlichen Verantwortung, Berichts- und Evaluationsregeln, Kontrolle durch die Bundesbeauftragte für Datenschutz und Informationsfreiheit und die jeweiligen Landesbeauftragten – unterliegen die Dateneinspeisung, der Zugriff auf die Daten und deren Nutzung sowie die weitere Datenverwendung bestimmten Anforderungen.¹⁰⁶ Die obligatorische Dateneinspeisung setzt im Ausgangspunkt voraus, dass die Kenntnis der Daten für die Aufklärung oder Bekämpfung des internationalen Terrorismus bzw. des gewaltbezogenen Rechtsextremismus erforderlich ist. Die einzuspeisenden Daten selbst werden mit Blick auf die Relevanz ihres Informationsgehalts und über mehr oder weniger bestimmte weitere Schwellen, u.a. hinsichtlich der betroffenen Personen, eingegrenzt. Die zu speichernden Datenarten differenzieren sich in Grunddaten, erweiterte Grunddaten, zusammenfassende besondere Bemerkungen sowie ergänzende Hinweise und Bewertungen. Außerdem werden weitere Angaben zur Identifizierung und nicht zuletzt die Behörde, die über die Erkenntnisse verfügt, das Aktenzeichen oder die Einstufung als Verschlussache festgehalten. Unter bestimmten Voraussetzungen – besondere Geheimhaltungsinteressen oder besonders schutzwürdige Interessen der Betroffenen – dürfen Daten beschränkt oder verdeckt gespeichert werden.¹⁰⁷ Der Zugriff auf die Daten ist

104 S. das Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz – ATDG), v. 22. 12. 2006, BGBl. I S. 3409, das dann insbes. aufgrund des einschlägigen Urteils des BVerfG durch das Gesetz zur Änderung des Antiterrordateigesetzes und anderer Gesetze v. 18. 12. 2014, BGBl. I 2318, geändert wurde. Zur Rechtsextremismusdatei s. das Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz – RED-G), v. 20. 08. 2012, BGBl. I S. 1797; vgl. zur Begründung auch den Gesetzentwurf der Bundesregierung, BT-Drs. 17/8672. Übergreifender zu solchen Verbunddateien am Beispiel der Antiterrordatei *Julia Stubenrauch*, Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten, Baden-Baden 2009.

105 § 1 ATDG, § 1 RED-G.

106 S. auch BVerfG, Urteil v. 24. 04. 2013, 1 BvR 1215/07 = BVerfGE 133, 277 – *Antiterrordatei-Gesetz*.

107 In solchen Fällen wird die Möglichkeit einer Übermittlung nach automatisierter Information der eingegebenen Behörde über das Abfrageereignis ggf. in unmittelbarem Kontakt zwischen eingebender und abfragender Behörde geklärt, §§ 4 Abs. 2 ATDG, 4 Abs. 2 REDG.

im Ausgangspunkt an die Erforderlichkeit für Erfüllung der näher eingegrenzten Aufgaben im Bereich der Aufklärung oder Bekämpfung des internationalen Terrorismus bzw. des gewaltbezogenen Rechtsextremismus geknüpft. Im Falle eines Treffers erhält die abfragende Behörde Zugriff auf Grunddaten. Unter bestimmten Voraussetzungen sind auch erweiterte Grunddaten zugänglich. Die erhaltenen Daten dürfen grundsätzlich nur zur Prüfung der Einschlägigkeit des Treffers und sodann für ein Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung der jeweiligen Aufgabe verwendet werden.¹⁰⁸ Von der Möglichkeit einer erweiterten projektbezogenen Datennutzung abgesehen¹⁰⁹ sind die Antiterrordatei und die Rechtsextremismusdatei somit auf eine Kontakt- und Informationsanbahnung zugeschnitten. Ein Treffer und der Zugriff auf die Grunddaten oder erweiterten Grunddaten wird ggf. ein Ersuchen auslösen. Der weitere Datenaustausch zwischen den beteiligten Behörden richtet sich dann nach den jeweils geltenden Datenübermittlungs- und Datenempfangsvorschriften der einschlägigen Gesetze.

Anwendungserfahrungen mit dieser spezifisch zugeschnittenen Vernetzung zwischen Polizeien und Nachrichtendiensten ergeben sich aus den jeweiligen Evaluationen der Gesetze.¹¹⁰ Danach können, vermittelt über die Informationen aus den Dateien, Kontakte aufgebaut und intensiviert werden. Gestärkt werden auch die Kooperationsbereitschaft und das gegenseitige Vertrauen darauf, dass die jeweils vorhandenen Daten angesichts der Pflicht sowohl der Polizeien als auch der Nachrichtendienste, diese Daten einzuspeisen, vollständig zur Verfügung gestellt sind. Die Dateien ermöglichen die Recherche in einem breiten Bestand und über die „Treffer“ können zielgerichteter gerade die Behörden um die Übermittlung weiterer Daten ersucht werden, bei denen Daten vorliegen. Ansonsten ergibt sich aus den Evaluationen der komplementäre Charakter der auf eine Kontakt- und Informationsanbahnung zugeschnittenen Verbunddateien zwischen Polizeien und Nachrichtendiensten. Das gilt sowohl im Hinblick auf die Vernetzung mittels anderweitiger Verbundsysteme als auch im Hinblick auf die Vernetzung in Gemeinsamen Abwehrzentren.

24

108 Eine Verwendung zu einem anderen Zweck, also eine Zweckänderung und anderweitige Verwendung, ist an enge Voraussetzungen geknüpft, §§ 6 Abs. 1 S. 2 ATDG, 6 Abs. 1 S. 2 REDG.

109 Kritik an dieser Möglichkeit etwa bei *Clemens Arzt*, in: Schenke/Graulich/Ruthig (Fn. 82), REDG § 7 Rn. 2 ff.

110 Unterrichtung durch die Bundesregierung, Bericht zur Evaluierung des Antiterrordateigesetzes v. 7. 03. 2013, BT-Drucks. 17/12665 (neu), bes. S. 48 ff.; Unterrichtung durch die Bundesregierung v. 7. 04. 2016, Evaluierung des Rechtsextremismus-Datei-Gesetzes, BT-Drucks. 18/8060, S. 50 ff. S. außerdem Bundeskriminalamt, Bericht zum 1. 08. 2017 an den Deutschen Bundestag, Datenbestand und Nutzung der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) in den Jahren 2014 – 2017. Übergreifender zur Evaluierung *Marion Albers*, Funktionen, Entwicklungsstand und Probleme von Evaluationen im Sicherheitsrecht, in: dies./Ruth Weinzierl (Hrsg.), Menschenrechtliche Standards in der Sicherheitspolitik. Beiträge zur rechtsstaatsorientierten Evaluierung von Sicherheitsgesetzen, Baden-Baden 2010, S. 25–54.

IV. Gemeinsame Abwehrzentren

- 25 In Abgrenzung gegen die bisherigen Formen der Vernetzung der Sicherheitsbehörden und die dabei entstehenden „Netze“ kann man die Gemeinsamen Abwehrzentren als „Netzwerke“ einstufen. Als Interaktionsnetzwerke, die persönliche Kontakte stabilisieren und darüber funktionieren, haben die Zentren gerade auch die Funktion, Dysfunktionalitäten technisierter Vernetzungen auszugleichen, und insofern eine komplementäre Rolle.¹¹¹ Paradigmatisch ist das Gemeinsame Terrorismusabwehrzentrum (GTAZ). Seitens des Bundesamtes für Verfassungsschutz wird es beschrieben als „gemeinsame Kooperations- und Kommunikationsplattform von 40 nationalen Behörden aus dem Bereich der Inneren Sicherheit“.¹¹² Dem Vorbild des GTAZ folgen das Gemeinsame Analyse- und Strategiezentrum illegale Migration (GASiM), das Gemeinsame Internetzentrum zur Sichtung und systematischen Auswertung des Internets im Bereich des islamischen Terrorismus (GIZ) und das Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ). Daneben wurde im Zuge der Cyber-Strategie der Bundesregierung das Nationale Cyber-Abwehrzentrum (NCAZ) errichtet¹¹³, dessen Kernbehörde das Bundesamt für Verfassungsschutz ist. Bundeskriminalamt, Bundespolizei, Zollkriminalamt, Bundesnachrichtendienst sind assoziierte Behörden.¹¹⁴

Zu den Zielen des GTAZ gehört die Verbesserung der behördenübergreifenden Zusammenarbeit bei der Bekämpfung des internationalen Terrorismus auf konzeptionell-analytischer Ebene und im operativen Bereich.¹¹⁵ In ihm kommen Vertreter aus unter anderem dem Bundesamt für Verfassungsschutz, dem Bundeskriminalamt, dem Bundesnachrichtendienst, der Generalbundesanwaltschaft, der Bundespolizei, dem Zollkriminalamt, dem Bundesamt für Migration und Flüchtlinge, dem Militärischen Abschirmdienst sowie den Landesämtern für Verfassungsschutz und den Landeskriminalämtern zusammen.¹¹⁶ Der Austausch von Daten und Informationen findet zentral in der täglichen Lagebesprechung statt. Angestrebt wird unter Hinzuziehung aller beteiligten Behörden und Stellen und verschiedenen Arbeitsgruppen ein „Echtzeit-Informationsaustausch“.¹¹⁷ Den Vertretern der jeweiligen Behörde kommt die Aufgabe zu, das behördliche Fach-

111 Vgl. oben Rn. 4, 7 und 24.

112 <https://www.verfassungsschutz.de/de/arbeitsfelder/af-islamismus-und-islamistischer-terrorismus/gemeinsames-terrorismusabwehrzentrum-gta-z>, abgerufen am 10.05.2018.

113 Über damit verbundene Rechtsfragen s. *Tobias Linke*, Rechtsfragen der Einrichtung und des Betriebs eines Nationalen Cyber-Abwehrzentrums als informelle institutionalisierte Sicherheitskooperation, *DÖV* 2015, 128–139.

114 S. auch die Antwort der Bundesregierung auf eine Kleine Anfrage, Die Strategie der Bundesregierung zur Bekämpfung der Internetkriminalität – Das Nationale Cyber-Abwehrzentrum, *BT-Drs.* 17/5694.

115 Näher *Niclas-Frederic Weisser*, Das Gemeinsame Terrorismusabwehrzentrum (GTAZ) – Rechtsprobleme, Rechtsform und Rechtsgrundlage, *NVwZ* 2011, S. 142–146, 143.

116 S. die Antwort der Bundesregierung auf eine Kleine Anfrage, Das Gemeinsame Terrorismusabwehrzentrum – Sachstand 2008, *BT-Drs.* 16/10007, S. 1 ff.

117 Antwort der Bundesregierung (Fn. 116), S. 6.

wissen in das Netzwerk und die über das Netzwerk gewonnenen Informationen wiederum in das behördliche Wissen einzuspeisen.

Für die Arbeit der Gemeinsamen Zentren existieren bisher keine speziellen gesetzlichen Grundlagen. Die Bundesregierung bewertet die Zentren als eine Form der Zusammenarbeit der beteiligten Behörden und als einen Daten- und Informationsaustausch, für den die jeweiligen Übermittlungs- und Empfangsvorschriften der einzelnen Fachgesetze als Rechtsgrundlagen ausreichen.¹¹⁸ Demgegenüber führen einige Mitglieder der Regierungskommission zur Evaluation der Sicherheitsgesetzgebung in ihrem Bericht zutreffend aus: „Eine derartige Zusammenarbeit erzeugt also aus den bei den verschiedenen Behörden vorhandene Datenbeständen durch geeignete gemeinsame Weiterverarbeitung neue Daten.“¹¹⁹ Netzwerke wie das GTAZ haben eigenständige Funktionen der Generierung emergenten Wissens und des Wissensmanagements, die mit den Übermittlungs- und Empfangsbefugnissen der beteiligten Behörden unzureichend erfasst werden. Im Übrigen stellen sich, wie die Erkenntnisse zum Terroranschlag vom Breitscheidplatz gezeigt haben¹²⁰, auch Fragen danach, wem innerhalb des Netzwerks wofür engere Verantwortlichkeiten zuzuweisen sind. Somit ist es erforderlich, einerseits den Netzwerkcharakter zu bewahren und andererseits unter verschiedenen Aspekten grundlegende Maßgaben zu verankern. Insgesamt geht es dann um durchaus komplexe Rechtsfragen und schon aus Gründen der Gesetzgebungskompetenz nicht um „eine“ spezialgesetzliche Grundlage für das jeweilige Gemeinsame Abwehrzentrum. Damit der Netzwerkcharakter angemessen erfasst wird, müssen zudem die Schnittstellen zu den beteiligten Fachbehörden dahingehend untersucht werden, inwiefern Reformbedarf besteht.

E. Fazit

Die öffentliche Diskussion um die Befugnisse der Sicherheitsbehörden konzentriert sich oft auf die Datenerhebung und auf bestimmte, als eingriffsintensiv bewertete Ermittlungsmethoden. Dabei ist es mindestens gleichermaßen, wenn nicht noch wichtiger, was nach der Erhebung mit den Daten geschieht, wie sie verknüpft und verändert werden, wohin sie von wo aus in welcher Form weitergeleitet werden oder wem sie in welcher Form zum Abruf zur Verfügung stehen und welche Informationen und welches Wissen wie bei welcher Stelle und in welchen Zusam-

118 S. auch *Christian Rathgeber*, Terrorismusbekämpfung durch Organisationsrecht, DVBl 2013, S. 1009–1016; mit der Forderung einer parlamentarischen Kontrolle *Matthias Dombert/Kaya Räuher*, Am Beispiel der deutschen Sicherheitsarchitektur: Zum Grundrechtsschutz durch Organisation, DÖV 2014, S. 414–422.

119 *Matthias Bäcker/Volkmar Giesler/Burkhard Hirsch/Heinrich-Amadeus Wolff*, Bericht der Regierungskommission zur Überprüfung der Sicherheitsgesetzgebung in Deutschland vom 28. 08. 2013, <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/regierungskommission-sicherheitsgesetzgebung.pdf>, abgerufen am 10. 05. 2018, S. 174. S. auch *Sommerfeld* (Fn. 27), S. 262 ff.

120 S. oben Rn. 1.

menhängen entsteht. Das gilt umso mehr mit Blick auf den künftig voraussichtlich zunehmenden Einsatz komplexer und gegebenenfalls selbstständig lernender automatisierter Analyse- und Auswertungsprogramme und mit Blick auf den Ausbau technisierter informationeller Vernetzungen. Die Digitalisierung und die damit eröffneten Datenverarbeitungsmöglichkeiten zwingen dazu, der Vernetzung der Sicherheitsbehörden sowohl unter Aspekten der Aufgabenwahrnehmung als auch unter Aspekten des Datenschutzes verstärkte Aufmerksamkeit zu widmen. Eine Reihe der dabei auftauchenden Regelungsprobleme sind bisher unzureichend gelöst.