Kapitel III. Normative Rahmenbedingungen des polizeilichen Informationswesens

Nachdem die theoretischen Grundlagen und die historische Entwicklung des polizeilichen Informationswesens dargelegt worden sind, soll nun die Gegenwart polizeilicher Informationsverarbeitung in Deutschland in den Blick genommen werden. Ihren Ausgangspunkt nimmt diese Betrachtung bei den normativen Rahmenbedingungen des polizeilichen Informationswesens, also präskriptiven Strukturen, die Aufschluss darüber geben, wie das Informationswesen und die in ihm stattfindenden Informationspraktiken sein *soll*, um dann im darauffolgenden Kapitel eine Annäherung an die tatsächlichen Dynamiken dieses sozio-technischen Systems zu unternehmen.[530]

Die normativen Rahmenbedingungen des polizeilichen Informationswesens lassen sich zunächst einmal grob in die übergesetzlichen Vorgaben des Verfassungs- und Unionsrecht und die einfachgesetzlichen Vorgaben unterteilen, die sich wiederum vorrangig aus den Polizeigesetzen und dem Strafverfahrensrecht zusammensetzen. Zusätzlich könnte man noch polizeiinterne Verordnungen und Richtlinien, wie die Polizeidienstvorschrift und die Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen (KpS-Richtlinien) heranziehen, deren Abbildung eine Arbeit, die nicht auf die systematische und umfassende Darstellung des gesamten normativen Rahmens polizeilicher Datenverarbeitung abzielt, allerdings überladen würde.[531] Die folgenden Ausführungen verstehen sich daher explizit als Überblick, wobei die mangelnde Vollständigkeit einerseits der bereits angedeuteten Komplexität des polizeilichen Informationsrechts geschuldet ist und andererseits ohnehin eine selektive Darstellung erfolgen soll, die auf den normativen Rahmen der grundsätzlichen Strukturen des polizeilichen Informationswesens und der grundsätzlichen, in ihm stattfindenden Informationsverarbeitungsformen fokussiert, statt jede denkbare rechtliche Konstellation polizeilicher Informationsverarbeitung durchzuspielen. Dazu werden die Steuerungsebenen des Verfassungsrechts und Unionsrechts in

530 Siehe dazu unten S. 377 ff.

531 Zur normativen Bedeutung dieser Vorschriften in der polizeilichen Informationspraxis siehe aber unten S. 416 ff.

ihren Bezügen zur polizeilichen Informationsverarbeitung beschrieben, um daran anknüpfend den einfachgesetzlichen Rahmen für das polizeiliche Informationswesen – wo es denn normative Ankerpunkte hat – zu konturieren und Problemfelder aufzuzeigen. Dabei werden auch immer wieder Bezüge zum Datenschutzrecht gezogen, das die polizeiliche Informationsordnung durchzieht und gleichfalls verklammert.

A. Grund- und menschenrechtliche Vorgaben für polizeiliche Datenverarbeitung

Zuerst muss – vor die Klammer gezogen – eine Darstellung der verfassungsrechtlichen Vorgaben für die polizeiliche Datenverarbeitung erfolgen, die für alle Polizeibehörden des Bundes und der Länder gelten. Polizeiliches Informationshandeln betrifft eine Vielzahl verschiedener Grundrechte, die sich der „grundrechtlichen Identitätsschicht" der Privatheit[532] (*Schwabenbauer*) zuordnen lassen. Da es vorliegend jedoch vorrangig um Datenverarbeitungen geht, die an die verschiedenen Erhebungsmaßnahmen anknüpfen, also – zeitlich besehen – um solche Datenverarbeitungen, die stattfinden, nachdem die Daten in den Einflussbereich der Polizei gelangt sind, ist vor allem das Recht auf informationelle Selbstbestimmung von zentraler Bedeutung. Denn auch wenn grundrechtliche Eingriffe, etwa in das Wohnungsgrundrecht, durch weiteren Umgang mit derart erlangten Daten fortgesetzt werden, ist es das Recht auf informationelle Selbstbestimmung, das jeden Datenumgang durch die Sicherheitsbehörden verfassungsdogmatisch abbildet, sodass die übrigen Grundrechte der Identitätsschicht vorliegend vernachlässigt werden. Ausgangspunkt für das Recht ist, wie für das deutsche Datenschutzrecht insgesamt, das bereits zuvor erwähnte Volkszählungsurteil des Bundesverfassungsgerichtes aus dem Jahr 1983. Das Gericht schuf mit seinem Urteil ein neues Grundrecht auf informationelle Selbstbestimmung, als es damals proklamierte:

> „Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht

532 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, Rn. 62 ff.

des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[533]

I. Das Recht auf informationelle Selbstbestimmung

Im System der grundrechtlichen Dogmatik findet das Recht auf informationelle Selbstbestimmung seinen Ursprung im allgemeinen Persönlichkeitsrecht,[534] das ideengeschichtlich wiederum auf das von *Warren* und *Brandeis* formulierten „right to be let alone"[535] zurückgeht.[536] Im Vergleich zum US-amerikanischen „right to be let alone", das sich zunächst auf die Interaktion zwischen Bürger:innen der Vereinigten Staaten bezog,[537] ist die deutsche Grundrechtsdogmatik hingegen stärker auf den Schutz des Einzelnen vor staatlicher Macht ausgerichtet. Das allgemeine Freiheitsrecht aus Art. 2 Abs. 1 GG als eine der beiden wesentlichen Quellen des Persönlichkeitsrechts ist dabei zentral für das Verständnis des grundrechtlichen Freiheitsverständnisses.

> „Im Wertsystem der Grundrechte macht Art. 2 Abs. 1 unbezweifelbar, worin inhaltlich (materiell) die Würde des Menschen (Art. 1 Abs. 1) vornehmlich besteht: – in der ‚freien Entfaltung seiner Persönlichkeit'."[538]

Vor diesem Hintergrund wirkt die teils herablassende Titulierung des Art. 2 Abs. 1 GG als „Auffangrundrecht" nicht angemessen, mag sie auch rechtstechnisch zutreffend sein.[539] Die, vor allem für die moderne Informationsgesellschaft, immense Bedeutung des Grundrechtes zeigt sich in seinen besonderen Ausprägungen des allgemeinen Persönlichkeitsrechts, also in Verbindung mit Art. 1 Abs. 1 GG. Diese – zunächst das Recht am eigenen Bild und das Recht am eigenen Wort – sind dabei rechtsdogmatische

533 BVerfGE 65, 1 (42) – Volkszählung.
534 *Brink* in DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 10.
535 *Warren/Brandeis* Harvard Law Review, pp. 193-220. Vol. 4 (1890), 193 ff. (193).
536 *Brink* in DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 5.
537 Es ging hier vor allem um die Abschirmung des privaten Lebens vor der „vierten Gewalt", insbesondere in ihrer Manifestation als invasive Reporter. Dabei stand zunächst die Privatheit der privilegierten Gesellschaftsschichten im Mittelpunkt dieses neuen, normativen Anspruchs, vgl. *Igo,* The Known Citizen.
538 *Dürig* zitiert nach *DiFabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 1.
539 *Di Fabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 7.

Reaktionen auf die technischen und gesellschaftlichen Entwicklungen des 19. und 20. Jahrhunderts, die eine Fixierung und Reproduzierbarkeit des eigenen Bildes sowie des gesprochenen Wortes mit sich brachten und die Sozialbezüge des Individuums in erheblichem Maße ausweiteten.[540] Die jüngeren Entwicklungen in der Informationstechnologie führten schließlich zum gegenwärtigen Stand des Möglichen: Jeder wahrnehmbare Ausdruck der Persönlichkeit ist „prinzipiell unbegrenzt fixierbar, transferierbar, multiplizierbar und digital manipulierbar".[541]

Diese Fluidität[542] von (personenbezogenen) Daten macht letztlich ihren einzigartigen Wert aus, gibt ihnen aber zeitgleich ihr Gefährdungspotenzial. Dies gilt uneingeschränkt und besonders auch für polizeiliche Datenverarbeitungen. Die Daten, die dort über tatsächliche und potenzielle Straftäter:innen, Zeugen und sonstige Personen gespeichert wurden und werden führen für die Betroffenen dazu, dass sie über diese Daten – wenn sie denn überhaupt von ihnen wissen – regelmäßig kaum noch selbst bestimmen können. Gleichzeitig ist eine Polizei ohne die Möglichkeit, zeitgemäß mit Daten umzugehen, in der modernen Informationsgesellschaft blind. Für eine weiterhin funktionale Kriminalitätskontrolle ist dementsprechend unerlässlich, dass die deutschen Polizeien die technischen und auch rechtlichen Voraussetzungen zum Umgang mit Massendaten besitzen.[543]

Dieses Spannungsfeld polizeilicher Sozialkontrolle in der digitalen Gesellschaft verfassungsrechtlich auszutarieren ist eine der wesentlichen Aufgaben des Rechts auf informationelle Selbstbestimmung im Verhältnis zwischen Bürger:innen und Staat. Insofern ist zunächst darzulegen, welche normativen Postulate für diese Beziehung aus der Verfassung abgeleitet werden. Ein besonderer Fokus liegt dabei darauf, inwiefern dabei Dynamiken des Massendatenphänomens in diesem Rahmen Berücksichtigung finden. In diesem Zusammenhang muss auch beachtet werden, wie die gegenwärtig geplante Umstrukturierung des polizeilichen Informationswesens im Lichte der Verfassung zu bewerten ist.

---

540 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 7, 46ff.

541 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 7.

542 Siehe zur Idee der Fluidität im Kontext von Daten *Cheney-Lippold,* We are data, passim.

543 Näher zu diesen Dynamiken bereits oben S. 66 ff.

I. Schutz, Eingriff, Rechtfertigung – Grundsätze und Entwicklungen

a) Schutz

Kern des Rechts auf informationelle Selbstbestimmung ist in subjektivrechtlicher Hinsicht nach wie vor die bereits im bundesverfassungsgerichtlichen Eingangszitat genannte Befugnis des Individuums, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen.[544] So soll der „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten"[545] gewährleistet werden.

Grundgedanke ist hierbei, dass die Entfaltung der Persönlichkeit die Begrenzung der Wahrnehmung des Individuums durch Dritte erforderlich machen kann,[546] da sich die Persönlichkeit in erster Linie in Rückkopplung mit sozialen Prozessen bildet und weiterentwickelt,[547] also auf Grundlage von Daten bzw. Informationen konstruiert wird.[548] Erst im Kontakt zu anderen können Eigenarten der Persönlichkeit gezeigt und geschärft werden. Dazu muss es dem Individuum möglich sein, sein Selbstbild in verschiedenen sozialen Interaktionen kontextspezifisch zu präsentieren.[549] Was durch das normative Konzept der informationellen Selbstbestimmung bewahrt werden soll, ist der theoretische Facettenreichtum der individuellen Persönlichkeit in den verschiedenen Kontexten, also ihre Wandelbarkeit.[550] Ein durch Informationsvorsprung aggregiertes Gegenbild der jeweiligen Person, das sich ihrem Einfluss gänzlich entzieht, schränkt diese Entfaltungsräume ein. Eine erfolgreiche Selbstinszenierung erfordert aber gerade eine solche Einflussmöglichkeit. Nimmt der eigenen Einfluss auf das nach außen reflektierte Persönlichkeitsbild ab und nimmt damit gleichzeitig die Deutungshoheit der durch andere erzeugten Gegenbilder zu, so kann das Individuum sich nicht mehr autonom darstellen und entfalten. Zu Ende

544 BVerfGE 65, 1 (42) – Volkszählung.
545 BVerfGE 65, 1 (43) – Volkszählung.
546 BVerfGE 65, 1 (43) – Volkszählung.
547 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 8.
548 Siehe dazu bereits oben S. 50 ff.
549 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 37f.
550 Siehe dazu bereits *W. Steinmüller/Lutterbeck/Mallmann* ua, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. 6/3826, 1971, 86 ff.

gedacht, führt dies zu einer überbordenden Fremdbestimmung der Persönlichkeit.[551] Damit unterstützt das Recht auf informationelle Selbstbestimmung auf der einen Seite das allgemeine Persönlichkeitsrecht, geht aber andererseits auch über den von diesem Grundrecht gewährleisteten Schutz hinaus, indem es schon in seinem Vorfeld eingreift, nämlich dort, wo das allgemeine Persönlichkeitsrecht personenbezogene Informationen nicht erfasst, weil sie im gegenwärtigen Zeitpunkt noch nicht persönlichkeitsrelevant sind oder es gegebenenfalls niemals sein werden. Das Recht auf informationelle Selbstbestimmung verlagert den grundrechtlichen Schutz des Individuums damit weg von konkreten Verletzungshandlungen – vor denen das allgemeine Persönlichkeitsrecht schützt – hin zum Schutz vor abstrakten Gefährdungen der Persönlichkeit.[552]

Um dies zu bewerkstelligen, gewährt das in dieser Hinsicht seit dem Volkszählungsurteil unverändert gebliebene Recht[553] grundsätzlich Selbstbestimmung für jeglichen Datenumgang.[554] Begrenzend wirkt insoweit, dass es sich um „personenbezogene" Daten handeln muss. Dabei orientierte sich das Bundesverfassungsgericht am ehemaligen § 2 Abs. 1 BDSG-alt[555], dessen Regelungsgehalt sich zwischenzeitlich in § 3 Abs. 1 BDSG-alt[556] fand. Heute enthält unter anderem § 46 Nr. 1 BDSG die maßgeblichen Legaldefinitionen zu „personenbezogenen Daten". Es sind dies „alle Informationen, die sich auf eine identifizierte oder identifizierbare Person (betroffene Person) beziehen." Bei allen Daten, die nicht direkt zu einer Identifizierung einer Person führen, vertrat das Bundesverfassungsgericht bereits im Volkszählungsurteil ein weites Verständnis von Identifizierbarkeit, bzw. Bestimmbarkeit und zog damit den Schutzbereich der informationellen Selbstbestimmung grundsätzlich weit: Neben dem Inhalt erhobener Daten war vor allem die durch die Informationstechnologie ermöglichte Nutzbarkeit und Verwendungsmöglichkeit für die Klassifizierung staatlicher Datenverarbeitung als Grundrechtseingriff entscheidend. Verarbeitungs- und Verknüpfungsmöglichkeiten können noch aus einem auf den ersten

551 Ähnlich *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 51f.

552 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 61ff.; vgl. auch BVerfGE 118, 168 (184): „Persönlichkeitsgefährdung".

553 Siehe dazu *Held,* Intelligente Videoüberwachung, 2014, S. 78 m.w.N.

554 *Di Fabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 176.

555 BDSG vom 27.01.1977, BGBl. I, S. 201.

556 BDSG vom 14.08.2009, BGBl. I S. 2814.

Blick „belanglosen Datum" Bedeutung, also insbesondere Personenbezug, gewinnen. Das Bundesverfassungsgericht äußert dementsprechend bereits bei Schaffung des Rechts auf informationelle Selbstbestimmung: Es „gibt [...] unter den Bedingungen der automatischen Datenverarbeitung *kein* (Hervorh. FB) belangloses Datum mehr." Dieser Schutz von auf den ersten Blick vielleicht weniger relevanten Daten ist der unüberschaubaren Komplexität der automatisierten Datenverarbeitung geschuldet: Diese macht es dem Individuum unmöglich, die Bedeutung der es betreffenden personenbezogenen Daten in Gegenwart und Zukunft abschließend einzuschätzen. Jedes Datum kann durch Rekontextualisierung Bedeutung erlangen. Vor diesem Hintergrund besteht eine unwiderlegliche Vermutung der Relevanz aller personenbezogenen Daten.[557] Mit Blick auf den zur Zeit des Volkszählungsurteils im Gegensatz zu heute noch überschaubaren Entwicklungsstand elektronischer (Massen-)Datenverarbeitung war diese weite Konzeptualisierung schützenswerter Daten vorausschauend, auch wenn das Urteil genau unter diesem Gesichtspunkt kritisiert worden ist[558] und mit Blick auf das Datenvolumen der Gegenwart zu einer unübersehbaren Zahl von grundrechtstangierenden Situationen führt. Indessen hält gerade diese hohe Sensibilität des Rechts auf informationelle Selbstbestimmung auch neue Potenziale für die Quantifizierung seiner Beeinträchtigungen bereit.

Die Absage an die Belanglosigkeit von Daten, also an die Begrenzung des Schutzbereiches, wird im Wesentlichen auch vom EU-Datenschutzrecht gestützt. Um bei Daten einen Personenbezug herstellen zu können, kommt es in der Terminologie des unionalen Datenschutzrechts dafür maßgeblich darauf an, wann eine Identifizierbarkeit gegeben ist. Dies bestimmt sich danach, ob „nach allgemeinem Ermessen wahrscheinlich" ein Mittel zur Identifizierung eingesetzt werden würde, was sich wiederum nach objektiven Kriterien bemisst, wie Kostenaufwand, Zeitaufwand oder verfügbarer Technologie (ErwGr 21 JI-Richtlinie[559]). Wenn es dazu heißt, dass es im

557 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 71.

558 Siehe etwa *Aulehner,* Polizeiliche Gefahren- und Informationsvorsorge, 359 ff.

559 Die JI-Richtlinie ist die Abkürzung für die „RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 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". Ihre Bedeutung wird unten S. 186 ff. näher erläutert.

sicherheitsrechtlichen Bereich vor allem darauf ankommen würde, „ob die Behörde als Verantwortliche über rechtliche Mittel verfügt, um sich die Daten verfügbar zu machen“[560] ist das als grundsätzlicher Rahmen einer rechtsstaatlich agierenden Polizeibehörde begrüßenswert. Allerdings dürften vor allem die technologischen Möglichkeiten regelmäßig stärker determinierend wirken.

Mit Blick auf polizeiliche Informationsinteressen bedeutet dies ganz grundsätzlich zunächst, dass informationelles Handeln der Polizei in der Regel den Schutzbereich des Rechts auf informationelle Selbstbestimmung tangieren wird, denn die Polizei interessiert sich vor allem für Personen. Selbst wenn Objekte in ihren Fokus geraten, ist fast immer auch das Verhältnis von Personen zum in Frage stehenden Objekt relevant.

So gefasst ist der Schutz, den das Recht vermittelt, indessen in erster Linie nur von individualistisch-partikularer Natur: Es sollen einzelne Grundrechtsträger:innen vor einzelnen Datenverarbeitungshandlungen geschützt werden. In eine ähnliche Richtung deutet auch die Formulierung des Bundesverfassungsgerichts, das informationelle Selbstbestimmungsrecht schütze „vor einzelne(n) Datenerhebungen“, trage aber Persönlichkeitsgefährdungen „nicht vollständig Rechnung […], die sich daraus ergeben, dass der Einzelne zu seiner Persönlichkeitsentfaltung auf die Nutzung informationstechnischer Systeme angewiesen ist und dabei dem System persönliche Daten anvertraut oder schon allein durch dessen Nutzung zwangsläufig liefert.“[561]

Vor diesem Hintergrund stellt sich die Frage, inwiefern vor der staatlichen Aggregation von Daten – denn diese stehen selten für sich allein, sondern dem Netzwerkparadigma der Gegenwart entsprechend fast ausschließlich in relationalen Verhältnissen zu anderen Daten – im Rahmen des informationellen Selbstbestimmungsrechts geschützt wird. Diese kollektive Dimension ist etwa mit der Diskussion um den Schutz vor Einschüchterungseffekten (auch: „chilling effects“[562]) angesprochen, die sich auch an einer Passage im Volkszählungsurteil des Bundesverfassungsgerichts festmachten lässt.[563] Allerdings wurde die Frage, ob dem einzelnen

560 So etwa *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 434 auch mwN.

561 BVerfGE 120, 274 (312 f.) – Online-Durchsuchung.

562 *Townend* in Tumber/Waisbord (Hrsg.), The Routledge companion to media and human rights, 73.

563 BVerfGE 65, 1 (43) – Volkszählung: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechts-

Bürger auch ein subjektiv-rechtlicher Schutz vor Einschüchterungseffekte zusteht, die sich aus der Unüberschaubarkeit der Wirkweisen und erfassten Daten automatisierter Datenverarbeitungsverfahren, insbesondere durch staatliche Stellen, ergeben, bisher nur wenig diskutiert.[564] Eine Auseinandersetzung damit liefert beispielsweise *Held*, der einen subjektiv-rechtlichen Schutz im Ergebnis verneint, da andere Freiheitsgrundrechte einen spezielleren Schutz der grundrechtlichen Entschließungsfreiheit vermitteln, während die informationelle Selbstbestimmung nur in wenigen Einzelfällen überhaupt einschlägig wäre.[565] Vor dem Hintergrund der eingangs erwähnten Passage des Volkszählungsurteils wäre indessen auch ein Schutz vor Einschüchterungseffekten durch die objektiv-rechtliche Dimension der informationellen Selbstbestimmung denkbar. Umfassende und kontinuierliche Beobachtung bzw. das Gefühl einer solchen sind generell geeignet, sich negativ auf das verfassungsrechtlich gewährleistete freiheitlich demokratische Gemeinwesen auszuwirken.[566]

Sinnvoller erscheint es aber den Ausgangspunkt in bereits gefestigter Dogmatik zu wählen: Informationelle Selbstbestimmung will die Freiheit gewähren, grundsätzlich selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen. Dieses Recht ist nicht nur in seinem Stellenwert für die Persönlichkeitsentwicklung zu sehen. Vielmehr ist die informationelle Selbstbestimmung in unserer zunehmend digitalisierten Umgebung von zentraler Bedeutung, insbesondere da diese Umgebungen tendenziell auf die Preisgabe und Verwendung personenbezogener Daten ausgelegt sind oder zunehmend nur darüber wirklich

ordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

564 Kritisch insoweit *Braun* in *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 25.

565 *Held,* Intelligente Videoüberwachung, 2014, S. 82ff.

566 Vgl. dazu ausführlicher *Knierim* ZD 2011, 17, (20f.); siehe auch *Held, Intelligente Videoüberwachung*, 2014, S. 92.

funktionieren.[567] Im Hinblick auf Einschüchterungseffekte lautet die Frage dann, ob staatliches Handeln in irgendeine Richtung zwingend auf die Ausübung des Rechts (d.h. der Selbstbestimmung über Preisgabe und Verwendung personenbezogener Daten) wirkt. Denkbar ist dabei einerseits, dass Verhalten gemieden wird, das an die Verwendung oder Preisgabe der eigenen personenbezogenen Daten geknüpft ist, obwohl dies eigentlich von den Grundrechtsträger:innen gewünscht wäre.[568] Mit Blick auf normative Zwänge in Mehrheitsgesellschaften können davon etwa ohnehin bereits marginalisierte Gruppen betroffen sein.[569] Andererseits ist auch denkbar, dass personenbezogene Daten entgegen des eigenen Wunsches preisgegeben und verwendet werden, insbesondere, weil sich gesellschaftliche Normvorstellungen basierend auf den hierzu geschaffenen technologischen Möglichkeiten teilweise in die Richtung bewegen, mehr personenbezogenen Daten in den allgegenwärtigen digitalen Sphären öffentlich zu machen.[570] Um vor dem Hintergrund eines geänderten gesellschaftlichen Umgangs mit Daten potentiellen staatlichen Beobachtern nicht nachteilig aufzufallen, ist es zudem denkbar, dass sich Individuen gezwungen fühlen, mehr personenbezogene Daten preiszugegeben und zu verwenden.[571]

Dementsprechend geht es vorrangig darum, zu beantworten, wann staatliches Informationshandeln vermittelt über Einschüchterung dazu führt, dass nicht mehr selbstbestimmt über die Preisgabe von personenbezogenen Daten bestimmt wird – es handelt sich folglich stärker um eine Frage des Eingriffsverständnisses als um die Definierung des Schutzbereiches per se.

---

567 *Oermann/Staben* Der Staat 52 (2013), 630, (634);

568 Vgl. zu diesem Phänomen der „Selbst-Zensur" *Oermann/Staben* Der Staat 52 (2013), 630 (648f.), dort insb. Anm. 76 mit ausführlichen Nachweisen zu empirischen Erkenntnissen.

569 So hat sich in empirischen Untersuchungen in den Vereinigten Staaten gezeigt, dass dort lebende Muslim:innen ihr Online-Verhalten aufgrund von Online-Überwachungsmaßnahmen anpassen, siehe dazu *Sidhu* University of Maryland Law Journal of Race, Religion, Gender 7 (2007), 375 (391); gemessen wurden Einschüchterungseffekte aber auch im Zusammenhang mit den NSA-Enthüllungen durch *Edward Snowden*, vgl. etwa *Penney* Berkeley Tech. L.J. 31 (2016), 117, 117ff.; *Kaminski/Witnov* University of Richmond Law Review 49 (2015), 465 ff.; *Marthews/Tucker*, Government Surveillance and Internet Search Behavior, 2017, 2017.

570 So zeigt etwa die Studie von *Kezer/Sevi/Cemalcilar* ua Cyberpsychology 10 (2016), dass jüngere Nutzer:innen sozialer Netzwerke mehr Informationen über sich preisgeben. Gleichzeitig ssetzen sie hingegen auch häufiger Maßnahmen zum Schutz ihrer Privatsphäre in den sozialen Medien ein. .

571 So berichtet etwa *Boyd,* It's complicated, 74 ff. von strategischem Verhalten in der Informationspreisgabe in den sozialen Medien.

Während es nach Rechtsprechung des Bundesverfassungsgerichts jedenfalls einen Eingriff darstellt, wenn „Informationen […] gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt“,[572] ist es denkbar, bereits durch die einfache Möglichkeit umfassender staatlicher Beobachtung einen Eingriff anzunehmen. Einen dogmatisch schlüssigen Weg dazu liefern *Oermann und Staben*: Nehmen Grundrechtsträger:innen Einschränkungen ihrer Grundrechte aus eigenen Stücken anlässlich bestimmter staatlicher Handlungen vor, so kann ein „mittelbar-faktischer“ Eingriff vorliegen. Dazu ist es erforderlich, dass den Grundrechtsträger:innen aufgrund des staatlichen Handelns nicht mehr möglich ist, ihre Grundrechte in vollem Umfang zu verwirklichen, die Beeinträchtigung dem Staat zurechenbar ist und eine bestimmte Erheblichkeit erreicht.[573] *Oermann und Staben* erläutern mittelbare Grundrechtseingriffe durch Abschreckung vor dem Hintergrund der verbreiteten Praxis der Online-Streife, bei der es sich weitestgehend um heimliche Überwachungsmaßnahmen handelt, deren Abschreckungseffekt „nicht auf der konkreten Einzelmaßnahme und deren Wirkungen auf den einzelnen Grundrechtsträger, sondern […] aus dessen Bewusstsein über die Möglichkeit, jederzeit Betroffener einer entsprechenden Maßnahme sein zu können, [erwächst].“[574] Derartige panoptische Effekte können sich aber letztlich bei vielen staatlichen Handlungsweisen im Sicherheitsbereich ergeben, wenn sie für den Einzelnen nur unüberschaubar und undurchdringbar genug sind.

Damit wären polizeiliche Maßnahmen mit entsprechenden Wirkungen wie die Online-Streife nicht per se ausgeschlossen, nur stünden sie aufgrund ihrer freiheitsrechtlichen Wirkungen unter einem Gesetzesvorbehalt, womit sich die Möglichkeit der normativen Steuerung von informationellen Tätigkeiten der Polizei böte, die derzeit diffus und ungeregelt das Ensemble technologischer Überwachungsmöglichkeiten vergrößern.

Etwas eindeutiger ist die Verfassungslage hingegen bezüglich des Schutzes von Individuen in typischeren Massendatenverarbeitungskontexten, sowohl in individuell- als auch in kollektiv-aggregierter Hinsicht. So verbietet die Menschenwürde als Bestandteil der informationellen Selbstbestimmung

572 BVerfGE 120, 274 (344) – Onlinedurchsuchung.

573 *Oermann/Staben* Der Staat 52 (2013), 630 (637) mwN; näher zu den Einzelnen Voraussetzungen siehe a.a.O., (640ff.).

574 *Oermann/Staben* Der Staat 52 (2013), 630 (644).

eine Überwachung, die „sich über einen längeren Zeitraum erstreckt und derart umfassend ist, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage für ein Persönlichkeitsprofil werden können."[575] Eine solches Totalausforschungsverbot soll aber aufgrund seiner Einzelfallbezogenheit grundsätzlich wenig materiellen gesetzgeberischen Handlungsbedarf auslösen. Vielmehr soll den potentiell beeinträchtigten individuellen Schutzbedürfnissen durch prozedurale Regelungen Rechnung getragen werden, wo es zu solchen „additiven Grundrechtseingriffen" kommt.[576] Teilkongruenzen mit der Ausforschung von tiefliegenden Persönlichkeitsstrukturen weist auch die Figur des sogenannten Kernbereichsschutzes aus, der explizit seit den Siebzigern vom Bundesverfassungsgericht ausgearbeitet wurde.[577] Zum Kernbereichsschutz „gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität."[578] Allerdings ist auch dieses dogmatische Konzept sehr stark anhand von Eingriffsbefugnissen, wie der Wohnraumüberwachung, entwickelt worden, sodass die Frage, inwieweit durch auswertende, verknüpfende und analysierende Datenverarbeitungen möglicherweise kernbereichsrelevante Informationen zutage gefördert werden können, ungeklärt ist.[579] Im BKAG-Urteil deutet das Bundesverfassungsgericht allerdings eine Zuwendung auch der Auswertungsebene an. Anders als bei Kernbereichsgefahren die bei der Überwachung eines Ortes „privater Zurückgezogenheit" bestehen, geht es bei der Auswertung von Massendatenbeständen – im BKAG-Urteil im Kontext der Online-Durchsuchung – darum, das „Auslesens höchstvertraulicher Informationen aus einem Gesamtdatenbestand von ohnehin digital vorliegenden Informationen [zu verhindern], die in ihrer Gesamtheit typischerweise nicht schon als solche den Charakter der Privatheit wie das Verhalten oder die Kommunikation in einer Wohnung aufweisen."[580]

575 BVerfGE 109, 279 (322) – Großer Lauschangriff.
576 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 171.
577 Erstmals so bezeichnet in BVerfGE 34, 238 (245) – Tonband.
578 BVerfGE 109, 279 (313) – Großer Lauschangriff.
579 So *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 146.
580 BVerfGE 141, 220 (307) – Bundeskriminalamtgesetz.

Da datenintensive Maßnahmen wie die Online-Durchsuchung dem Prinzip „ganz oder gar nicht“[581] folgten, müssen – wenn kernbereichssensible Informationen nicht bereits vor Erhebung technisch ausgesiebt werden können – Sicherungen auf der Auswertungsebene eingezogen werden. Das Gericht schlägt hier die Sichtung durch eine unabhängige Stelle vor, die „kernbereichsrelevante Informationen vor ihrer Kenntnisnahme und Nutzung“ durch die jeweilige Polizei „herausfiltert“.[582] Ein solches Verständnis von kernbereichssensiblen Informationen geht hingegen weiter davon aus, dass sich diese eindeutig als einzelne Datenpunkte identifizieren lassen. Höchstpersönliche Informationen können jedoch – und das ist die eigentliche Schwierigkeit im Bereich des persönlichkeitsrechtlichen Kernbereichsschutzes – auch durch die Verknüpfung von augenscheinlich „belanglosen“ Datenpunkten gewonnen werden.[583]

Während diese individuell-aggregierte Datenebene bisher nur begrenzt dogmatisch verarbeitet wurde, ist die akademische Diskussion um die Bevorratung von Massendaten einer großen Zahl von Menschen als kollektiv-aggregierte Datenebene insbesondere aufgrund der öffentlichen Debatte und dadurch bedingter Urteile von Bundesverfassungsgericht und Europäischem Gerichtshof wesentlich weiter. Generell gilt für das deutsche Verfassungsrecht ein Verbot der Bevorratung personenbezogener Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken, was sich aus der für das informationelle Selbstbestimmungsrecht zentralen Zweck-Dogmatik ergibt.[584] Damit ist eine Bevorratung zu Zwecken der Sicherheitsgewährleistung zwar nicht per se ausgeschlossen, hängt in ihrer Verfassungsmäßigkeit aber von der konkreten Ausgestaltung im jeweiligen Gesetz ab.[585] Die Diskussion zu den zulässigen Zwecken und damit letztlich zur Reichweite des Schutzes vor der Bevorratung von Daten ist indessen noch stark

581 BVerfGE 141, 220 (307) – Bundeskriminalamtgesetz.

582 BVerfGE 141, 220 (307) – Bundeskriminalamtgesetz.

583 Bekanntes Beispiel hierfür ist etwa die Ableitung von sexueller Orientierung aus Freundschaftsbeziehungen oder sonstigem Online-Verhalten in sozialen Medien wie facebook, s. *Jernigan/Mistree* FM 2009; *Nikhil X. Bhattasali/Esha Maiti*, Machine “Gaydar”: Using Facebook Profiles to Predict Sexual Orientation, https://cs229.stanford.edu/proj2015/019_report.pdf (Stand: 01.10.2023); *Aaron Loh/Kenneth Soo/Hui-lin Xing*, Predicting Sexual Orientation based on Facebook Status, http://cs229.stanford.edu/proj2016/report/LohSooXing-PredictingSexualOrientationBasedOnFacebookStatusUpdates-report.pdf (Stand: 01.10.2023).

584 BVerfGE 65, 1 (45) – Volkszählung.

585 *Müller/Schwabenbauer in Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 174.

im Fluss: Zwar hat der Europäische Gerichtshof hier gerade einige Zwecke festgelegt, etwa die Bekämpfung schwerer Kriminalität, wobei hier weitere Beschränkungen wie ihre Vorhersehbarkeit postuliert wurden.[586] Jedoch geschah dies in einem Urteil, in dem zuvor der auf die deutsche Rechtslage bezogene Verfahrensteil abgetrennt worden war, sodass sich – auch in Anbetracht dann zu erwartender Gesetzgebungsaktivität und darauf antwortender Verfassungsrechtsprechung – die Rahmenbedingungen für den Schutz vor Bevorratung gegenwärtig noch in der Diskussion befinden.

Insgesamt ist auf Ebene des Schutzes, den das Recht auf informationelle Selbstbestimmung gewährleistet, eine starke individualistische Verortung auszumachen, was auch der prinzipiellen Struktur grundrechtlicher Freiheitsrechte entspricht. Da Massendaten jedoch vor allem in ihrer Vernetzung und Aggregation Aussagekraft entwickeln und zur Akkumulation von Datenmacht bei gesellschaftlichen Akteuren führen können, erscheint die Dimension eines Schutzes, die Kollektive und Datenakkumulationen stärker in den Blick nimmt, zunehmend wichtiger, worauf die Verfassungsdogmatik konzeptuell bisher eher im Eingriffs- und Rechtfertigungsverständnis reagiert hat.

b) Eingriff

Lange Zeit galt der Umgang mit personenbezogenen Daten durch Sicherheitsbehörden nicht als Grundrechtseingriff.[587] Der dogmatische Wandel hin zum heutigen Eingriffsverständnis ist in erster Linie durch das Volkszählungsurteil vollzogen worden. Dabei war nicht so sehr der Schritt vom klassischen zum modernen Eingriffsbegriff für diese Entwicklung entscheidend. Vielmehr war die „fortschreitende grundrechtliche Ausfaltung des Persönlichkeitsschutzes“[588] – auch schon in der Zeit vor dem Volkszählungsurteil[589] – derjenige Faktor, der zu dem für das Recht auf informationelle Selbstbestimmung eigenen „Informationseingriff“ führte.[590]

586 EuGH, 05.04.2022 - C-140/20, Rn. 59 ff.
587 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 4.
588 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 6.
589 Vgl. etwa beispielhaft das einflussreiche *Steinmüller*-Gutachten, BT-Drs. VI/3826, S. 86.
590 *Kowalczyk,* Datenschutz im Polizeirecht, S. 49

Nach diesem Verständnis stellt nunmehr prinzipiell jeder Verarbeitungsschritt im „Lebenszyklus" eines personenbezogenen Datums einen Eingriff dar.[591] Die Breite der damit erfassten Umgangsweisen mit Daten wird einfachgesetzlich adäquat durch Art. 3 Nr. 2 JI-Richtlinie, umgesetzt in § 46 Nr. 2 BDSG, abgebildet: „Verarbeitung" meint demzufolge „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung […]".

Ein solcher Eingriff infolge der Verarbeitung von Daten ist nicht an menschliche Wahrnehmung der Daten geknüpft, sondern ist bereits bei technischer Fixierung der Daten oder bei technischem Datenumgang gegeben.[592] Vor dem Hintergrund, dass die Bejahung eines Eingriffes nicht von einem konkret festgestellten Nachteil abhängt, sondern jede Datenverarbeitung per se durch die möglicherweise daraus folgende Ent- und Neukontextualisierung benachteiligend wirkt, schlägt *Schwabenbauer* ein Wiederaufgreifen der Formulierung *Schwans* vor, die mit Blick auf das Recht auf informationelle Selbstbestimmung als zutreffende Charakterisierung eines wichtigen Teilaspektes erscheint:[593] Es gibt eine grundrechtlich geschützte „Freiheit vor staatlicher Informationssammlung und Informationsweitergabe"[594]. Darin erschöpft sich der verfassungsrechtliche Schutz der Privatheit indessen nicht. Während das Grundgesetz an verschiedenen Stellen Artikel zum Schutz unterschiedlicher Privatheitssphären[595] bereithält – etwa Art. 13 Abs. 1 GG, der eine räumliche Dimension schützt, die wiederum durch Art. 10 Abs. 1 GG bis zu einem gewissen Grad ausgedehnt wird[596]– ist für die vorliegende Arbeit vor allem die informationelle Privatheit[597] und ihr

591 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 9.
592 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 10.
593 Ebd.
594 *Schwan* VerwArch 66 (1975), 120 (121).
595 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 46, spricht in diesem Zusammenhang von „Privatheit als grundrechtliche Identitätsschicht".
596 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 59.
597 Für *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 54, beschreibt die informationelle Privatheit die Beherrschung des Einzelnen darüber, wer was von ihm weiß.

Schutz durch das informationelle Selbstbestimmungsrecht von Interesse.[598] Denn der Umgang mit den Daten im polizeilichen Informationswesen, worunter im Grunde bis auf das Erheben alle Verhaltensweisen der Legaldefinition des § 46 Nr. 2 BDSG fallen,[599] spielt sich nicht in der räumlichen oder kommunikativen Sphäre des Individuums, sondern im genuin informationellen Bereich ab. Dabei stellen alle Akte des polizeilichen Datenumgangs einen Eingriff dar, sofern sie diesen nicht gerade beenden, wie etwa die Löschung von Daten.

Neben der Frage, welche Arten des Datenumgangs als Eingriffe zu werten sind, ist aus grundrechtlicher Sicht auch zentral, wie intensiv durch bestimmte Datenverarbeitungen in das Recht auf informationelle Selbstbestimmung eingegriffen wird. Wesentliche Kriterien hierfür sind der Informationsgehalt des erhobenen Datums, die Heimlichkeit der Erhebungsmaßnahme sowie ihre Streubreite.[600]

Der Informationsgehalt ist hierbei im Sinne einer mehr oder weniger stark ausgeprägten Persönlichkeitsrelevanz zu verstehen. Insbesondere solche Daten, die informationell bestimmten grundrechtlichen Schutzbereichen wie beispielsweise Art. 3 Abs. GG zugeordnet werden können und somit als hoch persönlichkeitsrelevant einzustufen sind, steigern die Intensität eines Eingriffs. Mit Blick auf die inferenzielle Informationsgewinnung wie sie für die ständige Rekombination von einzelnen Datenpunkten im Rahmen von Massendatenverfahren typisch ist, erweist sich der Informationsgehalt *eines* Datums allerdings zunehmend als unzureichend für Eingriffsintensitätsbestimmungen. Der Informationsgehalt eines Datums wird insofern zunehmend relational. Er ergibt sich in Verbindung zu anderen verfügbaren Daten, für die wiederum dasselbe hinsichtlich ihres Informationsgehalts gilt. Diese Fluidität der informationellen Implikationen von (Massen-)Daten in die Eingriffsdogmatik zu übersetzen, steht im Wesentlichen noch aus. Zwar ist mit dem sog. „additiven" Grundrechtseingriff[601] in Ansätzen eine Figur kreiert, die Akkumulationen von Daten abbildet. Je-

598 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 60.

599 Das heißt das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von Daten.

600 Siehe dazu und zum Folgenden *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 119 ff., der freilich noch weitere Aspekte als Kriterien nennt, die hier indessen als eher nachrangig betrachtet werden.

601 Siehe dazu weiter unten im selben Unterabschnitt.

doch bezieht sich dieser Spezialfall des Eingriffs auf eine Person und nicht auf die Aggregierung von Daten über viele Personen und den Inferenzen, die man daraus wiederum für einzelne oder mehrere Individuen ableiten kann.

Zweites wesentliches Kriterium zur Bestimmung der Intensität von Informationseingriffen ist die Heimlichkeit der Maßnahme. Ausgehend von dem Gedanken, dass die Polizei im Umgang mit Daten ganz überwiegend dem Grundsatz der Offenheit folgen soll,[602] wird mit Blick auf das praktische Erfordernis nach heimlichen Ermittlungsmaßnehmen von einer Intensitätssteigerung ausgegangen. Die Gründe dafür sind vielfältig. *Schwabenbauer* nennt etwa das der Heimlichkeit inhärente Konfliktpotenzial mit der Privatheit, mögliche Steuerungsausfälle bezüglich der Rechtskontrolle, auch im Wege des Rechtsschutzes, die Gefahr der Schwächung der exekutiven Gesetzesbindung sowie Authentizitätsprobleme, also die Schwierigkeit, die Richtigkeit der Daten ohne Mitwirkung von Betroffenen zu überprüfen.[603] Diese Kriterien wurden vor allem anlässlich von verdeckten Ermittlungsmethoden entwickelt. Aber auch Datenverarbeitungen, die sich an die originäre Erhebung anschließen, also intern im polizeilichen Informationswesen durchgeführt werden, lassen sich prinzipiell mit dem Etikett der Heimlichkeit versehen, denn sie laufen zumeist ohne Beteiligung und ohne Wissen der Betroffenen ab. Zudem sind auch diese nachgeschalteten Datenverarbeitungen mit exakt denselben Problemen behaftet wie heimliche Erhebungsmaßnahmen. Durch rekombinierende und analysierende Auswertungsverfahren etwa können Sachverhalte bekannt werden, die dem polizeilich nicht-relevanten Privatbereich zufallen. Auch die Rechtskontrolle ist erschwert, wenn fachliche Verfahren (den Bürger:innen) nicht oder (den Aufsichtsbehörden) nur begrenzt bekannt sind. Zudem bestehen bei Datenverarbeitungen im Rahmen des Informationswesens gleichfalls die Gefahr der Schwächung der Gesetzesbindung sowie das Problem der mangelnden Authentifizierbarkeit der informationellen Konstruktionen, zu denen Polizist:innen auf Grundlage von Daten gelangen. Insofern lässt sich dem Datenumgang im polizeilichen Informationswesen ganz grundsätzlich eine gesteigerte Eingriffsintensität zusprechen.

Drittes wichtiges Kriterium ist die Streubreite eines Eingriffs, also die Zahl betroffener Personen. Je höher die Streubreite, desto intensiver der

602 BVerfGE 133, 277 (328) – Antiterrordateigesetz.

603 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 126.

Eingriff, denn auch wenn mit der Streubreite als quantitativer Kategorie noch nichts über die Ausforschungstiefe gesagt ist, werden mit streuenden Maßnahmen tendenziell viele Personen erfasst, die keinen direkten Anlass hierfür gegeben haben. Auch dieses Kriterium bezieht sich im Ursprung eher auf Massendatenerhebungsmaßnahmen. Es lässt sich aber auf Datenauswertungsverfahren übertragen, die mit breiter Datenbasis agieren.

Neben dieser Intensitätsbestimmung einzelner punktueller Eingriffe ist aber mit Blick auf das Volumen an verfügbaren Daten und die Vielzahl von Verarbeitungstechniken eine Weitung der Perspektive auf Eingriffskonstellationen geboten. In diesem Sinne hat sich bereits die Figur des additiven (oder auch: kumulativer) Grundrechtseingriff herausgebildet, der das kumulative Zusammentreffen von mehreren Datenerhebungsmaßnahmen in ein und derselben Person erfassen möchte. Der oder den beteiligten Ermittlungsbehörde(n) sind insofern Verfahrensanforderung auferlegt, um einem unverhältnismäßigen additiven Grundrechtseingriff vorzubeugen.[604] Neben dem Gesetzgeber, der beobachten muss, „ob die bestehenden verfahrensrechtlichen Vorkehrungen auch angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern", sodass „unkontrollierte Ermittlungsmaßnahmen verschiedener Behörden verlässlich verhindert werden können",[605] ist damit auch die Rechtsanwendungsebene angesprochen. Sicherheitsbehörden müssen „koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt."[606] Dogmatisch operationalisieren lässt sich dies bisher grundsätzlich über die Verhältnismäßigkeit einer neu hinzukommende Maßnahme in einem laufenden Verfahren mit bereits eingesetzten Maßnahmen.[607] Insgesamt scheint das Konzept des additiven Grundrechtseingriffs weiterhin ausbaufähig. Vor allem der starke Fokus auf Datenerhebungsmaßnahmen wirkt in Anbetracht des Umstandes, dass es die *Daten* selbst sind, die letztlich die Informationstiefe polizeilicher Erkenntnis bestimmen, etwas falsch fokussiert. Sinnvoll könnte es insofern sein, dem additiven Eingriff die Facette des *aggregierten* Eingriffes hinzuzufügen. Damit ist ein Eingriff gemeint, der durch die Anhäufung, das Zusammentragen und Zusammen-

604 BVerfGE 112, 304 (319 f.) – Global Positioning System.
605 BVerfGE 112, 304 (319 f.) – Global Positioning System, kritisch dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 346.
606 BVerfGE 141, 220 (280 f.) – Bundeskriminalamtsgesetz.
607 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 372.

führen von Daten über eine Person zu charakterisieren ist. Auf diese Weise könnte ein Eingriffsverständnis ermöglicht werden, das sich weniger an dem Zusammenkommen von Erhebungsmaßnahmen festmacht, sondern stärker die letztlich anfallenden Daten und deren informationellen Gehalt, wie er sich im Wege von variablen und relationalen Rekombinationen der Daten ergibt, in den Blick nimmt.

c) Rechtfertigung

Das Recht auf informationelle Selbstbestimmung wird nicht schrankenlos gewährleistet. Schon im Volkszählungsurteil hat das Bundesverfassungsgericht die Sozialbezüge von Kommunikation und Information herausgestellt und einer Daten-"Herrschaft" des Einzelnen eine Absage erteilt. Es müssen vielmehr Einschränkungen des Rechts im überwiegenden Allgemeininteresse hingenommen werden.[608] Für das verfassungsrechtlich in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verankerte Grundrecht finden in erster Linie die Schranken des Art. 2 Abs. 1 GG – dabei ist insbesondere die verfassungsmäßige Ordnung, d.h. die Gesamtheit der mit der Verfassung in Einklang stehenden Normen, von Belang[609] – Anwendung, sodass für Einschränkungen der informationellen Selbstbestimmung zunächst eine formalgesetzliche Grundlage erforderlich ist.[610] Eine solche muss den Grundsätzen der Verhältnismäßigkeit sowie der Bestimmtheit genügen.[611] Dreh- und Angelpunkt hierfür ist der Zweck der gesetzlichen Grundlage; ohne Bestimmung der Erhebungs- und Verarbeitungszwecke ist eine Prüfung der Rechtmäßigkeit von Eingriffen – sowohl auf Rechtsetzungs- als auch auf Rechtsanwendungsebene – in das Recht auf informationelle Selbstbestimmung nicht möglich.[612] Dieser „Grundsatz der Zweckbindung" ist das zentrale normative Instrument zur Steuerung von Informationseingriffen. Als solches kann es bei der Veränderung von informationstechnologischen

608 BVerfGE 65, 1 (42f.) – Volkszählung.
609 BVerfGE 6, 32 (38ff.) – Elfes.
610 *Brink* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. C. Verfassungsrechtliche Grundlagen Rn. 93.
611 BVerfGE 65, 1 (43, 46) – Volkszählung.
612 Vgl. schon BVerfGE 65, 1 (45) – Volkszählung: „Erst wenn Klarheit darüber besteht, zu welchen Zwecken Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, läßt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten."

Zusammenhängen nicht in Stein gemeißelt bleiben und wird dementsprechend vom Bundesverfassungsgericht fortlaufend ausgestaltet.

aa) Der verfassungsrechtliche Grundsatz der Zweckbindung

Aus dem Verhältnismäßigkeitsgrundsatz ergibt sich, dass jedwede Verarbeitung personenbezogener Daten einem (zulässigen) Ziel zu dienen hat, also nicht reiner Selbstzweck sein darf. Um nicht das Bestimmtheitsgebot zu verletzten muss dieser Zweck wiederum hinreichend bestimmt sein; eine Verarbeitung ziellos „ins Blaue hinein" darf dementsprechend nicht erfolgen. Schließlich muss die inhaltliche Bestimmung des Zweckes im Kern durch den Gesetzgeber erfolgen, soll nicht das verfassungsrechtliche Demokratiegebot missachtet werden. Für polizeiliche Datenverarbeitungen ergibt sich aus diesen Vorgaben das verfassungsrechtliche Gebot der Zweckbindung. Möglich ist die Festlegung mehrerer Zwecke innerhalb der jeweiligen Rechtsgrundlage für die Verarbeitung, wobei jeder der Zwecke nachvollziehbar begründet werden muss.[613]

Die vom Zweckbindungsgrundsatz ausgehende Steuerungswirkung ist dabei maßgeblich vom Bestimmtheitsgrundsatz abhängig. Je präziser bzw. enger eine Zweckfestlegung auf einfachgesetzlicher Ebene erfolgt, desto eher kommt es zu einem erneut rechtfertigungsbedürftigen zweckändernden Datenumgang. Diese Unterstützungswirkung des Bestimmtheitsgebots wird vom Bundesverfassungsgericht dahingehend interpretiert, dass für den öffentlichen Bereich eine hinreichend präzise Beschreibung des Verarbeitungszweckes der betroffenen personenbezogenen Daten erforderlich ist.[614] Die Beurteilung muss für jede Rechtsgrundlage einzelfallbezogen erfolgen, kann sich jedoch an einer Je-desto-Formel orientieren: Je intensiver der Eingriff, desto bestimmter muss die Zweckbestimmung sein. Kriterien für die Beurteilung der Intensität sind dabei zumindest die Art der betroffenen Daten, der Bezug der Daten zum allgemeinen Persönlichkeitsrecht, die möglichen Verwendungszusammenhänge der Daten, die Datenmenge, die Art der Datenerhebung, die Verknüpfungsmöglichkeiten, die Verbrei-

613 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 12, vgl. auch *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. A. Prinzipien des Datenschutzrechts Rn. 11ff.

614 BVerfGE 120, 351 (366) – Steuerliche Auslandsdaten.

tungsfähigkeit und die Missbrauchsgefahr.[615] Im Bereich polizeilicher Datenverarbeitung, in dem es unter Effektivitätsgesichtspunkten oftmals auf die Maximierung der vorgenannten Aspekte ankommt, ist daher ein besonderes Augenmerk auf die Bestimmtheit von Datenverarbeitungsbefugnissen zu legen.

Zudem kann auch erst über die Festsetzung eines Zwecks im Sinne eines legitimen Ziels die Verhältnismäßigkeit eines Eingriffs – also seine Geeignetheit, Erforderlichkeit und Angemessenheit zur Zweckerreichung – bestimmt werden. Zwecke der polizeilichen Datenverarbeitung lassen sich mit der Verhütung, Aufklärung und Verfolgung von Straftaten sowie der Gefahrenabwehr sehr breit fassen und werden in dieser Reichweite auch häufig in den gesetzlichen Grundlagen polizeilichen Datenumgangs als Zweckbestimmungen verwendet. Im Rahmen der Verhältnismäßigkeit ist vor allem auch der Grundsatz der Erforderlichkeit für die Umsetzung des Zweckbindungsgrundsatzes von großer Bedeutung. Danach ist eine Datenverarbeitung nur dann zulässig, soweit sie zur Erreichung des Zweckes notwendig ist. Vor allem für die Ebene der Rechtsanwendung sollten vom Grundsatz der Erforderlichkeit wichtige Steuerungsimpulse ausgehen, indem Rechtsanwender:innen dazu angehalten werden, den gegenwärtigen Datenverarbeitungsprozess auf mögliche Alternativen hin zu reflektieren. Zudem lässt sich nur über den Zweck einer Datenverarbeitung ihre Angemessenheit – generell wie im Einzelfall – bewerten. Hier sind die Zwecke, aus polizeilicher Sicht also in erster Linie der Schutz vor mehr oder weniger erheblichen Gefahren oder die Verhütung, Aufklärung und Verfolgung von mehr oder weniger schweren Straftaten, mit der jeweils durch die Maßnahme im Allgemeinen oder speziellen Anwendungsfall ausgehenden Eingriffsintensität in ein ausgeglichen abgewogenes Verhältnis zu bringen.[616] Insoweit lässt sich auch von „Zweckhierarchien"[617] sprechen: Werden weniger sensible Daten verarbeitet, so können die generellen Polizeizwecke der Gefahrenabwehr und Strafverfolgung ausreichende Zweckbestimmungen darstellen. Sensiblere Daten oder sonst eingriffsintensivere Maßnahmen erfordern demgegenüber spezifischere und anspruchsvollere Zwecke wie etwa die Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer

615 Siehe dazu etwa *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, DS-GVO Syst. A. Prinzipien des Datenschutzrechts Rn. 19 ff.

616 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 195 ff.

617 *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 18.

Person oder die Verfolgung von schwere(re)n Katalogstraftaten. Auch diese Abstufung geht indessen von einer prinzipiell im Vorhinein feststellbaren Sensibilität des informationellen Gehalts eines Datums aus, was bei einem Fokus auf die Invasivität der Erhebungsmaßnahme auch noch sinnvoll sein kann. Im Rahmen der anschließenden Verarbeitung hingegen können aus der relationalen Zusammenführung wenig sensibler Daten tiefgehende Persönlichkeitsinformationen rekonstruiert werden, sodass insofern stets eine hohe Zweckschwelle in der Rechtsgrundlage festzuschreiben ist und in der Rechtsanwendung besondere Anforderungen an die Prüfung der zweckbezogenen Verhältnismäßigkeit zu stellen sind.

bb) Die zweckwahrende Weiternutzung

Im Bereich polizeilicher Datenverarbeitung hat der Grundsatz der Zweckbindung zusätzliche Konkretisierung erfahren. Dem BKAG-Urteil des Bundesverfassungsgerichts nach wird die Reichweite der Zweckbindung durch die jeweilige Datenerhebungs- bzw. Datenverarbeitungsbefugnis determiniert und diese erhalten ihren Zweck aus dem zugrundeliegenden polizeilichen Verfahren.[618] Anhand dieser einzelfallbezogenen Zweckfestlegung eines Datums kann dann beurteilt werden, ob ein Datenumgang die Zweckbindung einhält oder zweckändernd erfolgt. Dabei ist allerdings zu beachten, dass nunmehr nicht mehr jede Verarbeitung von Daten außerhalb des ursprünglichen Verfahrens eine Zweckänderung darstellt.

Während das Gericht selbst und etliche Stimmen aus dem Schrifttum bis 2016 davon ausgingen,[619] dass die Datenverarbeitung über das konkrete Anlassverfahren hinaus prinzipiell als Zweckänderung zu behandeln sei, hat das BKAG-Urteil die verfassungsrechtlichen Rahmenbedingungen neu gesteckt:

> „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

618 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.

619 Siehe die Nachweise bei *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 16 Fn. 52, 53.

> begrenzt dies deren unmittelbare sowie weitere Verwendung auch in derselben Behörde, soweit keine gesetzliche Grundlage für eine zulässige Zweckänderung eine weitergehende Nutzung erlaubt."[620]

Damit ist der Bereich innerhalb dessen Akte polizeilicher Datenverarbeitung noch als zweckerfüllend anzusehen sind in nicht unerheblicher Weise ausgeweitet worden. Aus dem zweiten Satz des angeführten Urteilszitates scheint sich überdies noch zu ergeben, dass keine Identität zwischen den geschützten Rechtsgütern und zu verhütenden Straftaten im Anlassverfahren und im Verfahren, in dem es zur zweckwahrenden[621] Weiternutzung kommt, bestehen muss. Gewährt eine Rechtsgrundlage etwa einer Polizeibehörde die Erhebung von Daten zur Abwehr einer Gefahr für das Leben und die Freiheit einer Person, so können Daten, die im Anlassverfahren zur Abwehr einer Lebensgefahr erhoben worden sind, ebenfalls von derselben Polizeibehörde zur Abwehr einer Gefahr für die Freiheit einer Person weiter genutzt werden.[622] Damit wird insbesondere der sog. Zufallsfund erfasst.[623] Es besteht allerdings das Risiko, dass die Polizei durch eine extensive Festlegung der im Ausgangsverfahren zu schützenden Rechtsgüter oder zu verhütenden Straftaten die Reichweite der Befugnis zur zweckwahrenden Weiternutzung ausweitet und die beabsichtigte Begrenzungsfunktion leer läuft.[624]

Zudem ist für die zweckwahrenden Weiternutzung nicht erforderlich, dass dieselbe Eingriffsschwelle wie im Rahmen der Datenerhebung – etwa eine bestimmte Stufe einer Gefahr oder des Tatverdachts – erreicht ist. Diese Schwellen, die für die Datenerhebung erreicht sein müssen, gehören nicht zu „den Zweckbindungen, die für jede weitere Nutzung der Daten seitens derselben Behörde je neu beachtet werden müssen".[625] Das Bundesverfassungsgericht führt weiter aus, dass die Eingriffsschwellen lediglich „den Anlass, aus dem entsprechende Daten erhoben werden dürfen [bestimmen], nicht aber die erlaubten Zwecke, für die die Daten der Behörde

620 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.
621 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), passim.
622 Beispiel nach *Bäcker* Stellungnahme BKAG, A-Drs. 18(4)806 D, S. 12.
623 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 18.
624 So in der Auslegung durch *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 12 BKAG Rn. 10; zu Recht kritisch dazu *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 17.
625 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.

dann zur Nutzung offen stehen."[626] Neben den bereits genannten Anforderungen an eine zweckwahrende Weiternutzung der Daten ist folglich keine weitere Anforderung zu erfüllen, wenn diese als Spurenansatz für folgende Ermittlungen genutzt werden. Der entsprechenden Behörde steht es mithin – bei entsprechender Rechtgrundlage – frei,

> „die insoweit gewonnenen Kenntnisse zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellung – allein oder in Verbindung mit anderen ihr zur Verfügung stehenden Informationen – als schlichten Ausgangspunkt für weitere Ermittlungen nutzen. Dies trägt dem Umstand Rechnung, dass sich die Generierung von Wissen – nicht zuletzt auch, wenn es um das Verstehen terroristischer Strukturen geht – nicht vollständig auf die Addition von je getrennten, nach Rechtskriterien formell ein- oder ausblendbaren Einzeldaten reduzieren lässt. In den dargelegten Grenzen erkennt das die Rechtsordnung an. Diese Grenzen gewährleisten zugleich, dass damit keine Datennutzung ins Blaue hinein eröffnet ist."[627]

Etwas anderes gilt indessen für die besonders eingriffsintensiven Maßnahmen der Wohnraumüberwachung und der Online-Durchsuchung. Eine weitere Nutzung der Daten bewegt sich nur dann noch im ursprünglichen Erhebungszweck, „wenn sie auch aufgrund einer den Erhebungsvoraussetzungen entsprechenden dringenden Gefahr oder im Einzelfall drohenden Gefahr erforderlich ist." Ausgeschlossen ist hingegen eine Nutzung als Spuren- oder Ermittlungsansatz „unabhängig von einer dringenden oder im Einzelfall drohenden Gefahr."[628] Insgesamt gibt dieser als zweckwahrende Weiternutzung bezeichnete verfassungsrechtliche Spielraum den Polizeien in Deutschland die Möglichkeit, recht frei mit Daten umzugehen, ohne durch die weitergehenden verfassungsrechtlichen Anforderungen an eine Zweckänderung behindert zu werden,[629] sodass sich diese Flexibilisierung des polizeilichen Datenumgangs als verfassungsrechtliche Anpassung an das Zeitalter der Massendaten deuten lässt, womit auch weitere evolutive Entwicklungen der Zweckdogmatik in Zukunft nicht ausgeschlossen erscheinen.

---

626 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.
627 BVerfGE 141, 220 (324f.) – Bundeskriminalamtgesetz.
628 BVerfGE 141, 220 (325) – Bundeskriminalamtgesetz.
629 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 57, spricht von „kaum […] überprüfbare[r] Definitionsmacht."

Die Urteile zu dieser Evolution fallen in der Literatur unterschiedlich aus.[630] Vor dem Hintergrund der faktischen Außerkraftsetzung des Zweckbindungsgrundsatzes durch die Praxis der polizeilichen Datenverarbeitung schon vor dem Urteil nähert sich die Rechtsprechung des Bundesverfassungsgerichts jedenfalls klar polizeipraktischen Bedürfnissen und Realitäten an. Dieser judikative Pfad erscheint mit Blick auf die Zwänge des Massendatenphänomens insoweit nachvollziehbar, als der Polizei Handlungsmöglichkeiten im flexibleren Datenumgang eröffnet werden sollen. Allerdings lässt sich kaum von der Hand weisen, dass damit normative Stützpfeiler der Idee der informationellen Selbstbestimmungen an Tragkraft verlieren. Zwar soll diese Reduzierung materieller Grenzen wohl durch die Prozeduralisierung des Grundrechtsschutzes, wie er auch paradigmatisch für die JI-Richtlinie ist, aufgefangen werden – ob sich diese Hoffnung als zutreffend erweisen wird, gilt es jedoch aufmerksam zu beobachten.

cc) Die Zweckänderung

Der – nunmehr auch verfassungsrechtlich durch die zweckwahrende Weiternutzung aufgeweichte – Zweckbindungsgrundsatz soll die Datenverarbeitung steuern und rechtlich handhabbar machen. Eine im vorliegenden Kontext relevante und auch beabsichtigte Folge ist die Trennung staatlicher Datenbestände voneinander (sog. „informationelle Gewaltenteilung“[631]), die eine funktionierende Aufgabenerfüllung seitens der staatlichen Behörden erschwert, indem es die Zusammenführung vorhandener Informationen zu tiefergehendem Wissen an Voraussetzungen knüpft. Allerdings ist staatliches Handeln von soliden und auch möglichst umfassenden Informationen abhängig, sodass die Frage, wann es zu einer Durchbrechung des Zweckbindungsgrundsatzes und damit zu einer Zusammenführung von Daten kommen soll, als „Grunddilemma des Datenschutzrechts“[632] in Deutschland gelten kann. Dogmatisch ist es mit der Lösung des Problems letztlich nicht weit her: Der zweckentfremdende Umgang mit bereits

630 *Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 17, sieht hier „zumindest eine Neujustierung“; *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 3, sieht hingegen einen Dammbruch.

631 *Di Fabio* in *Dürig/Herzog/R. Scholz,* Grundgesetz, Art. 2 Rn. 184, siehe auch dort zu grundsätzlicher Kritik an diesem Prinzip.

632 *H. Wolff* ZG 31 (2016), 361 (380).

gespeicherten Daten ist wiederum ein rechtfertigungsbedürftiger Eingriff, dessen Rechtfertigung möglich, aber auch nötig ist – insoweit also einem neuen, bestimmten Zweck in verhältnismäßiger Weise dienen muss.[633] Tangiert werden damit die schon durch die Datenerhebung beeinträchtigten Grundrechte.[634]

Die Verfassungsrechtsprechung hat die Anforderungen an die Zweckänderung seit dem Volkszählungs-Urteil beständig weiterentwickelt und für die polizeiliche Datenverarbeitung im BKAG-Urteil konsolidiert. Wie bereits im Rahmen der Erhebung müssen die geänderten Zwecke hinreichend bestimmt festgelegt werden.[635] Zusätzlich muss die Bedeutung der Daten in verhältnismäßiger Weise berücksichtigt werden. Daten aus besonders eingriffsintensiven Maßnahmen, dürfen nur zu besonders gewichtigen, anderen Zwecken genutzt werden,[636] worin sich einmal mehr das stark auf Erhebungsmaßnahmen und nicht so sehr auf Daten fokussierte Eingriffsverständnis zeigt. Das BKAG-Urteil hat hier mit der Formulierung des Grundsatzes der hypothetischen Datenneuerhebung weitere Spezifizierung mit Blick auf die Zweckänderung im Bereich polizeilicher Datenverarbeitung gebracht. Danach ist nun ausschlaggebend für die Zulässigkeit einer Zweckänderung, ob mit ihr „grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, die Informationen also für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen." [637] *Wolff* zufolge stellt sich in diesem Zusammenhang die Frage, ob der Gesetzgeber befugt wäre, der konkreten empfangenden Behörde eine Befugnis einzuräumen, die erhaltenen Daten mit vergleichbaren Mitteln, also vergleichbaren Eingriffen, selbst zu erheben.[638] Dabei ist indessen zu beachten, dass die hypothetische Datenneuerhebung nicht bedeutet, dass exakt dieselben Anforderungen wie bei der Datenerhebung gelten[639] sondern die Zweckänderung eine gewisse „Selbst-

633 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 13.
634 Vgl. BVerfGE 141, 220 (327) – Bundeskriminalamtgesetz mwN.
635 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 186.
636 BVerfGE 141, 220 (327) – Bundeskriminalamtgesetz.
637 Zuvor war darauf abgestellt worden, ob Erhebungs- und neuer Verwendungszweck miteinander (nicht) unvereinbar sind, vgl. etwa BVerfGE 130, 1 (33 f.) – Verwertungsverbot Wohnraumüberwachung; zum Rechtsprechungsverlauf, der dieses Kriterium durch den Grundsatz der hypothetischen Datenneuerhebung „konkretisiert und ersetzt" hat, vgl. hierzu und zur zitierten Stelle BVerfGE 141, 220 (327 f.) – Bundeskriminalamtgesetz.
638 *H. Wolff* ZG 31 (2016), 361 (382).
639 BVerfGE 141, 220 (327 f.) – Bundeskriminalamtgesetz.

ständigkeit" besitzt.[640] Wichtiger ist vielmehr die „Gleichgewichtigkeit der neuen Nutzung".[641] Die jeweils verfolgten Zwecke von alter und neuer Nutzung müssen also vergleichbar sein, sodass die neuen Zwecke umso gewichtiger sein müssen, je eingriffsintensiver die ursprüngliche Erhebung war.[642] Zusätzlich soll der Grundsatz der hypothetischen Datenneuerhebung davor schützen, dass mittels einer Zweckänderung grundrechtliche Erhebungsbeschränkungen unterlaufen werden.[643] Im Bereich polizeilicher Datenverarbeitung ist mit Blick auf materielle Rahmenbedingungen der Zweckänderung zudem noch relevant, dass ein „allgemeine[r] Austausch personenbezogener Daten aller Sicherheitsbehörden oder de[r] Abbau jeglicher Informationsgrenzen zwischen ihnen" unzulässig ist.[644]

Von diesen inhaltlichen Anforderungen an die Zweckänderungen sind schließlich noch die Mindestvoraussetzungen zu unterscheiden, die an den Anlass einer Zweckänderung zu stellen sind. Der Anlass zu einer Zweckänderung bedarf dabei nicht desselben „Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts", da

> „[d]ie diesbezüglichen Anforderungen […] unter Verhältnismäßigkeitsgesichtspunkten primär den Anlass nur unmittelbar für die Datenerhebung selbst [bestimmen]. […] Als neu zu rechtfertigender Eingriff bedarf aber 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."[645]

Anders ist dies im Falle der Wohnraumüberwachung sowie des Zugriffs auf informationstechnische Systeme, bei der eine der Erhebung gleich hohe Anlassschwelle erforderlich ist.[646] Was genau aber unter dem konkreten Ermittlungsansatz zu verstehen ist, ist bis dato noch nicht abschließend

640 *H. Wolff* ZG 31 (2016), 361 (382).
641 BVerfGE 141, 220 (328) – Bundeskriminalamtgesetz; *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 190, spricht insoweit von der „alles überwölbende[n] Großformel".
642 BVerfGE 141, 220 (327) – Bundeskriminalamtgesetz.
643 Bspw. im Fall der optischen Wohnraumüberwachung, BVerfGE 141, 220 (338 f.) – Bundeskriminalamtgesetz.
644 BVerfGE 133, 277 (321) – Antiterrordateigesetz.
645 BVerfGE 141, 220 (328 f.) – Bundeskriminalamtgesetz.
646 BVerfGE 141, 220 (328) – Bundeskriminalamtgesetz.

geklärt.[647] Außerdem wird bezweifelt, ob die dadurch bewirkte Absenkung der Eingriffsschwelle für Zweckänderungen überhaupt noch rechtsstaatlich vertretbar ist.[648] Auch hier zeigen sich Anpassungsbemühungen der Verfassungsrechtsprechung an die zunehmend datengesättigten Umwelten, in denen die deutschen Polizeien mit wachsenden Datenvolumina agieren müssen.

Ebenfalls relevant im Kontext der Zweckänderung ist die Datenübermittlung zwischen unterschiedlichen (Polizei-)Behörden wie sie im polizeilichen Informationswesen mit seinen unterschiedlichen Datenbanken und Informationssystemen täglich vielfach geschieht. Daneben sind vor allem auch Datenübermittlung zwischen Polizeien und Justiz, insbesondere den Staatsanwaltschaften, besonders relevant in diesem Kontext. Kommt es zu einem zweckändernden Austausch von Daten, sind regelmäßig[649] zwei Akteure – ein abgebender und ein empfangender – beteiligt. Durch einen solchen Austausch erfolgen somit genau genommen zwei Grundrechtseingriffe, sodass auch zwei Rechtsgrundlagen erforderlich sind. Klärungsbedürftig ist nicht nur die Frage, unter welchen Bedingungen Daten abgegeben werden, sondern auch unter welchen Bedingungen sie entgegengenommen werden dürfen:

> „Ein Datenaustausch vollzieht sich durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung [*Schwabenbauer* zufolge auch „Nutzung“[650]], die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten. Dies schließt – nach Maßgabe der Kompetenzordnung und den

---

647 So etwa *Spiecker gen. Döhmann*, Bundesverfassungsgericht kippt BKA-Gesetz: Ein Pyrrhus-Sieg der Freiheitsrechte?, https://verfassungsblog.de/bundesverfassungsgericht-kippt-bka-gesetz-ein-pyrrhus-sieg-der-freiheitsrechte/ (Stand: 01.10.2023).

648 So *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 35.

649 Das ist nicht der Fall, wenn Daten innerhalb der Erhebungsbehörde nicht zweckkonform weitergenutzt werden, wobei wohl letztlich dieselben verfassungsrechtlichen Anforderungen gelten, vgl. *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 177.

650 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 176.

Anforderungen der Normenklarheit – nicht aus, dass beide Rechtsgrundlagen auch in einer Norm zusammengefasst werden können."[651]

Dieses sog. „Doppeltürmodell" ist im Bereich polizeilicher Datenbanken – vor allem mit Blick auf die starke Föderalisierung der Polizei – von großer Bedeutung und hat in den entsprechenden Rechtsmaterien einfachgesetzliche Ausgestaltung erfahren. Im Rahmen der Darstellung relevanter strafprozess- und polizeirechtlicher Regelung wird darauf zurückzukommen sein.[652] Verfassungsrechtlich jedenfalls bestehen auch hier wieder vor allem hohe Anforderungen an die Bestimmtheit der Zwecke in Übermittlungsregelung (erste Tür) und Abrufregelung (zweite Tür), sodass vor allem abrufende Stellen die verfügbaren Daten nicht unabhängig vom ursprünglichen Zweck bevorraten können.[653] Im Bereich der zweckändernden Übermittlung kommt denn auch wieder der Grundsatz der hypothetischen Datenneuerhebung zum Tragen. Dabei gilt dieser „nicht schematisch". So kann aus Vereinfachungs- und Praktikabilitätsgründen bei der Schaffung von Übermittlungsvorschriften eine geringere Detailliertheit in den Voraussetzungen im Vergleich zu Erhebungsvorschrift gerechtfertigt sein. Auch der Umstand, dass die Zielbehörde wegen ihres Aufgabenspektrums bestimmte Datenerhebungen, zu denen die Ausgangsbehörde berechtigt ist, nicht vornehmen darf, steht einem Datenaustausch nicht grundsätzlich entgegen. Zentrales Kriterium ist vielmehr die Gleichwertigkeit der neuen Datennutzung.[654] Hiermit werden, wie mit der Figur der zweckwahrenden Weiternutzung, Datenflüsse zwischen sicherheitsbehördlichen und sonstigen (staatlichen) Stellen ebenfalls flexibilisiert, wobei weiterhin Informationsgrenzen zwischen den behördenspezifischen Datenbeständen bestehen bleiben müssen.[655]

2. Aggregiert-kollektive Datenakkumulation als blinder Fleck der individualistischen Verfassung?

Mit dem fortschreitenden Ausbau der informationellen Befugnisse der Bundes- und Länderpolizeien stellt sich – ähnlich wie bereits im Rahmen

651 BVerfGE 130, 151 (184) – IP-Adresse.
652 Siehe dazu unten S. 350 ff.
653 BVerfGE 155, 119 (179 f.) – Bestandsdatenauskunft II.
654 BVerfGE 141, 220 (328) – Bundeskriminalamtgesetz.
655 BVerfGE 133, 277 (321) – Antiterrordateigesetz.

der Überlegung, ob Einschüchterungseffekte einen Eingriff darstellen können – die Frage nach den globalen gesellschaftlichen Auswirkungen des Anwachsens staatlicher bzw. spezieller: polizeilicher Datenbestände. Neben den individuellen Schranken, die das Recht auf informationelle Selbstbestimmung und andere möglicherweise betroffene Grundrechte polizeilicher Datenverarbeitung punktuell auferlegen können, wird zunehmend auch über globalgesellschaftliche Perspektiven zum Schutz vor sicherheitsbehördlicher Überwachung nachgedacht. Denn die umfassende Verfügbarkeit von Daten im polizeilichen Informationswesen erhöht die Eingriffsintensität, die in jeder Verarbeitung eines Datums liegt, insgesamt, da der potenzielle Informationsgehalt durch die Potenzierung der Verknüpfungsmöglichkeiten stark zunimmt. Gegenwärtig zentral in der Diskussion um die Auswirkungen der Expansion polizeilicher Informationsbefugnisse und Datenbestände ist die sogenannte Überwachungsgesamtrechnung, die *Roßnagel*[656] in Auseinandersetzung mit der verfassungsgerichtlichen Entscheidung zur Vorratsdatenspeicherung[657] konzeptuell formuliert hat. Seitdem hat es bereits Versuche der dogmatischen Operationalisierbarkeit, etwa in Form einer doppelten Verhältnismäßigkeitsprüfung, gegeben,[658] jedoch bisher ohne nachhaltigen Anschluss zu finden.

An das Konzept anknüpfend, aber zunächst auf die faktische Operationalisierung bedacht, ist das sogenannte „periodische Überwachungsbarometer" von *Poscher et al.*[659] Zentrales Anliegen dieses Konzepts ist zunächst eine quantitative Analyse der „Zugriffe von Sicherheitsbehörden auf Massendatenbestände in öffentlicher oder privater Hand, in denen jedermann anlasslos erfasst ist", um so statistische Aufbereitungen und Veranschaulichungen der gezogenen Erkenntnisse zu ermöglichen. So sollen sich in verschiedenen Dimensionen – etwa regional, zeitlich, behördlich – die Akkumulationen von Daten darstellen lassen. Auf der höchsten, gesamtgesellschaftlichen Aggregationsstufe ließe sich schließlich das namensgebende Überwachungsbarometer erstellen, das einen „Eindruck von dem Gesamtüberwachungsstatus durch die Sicherheitsbehörden" vermitteln soll. Erst auf Grundlage dieser empirisch-faktischen Basis sollen dann direktere dogmatische Reaktionen insbesondere durch das Bundesverfassungsgericht

656 *Roßnagel* Neue Juristische Wochenschrift 63 (2010), 1238.
657 BVerfGE 125, 260 (323 f.) – Vorratsdatenspeicherung.
658 *Knierim* ZD 2011, 17.
659 *Poscher*, Konzept für ein periodisches Überwachungsbarometer, Deutscher Bundestag, Ausschussdrucksache 19(4)732 E, 2021; siehe auch *Poscher/Kilchling/Landerer* Zeitschrift für das Gesamte Sicherheitsrecht (GSZ) 4 (2021), 225.

möglich sein, etwa indem es daraus Rechtfertigungslasten für die abstrakte Zulässigkeit neuer Überwachungsinstrumente oder auch der Anwendung bestehender Maßnahmen im Einzelfall ableitet. Daneben sind aber vor allem auch Einflussnahmen durch öffentliche Diskussion und damit letztlich Gesetzgebung beabsichtigte Folge der Aggregierung der „Überwachungslast". Zur Realisierung des periodischen Überwachungsgesamtbarometers sind drei Phasen angedacht, wobei die dritte explizit auf einen nicht näher spezifizierten zukünftigen Zeitraum verschoben ist.

Die erste Phase dient einer Exploration der einzubeziehenden Datenbestände, wobei ein Fokus auf anlasslos gespeicherte Massendaten gelegt wird. Ausdrücklich ausgeklammert werden die verschiedenen anlassbezogenen sicherheitsbehördlichen Datenbanken, wobei eine spätere Einbeziehung denkbar erscheint, sodass testweise die Antiterror-Datei mitberücksichtigt wird. Allerdings sollen auch private Datenbestände, auf die staatliche Zugriffsrechte bestehen, mit in die Zusammenschau staatlicher Datenaggregationen einbezogen werden. So sollen dann beispielsweise Datenbestände mit Telekommunikationsdaten, finanzbezogenen Daten, Mobilitätsdaten, Daten aus dem privaten Lebensbereich, Gesundheitsdaten und Meldedaten in das Barometer einfließen. Die darin zum Ausdruck kommende Modularität des Konzepts soll zudem auch in Zukunft die Erweiterbarkeit durch sonstige relevante Datensammlungen wie beispielsweise Videoüberwachungen im öffentlichen Raum ermöglichen.

In der zweiten Phase sollen einerseits die Zugriffstatbestände der Sicherheitsbehörden rechtlich analysiert und normativ bewertet werden, „um eine gewichtete Aggregation der verschiedenen Zugriffszahlen zu ermöglichen." Andererseits sollen in diesem Projektschritt aber auch die vorhandenen Dokumentationspflichten der Behörden analysiert werden, die Grundvoraussetzung für das gesamte Konzept sind. Denn ohne eine Dokumentation, aus der sich eine zahlenmäßige Beschreibung des Zugriffsverhaltens ableiten lässt, kann keine quantitative Aggregation stattfinden. Das gilt umso mehr, als dass öffentlich verfügbare Daten lückenhaft sind und insofern die „elektronisch dokumentierten Einsatzprotokolle" zentrale Erkenntnisquelle für das tatsächliche Zugriffsverhalten sind. Für den privaten Sektor sind vor allem die internen Daten zu Zugriffen durch Sicherheitsbehörden relevant. Hier besteht aufgrund der hohen Marktmacht einiger weniger Akteure eine gute Chance über deren Daten ein halbwegs repräsentatives Bild zu zeichnen.

Insbesondere die quantitative Herangehensweise des Konzepts ist sehr zu begrüßen, da sich nur so eine verlässliche und weiterführende Diskussionsgrundlage für Rechtswissenschaft und Öffentlichkeit schaffen lässt, die wesentlich faktenbasierter sein könnte als die gegenwärtige, vor allem normative Auseinandersetzung. Darüber hinaus ist auch der Fokus auf gesetzliche Dokumentationspflichten der Sicherheitsbehörden sinnvoll, da die in diesem Rahmen anfallenden Daten so endlich einer überindividualistischen Nutzung zufließen und an Wirkkraft gewinnen können. Der in diesem Zusammenhang geäußerte Vorschlag einer Standardisierung für die Aufarbeitung der Daten für das Überwachungsbarometer ist dementsprechend vollumfänglich zu unterstützen. Indessen erscheint die (bisherige und nahezu vollständige) Ausklammerung von sicherheitsbehördlichen Datensammlungen für das Konzept selbst problematisch, auch wenn sie aus forschungs- und umsetzungspraktischen Gründen natürlich nachvollziehbar ist. Nichtsdestotrotz sind die behördeneigenen Datenspeicher immer Ausgangspunkt für Überwachungsmaßnahmen wie Zugriffe auf externe Datensammlungen, sodass eine diesbezügliche Aussparung im Konzept Gefahr läuft, einen zentralen Baustein der polizeilichen Datenakkumulationsmacht zu vernachlässigen. Denn einerseits können – wie es im Konzeptpapier auch gesehen wird – solche Datenbestände bereits den Charakter einer behördlichen Vorratsdatenspeicherung annehmen und andererseits ist auch hier zu bedenken, dass sich der informationelle Gehalt von Datensammlungen durch ihre relative Modularität ergibt, wie man sie schon von der Rasterfahndung kennt: Durch die Kombination verschiedener Datenbestände, die dann wiederum mit den datenförmigen Erkenntnissen der Polizei abgeglichen werden, können sich je nach modularer Konstellation – auch in ihrem Intensitätsgehalt – ganz unterschiedliche Informationen ergeben. Insofern sollten – wie es auch geplant zu sein scheint – die sicherheitsbehördlichen bzw. polizeilichen Datensammlungen auf mittelfristige Sicht mit in das Konzept integriert werden.[660]

II. Polizeiliches Vorfeld und Verfassung

Bereits im Rahmen der historischen Rückschau auf polizeiliche Informationsverarbeitung hat sich gezeigt, dass das Sammeln von möglichst umfas-

660 Siehe dazu noch einmal unten S. 531 ff.

senden Informationen ein der Polizei als Institution inhärenter Impetus ist. Die rechtsstaatlichen Zähmungsversuche in Form von Gefahren- und Verdachtsdogmatik waren indessen nur so lange ausreichend, wie der Umgang mit Daten unabhängig von konkreten Straf- oder Gefahrenabwehrverfahren als nicht oder kaum grundrechtsbedenklich galt, sodass mit dem Volkszählungsurteil auch das polizeiliche Handeln im Vorfeld von Gefahr und Verdacht stärker in die rechtswissenschaftliche Aufmerksamkeit geraten ist. Dabei geht es allerdings längst nicht mehr nur um die Einhegung hergebrachter informationeller Praktiken der Polizei. Vielmehr befindet sich das polizeiliche Vorfeld durch gesellschaftlichen Risikodiskurses, die maßgeblich durch *Beck* explizit ins allgemeine Bewusstsein gebracht wurden,[661] bereits seit Jahrzehnten in einem Wandlungsprozess. In diesem tarieren sich die Grenzen des Nötigen, Möglichen und Erlaubten im polizeilichen Vorfeld stetig durch Wechselwirkungen zwischen den diskursiven, technischen und rechtlichen Aspekten des gesellschaftlichen Sicherheitsensembles ständig neu aus.

Relevant ist die Form der (verfassungs)rechtlichen Ausgestaltung der polizeilichen Vorfeldbefugnisse vorliegend deshalb, weil darüber die Reichweite polizeilicher Datenerhebungen und somit auch des Informationswesens strukturell erweitert werden. Statt reaktiv und einzelfallbezogen Daten zu erheben, ermöglicht das Vorfeld die proaktive Generierung von einzelfallübergreifenden Datenaggregationen.[662] Begründet wird die Notwendigkeit dieses Handlungsmodus, der in den Grenzen von Verdacht und Gefahr nicht möglich ist,[663] vor allem mit der sonst kaum zu bewältigenden Aufklärung und Bekämpfung komplexer krimineller Strukturen – also im Wesentlichen organisierte Kriminalität und Terrorismus.[664]

661 *Beck,* Risikogesellschaft.

662 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 237 ff.

663 *Bäcker* in*Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 239.

664 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 241 et passim Zur den Ausweitungsproblematiken solcher Begründungsmuster und der epistemischen Ursachen siehe bereits oben S. 124 ff.

1. Das strafverfahrensrechtliche Vorfeld

Das polizeiliche Vorfeld ist dabei konzeptuell sowohl im repressiven als auch im präventiven Handlungsfeld denkbar. Lange Zeit waren Eingriffsmaßnahmen aus beiden Feldern ausschließlich im Polizeirecht verortet. Unter der Aufgabenzuweisung der vorbeugenden Bekämpfung von Straftaten wurde neben der präventiven Verhütung auch die repressive Vorsorge für die Verfolgung von Straftaten gefasst und so kompetenziell den Polizeigesetzgebern zugesprochen.[665] Dieser Verteilung hat das Bundesverfassungsgericht jedoch in seinem „Niedersachsenurteil" einen Riegel vorgeschoben, in dem es die Gesetzgebungskompetenz des Bundes bezogen auf das Strafverfahren zweckbezogen interpretierte und „vorsorgende Maßnahmen, die sich auf die Durchführung künftiger Strafverfahren beziehen", dieser Gesetzgebungskompetenz zusprach.[666] Folglich entfaltet Art. 72 Abs. 1 GG nur insoweit Spielräume für die Landesgesetzgeber, wie der Bund von seiner strafverfahrensrechtlichen Gesetzgebungskompetenz keinen abschließenden Gebrauch gemacht hat. Nach Ansicht des Verfassungsgerichts hat der Bundesgesetzgeber jedoch gerade unterlassen, Überwachungsmaßnahmen und die mit ihnen bezweckte Datenermittlung für Zwecke zukünftiger Strafverfahren von einem Tatverdacht zu entkoppeln und damit gleichzeitig das strafverfahrensrechtliche Vorfeld insoweit gesperrt.[667] Legislative Freiheiten verbleiben den Ländern daher nur begrenzt in Fällen ohne Bezug zu Personen, worunter etwa sach- oder ortsbezogene sowie an allgemeine Bedrohungslagen anknüpfende Maßnahmen fallen, sodass vor allem das Feld der gelegenheitsorientierten Kriminalprävention auch zu Zwecken der Strafverfolgung weiter für Landesgesetzgeber offen bleibt. [668] Zudem – und wesentlich relevanter – dürfen die Landesgesetzgeber Rechtsgrundlagen für die Weiterverarbeitung von Strafverfahrensdaten nach Maßgabe der Polizeigesetze schaffen, wie es der Bundesgesetzgeber mit § 481 StPO explizit zum Ausdruck gebracht hat.

Insofern besteht bis auf punktuelle Maßnahmen wie §§ 81a, 81b StPO kein strafverfahrensbezogenes Vorfeldrecht mit präventiver Ausrichtung,[669]

665 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 320.
666 BVerfGE 113, 348 (371) – Vorbeugende Telekommunikationsüberwachung.
667 BVerfGE 113, 348 (371 f.) – Vorbeugende Telekommunikationsüberwachung.
668 Siehe dazu *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 321, insb. auch Fn. 589 mit Fallnachweisen.
669 BVerfGE 113, 348 (373.) – Vorbeugende Telekommunikationsüberwachung.

sodass dessen Grenzen, insbesondere mit Blick auf die Entkoppelung von Maßnahmen vom Verdachtserfordernis, ungeklärt sind. Theoretisch wären eine Erschließung und Ausgestaltung durch den Gesetzgeber aber möglich. Gleichzeitig scheint sich die gesetzgeberische Energie mit Blick auf die Erschließung des Vorfelds im repressiven Bereich eher in Form eines kriminalpräventiv ausgerichteten Strafrechts zu entladen.[670]

2. Das polizeirechtliche Vorfeld

Im polizeirechtlichen Bereich wurden indessen durch iterative Runden aus Gesetzgebung und darauf antwortender Verfassungsrechtsprechung Vorfeldermächtigungen geschaffen und konturiert, sodass hier ein vom klassischen Gefahrerfordernis abweichendes polizeiliches Handlungsfeld entstanden ist. Um dieses dreht sich eine durch die judikativen Impulse der Verfassungsgerichte ständig neu angetriebene Diskussion bezüglich der Grenzen des verfassungsrechtlich Zulässigen im polizeirechtlichen Vorfeld. Während einige die Steuerungsleistung der bundesrepublikanischen Verfassung mit Blick auf derartige Entgrenzungen polizeilichen Handelns bezweifeln[671] und demgegenüber eher auf eine Grundrechtssicherung durch Verfahren setzen,[672] hat das Bundesverfassungsgericht in seiner jüngeren Rechtsprechung eine materielle Ausgestaltung des polizeirechtlichen Vorfelds unternommen.[673]

---

670 Siehe dazu unten S. 182 ff.

671 So spricht *Grimm* Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV) 1 [69] (1986), 38 (54), in diesem Kontext davon, dass entsprechendes Tun "nicht mehr ausreichend normativ steuerbar" wäre; ähnlich *P.-A. Albrecht,* Der Weg in die Sicherheitsgesellschaft, 238 f.

672 Ausführlich *Bonin,* Grundrechtsschutz durch verfahrensrechtliche Kompensation bei Maßnahmen der polizeilichen Informationsvorsorge; siehe auch *Kugelmann/Dalby* in D. Busch/Roggan (Hrsg.), Das Recht in guter Verfassung?, 105; konkret am Beispiel des nach wie vor wichtigen Richtervorbehalts *Gusy* in Barton/Kölbel/Lindemann (Hrsg.), Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens, 193.

673 Vgl. BVerfGE 156, 11 – Antiterrordateigesetz II; 155, 119 – Bestandsdatenabruf II; 150, 309 – Kfz-Kennzeichenerfassung III; 150, 244 – Kfz-Kennzeichenerfassung II; 141, 220 – Bundeskriminalamtgesetz; 133, 277 – Antiterrordateigesetz I; 125, 260 – Vorratsdatenspeicherung; 120, 378 – Kfz-Kennzeichenerfassung I; 115, 320 – Rasterfahndung; 113, 348 – Telekommunikationsüberwachung nach dem niedersächsischen SOG; Nachweise nach *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 251.

Die Auswirkungen auf die hergebrachte polizeirechtliche Eingriffsdogmatik hat vor allem *Bäcker* konsistent systematisiert und aufgearbeitet. Die Entkoppelung polizeirechtlicher Maßnahmen vom Erfordernis einer konkreten, ereignisbezogenen Gefahr erfolgt danach über zwei unterschiedliche Modifizierungsmöglichkeiten: Einerseits kann von einem „ereignisbezogenen Wahrscheinlichkeitsurteil auf ein individualbezogenes Wahrscheinlichkeitsurteil" umgestellt werden.[674] Andererseits lassen sich polizeiliche Vorfeldbefugnisse auch an den klassisch ereignisbezogenen Prognosemodus der Gefahr anknüpfen, wenn „die Anforderungen an die Konkretisierung des Schadensereignisses abgesenkt" werden.[675]

Die Anforderungen an Vorfeldmaßnahmen, die auf ein individualbezogenes Wahrscheinlichkeitsurteil gestützt werden sollen, hat das Bundesverfassungsgericht im BKAG-Urteil von 2016 formuliert, womit dieser polizeiliche Handlungsmodus zugleich verfassungsrechtlich abgesegnet wurde. Es wird hier wiederum in zwei verschiedene Prognosetypen, die Vorfeldmaßnahmen legitimieren können, unterteilt:

Zum einen kann eine solche Prognose eine Maßnahme legitimieren, wenn

> „sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann".[676]

674 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 258.

675 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 259.

676 BVerfGE 141, 220 (272) - Bundeskriminalamtgesetz. Nach *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 267, handelt es sich dabei um eine Reformulierung des Gefahrenverdachts, sodass hierdurch - entgegen der Intention des Gerichts keine weitere Vorverlagerung des Eingriffsanlasses erfolgt. .

Daneben können nach dem Urteil

> „[i]n Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, […] Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird."[677]

Die in der zweiten Variante zum Ausdruck kommende Fokussierung auf individuelles Verhalten zur Kompensation der weitestgehenden Aufgabe des Ereignisbezuges in derartigen Fällen ist eine durchaus bemerkenswerte Entwicklung, da es hierdurch möglich wird, polizeiliche Maßnahmen auf eine rein personenbezogene Gefährlichkeitsprognose zu stützen.[678] Die Anwendung dieser Rechtsfigur auf rein terroristische Sachverhalte hat das Bundesverfassungsgericht in der Zwischenzeit in ein stärker relationales Konzept überführt, in dem die Anforderungen an die zu schützenden Rechtsgüter steigen, je eingriffsintensiver die Maßnahmen sind oder je weiter sie ins Vorfeld verlegt werden.[679]

Daneben können sich polizeiliche Vorfeldmaßnahmen auch gegen Personen richten, die zum Umkreis der Zielperson gehören. Erforderlich dafür sind bestimmte Nähekriterien (s. etwa § 19 Abs. 1 Nr. 3, 4 BKAG), die bloße Tatsache des Kontakts ist also nicht ausreichend. Diese Kriterien wurden vom Bundesverfassungsgericht ausdrücklich gebilligt, wobei das Gericht explizit auch das Problem der möglichen zirkelschlüssigen Rechtsanwendung (Bejahung des Nähekriteriums auf Grundlage allein des tatsächlichen Kontakts) hinweist,[680] ohne jedoch weiter auf die damit möglicherweise weitergehenden Probleme polizeilicher Definitionsmacht einzugehen.

Neben personenbezogenen Vorfeldtatbeständen besteht auch die Möglichkeit, Vorfeldmaßnahmen an sach- oder ortsbezogene Schadensprognosen zu knüpfen. Dabei werden Personen, die mit der jeweiligen Sache oder dem jeweiligen Ort in Verbindung treten, Ziel der Vorfeldmaßnahmen.

677 BVerfGE 141, 220 (272 f.) – Bundeskriminalamtgesetz.
678 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 268.
679 BVerfGE 155, 119 (187 f.) – Bestandsdatenauskunft II.
680 BVerfGE 141, 220 (292) – Bundeskriminalamtgesetz.

Im Kontext der Kennzeichenkontrolle hat das Bundesverfassungsgericht solche Orte dahingehend charakterisiert, dass „dort Personen Straftaten verabreden, vorbereiten oder verüben, sich Personen ohne erforderliche Aufenthaltserlaubnis treffen, sich Straftäter verbergen oder Personen der Prostitution nachgehen."[681] Da sich Etwaiges für eine Vielzahl von Orten zumindest vermuten ließe, müssen darüber hinaus konkrete polizeiliche Erkenntnisse – etwa in Form von Lageerkenntnissen – bezüglich eines konkretisierten Raumbereichs vorliegen, die eine Frequentierung des Ortes durch entsprechende Personen nahelegen.[682] Ähnlich wie bei den Nähekriterien besteht auch hier eine gewisse Gefahr zirkelförmiger Pfadabhängigkeiten entsprechender polizeilicher Maßnahmen: Orte zu denen bestimmte Lageerkenntnisse bestehen werden überwacht, wodurch weitere, neue Überwachung legitimierende Lageerkenntnisse zutage gefördert werden. Besonders problematisch kann eine solche Feedback-Schlaufe sein, wenn der in Frage stehende Ort durch eine prekäre sozio-ökonomische Struktur geprägt ist und durch den polizeilichen Überwachungsdruck zusätzliche Marginalisierung erfährt.

Als niedrigste Legitimationsschwelle für Vorfeldeingriff soll es zudem noch eine unterhalb der beschriebenen Gefahrenkonturen liegende situative Konstellation geben. *Bäcker* spricht insofern von einer allgemeinen Bedrohungslage, die dann anzunehmen sei, „wenn sich die Wahrscheinlichkeit eines Schadens aus dem allgemeinen Risikorauschen abhebt, das alle immer umgibt."[683] Diese diffuse Bedrohungslage sei notwendig, da etliche wenig eingriffsintensive Regelungen der polizeilichen Datenverarbeitung (einschließlich der Erhebung) lediglich die Erforderlichkeit für die Erfüllung polizeilicher Aufgaben als Tatbestandskriterium kennen. Gäbe es mangels allgemeiner Bedrohungslage[684] überhaupt keinen Anlass, so ließe sich die Erforderlichkeit nicht prüfen, die Polizei könnte anlasslos agieren.[685] Inwiefern aber Bedrohungslagen, in denen die „drohenden Schadensereig-

681 BVerfGE 150, 244 (290) – Kennzeichenkontrolle Bayern.
682 BVerfGE 150, 244 (290 f.) – Kennzeichenkontrolle Bayern.
683 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 286.
684 Auch geläufig sind Begriffe wie „allgemeine Gefahrenlage" (Knemeyer zitiert nach *Weßlau,* Vorfeldermittlungen, S. 138); oder "allgemeine Gefahren", s. dazu *Albers,* Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, S. 42 mwN.
685 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 288.

nisse […] sich […] räumlich, zeitlich, örtlich und hinsichtlich der Beteiligten noch nicht näher beschreiben lassen [müssen]",[686] groß Steuerungswirkung für das polizeiliche Informationshandeln entfalten sollen, erschließt sich nicht. Die gegen eine solche Bedrohungslage im Vorhof der Gefahr vorgebrachte Kritik der Entgrenzung[687] erscheint hingegen mit Blick auf den begrenzten Handlungsbereich, für den eine allgemeine Bedrohungslage als legitime Grundlage zählen darf – etwa informatorische Befragungen oder unspezifizierte Datenverarbeitungen – ebenfalls nur begrenzt stichhaltig. Problematisch dürfte hier in erster Linie das unreflektierte Heranziehen von falsch positiven Prognosen als Grundlage intensiverer polizeilicher Maßnahmen sein, für deren (der Prognosen) Auftreten es aufgrund der Diffusität in der allgemeinen Bedrohungslage besonders viel Potenzial gibt.[688] Inwieweit hiergegen durch materielle verfassungsrechtliche Vorgaben Schutz geboten werden könnte, ist jedoch fraglich.

Bemerkenswert im Kontext des Vorfelds ist schließlich die Rechtsprechung des Bundesverfassungsgerichts zu automatisierten Kennzeichenkontrollen in Bayern: Mit dem diesbezüglichen Urteil ebnet das Gericht anlasslosen Kontrollen den Weg. Demnach sind anlasslose Kontrollen nicht generell ausgeschlossen. Insbesondere kann bereits das Anknüpfen „an ein gefährliches oder risikobehaftetes Tun bzw. an die Beherrschung besonderer Gefahrenquellen" einen hinreichenden Grund für derartige Kontrollen bieten, wie es etwa im Straßenverkehr anlasslos und stichprobenhaft der Fall ist.[689] Verfahrensgegenstand war unter anderem die anlasslose Kennzeichenkontrolle als Mittel der Schleierfahndung bei Vorliegen entsprechender Lageerkenntnisse zur Verhütung oder Unterbindung des unerlaubten Aufenthalts und zur Bekämpfung der grenzüberschreitenden Kriminalität. Das Bundesverfassungsgericht hält dies in einem Grenzgebiet von bis zu 30 km Tiefe sowie an öffentlichen Einrichtungen des internationalen Verkehrs für zulässig. Lediglich Kontrollen allgemein auf Durchgangsstraßen sind ausgeschlossen, weil dazu in der zu prüfenden Norm auch „andere Straßen von erheblicher Bedeutung für den grenzüberschrei-

686 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 286.

687 Siehe etwa *Weßlau,* Vorfeldermittlungen, S. 131 ff; *Albers,* Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, S. 44 f.

688 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 289.

689 BVerfGE 150, 244 (281) – Kennzeichenkontrolle Bayern.

tenden Verkehr" genannt waren, was eine hinreichende Konkretisierung verunmöglicht.[690] Begründet wird diese „Befugnis zu praktisch anlasslosen, nur final angeleiteten Maßnahmen", die grundsätzlich nicht mit der Verfassung vereinbar ist, mit der besonderen Rechtfertigung des Ausgleichs für den Wegfall der innereuropäischen Grenzkontrollen.[691] Dahinter steht die Idee der Kompensierung von Kontrolldefiziten durch Kontrollüberschüsse, die im Zuge der Digitalisierung in neuer Qualität produziert werden können,[692] wie man sie auch in anderen Bereichen staatlicher Risikokontrolle kennt.[693] Anders aber als beispielsweise in der Risikokontrolle durch das Atomrecht, wo ein technischer Kontrollüberschuss nicht groß genug sein kann und darüber hinaus stets ein klar umgrenzter Bezugspunkt besteht, unterliegt die Polizei mit ihrer Fokussierung auf prinzipiell jedes Verhalten, das zumindest von rechtlichen Normen abweicht, weniger sachinhärenten Begrenzungen.[694] Das erkennt auch das Bundesverfassungsgericht an, wenn es den Ausnahmecharakter anlassloser, lediglich zweckgerichteter Kontrollen hervorhebt und die Begrenzungen und Sicherungen der Maßnahme betont und auch verstärkt.[695] Nichtsdestotrotz bleibt mit Blick auf die Bedeutung staatlicher Risikopolitik für die moderne Gesellschaft[696] abzuwarten, inwieweit sich dieses Muster der Kompensation von Kontrolldefiziten als anschlussfähig erweist.

3. Die Ausweitung des Vorfelds

Das polizeiliche Vorfeld erfährt quantitativ und qualitativ zunehmende Ausweitung. Zahlenmäßig wachsen die Vorfeldermächtigungen an, die sich zwar häufig noch auf Terrorismusabwehr beschränken, teilweise aber auch (nur noch) die Verhinderung schwerer Schäden zum Zweck haben.[697] Aber auch die Qualität polizeilicher Vorfeldbefugnisse ändert sich – im Sinne einer Intensitätssteigerung – überall dort, wo imperative Eingriffe im

690 BVerfGE 150, 244 (299) – Kennzeichenkontrolle Bayern.
691 BVerfGE 150, 244 (296) – Kennzeichenkontrolle Bayern.
692 *Nassehi,* Muster, S. 43.
693 *Stoll,* Sicherheit als Aufgabe von Staat und Gesellschaft, S. 448.
694 *Albers,* Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, S. 43 f.
695 BVerfGE 150, 244 (298 ff.) = NJW 2019, 827 (839 f.) – Kennzeichenkontrolle Bayern.
696 *Reckwitz* in Volkmer/K. Werner (Hrsg.), Die Corona-Gesellschaft, 241.
697 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 274.

Vorfeld der traditionellen Gefahrenschwelle ermöglicht werden.[698] Damit einher geht eine problematische Verfestigung informationeller Repräsentationen von Personen: Denn während sich bei reinen Überwachungsmaßnahmen durch die stete Fortentwicklung der überwachten Situationen und in ihnen agierenden Personen eine mitlaufende Korrekturmöglichkeit für die Abbilder der Realität gibt, wie sich aus den polizeilichen Daten konstruiert werden, wird diese Möglichkeit durch einen imperativen Eingriff eher abgeschnitten. Wird jemand im Vorfeld mit entsprechenden Maßnahmen vom alltäglichen Sozialleben abgeschnitten – etwa durch Aufenthaltsvorgaben oder Kontaktverbote wie in § 55 BKAG geregelt oder gar durch Präventivgewahrsam wie durch Art. 17 PAG ermöglicht – wird es der betroffenen Person schwerfallen, in dieser Ausnahmesituation durch ihr an den Tag gelegtes Verhalten die Anhaltspunkte für die von ihr ausgehende Gefahr wieder zu entkräften. Gelingt ihr dies nicht, können aufgrund angenommener weiterer Gefährlichkeit weiter Maßnahmen verhängt werden.[699] Diese Entwicklung ist umso bemerkenswerter, als dass es sich bei einer drohenden Gefahr, die auf Grundlage polizeilicher Erkenntnisse angenommen wird, um eine besonders fragile und mit Unschärfen besetzte informationelle Repräsentation der Wirklichkeit handelt.

Trotz gesetzgeberischer Zurückhaltung bei der strafverfahrensrechtlichen Ausgestaltung des Vorfelds ist auch das Strafrecht indessen nicht unbeteiligt an der Ausweitung des polizeilichen Vorfelds. Hier tragen materielle Vorfeldtatbestände wie § 89a ff., 129a f. StGB und andere maßgeblich zur Ausweitung des polizeilichen Maßnahmenspektrums bei, indem Verhalten kriminalisiert wird, das weit im Voraus der eigentlich Rechtsgutverletzung anzusiedeln ist. Zudem fußt die Strafbarkeit maßgeblich auf der Aufdeckung von netzwerkartigen Verbindungen zwischen Akteur:innen (und Objekten) sowie großen Teilen der persönlichen Lebensführung. Durch die Kombination der Tatbestände mit polizeilichen Ermittlungsbefugnissen können als kriminell verdächtigte Strukturen insbesondere terroristischer oder organisierter Natur weitläufig und früh überwacht werden.[700]

Insgesamt bedeutet diese Vorfeldausweitung eine immer stärkere Erweiterung des polizeilichen Blicks. Denn heruntergebrochen gelangen durch

698 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 276.

699 So *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 27.

700 Siehe näher dazu *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 325 ff.

mehr und breitere Vorfeldbefugnisse – seien sie nun explizit wie im Polizeirecht oder eher indirekt wie im zunehmend präventiv orientierten materiellen Strafrecht – zunächst schlicht mehr Daten über potenziell mehr Personen, Sachen und Umgebungen in die Datenspeicher der Polizei. Diese klaren Ausweitungstendenzen werden auch in der Rechtsprechung des Bundesverfassungsgerichts gespiegelt, wobei dessen Rolle mit Blick auf die Handlungsspielräume der Polizei unterschiedlich interpretiert wird, wie nun im Folgenden beschrieben wird.

III. Sicherheitsverfassungsrecht: Polizeiliches Informationswesen zwischen Hypertrophie und gesetzgeberischer Steuerungsverweigerung

Bereits die hier nur ausschnittsweise dargestellten verfassungsrechtlichen Vorgaben zur polizeilichen Datenverarbeitung deuten auf den Komplexitätsgrad der Karlsruher Rechtsprechung hin. In der Auseinandersetzung mit den vielfältigen Urteilen zu sicherheitsbehördlichen Datenverarbeitungen hat sich nicht nur das Sicherheitsrecht als Disziplin gebildet. Aus dem Wechselwirkungsverhältnis zwischen Sicherheitspolitik und Verfassungsdogmatik ist auch das Konzept des Sicherheitsverfassungsrechts entstanden, das von einem besonderen Wandlungsprozess der Verfassung im Spezialbereich sicherheitsbehördlicher Tätigkeiten ausgeht.[701] Durch immer neue verfassungsrechtliche Vorgaben, deren sicherheitspolitische Verarbeitung in Form von neuen Gesetzen wiederum neue Anknüpfungspunkte für weitere Ausgestaltungen der Sicherheitsverfassung bietet, ist der Detail- und Komplexitätsgrad aber inzwischen so stark angewachsen, dass vermehrt Kritik insbesondere am Bundesverfassungsgericht als zentraler Treiber dieser Entwicklung geäußert wird. Prägnant in diese Richtung äußert sich etwa *Löffelmann*, der die Gefahr einer Hypertrophie des Rechts sieht:

> Obwohl jedes Wort aus Karlsruhe vom Gesetzgeber auf die Goldwaage gelegt wird, um das Verdikt der Verfassungswidrigkeit zu vermeiden, gelingt es im Bereich des Sicherheitsrechts immer schwerer, Gesetze zu schaffen, die den Ansprüchen des Verfassungsrechts genügen. Die hohe Intellektualität der Karlsruher Vorgaben grenzt zuweilen an Überforde-

701 Siehe dazu beispielsweise *Steffen Tanneberger,* Die Sicherheitsverfassung; *Würtenberger/Steffen B. Tanneberger* in S. Fischer/Masala (Hrsg.), Innere Sicherheit nach 9/11, 35; *Poscher* in Korioth/Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 245.

> rung. Das liegt nicht nur an der Komplexität der Materie, sondern auch an der Einführung immer neuer begrifflicher Differenzierungen, die Genauigkeit suggerieren, tatsächlich aber am Fehlen eines übergreifenden und schlüssigen Bezugssystems und einer induktiven, aus den Bedürfnissen der Praxis gewonnenen Herleitung leiden.[702]

Um dieser Gefahr zu begegnen, müsse man zu einer Einfachheit in der Rechtssetzung zurück, die aber nicht mit Simplifizierung zu verwechseln sein. Vielmehr brauche es statt stark technischer Normen normative Strukturen, die einen klaren handlungsleitenden Rahmen und grundsätzliche gesetzgeberische Wertungen erkennen lassen und damit für die Rechtsanwendung eine echte Orientierung und Hilfe darstellen.[703] Wie das gelingen können soll, führt *Löffelmann* an anderer Stelle in Bezug auf den Grundsatz der hypothetischen Datenneuerhebung aus. Dabei sollen vor allem Normen klarer für die Anwender:innen werden, was über die Gewichtung von Aufgabenbeschreibungen oder die Intensität von Eingriffen im Wege der ordinalen Schematisierung der Schutzwürdigkeit von Daten bewerkstelligt werden soll.[704]

Dieser Perspektive eher entgegengesetzt sind solche Stimmen, die in den gesetzgeberischen Aktivitäten im Sicherheitsrecht der letzten Jahre und Jahrzehnte eine Steuerungsverweigerung oder einen Steuerungsausfall sehen.[705] Die Folge ist eine Gesetzgebung, die eher darauf bedacht scheint, den Sicherheitsbehörden den Erhalt ihrer eingeübten Praktiken[706] und, mit Blick auf Wandlungen, eine exekutivische Selbstprogrammierung zu ermöglichen.[707]

Beide Positionen haben zwar inhaltliche Schnittmengen, widersprechen sich in ihrer Deutungsrichtung fundamental. Gemein ist ihnen aber eine Absage an den status quo gesetzgeberischer Handhabung des sicherheitsbehördlichen bzw. polizeilichen Informationsrechts. Ohne an dieser Stelle für

---

702 *Löffelmann* Zeitschrift für das Gesamte Sicherheitsrecht 3 (2020), 182 (186).
703 *Löffelmann* Zeitschrift für das Gesamte Sicherheitsrecht 3 (2020), 182.
704 *Löffelmann* Zeitschrift für das Gesamte Sicherheitsrecht 2 (2019), 16 (21 f.).
705 In diese Richtung beispielsweise *Aden/Fährmann* Zeitschrift für Rechtspolitik 2019, 175 (175). *Aden/Fährmann* vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik 227 (2019), 95 (98 ff.).
706 So bereits *Riegel* Neue Juristische Wochenschrift 50 (1997), 3408 (3411).
707 Allgemein zur Selbstprogrammierung *Schuppert,* Governance und Rechtsetzung, 182 f., kritisch dazu *Habermas,* Faktizität und Geltung, S. 60, 212 f., 230 f. et passim; im Kontext der Polizei siehe etwa *Goeschel/Heyer/G. Schmidbauer,* Beiträge zu einer Soziologie der Polizei, 74 ff.

eine Seite Partei zu ergreifen ist dieser kleinste gemeinsame Nenner der Perspektiven zu befürworten. Das (Verfassungs-)Recht des polizeilichen Informationswesens wird mit einem „weiter so" in zunehmende Schwierigkeiten geraten und an normativem Steuerungs- und Strukturierungspotenzial einbüßen.[708]

B. Unionsrechtliche Vorgaben für polizeiliche Datenverarbeitung

Auch auf europäischer Ebene gibt es zunächst einen dem Grundgesetz vergleichbaren Grundrechtsschutz durch die Europäische Grundrechtecharta und die EMRK. So schützen Art. 7 GRCh und Art. 8 EMRK das Privatleben, wobei der EMRK wegen Art. 52 Abs. 3 GRCh vorrangige Bedeutung bei der Auslegung zukommt. Zudem statuiert Art. 8 GRCh das Recht auf Schutz personenbezogener Daten. Auch dieser grundrechtliche Schutz kann indessen unter Beachtung der Rechtfertigungserfordernisse eingeschränkt werden. Insgesamt spielt insoweit die verfassungsrechtliche Struktur, wie sie zuvor dargestellt wurde, für den nationalen Kontext die größere Rolle.[709]

Jedoch hat die Bedeutung des Unionsrechts für die polizeiliche Datenverarbeitung in jüngerer Zeit in erheblichem Maße zugenommen. Grund dafür ist die am 05.05.2016 in Kraft getretene und bis zum 06.05.2018 umzusetzende „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"[710]. Diese gestaltet das Datenschutzrecht – gemeinsam mit der DS-GVO – im europäischen Raum an viele Stellen um. Für unionsrechtliche Vorgaben im Bereich polizeilicher Datenverarbeitung ist dieser sekundärrechtliche Rechtsakt zentral, weswegen im Folgenden die JI-Richtlinie und nicht die sehr viel mehr im

708 Siehe dazu auch unten S. 358 ff.

709 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 381 ff., zur Frage nach dem Verhältnis von unionalen und nationalen Grundrechten, siehe a.a.O. Rn. 385 ff.

710 EU ABl. 119 vom 04.05.2016; im Folgenden „JI-Richtlinie" (J=Justiz, I=Inneres, vgl. *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, BDSG, § 45 Rn. 4).

wissenschaftlichen und öffentlichen Fokus stehende Datenschutzgrundverordnung im Zentrum der Ausführungen steht.

Nach Art. 1 Abs. 1 JI-Richtlinie zielt der Rechtsakt auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten ab. Gegenüber dem vorherigen Rahmenbeschluss ist insoweit zunächst die Regulierung auch rein innerstaatlicher Datenverarbeitung neu,[711] sodass Unionsgrundrechte nunmehr auch in diesem Bereich Anwendung finden können, sofern es sich um nationale Regelungen handelt, die auf der Richtlinie basieren, also wenn Recht der Union durchgeführt wird.[712] Die extensive Auslegung des Merkmals der „Durchführung von Unionsrecht" durch den Europäischen Gerichtshof[713] gepaart mit der inhaltlichen Weite der zugrundeliegenden Kompetenzgrundlage des Art. 16 Abs. 2 AEUV führen dabei im Ergebnis zu einer Ausweitung der unionsrechtlichen Regelungsmöglichkeiten und -inhalte: Mit dem datenschutzrechtlichen Zugriff auf das mitgliedstaatliche Polizei- und Strafverfahrensrecht als (eine) tragende Säule staatlicher Souveränität schreitet die „Europäisierung des Sicherheitsverfassungsrechts"[714] voran, was trotz gegebenenfalls bestehender praktischer Erfordernisse nicht ohne Kritik geblieben ist.[715]

I. Grundlegende Strukturen der JI-Richtlinie

Die JI-Richtlinie regelt den Bereich der personenbezogenen Datenverarbeitung „zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentlichen Sicherheit" (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-Richtlinie; vgl. auch § 45 Satz 1 BDSG) und hat mit diesem Programm ein entsprechend breites Umsetzungserfordernis

711 Siehe Erwägungsgründe 6, 7 und 26 der JI-Richtlinie.
712 *Weinhold/Johannes* Deutsches Verwaltungsblatt 131 (2016), 1501, 1503.
713 *Weinhold/Johannes* Deutsches Verwaltungsblatt 131 (2016), 1501, 1504.
714 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 337
715 Vgl. etwa *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 341 ff., der Art. 16 Abs. 2 AEUV für keine ausreichende Regelungskompetenz hält; siehe auch *H. Wolff* in Kugelmann/Rackow (Hrsg.), Prävention und Repression im Raum der Freiheit, der Sicherheit und des Rechts, 61 ff.; ebenfalls kritisch, aber Art. 16 Abs. 2 AEUV als passende Regelungskompetenz anerkennend *Bäcker*, Stellungnahme JI-Richtlinie, A-Drs. 17(4)585 B, 3 ff.

in der deutschen Gesetzteslandschaft zur Folge gehabt.[716] Nicht nur im Bundesdatenschutzgesetz, sondern auch in jeweils bereichsspezifisch betroffenen Normkomplexen des Bundes und der Länder gab es Umsetzungsbedarf.[717] Die dazu notwendigen Erläuterungen erfolgen an den jeweils relevanten Stellen der Darstellung der einfachgesetzlichen Rahmenbedingungen. Nachfolgend sollen lediglich noch einige grundlegende Aspekte zum Anwendungsbereich der JI-Richtlinie dargestellt werden.

Wesentlich für die Anwendbarkeit der JI-Richtlinie ist zunächst der Begriff der personenbezogenen Daten, der in Art. 3 Nr. 1 definiert ist als alle Informationen über eine identifizierte oder identifizierbare natürliche Person. Es sind grundsätzlich alle Arten von Informationen erfasst, wenn sie aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit einer bestimmten Person verknüpft sind. Lediglich reine Sachdaten sind nicht erfasst. Auch persönliche Einschätzungen über eine Person wie sie im polizeilichen Kontext häufig zustande kommen, sind personenbezogene Daten (vgl. auch Art. 7 JI-Richtlinie).[718] Die Identifizierbarkeit bemisst sich gemäß Erwägungsgrund 21 im wesentlich danach, ob der für die Verarbeitung Verantwortliche ein Identifizierungsmittel vernünftigerweise einsetzt oder ob dies etwa aus Kosten-, Zeit- oder Technikgründen nicht geschieht. Zudem wird gemäß Art. 3 Nr. 2 JI-Richtlinie die gesamte Bandbreite möglicher Datenumgangsformen erfasst.

Die nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-Richtlinie „zuständigen Behörden" sind aufgabenbezogen zu bestimmen, d.h. erfasst werden alle Behörden, die die in Art. 1 Abs. 1 JI-Richtlinie erfassten Zwecke zu erfüllen haben. So fallen beispielsweise auch Strafgerichte darunter. In jedem Fall erfasst werden aber die hier untersuchten Polizeibehörden.[719] Mit der zunehmend flächendeckende Verbreitung elektronischer Vorgangsbearbeitungssysteme bei den Polizeibehörden dürften in Zukunft fast alle dortigen Datenverarbeitungen in den Anwendungsbereich der Richtlinie fallen,[720] denn gemäß Art. 2 Abs. 2 JI-Richtlinie genügt auch eine nicht-automatisierte Verarbeitung, wenn sie personenbezogene Daten betrifft, die in einem Dateisystem

716 So auch *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 380.
717 *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, BDSG, § 45 Rn. 4.
718 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 426, 429 ff.
719 *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 367.
720 *Bäcker/Hornung* ZD 2012, 147, 148 f.

gespeichert werden (sollen). Die Menge nicht vom Anwendungsbereich der Richtlinie erfasster personenbezogener Daten dürften marginal sein.[721]

In sachlicher Hinsicht erstreckt sich der Anwendungsbereich der Richtlinie zunächst auf die Aufdeckung, Untersuchung oder Verfolgung von Straftaten, wobei der Begriff der Straftat unionsrechtlich auszulegen ist. Darunter fällt in Deutschland jedenfalls der Bereich der in der StPO geregelten Strafverfolgung.[722] Darüber hinaus sind jedoch auch Ordnungswidrigkeiten erfasst.[723] Bis dato noch nicht vollständig geklärt ist indessen, in welchem Ausmaße auch präventivpolizeiliche Datenverarbeitung – die „Verhütung von Straftaten – von der JI-Richtlinie erfasst wird. Während nach deutschem Verständnis die Verhütung von Straftaten (und Ordnungswidrigkeiten[724]) Teil des allgemeinen Polizei- und Ordnungsrechts ist, ist dies nach unionalem Verständnis nicht unbedingt der Fall, was zu gespaltenen unionsrechtlichen Rahmenbedingungen im Bereich der Gefahrenabwehr führt.[725] Es muss jedoch noch weiter differenziert werden: Während für straftatenbezogene präventivpolizeiliche Tätigkeit die JI-Richtlinie zweifelsohne gilt, ist fraglich, ob es im Bereich der Gefahrenabwehr auch einen Anwendungsbereich der Richtlinie gibt, ohne dass ein direkter Straftatenbezug besteht. Diese Überlegung lässt sich an Art. 1 Abs. 1 aE JI-Richtlinie („Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit“) festmachen, wodurch die Möglichkeit eines Straftaten-unabhängigen Anwendungsbereiches der JI-Richtlinie suggeriert wird. Auch Erwägungsgrund 12 scheint davon auszugehen, wenn dort von „polizeilichen Tätigkeiten, in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht“ die Rede ist. Weiter heißt es an dieser Stelle: „Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen.“ Angesichts dieses Textbefundes scheint es sinnvoll, nur dann der JI-Richtlinie im Bereich polizeilicher Tätigkeit den Anwendungsbereich zu versagen da-

721 Nach Erwägungsgrund 18 der JI-Richtlinie soll der Anwendungsbereich nur dann nicht eröffnet sein, wenn sich um personenbezogene Daten in „Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind,“ handelt.

722 *Wolff* in *Schantz/H. Wolff,* Das neue Datenschutzrecht, Rn. 242.

723 *Wolff* in *Schantz/H. Wolff,* Das neue Datenschutzrecht, Rn. 248 ff.

724 Siehe näher dazu *Wolff* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, BDSG, § 45 Rn. 40.

725 *Wolff* in *Schantz/H. Wolff,* Das neue Datenschutzrecht, Rn. 243.

mit und der DS-GVO, bei unionsrechtlichem Bezug, die Anwendung zu eröffnen, wenn von vornherein aus ex-ante-Sicht (aus verständiger Beamt:innensicht) überhaupt keinen Straftaten- oder Ordnungswidrigkeitenbezug gibt.[726] Für den von der vorliegenden Untersuchung erfassten Tätigkeitsbereich der Polizeien des Bundes und der Länder gilt die JI-Richtlinie damit umfassend.

II. Wesentliche Inhalte der JI-Richtlinie

Die JI-Richtlinie macht weitreichende und umfassende Vorgaben für den polizeilichen Umgang mit personenbezogenen Daten. Während Grundsätze wie der des Gesetzesvorbehalts (Art. 8 Abs. 1 JI-Richtlinie) oder der Zweckbindung (Art. 4 Abs. 1 lit. c JI-Richtlinie) bereits aus dem nationalen Recht bekannt sind, hat der unionale Rechtsakt auch originäre Neuerungen für das Recht des polizeilichen Informationswesens mit sich gebracht.

So ist aufgrund der Ambivalenz der JI-Richtlinie bezüglich der Einwilligung als möglicher Rechtsgrundlage für polizeiliche Datenverarbeitungen die Frage aufgekommen, inwieweit diese noch als Anknüpfungspunkt für polizeiliche Maßnahmen wie etwa 81e, 81g und 81h StPO herangezogen werden kann. Die Frage besitzt also eine nicht unerhebliche Praxisrelevanz für die deutschen Polizeien. Problematisch ist in erster Linie die Frage nach der Freiwilligkeit einer Einwilligung im Angesicht des durch die Polizei verkörperten staatlichen Gewaltmonopols. Die Diskussion ist in vielen speziellen Fragen zu diesem Problem noch im Fluss.[727] Allerdings erscheint insgesamt zweifelhaft, wie weit die legitimierende Wirkung einer Einwilligung mit Blick auf die Komplexitäten des polizeilichen Informationswesens reichen kann. Die Verwendung von Daten, die auf dieser Grundlage verarbeitet werden, muss von vornherein durch entsprechende Vorkehrungen auf das vorgegebene Maß begrenzt werden. Auch wird der überwiegende Teil der polizeilichen Datensammlungen nicht aus solcherart mehr oder weniger „freiwillig" preisgegebenen Daten bestehen.

726 So *Schwabenbauer* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 375 ff.; denkbare Fälle sind Selbstgefährdung, der Schutz privater Rechte und sonstiges datenschutzrechtliches Verhalten der Polizei wie das Führen von Personalakten, vgl. a.a.O. G. Rn. 377.

727 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 472 ff.

Neu, zumindest in dieser Ausdrücklichkeit, ist auch der Verarbeitungsgrundsatz der Richtigkeit und Aktualität in Art. 4 Abs. 1 lit. d JI-Richtlinie. Da es sich bei der sachlichen Richtigkeit um ein objektives Kriterium handelt, fallen polizeiliche Einschätzungen als Werturteile nicht darunter. Entsprechende Bewertungen sind damit einer Kontrolle insoweit entzogen.[728] Ferner sind die Daten auch auf dem neusten Stand zu halten, was Nacherhebungen notwendig machen kann, damit neue Maßnahmen nicht auf veraltete und möglicherweise nicht mehr zutreffende Erkenntnisse gestützt werden.[729] Die Norm, über deren Umsetzung bisher nichts bekannt ist, stellt die Polizei einerseits vor die durchaus herausfordernde Aufgabe, den Datenbestand im Grunde laufend auf Richtigkeit und Aktualität zu überprüfen, was praktisch wohl eher anlassbezogen geschehen wird. Gleichzeitig ist dem Grundsatz aber auch eine nicht unproblematische, expansive Dynamik inhärent. Denn die Prüfung von Richtigkeit und Aktualität legt eher nahe, mehr oder häufiger Daten zu beschaffen, wenn die vorhandenen Daten möglicherweise veraltet oder falsch sein könnten.

Weniger auf den Schutz der kontextuellen als vielmehr auf den der physischen Unversehrtheit bedacht ist der Grundsatz der Integrität und Vertraulichkeit in Art. 4 Abs. 1 lit. f JI-Richtlinie. Dazu müssen Daten „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen." Erwägungsgrund 28 spezifiziert insofern, dass Unbefugte weder Zugang zu Daten haben, noch Verarbeitungsgeräte nutzen können sollen sowie dass die technischen Verarbeitungsprozesse risikoadäquat geschützt werden müssen. Nähere Ausgestaltung erfährt der Grundsatz zudem in Art. 29 JI-Richtlinie. Auch dieser Aspekt des Datenumgangs wird immer wichtiger und in seiner Umsetzung schwieriger. Denn Schutz muss etwa nicht nur vor böswilligen Akteur:innen geboten werden, die im Wege von Cyberattacken auf Polizeien neben dem analogen nun auch einen virtuellen Zugang erlangen können. Vielmehr muss auch der Zugang von mit den Polizeien kooperierenden Privaten reglementiert werden. Zuletzt besteht auch innerhalb der Behörde,

728 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 494.

729 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 495.

wie man immer wieder aus Medienberichten erfährt,[730] ein Problem mit unberechtigten Zugängen zu polizeifremden Zwecken.

Rechtliche Abbildung in Form der sogenannten Auftragsverarbeitung findet nun auch die in den komplexen Strukturen des polizeilichen Informationswesens nicht ausbleibende Delegation von Datenverarbeitungsvorgängen an – rechtlich gesehen – andere Stellen als den Verantwortlichen. Die Daten können nur nach Weisung des Verantwortlichen verarbeitet werden und demnach auch nur nach dessen Zweckbindungen, Art. 22, 23 JI-Richtlinie. Durch die Beauftragung darf das Schutzniveau der JI-Richtlinie nicht unterlaufen werden, sodass Vorgaben bezüglich technischer und organisatorischer Maßnahmen zum Schutz der Prozesse ebenso gelten. Problematisch wird im polizeilichen Informationswesen die Verarbeitung von Daten der Länderpolizeien durch das Bundeskriminalamt im Auftrag ersterer gesehen, wenn hiervon Informationen betroffen sind, die mangels überregionaler Relevanz eigentlich nur auf Landesebene verarbeitet werden dürften. Hier drohe, „dass die von den jeweiligen Gesetzgebern getroffenen Aufgabenverteilungen zwischen Bundes- und Länderpolizeien unter dem „Etikett der Auftragsverarbeitung" unterlaufen werden", sodass § 2 Abs. 1 BKAG, der Unterstützung bei der Datenverarbeitung durch das Bundeskriminalamt ermöglicht, nunmehr als Ausnahmeregelung zu verstehen sein soll.[731]

Mit Blick auf die Relevanz von Kontext und informationellem Gehalt von Daten versucht die JI-Richtlinie zudem über die Kategorisierung von Daten Steuerungsimpulse für deren angemessene Verarbeitung zu setzen. Die Kategorisierung erfolgt nach betroffenen Personen, Datengrundlage und informationellem Gehalt. Art 6 JI-Richtlinie verpflichtet die Mitgliedstaaten zunächst dazu, soweit wie möglich zwischen den verschiedenen Kategorien betroffener Personen klar zu unterscheiden. Unterschieden werden soll zwischen a) Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben oder in naher Zukunft begehen werden, b) verurteilten Straftäter:innen, c) Opfern einer Straftat oder Personen,

730 Siehe etwa *Dachwitz* Netzpolitik.org; *Völlinger* Zeit Online v. 1. November 2019; *A. Becker* Nordkurier v. 31.05.2022 Damit soll nur ein kursorischer Überblick über entsprechende Medienberichte gegeben werden. Meistens sind Anfragen oder Tätigkeitsberichte der aufsichtsbehördlichen Datenschutzbeauftragten Anlass, mitunter aber auch Skandale wie die als „NSU 2.0" bezeichnete Affäre. Insgesamt deutet sich ein systemisch-strukturelles Defizit an.

731 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 507.

bei denen bestimmte Fakten darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und d) anderen Parteien im Zusammenhang mit einer Straftat, wie Personen, die bei Ermittlungen in Verbindung mit der betreffenden Straftat oder beim anschließenden Strafverfahren als Zeug:innen in Betracht kommen, Personen, die Hinweise zur Straftat geben können, oder Personen, die mit den unter den Buchstaben a) und b) genannten Personen in Kontakt oder in Verbindung stehen. Diese Kategorien decken sich nicht vollständig mit denen des deutschen Polizeirechts, das vor allem die Begriffe Beschuldigte:r, Verdächtige:r und sonstige Kontakt- oder Anlasspersonen anknüpft. Weil die Richtlinie insoweit aber nicht abschließend ist, kann die deutsche Kategorisierung beibehalten oder nach hiesigen gesetzgeberischen Vorstellungen abgeändert werden, sofern damit weiter im Wesentlichen der Richtlinie entsprochen wird.[732] Daneben differenziert die JI-Richtlinie zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten, Art. 7 Abs. 1 JI-Richtlinie. Diese Kategorisierung soll insbesondere vor Übermittlungen Überprüfungen der Datenqualität initiieren und gegebenenfalls dazu anhalten, kontextuelle Daten für die empfangende Stelle mit zu übermitteln, soweit dies durchführbar ist. Dadurch wird die Kategorisierung bzw. die an sie anknüpfende Pflicht stark relativiert, wenngleich sie anders sicherlich kaum in die Praxis der Polizeibehörden eingefügt werden könnte. Die letzte Kategorisierung erfolgt entlang des (besonders sensiblen) informationellen Gehalts von Daten. Das sind gem. Art. 10 JI-Richtlinie solche Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung. Die Verarbeitung ist nur dann erlaubt, wenn sie unbedingt erforderlich ist, vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt. Zudem muss a) die Verarbeitung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig sein b) der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dienen oder c) sich auf Daten beziehen, die die betroffene Person offensichtlich öffentlich gemacht hat. Zu geeigneten Garantien gehört gemäß Erwägungsgrund 37 „beispielsweise

732 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 500 ff.

[…], dass diese Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person erhoben werden dürfen, die erhobenen Daten hinreichend gesichert werden müssen, der Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger geregelt und die Übermittlung dieser Daten verboten wird." Die Umsetzung in § 48 BDSG enthält neben technisch-organisatorischen Maßnahmen zudem auch die Sensibilisierung der an der Verarbeitung Beteiligten. Insbesondere aber das Regulativ der unbedingten Erforderlichkeit für die Aufgabenerfüllung darf als weitestgehend ungeklärt gelten, sodass auch bezüglich dieser – in der Sache begrüßenswerten – Kategorisierung fraglich ist, inwieweit sie nachhaltigen Einfluss auf die polizeiliche Datenverarbeitungspraxis haben wird, vor allem weil die Kategorisierung selbst ohne Rechtsfolge ist.[733] Darüber hinaus ist auch bezüglich des besonders sensiblen informationellen Gehalts bestimmter Daten problematisch, dass sich dieser nicht nur ex- sondern, wie bereits dargelegt, auch implizit aus der Zusammenschau eher „belanglos" scheinender Daten ergeben kann.[734] Da einige der besonderen Dateninhalte, wie etwa sexuelle Orientierung, auch den Kernbereichsschutz tangieren, darf hier für den deutschen Rechtsraum als offen gelten, wie mit solchen in den Daten enthaltenen virtuellen Informationen[735] zu verfahren ist. Es bleibt vor dem Hintergrund des Art. 10 JI-Richtlinie insgesamt abzuwarten, wie sich der Umstand auswirken wird, dass sich die in der Norm genannten Informationen – wenn auch nur unbeabsichtigt – aus Datensätzen mit entsprechenden Analysemethoden zunehmend herauslesen lassen können.

Im Rahmen der immer stärkeren Nutzung von Massendatenverarbeitungsverfahren rückt ein gegenwärtig überall aufscheinendes Problem auch im polizeilichen Handlungsfeld in den Fokus: Entscheiden noch Menschen auf der Grundlage der zur Verfügung stehenden Daten oder wird bereits von maschinellen „Intelligenzen", von Algorithmen, in Sachverhalten entschieden, die andere Menschen betreffen? Die JI-Richtlinie greift dies in Art. 11 JI-Richtlinie auf und postuliert ein Verbot für eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die eine nachteilige Rechtsfolge für die betroffenen Personen hat oder sie erheblich beeinträchtigt, es sei denn – das Verbot ist mithin nicht absolut – die

733 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Vor §§ 45 ff. Rn. 2.

734 Siehe dazu bereits oben S. 147 ff. Siehe dort insb. auch Fn. 583, in der es um die Ableitung von sexueller Orientierung aus banal scheinenden sozialen Netzwerkdaten ging.

735 Zum Phänomen der virtuellen Informationen siehe bereits oben S. 74 f.

Entscheidung ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erlaubt, das zudem geeignete Garantien für die Rechte und Freiheiten der betroffenen Person, mindestens ein Recht auf menschliches Eingreifen seitens des Verantwortlichen, bieten muss. Fließen in eine solche Entscheidung besondere Kategorien personenbezogener Daten nach Art. 10 JI-Richtlinie ein, sind die Anforderungen noch einmal erhöht – erforderlich sind dann, dass geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigen Interessen der betroffenen Person getroffen werden. Bisher ist kein technisches System bei den deutschen Polizeien bekannt, dass aufgrund einer einzelfallbezogenen Entscheidung durch es selbst unter die skizzierten Vorgaben fallen würde. Zwar dürften Datenanalyseinstrumente wie die in 25a HSOG geregelte hessenDATA-Plattform menschliche Entscheidungen in einem nicht unerheblichen Maße vorstrukturieren und damit beeinflussen. Diese vorgelagerte Form des Einflusses auf die letztlich immer noch menschliche Entscheidung der handelnden Polizeibeamt:innen ist indessen nicht von Art. 11 JI-Richtlinie erfasst. Ob sich in Zukunft ein Anwendungsbereich hierfür auftun wird oder ob die technische Entwicklung weiter darauf achten wird, den „human in the loop" zu halten, ist offen.

Einen wesentlichen Schritt in Richtung einer vom Individuum abgelösten Datenschutzkontrolle geht die Rechenschaftspflicht aus Art. 4 Abs. 4 JI-Richtlinie. Der Verantwortliche (Art. 3 Nr. 8 JI-Richtlinie) muss demnach die Einhaltung der Datenschutzgrundsätze des Art. 4 Abs. 1-3 JI-Richtlinie nachweisen. Ergänzt wird die Vorschrift durch Art. 19 JI-Richtlinie. Danach hat der Verantwortliche „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen [umzusetzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt." Diese Maßnahmen sind zudem laufend zu überprüfen und erforderlichenfalls nachzubessern. Die explizite einfachgesetzliche Umsetzung hat der Bundesgesetzgeber scheinbar unterlassen.[736] Nichtsdestotrotz ist die aus der JI-Richtlinie fließende Pflicht der Polizei, Rechenschaft über ihre Datenverarbeitungsprozesse abzulegen ein integraler Be-

736 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 499.

standteil einer massendatenverarbeitenden Polizei, deren Kontrolle längst nicht mehr über individuellen Rechtsschutz organisiert werden kann.

Damit ist auch die wesentliche Innovation der JI-Richtlinie im Vergleich zur nationalen Rechtssituation angesprochen. Datenschutz oder genauer: die Kontrolle des polizeilichen Datenumgangs durchläuft mit dem unionalen Rechtsakt eine Prozeduralisierung bisher unbekannten Ausmaßes.[737] Neue technische, organisatorische und institutionelle Arrangements sollen den Datenschutz als Querschnittsmaterie in der polizeilichen Praxis verankern und so zu einen normativ angeleiteten und (besser) steuerbaren Datenumgang im sensiblen Aufgabenspektrum der Polizei führen, auch weil sich dieses Ziel nicht mehr durch das schlichte Aufstellen insbesondere materieller Vorgaben bewerkstelligen lässt.[738] Zentral dafür ist ein innerbehördliches Prüfungs- und Kontrollsystem, das durch die Betroffenenrecht in Art. 12 ff. JI-Richtlinie und das System der Aufsichtsbehörden gemäß Art. 41 ff. JI-Richtlinie ergänzt und vervollständigt wird. Dieses innerbehördliche Datenschutzkontrollregime ist auf den drei Säulen der behördlichen Datenschutzbeauftragten, der Dokumentationspflichten sowie der technisch-organisatorischen Datenschutzinstrumente errichtet.

Als personale Ausprägung des polizeiinternen Prüfungs- und Kontrollsystems schreibt die JI-Richtlinie in Art. 32 Abs. 1 zunächst die behördlichen Datenschutzbeauftragten vor. Nach Art. 34 JI-Richtlinie ist deren Aufgabe neben weiteren Aspekten vor allem die Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften und die Beratung der mit den Datenverarbeitungsprozessen betrauten Beamt:innen. Dabei geht es vor allem um die Anleitung der polizeilichen Fachlichkeit.[739] Um die Wirkmacht der Position zu maximieren sind die behördlichen Datenschutzbeauftragten gemäß Art. 33 Abs. 1 JI-Richtlinie frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Die Datenschutzbeauftragten dürfen daher nicht vor vollendete Tatsachen gestellt werden, sondern sind bereits von Beginn an in konzeptuelle Entwicklungen in einer Weise miteinzubeziehen, die ihren Anmerkungen Berücksichtigung verschafft.[740] Daneben sind die Datenschutzbeauftragten

737 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 461.
738 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (768).
739 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 510.
740 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (768).

auch Kontaktpunkte für die äußere Kontrolle durch die Aufsichtsbehörde, also für Bundes- und Landesdatenschutzbeauftragte. Mit diesen sind die behördlichen Datenschutzbeauftragen nach Art. 26 JI-Richtlinie zur Zusammenarbeit verpflichtet, wobei aber kein proaktives Tätigwerden der polizeilichen Beauftragten vorgesehen ist.[741] Flankiert wird das allgemeine Postulat der Zusammenarbeit durch spezielle Kooperationspflichten etwa im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten (Art. 24 Abs. 2 Satz 2 JI-Richtlinie), Protokollierungen (Art. 25 Abs. 3 JI-Richtlinie) und der Datenschutz-Folgenabschätzung (Art. 28 Abs. 1 lit. a JI-Richtlinie). Im Vergleich zur DSGVO ist die Stellung der polizeilichen Datenschutzbeauftragten hingegen schwächer ausgestaltet, da insbesondere das Gebot der Weisungsfreiheit und das Verbot der Abberufung bzw. Benachteiligung aufgrund ihrer Tätigkeit fehlt, wobei dies hingegen durch Erwägungsgrund 63 JI-Richtlinie abgemildert wird, der eine Auftrags- und Aufgabenerfüllung in unabhängiger Weise nahelegt.

Diese drei eben genannten Instrumente bilden auch den Kern der Säule der Dokumentationspflichten. Das gemäß Art. 24 JI-Richtlinie zu führende Verzeichnis von Verarbeitungstätigkeiten soll einen Überblick über die in einer Behörde durchgeführten Datenverarbeitungen bieten und so einen ersten Anhaltspunkt für die Prüfung der Rechtmäßigkeit eröffnen. Daneben dienen die Verzeichnisse auch der internen Bestandsaufnahme und damit der Vergegenwärtigung des Umfangs der polizeibehördlichen Datenverarbeitungen.[742] Der Analyse einzelner Datenverarbeitungsverfahren dient ergänzend die Datenschutz-Folgenabschätzung aus Art. 27 Abs. 1 JI-Richtlinie. Eine solche ist durchzuführen bei Verarbeitungsvorgängen, bei denen ein hohes Risiko für die Rechte und Freiheiten betroffener Personen anzunehmen ist. Ein solches ist wiederum gegeben, wenn die Verarbeitung zu einem physischen, materiellen oder immateriellen Schaden führen kann, was umfassend erhebliche wirtschaftliche oder gesellschaftliche Nachteile erfasst, die sich aus der fehlenden Kontrolle über die eine Person betreffenden Daten ergibt.[743] Relevant ist das insbesondere im Kontext der Verwendung neuer Technologien, wozu etwa moderne Videoanalyse-Verfahren,[744] sonstige moderne Datenanalyse-Verfahren aber auch niedrigschwelligere

741 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (768).
742 *Petri* in *Simitis/Hornung/Spiecker genannt Döhmann* (Hrsg.), Datenschutzrecht, Art. 30 Rn. 1.
743 Siehe die noch umfassendere Formulierung in Erwägungsgrund 75 DSGVO.
744 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (769).

Technologien wie etwa die Einführung von Bodycams zählen dürften. Zu enthalten hat die Folgenabschätzung gemäß Art. 27 Abs. 2 JI-Richtlinie „eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Richtlinie eingehalten wird." Infolge einer Datenschutzfolgenabschätzung kann sich, wie erwähnt, eine Pflicht zur Konsultation der Aufsichtsbehörde ergeben, wenn trotz festgestellten hohen Risikos keine Eindämmungsmaßnahmen ergriffen werden (Art. 28 Abs. 1 lit. a JI-Richtlinie), etwa weil es keine technologischen Lösungen gibt.[745] Dass dies nur bei „neu anzulegenden Dateisystemen" gilt, dürfte Praktikabilitätsüberlegungen im Kontext der Polizei geschuldet sein, ist aber mit Blick auf Altsysteme bedenklich, insbesondere, wenn es zu Umstrukturierungen von bestehenden Systemen kommt. Sowohl die Datenschutz-Folgenabschätzung als auch das Verzeichnis von Verarbeitungstätigkeiten helfen den Behörden selbst aber auch der Aufsicht, die Rechtmäßigkeit des polizeilichen Datenumgangs besser zu beurteilen. Allerdings vermitteln sie eher eine statische Momentaufnahme der Gesamtheit der Verfahren bzw. der Einzelheiten eines Verfahrens. Die Dynamiken der tatsächlich durchgeführten Datenverarbeitungen wird hingegen durch Protokollierungen dokumentiert und damit der Rechtmäßigkeitskontrolle zugeführt. Die Polizeibehörden haben gemäß Art. 25 Abs. 1 JI-Richtlinie bei automatisierten Verarbeitungssystemen die Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung von Daten zu protokollieren, wobei Begründung, Darum und Uhrzeit und – soweit möglich – Identität der abfragenden bzw. offenlegendenden und empfangenden Person zu protokollieren sind. Der Begriff der automatisierten Verarbeitung ist in seinem Bedeutungsgehalt aus den Texten der europäischen Datenschutzreform nur implizit ableitbar, was auch die inhaltliche Erfassung des Begriffs der „automatisierten Verarbeitungssysteme" erschwert. Anzunehmen ist, dass „alle Verfahren [erfasst werden], bei denen ein Datenverarbeitungsvorgang anhand eines vorgegebenen Programms ohne weiteres menschliches Zutun selbsttätig erledigt wird", wobei die Digitalisierung eines Prozesses

745 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (769).

hinreichend, aber nicht notwendig sein soll.[746] Noch extensiver ist ein Verständnis, dass darunter „sämtliche heute gebräuchlichen rechnergestützten Verarbeitungen personenbezogener Daten" fasst.[747] Vor allem mit Blick auf die vermehrte Umstellung auf die elektronische Akte nimmt die Bedeutung der Protokollierungspflicht somit weiter zu. Während sich gegenwärtig der Umgang mit in Papierakten gespeicherten Daten nicht festhalten lässt, hält die Digitalisierung insofern ein erhebliches Potenzial für die Kontrolle des polizeilichen Datenumgangs in seiner Gesamtheit bereit.[748]

Die letzte Säule des polizeiinternen Datenschutzkontrollregimes sind die technischen Datenschutzinstrumente. Mit Art. 20 legt die JI-Richtlinie fest, dass Technikgestaltung und datenschutzrechtliche Voreinstellungen die Rechtmäßigkeit der Datenverarbeitung durch entsprechende Designs sicherstellen oder zumindest fördern sollen. Den dahinterstehenden Gedanken hat *Roßnagel* bereits 2005 prägnant auf den Punkt gebracht:

> „Ohne technische Unterstützung droht Recht in einer technikgeprägten Welt folgenlos zu bleiben. Recht ist auf rechtsgemäße Technik angewiesen. Informationelle Selbstbestimmung ist durch, nicht gegen Technik zu ermöglichen. Schutz durch Technik ist oft die einzig mögliche Antwort auf Probleme der Globalisierung der Datenflüsse, der dynamischen Technikentwicklung und der zunehmenden Intransparenz der Systeme."[749]

Nach Art. 20 JI-Richtlinie müssen Polizeibehörden unter Berücksichtigung des Stands der Technik, der Kosten sowie von Art, Umfang, Umständen und Zwecken der Verarbeitung und der Risiken für die Rechte und Freiheiten betroffener Personen durchgängig angemessene technische und organisatorische Maßnahmen vornehmen, um die Datenschutzgrundsätze (Art. 4 JI-RL) und die übrigen Anforderungen der JI-RL wirksam umzusetzen. Dabei ist durch die explizite Nennung der Datenminimierung diese wohl leitendes Gestaltungskriterium. Offenkundig wird dadurch ein Spannungsverhältnis zur Arbeit einer modernen Polizei geschaffen, die im Wesentlichen auf die Verarbeitung von Informationen angewiesen ist. Verschärft wird dieser Konflikt durch die zunehmende Entwicklung hin „zu neuen, stark

746 *Bäcker* in *Brink/H. Wolff,* BeckOK Datenschutzrecht, DS-GVO Art. 2 Rn. 2
747 *Zerdick* in *Ehmann/Selmayr/J. Albrecht,* DS-GVO, Art. 2 Rn. 3.
748 *Roßnagel* in *Simitis/Hornung/Spiecker genannt Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 6 Rn. 12.
749 *Roßnagel* Informatik Spektrum 28 (2005), 462 (469).

datengetriebenen Ermittlungs- und Gefahrenabwehrwerkzeugen öffentlicher Stellen wie beispielsweise Predictive Policing oder automatisiert ausgewerteter Kameraüberwachung zur Gesichts- und Verhaltenserkennung."[750] Zwar ist bezüglich der genannten Technologien eine datensparsame Funktionsweise denkbar, etwa durch die direkte Löschung im Nichttrefferfall bei biometrischer Videoüberwachung oder die Nutzung von raumbezogenen Formen des Predictive Policings. Allerdings ist durchaus fraglich, ob eine unter dem Paradigma der Massendaten operierende Polizei das Postulat der Datenminimierung und -sparsamkeit auf Dauer wird durchhalten können. Unter die technischen Datenschutzprinzipien lässt sich auch die Datensicherheit fassen, die in Art. 29 JI-Richtlinie näher spezifiziert wird. Wie bereits in Art. 20 JI-Richtlinie sind auch hier der Stand der Technik, die Kosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Risiken für die Rechte und Freiheiten betroffener Personen zu berücksichtigen. Der Katalog des Art. 29 Abs. 2 JI-Richtlinie enthält verschiedene Mittel zur Gewährleistung der Datensicherheit, wie Speicherkontrolle, Benutzerkontrolle, Zugangskontrolle, Eingabekontrolle oder Übertragungskontrolle. Diese dienen der Nachverfolgung des Datenumgangs durch einzelne Beamt:innen. Wesentlich sind auch Zuverlässigkeit, also die Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und Datenintegrität, das heißt dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Diese Instrumente spielen auch bei der Verarbeitung besonderer Kategorien personenbezogener Daten eine wesentliche Rolle.[751]

Kommt es trotz dieser Vorkehrungen zu Verstößen gegen das polizeiliche Datenschutzrecht, so muss die jeweilige Polizeibehörde gemäß Art. 30 JI-Richtlinie dies der Aufsichtsbehörde melden, es sei denn – was im polizeilichen Kontext aufgrund der Sensibilität der Daten selten anzunehmen sein wird – dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Auch die betroffene Person ist zu benachrichtigen, wobei Art. 31 JI-Richtlinie hier mehr Ausnahmen als bei der aufsichtsbehördlichen Meldepflicht kennt und in Abs. 3 i.V.m. Art. 13 Abs. 3 JI-Richtlinie den

750 *Marnau* in *Gola/Heckmann/Klug* ua, BDSG, § 71 Rn. 23 f.
751 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 531 f.

praktisch wohl bedeutendsten Ausnahmefall der Behinderung behördlicher Ermittlungstätigkeit aufstellt.

Insgesamt wird man bezüglich der Neuerungen der JI-Richtlinie zustimmen können, dass sie den polizeilichen Datenumgang nicht „von Grund auf neu gestalte[t]" hat.[752] Nichtsdestotrotz scheint die Prozeduralisierung und personale sowie technische Institutionalisierung von Schutzmechanismen ein sinnvoller Weg für eine Polizei zu sein, die zunehmend Datenaggregationen handhaben muss, die weit über individuelle Verfahren und die von ihnen betroffenen Personen hinausgehen. Hier ein individuenzentriertes Datenschutzkonzept zu verfolgen, erscheint für sich genommen nicht weiter zukunftsfähig, sodass die Innovationen der europäischen Datenschutzreform als notwendiger Schritt in Richtung eines eingehegten polizeilichen Informationswesens gesehen werden müssen, was die Steuerungskraft des Rechts durch ein robustes Datenschutzkontrollregime sowohl intern wie extern erhöhen kann.

C. Einfachgesetzliche Rahmenbedingungen des polizeilichen Informationswesens

Die bisher dargestellten verfassungsrechtlichen und unionalen Normenkomplexe haben zwar durchaus auch direkte Auswirkungen auf die praktische Ebene der polizeilichen Datenverarbeitung. Mehrheitlich handelt es sich dabei aber um Vorgaben für Bundes- und Landesgesetzgeber, die verpflichtet sind, das polizeiliche Informationswesen mit dem Erlass entsprechender Gesetze zu strukturieren und zu steuern. Zu diesem Zweck gibt es im Wesentlichen seit dem Volkszählungsurteil einen Gesetzgebungsschub in den Polizeigesetzen und der Strafverfahrensordnung, um diesem legislativen Gestaltungsauftrag nachzukommen. Daraus ist ein komplexes Gesetzessystem evolviert, das aufgrund seiner Eigenständigkeit und Relevanz besser als polizeiliches Informationsrecht[753] oder polizeiliche Informationsordnung[754] denn als polizeiliches Datenschutzrecht bezeichnet werden kann. Die Schwierigkeit eines jeden Rechts, Lebensweltliches möglichst umfassend und für das übrige Rechtssystem anschlussfähig mit Begriffen und Verhältnissen zu erfassen, wird für das polizeilichen Informationswe-

752 *Borell/Schindler* Datenschutz und Datensicherheit 43 (2019), 767 (772).
753 So bereits oben S. 25.
754 *Bäcker,* Kriminalpräventionsrecht, S. 473.

sen allerdings dadurch erheblich erschwert, dass es prälegal, also weit vor seiner rechtlichen Erschließung, entstanden und zunächst weitestgehend unabhängig vom Recht gewachsen ist.[755] Insofern steht die rechtliche Rahmung polizeilicher Datenverarbeitung vor der Herausforderung, die Institutionen, Infrastrukturen und Praktiken des Informationswesen normativ zu erfassen und damit gesetzgeberisch gestaltbar zu machen. Im Folgenden sollen diese gesetzlichen Strukturen in ihren Grundzügen dargelegt und einer kritischen Überprüfung unterzogen werden.

Die systematische Darstellung der in diesem Kontext relevanten Normkomplexe ist indessen kein leichtes Unterfangen. Die Polizeilandschaft Deutschlands ist föderalistisch strukturiert. Sowohl Bundes- als auch Landespolizeibehörden verarbeiten im Rahmen ihrer wesentlichen Aufgaben – Strafverfolgung und Gefahrenabwehr – personenbezogene Daten, auf Grundlage unterschiedlicher Gesetze bzw. im Anwendungsbereich mehrerer Rechtsgrundlagen, etwa wenn Daten zweckändernd übertragen werden. Die folgende Darstellung der einfachgesetzlichen Rahmenbedingungen orientiert sich auf einer ersten Ebene nicht an den jeweiligen Gesetzesmaterien, sondern unternimmt den Versuch einer Systematisierung anhand von für das polizeiliche Informationswesen wesentlichen technischen Strukturen und Praktiken, da diese beiden Aspekte das polizeiliche Informationswesen im Kern ausmachen. Nach einem generellen Überblick über die einfachrechtliche Terminologie und Prinzipien der polizeilichen Datenverarbeitung erfolgt deshalb eine Darstellung der normativen Verankerung der informationstechnologischen Infrastrukturen des polizeilichen Informationswesens. Im Anschluss daran werden die normativen Vorgaben für die Praktiken der Informationsverarbeitung erläutert. Abschließend wird noch auf das interne Datenschutzkontrollregime eingegangen, das ebenfalls von zentraler Bedeutung für das polizeiliche Informationswesen sowie den empirischen Teil der Arbeit ist.

I. Einfachrechtliche Terminologie und Prinzipien der polizeilichen Datenverarbeitung

Für die unterschiedlichen Arten des Datenumgangs sahen und sehen die jeweiligen polizeirechtlichen Normenkomplexe auf Bundes- und Lan-

755 Siehe dazu bereits oben S. 101 ff.

desebene grundsätzlich eine einheitliche Terminologie vor. So unterscheiden die Gesetze oft zwischen Datenspeicherung, -veränderung. -nutzung, -übermittlung, -berichtigung, und -löschung. Diese Unterscheidung wurde jedoch von der JI-Richtlinie hinsichtlich der Verarbeitungsvoraussetzungen nicht aufgegriffen, sodass vermutet wird, die begriffliche Differenzierung zwischen den einzelnen Verarbeitungsphasen würde nach Umsetzung der unionsrechtlichen Vorgaben in den Landespolizeigesetzen weitestgehend bedeutungslos werden.[756] Zudem enthalten die entsprechenden Gesetze die den gesamten Prozess der Datenverarbeitung leitenden, verfassungsrechtlich geformten Verarbeitungsprinzipien. Gesetzestechnisch sind diese Grundsätze entweder isoliert geregelt oder in den jeweiligen Rechtsgrundlagen zur Datenverarbeitung inkorporiert.

I. Terminologie

Die Terminologie in den Landespolizeigesetzen ist insgesamt (noch) sehr einheitlich und differenziert zumeist zwischen den bereits genannten Verarbeitungsschritten der Datenspeicherung, -veränderung. -nutzung, -übermittlung, -berichtigung, und -löschung. Obwohl diese Differenzierung im europäischen Datenschutzrecht nunmehr obsolet zu sein scheint, halten etliche Landespolizeigesetze auch nach der Umsetzung der JI-Richtlinie daran fest. Aber die unionale Vereinheitlichung der Verarbeitungsschritte zeigt auch Wirkung: Auf Bundesebene, etwa im BKAG, ist diese Differenzierung nicht mehr in ihrer Detailliertheit vorhanden: Die zentrale Kategorie ist dort nunmehr die sog. Weiterverarbeitung, was insbesondere die Speicherung, Veränderung und Nutzung von Daten zusammenfassend meint. Auch einige Länder – wie etwa Nordrhein-Westfalen – haben die europarechtliche Terminologie übernommen. Im dortigen Polizeigesetz ist aber beispielsweise die Speicherung als eigenständige informationelle Befugnis erhalten geblieben. Mithin sind gegenwärtig sowohl traditionelle als auch neue Terminologie nebeneinander zu beachten.

756 So etwa *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 843.

a) Datenspeicherung

Die Datenspeicherung meint das Erfassen, Aufnehmen oder Aufbewahren von Daten auf (irgend)einem Datenträger zum Zwecke ihrer weiteren Verwendung. Fixiert die Polizei die Daten nicht selbst auf einem Speichermedium, sondern bekommt sie von dritter Stelle, ist ein Fall des Aufbewahrens gegeben.[757] Unerheblich ist im Rahmen der Speicherung der eingesetzte Träger. Diese für die rechtliche Einordnung zunächst bestehende Irrelevanz des gewählten Speichermediums macht die in einigen Polizeigesetzen noch bestehende Differenzierung zwischen der Speicherung in Dateien und in Akten prinzipiell überflüssig.[758] Auch die Polizeipraxis, in der physische Akten zunehmend vollständig oder zumindest ihr Index digitalisiert werden und in ihnen enthaltene Daten so besser auffindbar sind, zeugt von der schwindenden Bedeutung der Unterscheidung zwischen analoger Akte und digitaler Datei. Die sich aufgrund einer solchen Datenerfassung in automatisierten Dateien ergebenden tiefergehenden Verarbeitungsmöglichkeiten sind allerdings rechtlich alles andere als irrelevant: Es besteht hier regelmäßig eine höhere Eingriffsqualität, da größere Datenvolumina aufbewahrt, durchsucht und verknüpft werden können.[759] Darüber hinaus ist der Akt der Datenspeicherung für die polizeiliche Informationsverarbeitung ein schlechthin essenzieller Punkt, denn hierauf baut sie letztlich auf. Für die Speicherdauer kann jedes gespeicherte personenbezogene Datum – im Rahmen der gesetzlichen Befugnisse – in vielerlei Hinsicht genutzt werden. Mit dem Akt der Speicherung werden die Weichen hierfür gestellt. Gerade diese zentrale Position der Datenspeicherung müsste sie zum Gegenstand erhöhter legislativer Aufmerksamkeit machen.[760]

757 *Von der Grün* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 37 PolG BW, Rn. 16.

758 *Aulehner* in *Möstl/Schwabenbauer* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Sicherheitsrecht Bayern, Art. 53 PAG Rn. 6a.

759 So auch *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 20 PolG NRW, Rn. 26.1; *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 847.

760 Ähnlich *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 847; siehe dazu auch *Bäcker,* Kriminalpräventionsrecht, S. 473.

b) Datenveränderung

Werden gespeicherte Daten inhaltlich derart umgestaltet, dass es ihren Informationsgehalt und nicht nur ihre Darstellungsweise modifiziert, liegt eine Datenveränderung vor.[761] Neben dem Hinzufügen oder Löschen von Daten ist die Herstellung eines neuen Zusammenhang ein bedeutsamer Unterfall der Datenveränderung: Werden Daten etwa in eine einschlägige Datensammlung übertragen, kann diese Rekontextualisierung den Informationsgehalt erheblich beeinflussen, ohne dass an den Daten selbst inhaltliche Änderungen vorgenommen werden.[762] Das Risiko fluider und rekombinatorischer Informationsgehalte personenbezogener Daten betonte das Bundesverfassungsgericht bereits im Volkszählungsurteil.[763] Die rechtförmige Einhegung dieser Art des Datenumgangs hat dementsprechend vor der Verfassung besonderes Gewicht. Problematisch sind vor diesem Hintergrund Rechtsgrundlagen, die die Datenveränderung pauschal und niedrigschwellig freigeben, etwa soweit und solange sie zur Aufgabenerfüllung erforderlich sind.[764]

c) Datenübermittlung

Der Informationsfluss zwischen verschiedenen Polizeibehörden und zwischen Polizei und sonstigen (nicht-)öffentlichen Stellen wird rechtlich durch die sog. Datenübermittlung abgebildet. Übermitteln war bislang das Bekanntgeben personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.[765] Rechtlich beachtenswert ist diese Verwaltungspraxis vor allem deshalb, weil durch die Erweiterung des Kreises derjenigen Stellen, die Kenntnis von

761 *Von der Grün* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 37 PolG BW, Rn. 17.

762 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 884.

763 BVerfGE 65, 1 (44) – Volkszählung.

764 Siehe etwa § 15 Abs. 1 PolG BW, Art. 54 BayPAG, § 42 ASOG Berlin, § 36 PolDVG Hamburg. Ein Positivbeispiel ist etwa Bremen, dessen § 36a BremPolG Rechtmäßigkeit und Zweckbindung besonders betont, ähnlich ist es in Niedersachen § 38 NPOG.

765 *Röcker* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 41 PolG BW, Rn. 5.

den Daten haben, die Intensität des grundrechtlichen Risikos Betroffener erhöht wird.[766] Der Akt der Datenübermittlung erscheint im Bereich der polizeilichen Datenverarbeitung in verschiedenen Ausführungen, abhängig bspw. davon von wem, an wen, auf wessen Verlangen oder auf welche Weise Daten übermittelt werden.

Im Angesicht der JI-Richtlinie ist allerdings noch nicht sicher, ob und inwieweit die bisherige Terminologie unverändert beibehalten werden kann, da das EU-Datenschutzrecht insofern Bedeutungsverlagerungen auslösen könnte.[767] Zwar spielt die Übermittlung von Daten – obwohl nicht explizit definiert – auch in der Richtlinie eine Rolle. Kapitel V der Richtlinie soll sicherstellen, dass ihr Datenschutzniveau nicht durch Übermittlungen unterlaufen wird, womit das europarechtliche Begriffsverständnis weiter als das hiesige ist: Erfasst ist jeder Verarbeitungsvorgang, durch den personenbezogene Daten den Geltungsbereich der JI-Richtlinie verlassen und die Endbestimmung der Daten außerhalb des Unionsgebiets liegt oder die Daten von außerhalb der Union zugänglich sind.[768]

d) Datenberichtigung

Die Datenberichtigung, die als Pflicht auf Seiten der Polizei und korrespondierend zum Anspruch Betroffener besteht, wird dann relevant, wenn personenbezogene Daten unrichtig sind, d.h. ein unzutreffendes Bild von der Wirklichkeit vermitteln. Im Wege der Berichtigung wird der Informationsgehalt des in Frage stehenden Datums wieder in Übereinstimmung mit der Realität gebracht.[769] Sind die personenbezogenen Daten aktenförmig, so ist die Berichtigung zu bewerkstelligen, indem die Unrichtigkeit in der Akte vermerkt oder auf sonstige Weise festgehalten wird.[770] Bei der Datenberichtigung handelt es sich strenggenommen um eine besondere Form der Datenveränderung, sodass etwa auch durch die Speicherung neuer Daten berichtigt werden kann.[771]

766 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 483.
767 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 489.
768 So *Zerdick* in *Ehmann/Selmayr/J. Albrecht* ua (Hrsg.), DS-GVO, Art. 44 DS-GVO, Rn. 7, für die DS-GVO.
769 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 9 BKAG Rn. 14.
770 *Ogorek* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 32 PolG NRW, Rn. 3.
771 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 9 BKAG Rn. 14.

e) Datenlöschung

Das Löschen von Daten hat die Unkenntlichmachung gespeicherter personenbezogener Daten zum Gegenstand. Umfasst ist jede Form von Unkenntlichmachung vom Ausradieren, Schwärzen, Übermalen bis hin zur physischen Vernichtung. Entscheidend ist, dass die Information der verantwortlichen Stelle irreversibel nicht mehr zur Verfügung steht.[772] Nicht ausreichend ist eine Änderung der Datenorganisation derart, dass der gezielte Zugriff auf die zu löschenden Daten verhindert wird. Vor allem mit Blick auf Rekonstruktionsmöglichkeiten von Daten befindet sich der Bedeutungsgehalt der Datenlöschung im Wandel und hängt vom Stand der Technik ab.[773]

f) Datensperrung bzw. Einschränkung der Weiterverarbeitung

Sperren von Daten meint die Kennzeichnung von personenbezogenen Daten, um ihre weitere Verarbeitung einzuschränken,[774] etwa weil ihre Richtigkeit angezweifelt wurde. Im Rahmen der Umsetzung der JI-Richtlinie auf Bundes- und Landesebene ist der Begriff der Sperrung in etlichen Gesetzen durch denjenigen der Einschränkung der (Weiter)Verarbeitung ersetzt worden. Inhaltliche Änderungen sollen damit nicht verbunden sein.[775]

g) Datennutzung

Als Datennutzung gilt jede sonstige Verwendung, die nicht Erhebung, Speicherung, Veränderung, Übermittlung, Berichtigung, Sperrung, Löschung oder Vernichtung ist. Es handelt sich dementsprechend um einen Auffangtatbestand, der greift, wenn die Daten mit einer bestimmten Zweckrichtung ausgewertet, zusammengestellt, abgerufen oder zielgerichtet zur Kenntnis

772 *Hermesmeier/Brenz* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 46 PolG BW, Rn. 2.
773 Vgl. *Arzt* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 35 BPolG, Rn. 13.
774 *Hermesmeier/Brenz* in *Möstl/Trurnit* (Hrsg.), Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, § 46 PolG BW, Rn. 12.
775 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 78 Rn. 6; *Ogorek* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 32 PolG NRW Rn. 33.

genommen werden.[776] Als Verarbeitungsform spielt sie nur in denjenigen Polizeigesetzen noch eine Rolle, die noch zwischen Datenerhebung, Datenverarbeitung und Datennutzung unterscheiden und soll in ihren rechtlichen Voraussetzungen analog zur Datenspeicherung zu behandeln sein.[777]

h) Der neue Begriff der Weiterverarbeitung

In einigen Landespolizeigesetzen und auch im novellierten BKAG findet sich nunmehr der Begriff der „Weiterverarbeitung" personenbezogener Daten in den zentralen Datenverarbeitungsbefugnissen. Während sich in den Landespolizeigesetzen neben oder eher zwischen Datenerhebung und Weiterverarbeitung oft noch Befugnisnormen zum Akt der Datenspeicherung finden, ist die Datenweiterverarbeitung im BKAG zur Kernbefugnis für Datenumgang avanciert. Die Nivellierung der unterschiedlichen Datenverarbeitungsphasen, die mit der Einführung des Begriffs der Weiterverarbeitung einhergeht, ist vor allem auf die europäische Datenschutzreform zurückzuführen. Art. 3 Nr. 2 JI-Richtlinie kennt als übergeordnete Form der Datenumgangs allein noch die Verarbeitung, also jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Das BDSG und die jeweiligen Landesdatenschutzgesetze übernehmen diese Terminologie, sodass die darauf Bezug nehmenden Bundes- und Landespolizeigesetze nunmehr vom europarechtlichen Begriff der Verarbeitung geprägt sind. Es ist letztlich – bewusst auf Differenzierung, wie sie das deutsche Datenschutzrecht vorher kannte, verzichtend[778] – jeder Umgang mit Daten erfasst.[779]

776 *Graf* in *Möstl/Weiner* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 38 NPOG, Rn. 30.
777 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 885.
778 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG, Rn. 22.
779 *Schild* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, Art. 4 DS-GVO Rn. 32.

Während die Intention einer möglichst lückenlosen Erfassung und damit eines möglichst lückenlosen Schutzes per se zu begrüßen ist, bringt die begriffliche Einebnung auch ein Problem mit sich: Die mit verschiedenen Formen des Datenumgangs verbundene Eingriffsintensität lässt sich so begrifflich im Gesetz nur begrenzt operationalisieren. Wenn etwa das (eher administrativ anmutende) Ordnen terminologisch mit dem (tendenziell invasiveren) Verknüpfen[780] unter einen Oberbegriff vermengt wird und beide beispielsweise pauschal zur polizeilichen Aufgabenerfüllung freigegeben werden, ist die verhältnismäßige Handhabung der unterschiedlichen Intensitätsgrade in der Polizeipraxis zusätzlich erschwert. Eine begriffliche Trennung kann also dazu beitragen, ein differenziertes Bewusstsein und eine reflektiertere Anwendungspraxis zu schaffen.

2. Prinzipien der polizeilichen Datenverarbeitung

Neben der Terminologie der polizeilichen Datenverarbeitung enthalten die Polizeigesetze regelmäßig auch Ausführungen zu den allgemeinen, für jede Art des Datenumgangs geltenden Verarbeitungsprinzipien. Die Grundsätze sind verfassungs- oder europarechtlich determiniert, werden aber durch ihre einfachgesetzliche Umsetzung in der Gesetzessystematik konkretisiert und überhaupt erst wirkungsvoll gegenüber Rechtsanwender:innen. Die wichtigsten von ihnen sind der Zweckbindungsgrundsatz mit der darauf bezogenen Regelung der Zweckänderung sowie die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit.

a) Zweckbindung

Als zentrales Prinzip des deutschen Datenschutzrechtes ist auch in der polizeilichen Datenverarbeitung der Zweckbindungsgrundsatz normativ fest verankert.[781] In diesem Kontext bedeutet es zunächst für jedes in die Sphäre der Polizei gelangte Datum eine Beschränkung der Verarbeitung auf den ursprünglichen (zumeist Erhebungs-)Zweck. Ebenfalls noch im Rahmen der Zweckbindung enthalten, ist seit dem BKAG-Urteil des Bundesverfas-

780 Siehe zu den jeweiligen Begriffsinhalten *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 594.

781 *Braun* in *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 15.

sungsgerichts auch die zweckwahrende Weiternutzung.[782] So soll die multifunktionelle Nutzbarkeit von Daten in rechtlich zulässige Bahnen gelenkt werden.[783]

Die Übersetzung des Zweckbindungsgrundsatzes in seiner für die polizeiliche Datenverarbeitung seit dem BKAG-Urteil geltenden Form in einfaches Recht ist dabei nicht immer ganz unproblematisch, da oftmals lediglich der Urteilstext Wort für Wort übernommen wurde. Dabei wird zunächst missachtet, dass sich die Vorgaben des Bundesverfassungsgerichts an den Gesetzgeber und nicht an die Rechtsanwender:innen richten.[784] Durch die Schaffung wortlautgetreuer Rechtsnormen enthält sich der Gesetzgeber seiner legislativen Gestaltungsaufgabe und wälzt die Verantwortung zur verfassungskonformen Datenverarbeitung direkt auf die Exekutive ab,[785] der so nur die Möglichkeit der Selbstprogrammierung[786] bleibt. Die normative Orientierungslosigkeit auf Ebene der Rechtsanwendung wird zudem noch dadurch verstärkt, dass die Datenerhebungsbefugnisse in den Polizeigesetzen regelmäßig keine konsistente Zweckbestimmung enthalten. Vielmehr lassen solche sich im Wege der Auslegung aus dem Tatbestand extrahieren oder die Befugnisse verweisen generell auf die zu Beginn des Gesetzes definierten abstrakten Behördenaufgaben.[787] Eine dem Bestimmtheitsgrundsatz angemessene einfachgesetzliche Ausfüllung des verfassungsrechtlichen Zweckbindungsgrundsatzes wird so für den Bereich polizeilicher Datenverarbeitung höchstens ansatzweise geleistet.[788]

782 Siehe dazu bereits die Ausführungen oben S. 164 ff.

783 *Von der Grün* in *Möstl/Weiner* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 38 Rn. 24.

784 Siehe zu dieser Differenzierung allgemein *Härting* Neue Juristische Wochenschrift 2015, 3284.

785 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 36.

786 Allgemein zur Selbstprogrammierung *Schuppert,* Governance und Rechtsetzung, 182 f., kritisch dazu *Habermas,* Faktizität und Geltung, 60, 212 f., 230 f. et passim; im Kontext der Polizei siehe etwa *Goeschel/Heyer/G. Schmidbauer,* Beiträge zu einer Soziologie der Polizei, 74 ff.

787 *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 40.

788 So auch *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 41.

b) Zweckänderung

Die mangelnde Bestimmtheit der Zweckbindung und die Zulässigkeit weitreichender Zweckänderungen[789] machen das verfassungsrechtliche Zweckbindungsprinzip zu einem normativen Luftschloss: Die gesetzlich gewünschte Zweckbindung gibt es tatsächlich kaum.[790]

Nichtsdestotrotz finden auch die im BKAG-Urteil konsolidierten verfassungsrechtlichen Vorgaben für die Zweckänderung nunmehr Eingang in die Polizeigesetze. Vor allem das „Zentralparadigma des Sicherheits-Datenschutzverfassungsrechts",[791] der Grundsatz der hypothetischen Datenneuerhebung, erfordern gesetzgeberische Umsetzungshandlungen. Auch diese beschränken sich überwiegend darauf, die Verfassungsrechtsprechung in Paragraphenform zu gießen.[792] Von den verschiedenen Gesetzgebern ebenfalls zu beachten sind dabei die europarechtlichen Anforderungen an Zweckänderungen, die sich für die vorliegende Untersuchung aus Art. 4 Abs. 2, 3 JI-Richtlinie ergeben, wobei die Mitgliedstaaten strengere Anforderungen an die zweckändernde Verarbeitung stellen können, Art. 1 Abs. 3 JI-Richtlinie, was wohl auf die verfassungsrechtlichen Vorgaben zutrifft.

Vor dem Hintergrund der detaillierten verfassungsrechtlichen Vorgaben in diesem Bereich ist zweifelhaft,[793] ob diejenigen polizeilichen Zweckänderungsbefugnisse, die die Zweckänderung recht knapp dann erlauben, wenn die Polizei die in Frage stehenden Daten auch zu dem neuen Zweck hätte speichern und nutzen (also verarbeiten) können,[794] noch verfassungsgemäß sind. Sie müssten jedenfalls unter Berücksichtigung des Grundsatzes der hypothetischen Datenneuerhebung ausgelegt werden. Darüber hinaus

789 § 12 Abs. 2 BKAG, § 29 Abs. 1 S. 4 BPolG, § 15 Abs. 3 BW PolG, Art. 53 Abs. 2 S. 2 BayPAG, § 42 Abs. 2 S. 2 ASOG Bln, § 38 Abs. 1 S. 2 BbgPolG, § 36b Abs. 1 BremPolG, § 34 Abs. 2 PolDVG Hamburg, § 20 Abs. 2 HSOG, § 36 Abs. 2 SOG M-V, § 39 NPOG, § 23 Abs. 2 PolG NRW, § 50 Abs. 2 S. 2 RP POG, § 23 Abs, 2 SPolDVG, § 13b Abs. 2 SOG LSA, § 79 Abs. 2 SächsPVDG, § 188 Abs. 1 S. 2 LVwG SH. Die Zweckänderung ist in Thüringen, soweit ersichtlich, gestreckt über § 40 TPAG gergelt.

790 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 855.

791 *Gärditz* Zeitschrift für das Gesamte Sicherheitsrecht 2017, 1, 3.

792 Vorschriften, die den Grundsatz der hypothetischen Datenneuerhebung inkorporieren sind § 12 Abs. 2 BKAG, § 15 BW PolG, § 20 Abs. 2 HSOG, § 36 Abs. 2 SOG M-V, § 23 Abs. 2 PolG NRW, § 51 Abs. 3 RP POG, § 23 Abs, 2 SPolDVG, § 13b Abs. 2 SOG LSA, § 79 Abs. 2 SächsPVDG, § 188a Abs. 2 LVwG SH.

793 Zum Problem der „Erdrosselung" des Gesetzgebers siehe *Gärditz* Zeitschrift für das Gesamte Sicherheitsrecht 2017, 1 (3).

794 Siehe dazu bereits Fn. 789.

fehlen jedoch auch oftmals sonstige, durch Verfassungs- und Europarecht determinierte Tatbestandsvoraussetzungen, wie die der Erforderlichkeit. Zentrale Rechtmäßigkeitsvoraussetzungen des Datenumgangs der Auslegungskompetenz der jeweiligen Rechtsanwender:innen anheimzustellen, ist in Anbetracht der Bedeutung des Rechts auf informationelle Selbstbestimmung sowie europarechtlicher Parallelgrundrechte kaum angemessen. Daher kann die Tauglichkeit der entsprechenden Rechtsgrundlagen in den Polizeigesetzen bezweifelt werden.[795] Neben der fehlenden Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung verfehlen die jeweiligen Regelungen dementsprechend auch sonstige Vorgaben und sind daher dringend verfassungs- und europarechtskonform auszugestalten.

Allerdings ist auch die seit dem BKAG-Urteil vorherrschende Form der einfachgesetzlichen Formulierung von Zweckänderungsbefugnissen[796] nicht zufriedenstellend: Während einige der neuen Vorschriften ebenfalls keine Erforderlichkeitsvoraussetzung kennen,[797] besteht auch hier das Problem der wortlautgetreuen Übernahme der Verfassungsrechtsprechung. Die in erster Linie für den Gesetzgeber geltenden Anforderungen, die der Grundsatz der hypothetischen Datenneuerhebung aufwirft,[798] werden so ungefiltert an die Rechtsanwender durchgereicht. Mangels eines Beurteilungsmaßstabes für die vom Bundesverfassungsgericht geforderte Vergleichbarkeit der Schwere von Straftaten oder Gewichtigkeit von Rechtsgütern ist diese Verantwortungsverlagerung auf die einzelnen Polizeibeamt:innen unter Bestimmtheitsgesichtspunkten sowie mit Blick auf das Demokratieprinzip kritikwürdig.[799]

Insgesamt hat sich die polizeiliche Datenverarbeitung durch die Ausweitung der Zweckbindung durch die Möglichkeit der sogenannten zweckwahrenden Weiternutzung, weitreichender Ausnahmen vom Grundsatz der Zweckbindung durch Zweckänderungsbefugnisse in den Polizeigesetzen

795 So zu recht *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 Rn. 7 f. mwN.

796 Siehe dazu Fn. 792.

797 Eine Ausnahme ist etwa die Hessische Regelung, die allerdings so verschachtelt aufgebaut ist, dass ihre praktischen Anwendung nichtsdestotrotz herausfordernd ist, vgl. *Bäuerle* in *Möstl/Mühl* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Hessen, § 20 HSOG Rn. 10 ff.

798 Siehe dazu bereits Fn. 784.

799 So – bis auf die Bedenken hinsichtlich des Demokratieprinzips – auch *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 Rn. 31.

und die mangelnde Ausgestaltung dieser Befugnisse in eine nur noch lose mit dem Rechtssystem und seinen materiellen Vorgaben gekoppelte Sphäre verschoben. Mangels klarer normativer Vorgaben wird vor allem auch die Kontrolle durch Gerichte und Datenschutzbehörden schwieriger.[800] Diese Loslösung von einem das exekutive Handeln direkt steuernden Programm, das auch durch subjektiven Rechtsschutz einforderbar ist, lässt sich nach Vorstellung des Bundesverfassungsgerichts indessen durch aufsichtliche Kontrolle und Implementierung von Transparenzanforderungen in der behördlichen Praxis gegenüber der Öffentlichkeit kompensieren.[801]

Die verblassende Normwirkung des Zweckbindungspostulats wird auch an der gesetzgeberisch ermöglichten Nutzung von sogenannten doppelfunktionalen Maßnahmen durch die Polizei sichtbar. Will die strafverfolgende Polizei Maßnahmen zur Informationserlangung einsetzen, die sie nach Strafverfahrensrecht nicht oder nur mit erhöhten Anforderungen vornehmen könnte, so kann auch die entsprechende polizeirechtliche Gefahrenabwehrmaßnahme ergriffen und die erlangten Daten dann zweckändernd ins Strafverfahren überführt werden.[802] Die Bedeutung der rechtlichen Vorgaben verschiebt sich auf diese Weise immer mehr von einem wertegebundenem Verhaltensrahmen hin zu instrumentalisierbaren „Werkzeugkästen".[803]

c) Erforderlichkeit und Verhältnismäßigkeit

Bedeutsam im einfachgesetzlichen polizeilichen Datenverarbeitungsrecht ist neben dem Grundsatz der Zweckbindung auch der Begriff der Erforderlichkeit, der sowohl für gefahrabwehrrechtliche als auch für strafverfahrensrechtliche Zwecksetzungen gilt. Neben dem Verfassungsrecht verlangt dies nunmehr auch das Unionsrecht. Art. 4 Abs. 1 lit. c JI-Richtlinie fordert unter anderem, dass die Datenverarbeitung in Bezug auf den Verarbeitungszweck nicht übermäßig sein darf. Hieraus ergibt sich das Gebot der Datenminimierung. Die Zahl der verarbeiteten Daten und die Zahl der

800 *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 Rn. 33.
801 BVerfGE 141, 220 (281) – Bundeskriminalamtgesetz.
802 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn 580.
803 *Bäcker* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, D. Rn. 314.

Datenverarbeitungsvorgänge ist demnach auf das geringstmögliche Maß zu beschränken.[804] Auch soll das Erforderlichkeitsprinzip einer Sammlung von Daten auf Vorrat zu unbestimmten oder zu noch nicht bestimmten Zwecken einen Riegel vorschieben.[805] Besonders virulent wird die Erforderlichkeit im Bereich der Datenverarbeitung von Nichtbeschuldigten und unverdächtigen Personen. Datenverarbeitungen, die diese Personen betreffen, sind überhaupt nur unter strikten Voraussetzungen möglich; insbesondere bedarf es tatsächlicher Anhaltspunkte, dass die Datenverarbeitungen zur polizeilichen Aufgabenerfüllung nötig sind.[806]

Vor diesem Hintergrund ist bedenklich, wenn die Erforderlichkeit nicht als Tatbestandsvoraussetzung für die normierte Datenverarbeitungshandlung gesetzlich vorgesehen ist.[807] In Anbetracht der verfassungs- und unionsrechtlichen Bedeutung dieses Prinzips erscheint es zumindest zweifelhaft, ob die jeweiligen Normen taugliche Rechtsgrundlage für die mit ihnen beabsichtigten Datenverarbeitungsakte sein können.[808] Insofern wird man die Erforderlichkeit als ungeschriebenes Tatbestandsmerkmal in die entsprechenden Normen hineinzulesen haben, wobei diese Lösung insbesondere mit Blick auf die strukturierende Funktion der Vorschriften für die Praxis des polizeilichen Datenumgangs äußerst unbefriedigend ist.

Für die polizeiliche Datenpraxis ist zudem auch die einfachgesetzliche Nennung und Ausgestaltung des Verhältnismäßigkeitsgrundsatzes zentral. Neben seiner Bedeutung für die Dogmatik des Zweckbindungsgrundsatzes ist er zudem stets in der konkreten Rechtsanwendung zu beachten. Ein Datenverarbeitungsvorgang muss der Erfüllung seines Zwecks in geeigneter und erforderlicher Weise dienen und darf die betroffene Person nicht unangemessen beeinträchtigen. Die polizeilichen Sachbearbeiter:innen haben somit einzelfallbezogen die Eignung zu prüfen und potenzielle Alternativen zu berücksichtigen. Dabei ist auch eine Güterabwägung durchzuführen, in der die Eingriffsintensität mit dem verfolgten Zweck kontrastiert wird. Die Bestimmung der Eingriffsintensität ist ein komplexer Vorgang, in dem beispielsweise anhand einer Analyse der verwendeten Daten oder Datenverarbeitungsinstrumente die Tiefe der Privatheitsbeeinträchtigung bestimmt

804 *Braun* in *Gola/Heckmann/Klug* ua, BDSG, § 47 Rn. 21.
805 BVerfGE 125, 260 (321) – Vorratsdatenspeicherung m.w.N.
806 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 863.
807 Soweit ersichtlich nur § 23 PolG NRW, der lediglich für die Speicherung Erforderlichkeit fordert.
808 Ablehnend *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 23 PolG NRW Rn. 8.

werden muss.[809] Inwiefern diese fordernden Ansprüche der Rechtsordnung in der polizeilichen Praxis – vom Streifenbeamten bis zur Datenanalystin – beachtet werden (können), ist eine offene Frage.

d) Unional determinierte Verarbeitungsprinzipien

Mit der Umsetzung der JI-Richtlinie im Bundes- und den Landesdatenschutzgesetzen sind auch die unional vorgegebenen Verarbeitungsprinzipien greifbarer für die Rechtsanwendungsebene geworden, wenngleich sie wegen ihrer teilweisen Neuartigkeit noch nicht denselben Beachtungsgrad haben dürften wie die drei vorgenannten Grundsätze – zumal schon deren Beachtung in der polizeilichen Praxis als nicht (umfassend) gesichert gelten darf.

Neu, zumindest in dieser expliziten Form, ist der Grundsatz der Rechtmäßigkeit in § 47 Nr. 1 Alt. 1 BDSG, der allerdings nichts an der bisherigen Praxis der Verwendung von rechtswidrig erhobenen Daten in Polizei- und Strafverfahrensrecht ändern soll.[810] Theoretisch weitreichende Bedeutung für die Praxis der polizeilichen Informationsverarbeitung hat der Grundsatz der sachlichen Richtigkeit und Aktualität aus § 47 Nr. 4 BDSG. Ob und wie die Polizeien die damit verbundenen Aufwände werden bewältigen können, wird wesentlich über die generelle Qualität und Effektivität des polizeilichen Informationswesens sowie seine Akzeptanz entscheiden. So hat der Fall Amad A. in erschreckender Weise vergegenwärtigt, dass ein nachlässiger Informationsumgang im Extremfall tödlich sein kann: Amad A. war aufgrund einer in ihren Ursachen nicht ganz klaren Verwechslung auf Grundlage von Informationen in polizeilichen Datenbanken inhaftiert worden, wo er unter ungeklärten Umständen in seiner Zelle infolge eines Brands verstarb.[811] Noch expliziter als zuvor im Verfassungsrecht ist nunmehr auch der Grundsatz der Datensicherheit im nationalen Recht festgeschrieben, § 47 Nr. 6 BDSG. Da mit steigender Aussagekraft der gespeicherten Daten die ökonomischen Erwägungen als eine gegenüber der

809 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 601 f.
810 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 596.
811 *Golla*, Der virtuelle Mr. Hyde, 2019.

Datensicherheit zu beachtende Größe in ihrer Bedeutung abnimmt,[812] ist die technologische Fortentwicklung des Informationswesens, die auch eine bessere Nutzbarkeit der Daten mit sich bringt, zunehmend technisch abzusichern. Bisher fehlt auf Ebene des BDSG die Rechenschaftspflicht der für die Datenverarbeitung Verantwortlichen. Da diese dazu verpflichtet, die Einhaltung der Datenschutzgrundsätze laufend nachzuweisen, ist ihre Auslassung im Gesetz mit Blick auf den Aufbau eines internen Datenschutzkontrollsystems problematisch. Zwar lässt sich insoweit die JI-Richtlinie direkt heranziehen, aber der Gesetzgeber unterlässt es auf diese Weise, mittels normativer Leitsterne den Grundstein für eine Kultur der internen Kontrolle als Grundlage für die nach außen zu leistende Rechenschaft zu legen. Eine solche Signalwirkung für die interne Polizeikultur wäre indessen neben dem Ausbau der technischen, organisatorischen und institutionellen Grundlagen für ein internes Datenschutzkontrollregime angezeigt.[813]

II. Normative Verankerungen der Infrastruktur des polizeilichen Informationswesens

Nähert man sich ausgehend von dieser Terminologie und den einfachgesetzlichen Verarbeitungsprinzipien nun den Strukturen und Praktiken, die das polizeiliche Informationswesen ausmachen, so drängt sich zunächst die Frage nach der technischen Infrastruktur der deutschen Polizeien auf. Einen Zugang hierzu bekommt man jedoch nicht „von oben" oder „unten" und auch nicht „vom Anfang" oder gar „Ende", sondern gewissermaßen über die „Mitte". Stellt man sich die polizeiliche Datenverarbeitung als Netzwerk der verschiedenen deutschen Polizeibehörden vor, so ist das Bundeskriminalamt zentraler Knotenpunkt in diesem. Seine Bedeutung innerhalb der deutschen Polizeilandschaft hat in den letzten Jahrzehnten kontinuierlich zugenommen,[814] eine Entwicklung, die auch mit Blick auf die laufende Umgestaltung der polizeilichen Datenbank-Strukturen nicht abgeschlossen zu sein scheint.[815]

812 BVerfGE 125, 260 (326) – Vorratsdatenspeicherung.
813 Siehe näher dazu unten S. 361 ff. sowie S. 536 ff.
814 Siehe dazu etwa *Abbühl,* Der Aufgabenwandel des Bundeskriminalamtes.
815 Im Jahr 2016 hat das BKA seine Zentralstellen-Funktion nach Angaben des BMI aufgrund einer „heterogenen" IT-Verbundarchitektur – gemeint sind in erster Linie zu viele dezentrale Datenbanken mit unzureichend aufeinander abgestimmten Schnittstellen - nur unzureichend ausfüllen können: So waren von 151.000 Woh-

Um die Bedeutung des Bundeskriminalamtes für die polizeiliche Datenverarbeitung zu verdeutlichen, ist in einem ersten Schritt zunächst auf die rechtliche Rahmung der Behörde und insbesondere ihre Zentralstellen-Funktion gem. § 2 BKAG einzugehen, um dann darauf aufbauend die vom Bundeskriminalamt institutionell getragenen, aber auch wesentlich durch die anderen deutschen Polizeibehörden mitgeprägten Infrastrukturen des polizeilichen Informationswesens darzustellen.

I. Die Zentralstellenfunktion des Bundeskriminalamts

Das Bundeskriminalamt unterstützt gem. § 2 BKAG als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung. Damit werden dem Bundeskriminalamt die in Art. 87 Abs. 1 S. 2 GG genannten Aufgaben zugewiesen. Die zuletzt 2018 novellierte Regelung des § 2 BKAG zielt in seiner neuen Form insbesondere auch darauf ab, dem Bundeskriminalamt die erforderlichen Koordinierungs- und Unterstützungsaufgaben hinsichtlich der Polizeien von Bund und Ländern in adäquater Weise möglich zu machen.[816]

a) Verfassungsrechtlicher Inhalt des Zentralstellenbegriffes

Der Begriff der Zentralstelle stammt aus dem Verfassungsrecht, er wird dort aber lediglich einmal, in der eben genannten Vorschrift des Grundgesetztes, erwähnt. Die bereits 1985 von *Ahlf* konstatierte mangelhafte „wissenschaftlich-analytische Durchdringung der Zentralstellenfunktion des BKA"[817] ist bis heute nicht befriedigend geleistet worden. Weder für den Begriff der Zentralstelle noch für den der Zusammenarbeit gem. Art. 87 Abs. 1 S. 2 GG hat sich bisher eine allgemein anerkannte Interpretation durchsetzen können.[818] Einigkeit besteht indessen bezüglich der folgenden Aspekte des verfassungsrechtlichen Zentralstellenbegriffs: Zunächst ist der

---

nungseinbruchsdiebstählen im Jahr 2016 nur 2.100 zentral beim BKA erfasst, vgl. zum Ganzen Bundesministerium des Inneren, Polizei 2020 White Paper, S. 4f.

816 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 1.

817 *Ahlf,* Bundeskriminalamt, S. 2.

818 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.

Zentralstellenbegriff ausschließlich für Bundesbehörden reserviert, wie es sich insbesondere aus dem Systemzusammenhang des Art. 87 Abs. 1 S. 2 GG ergibt. Gegen die naheliegende Bezeichnung der Landeskriminalämter als Zentralstellen auf Landesebene hat sich der Bundesgesetzgeber mit der klaren Formulierung des § 1 Abs. 2 BKAG (§ 3 Abs. 1 S. 1 BKAG a.F.) bewusst entschieden.[819] Wie Bundesoberbehörden verfügen Zentralstellen nicht über einen eigenen Verwaltungsunterbau. Allerdings besitzt die Zentralstelle nicht die vollständige Kompetenz im ihr zugeordneten Aufgabenbereich, das heißt, sie nimmt nicht allein die zugewiesenen Aufgaben wahr. Vielmehr verbleiben auch den Ländern Reste an Verwaltungszuständigkeit.[820] Gerade diese Selbstständigkeit soll der Zentralstellenbegriff wohl ermöglichen. Während der Begriff der „bundeseigenen Verwaltung" in Art. 87 Abs. 1 S. 1 GG nach dem Prinzip der geteilten Verwaltungsräume bei gesetzlicher Einführung einer solchen eine Länderverwaltung auf demselben Gebiet vollständig verdrängt,[821] ermöglicht die Form der Zentralstelle eine „weiche Verknüpfung der Kriminalpolizeien des Bundes und derjenigen der Länder."[822] Insofern lässt sich von einer abgeschwächten Durchbrechung des verfassungsrechtlichen Verbots der Mischverwaltung sprechen.[823] Fraglich bleibt indessen, welche Kompetenzen nun tatsächlich inhaltlich dem Bund in diesem Bereich zugeordnet sind. Klarheit besteht insofern nur bezüglich der informationellen Verklammerung und Koordinierung der Landespolizeibehörden durch die als Zentralstelle eingerichtete Bundesbehörde – also das Bundeskriminalamt – in den Bereichen der Kriminalpolizei und des internationalen Verkehrs. Zudem ist unumstritten, dass die Länder durch die Einrichtung des Bundeskriminalamtes ihre Verwaltungszuständigkeit im Sicherheitsbereich nicht eingebüßt haben.[824]

b) Der Zentralstellenbegriff aus § 2 Abs. 1 BKAG

Von Interesse ist darüber hinaus der einfachgesetzliche Zentralstellenbegriff in der Prägung, die er durch das BKAG erfährt. Für die Zwecke der vorliegenden Untersuchung sind dabei insbesondere diejenigen Aspekte der

819 *Ahlf,* Bundeskriminalamt, S. 53.
820 *Hermes* in *H. Dreier,* Grundgesetz, Art. 87, Rn. 47.
821 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.
822 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.
823 *Ahlf,* Bundeskriminalamt, S. 31 spricht insoweit von „legaler Mischverwaltung".
824 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 3.

Zentralstellenfunktion des Bundeskriminalamtes relevant, die einen Bezug zur Informationsverarbeitung aufweisen.

Das BKAG nennt diesbezüglich zunächst in § 2 Abs. 1 „das polizeiliche Auskunfts- und Nachrichtenwesen". Gegenständlich erfasst werden damit gefahrenabwehr- und strafverfolgungsrelevante Daten sowie ihre Sammlung, Auswertung und Weitergabe.[825] Dabei sollen diese polizeilichen Aufgaben nicht auf das Bundeskriminalamt übertragen, sondern dort koordiniert und informationell verklammert werden, um anderen Polizeibehörden einen effektiven Umgang mit derartigen Informationen zu ermöglichen. Es lässt sich vor diesem Hintergrund auch von einer „Servicefunktion" des Bundeskriminalamtes sprechen. [826] *Ahlf* beschreibt den „typischen Ablauf" im Rahmen dieser „eigentlichen Zentralstellenaufgabe" für die achtziger Jahre, aber prinzipiell wohl immer noch gültig, folgendermaßen:

> „Eine Basiseinheit benötigt bei ihrer konkreten Ermittlungsarbeit eine Information, die überregionalen Bezug hat, so daß die landeseigenen Nachrichtenzentralen, die Zentralstellen im weiten, kriminalistischen Sinne [gemeint sind hier wohl die Landeskriminalämter FB], über diese Information nicht verfügen. Derartige Informationen sind allerdings beim BKA als Zentralstelle vorhanden, weil dieselben durch die Polizeidienststellen der Länder […] zugeleitet worden sind. Das BKA erteilt nun als Zentralstelle die erwünschte Auskunft. Entweder auf den traditionellen Wegen […] oder auf elektronischem Wege."[827]

In seiner Funktion als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen fehlt es dem Bundeskriminalamt indessen – abgesehen von der eingeschränkten Befugnis des § 9 Abs. 1 BKAG – grundsätzlich an Exekutivbefugnissen zur eigenen Erhebung personenbezogener Daten in Fällen, in denen der eigene Informationsbestand das gegebenenfalls indizieren würde.[828] Allerdings verfügt das Amt in seiner Funktion als Strafverfolgungs- und Gefahrenabwehrbehörde mitunter über weitreichende Erhebungsbefugnisse.

Zudem ist das Bundeskriminalamt der Knotenpunkt für die internationale polizeiliche Zusammenarbeit – insbesondere mit Interpol und Europol. In dieser Funktion kann das Bundeskriminalamt Daten aus dem

825 *Hermes* in *H. Dreier,* Grundgesetz, Art. 87, Rn. 50.
826 *Bäcker,* Terrorismusabwehr, S. 23.
827 *Ahlf,* Bundeskriminalamt, S. 409.
828 Ausführlicher hierzu siehe *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 6 ff.

Ausland anfordern und auf Anforderungen aus dem Ausland reagieren.[829] Insgesamt ist die Zentralstellenfunktion des Bundeskriminalamtes im Laufe der Jahre immer relevanter geworden.[830] Neben einer Gesetzesnovellierung von 1997, die die informationellen Regelungen erweitertet hat,[831] sieht *Bäcker* den Grund hierfür insbesondere im Wandel des polizeilichen Aufgabenprofils, das heute neben Strafverfolgung und Gefahrenabwehr in konkreten Fällen vor allem auch übergreifende Präventionsmaßnahmen beinhaltet, die regelmäßig eine möglichst breiten Informationsbasis benötigen. Daneben sind auch Fortschritte in der Informationstechnologie ausschlaggebend: Daten können sehr leicht aus ihren bisherigen Kontexten gelöst und für neue Zwecke mit anderen Daten kombiniert werden. Wegen der Erfahrung des Bundeskriminalamtes bei der Wahrnehmung zentraler informationeller Aufgaben und der bereits vorhandenen Technik, lag und liegt es weiterhin nahe, die Behörde mit der Erfüllung dieses neuen Aufgabenprofils (zumindest mit) zu betrauen.[832]

c) Formen der Ausübung der Zentralstellenfunktion aus § 2 BKAG

Die Essenz der Zentralstellenfunktion des Bundeskriminalamts ist der in § 2 Abs. 3 BKAG geregelte „polizeiliche Informationsverbund", also eine Vernetzung innerhalb der Sicherheitsarchitektur,[833] zu dessen Unterhaltung die Norm das Bundeskriminalamt verpflichtet und berechtigt. Dieses Verbundsystem ist ein Kernstück der alten wie neuen IT-Architektur des Bundeskriminalamtes.[834] Die genauere Ausgestaltung des nur losen normativen Programms des § 2 Abs. 3 BKAG erfolgt über das Gesetz verteilt und wird aufgrund seiner integralen Bedeutung im Anschluss dargestellt.[835]

In diesem Kontext ebenfalls von Bedeutung ist die Unterhaltung zentraler Einrichtungen und Sammlungen nach § 2 Abs. 4 BKAG, die gemäß Satz 2 der Norm elektronisch geführt werden können, was heute auch über-

829 *Bäcker,* Terrorismusabwehr, S. 23.
830 *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 3.
831 BGBL. I 1997, S. 1650.
832 *Bäcker,* Terrorismusabwehr, 24 f.
833 *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 9.
834 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 4.
835 Siehe dazu unten S. 226 ff.

wiegend der Fall ist.[836] Für die zentralen – also erkennungsdienstlichen sowie die Fahndung nach Personen und Sachen betreffenden – Einrichtungen und Sammlungen gilt nicht die Einschränkung, dass es um Straftaten mit länderübergreifender und internationaler oder erheblicher Bedeutung gehen muss.[837] Tätigkeiten in diesem Bereich der Zentralstellenfunktion des Bundeskriminalamtes umfassen unter anderem die Koordinierung der Polizeien des Bundes und der Länder, die Bereitstellung von Personen und Sachen sowie „kreative Mitgestaltung i.S.v. informationeller Mitwirkung und Förderung eines konkreten Ermittlungsverfahrens einer Polizeibehörde" etwa in Form von Analysen und Auswertungen.[838] Die zentralen Einrichtungen und Sammlungen sind integrale Bestandteile des polizeilichen Informationswesens, gestalten es also näher inhaltlich aus.

Neben diesen strukturellen Vorgaben erfolgt die Wahrnehmung der Zentralstellenaufgaben des Bundeskriminalamtes gem. § 2 Abs. 2 BKAG in praktischer Hinsicht durch die Sammlung und Auswertung aller hierfür erforderlichen Informationen (Nr. 1) und die unverzügliche Unterrichtung der Strafverfolgungsbehörden des Bundes und der Länder über die sie betreffenden Informationen und die in Erfahrung gebrachten Zusammenhänge von Straftaten (Nr. 2).

Erfasst werden dabei Informationen jeder Art, unabhängig von dem Medium der technischen Übermittlung. Neben verkörperten Informationen (etwa Akten oder Ähnliches) sind insbesondere auch mittels elektronischer Datenverarbeitung übermittelte Informationen gemeint.[839] Inhaltlich geht es vor allem um Informationen, die für eine zentrale Auswertung zur Verhütung und Verfolgung von Straftaten mit erheblicher Bedeutung geeignet und erforderlich sind.[840] „Hierzu", so heißt es in der Gesetzesbegründung, „zählen auch Informationen, die als solche noch nicht von länderübergreifender und internationaler oder erheblicher Bedeutung sind. Es reicht aus, daß sie im Zusammenhang mit anderen Informationen der Zentralstelle diese Qualität erreichen können."[841] Damit wird die inhaltliche Begrenzung der Übermittlungsmöglichkeiten in nicht unerheblicher Weise abge-

836 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 41; *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 61.
837 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 37.
838 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 37f.
839 *Ahlf,* Bundeskriminalamt, S. 294.
840 Zu den sonstigen Informationen siehe *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 32.
841 BT-Drs. 13/1550, S. 21.

schwächt, da sich argumentieren ließe, dass zu übermittelnde Daten erst durch Kombination mit den Informationsbeständen der Zentralstelle eine entsprechende Bedeutung erlangen werden, zumal die Bestimmung unter die polizeiliche Deutungsmacht fällt und nur begrenzt einer rechtlichen Überprüfung offensteht.

Der Begriff des „Sammelns" ist in seinem Gehalt etwas ambivalent: Neben der passiven Entgegennahme fremderhobener Informationen, etwa durch die Landeskriminalämter, also dem sogenannten „passiven Sammeln" könnte auch das „aktive Sammeln", also die Erhebung von Informationen aufgrund eigeninitiativer (exekutiver) Maßnahmen, erfasst sein.[842] Das Amt ist für die Koordination im polizeilichen Informationsverbund zuständig und grundsätzlich kein exekutives Ermittlungsorgan.[843] Zwar dürfte nach wie vor als Konsens gelten, dass mit dem Bundeskriminalamt gerade keine große Behörde zur bundesweiten Informationsbeschaffung kreiert werden sollte.[844] Ob allerdings seine Informations*verarbeitungs*funktion nach wie vor die allein dominierende im bundeskriminalamtlichen Aufgabenspektrum ist, darf bezweifelt werden. Vor dem Hintergrund der durchaus weitreichenden Datenverarbeitungsbefugnisse, die an die §§ 4, 5 BKAG geknüpft sind, erscheint das alte Konzept vom Bundeskriminalamt zunehmend in Richtung der Idee einer aktiveren, im klassischen Sinne polizeilich agierenden, Behörde verschoben zu haben, die sich zusätzlich aber durch eine starke Informationsmacht auszeichnet.

Insofern muss dem Begriff des „Sammelns" auch ein aktiver Gehalt zugeschrieben werden. So soll „Sammeln" in der Funktion des Bundeskriminalamtes als Zentralstelle auch in begrenztem Rahmen die aktive Informationsbeschaffung insoweit erlauben, wie es im Befugnisteil geregelt ist.[845] Diese, einer Gesetzesbegründung von 1995 entnommene, Interpretation des „Sammeln"-Begriffes nimmt auf den inzwischen geänderten § 7 Abs. BKAG Bezug, der die Erhebung von personenbezogenen Daten bei den Polizeien des Bundes und der Länder sowie bei anderen öffentlichen und nicht-öffentlichen Stellen regelte.[846] Die Norm ist vor allem im neugeschaffenen § 9 BKAG aufgegangen. Mit Blick auf die zusätzlichen Befugnisse im Rahmen der Strafverfolgung (§§ 34 ff. BKAG) und insbesondere zur

842 *Ahlf,* Bundeskriminalamt, S. 310.
843 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 33.
844 *Ahlf,* Bundeskriminalamt, S. 313.
845 BT-Drs. 13/1550, S. 21f.
846 BT-Drs. 13/1550, S. 7.

Abwehr von Gefahren des internationalen Terrorismus (§§ 38 ff. BKAG) ist allerdings von einer untergeordneten Rolle des aktiven Sammelns von Informationen im Aufgabenspektrum des Amts kaum mehr zu sprechen, wobei nicht ganz klar ist, wie Daten aus diesen Maßnahmen in die Erfüllung der Zentralstellenfunktion hineinspielen. Insgesamt bedeutet „Sammeln" i.S.d. § 2 Abs. 2 BKAG zumindest die Entgegennahme von fremderhobenen Informationen und ihre systematische Aufbewahrung.[847] Der aktive Gehalt des Begriffes umfasst indessen nur die Erhebung von Informationen zur Ergänzung bereits vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung mittels Auskünften oder Anfragen bei öffentlichen und nichtöffentlichen Stellen, soweit dies zur Erfüllung der Zentralstellenaufgabe aus § 2 Abs. 1 BKAG erforderlich ist.[848]

In seinem Begriffsgehalt klarer ist dagegen der Begriff des „Auswertens". Es handelt sich um ein „analytisch-intellektuelles" Verfahren, d.h. eine Bewertung und Interpretation von beim Bundeskriminalamt (oder den Landeskriminalämtern[849]) vorhandenen Informationen, bei dem „die anfallenden Informationen nach kriminalistischen Gesichtspunkten sortiert und verglichen werden müssen, um ihre Bedeutung und ihren Informationswert für die Verbrechensbekämpfung intensiv auszuloten."[850] Dabei können die Bedeutung und Informationswert auch nur marginale Relevanz haben.[851]

Zusätzlich wird die Zentralstellenfunktion des Bundeskriminalamtes noch durch die Unterrichtung der Strafverfolgungsbehörden wahrgenommen. Strafverfolgungsbehörden im Sinne des § 2 Abs. 2 Nr. 2 BKAG sind entsprechend der Aufgabenstellung des Bundeskriminalamtes Staatsanwaltschaft und Polizei, wobei eine Pflicht zur Unterrichtung der Staatsanwaltschaft nur dann besteht, wenn das Bundeskriminalamt bereits in Erfahrung bringen konnte, welche Staatsanwaltschaft die Ermittlungen leitet. Häufiger wird vermutlich die zuständige Polizeibehörde bekannt sein, sodass es seltener einen Informationsfluss zur Staatsanwaltschaft geben dürfte. Dementsprechend hat das Amt nur spezielle Erkenntnisse über bestimmte Täter

847 *Ahlf,* Bundeskriminalamt, S. 314.
848 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 33; *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 42.
849 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 34.
850 *Hessel* zitiert nach *Ahlf,* Bundeskriminalamt, S. 316.
851 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 34 spricht insofern von einer Relevanz „auch nur als Mosaikstein".

und Taten zu übermitteln, nicht dagegen „bloße Routinenachrichten" und „massenstatistisches Material".[852]

Die Zentralstellenfunktion des Bundeskriminalamts verändert sich hingegen nicht bloß durch den Wandel der Aufgaben der Behörde, sondern auch ganz unmittelbar. So hat § 2 Abs. 5 BKAG, der ursprünglich nur die Unterstützung der Polizeien der Länder durch das Bundeskriminalamt bei der Datenverarbeitung regelt, infolge der Novellierung des BKAG Änderungen erfahren. Ziel dieser Neuerungen war, das Bundeskriminalamt nach dem Vorbild Europols umzugestalten, also insbesondere seine Stellung als zentraler Dienstleister der Polizeien des Bundes und der Länder auszubauen.[853] Für die hier untersuchten Bereiche des polizeilichen Informationswesens sind vor allem § 2 Abs. 5 S. 1 Nr. 4 und § 2 Abs. 5 S. 2 BKAG erwähnenswert: Satz 1 Nr. 4, der weiterhin die Unterstützung der Länder bei der Datenverarbeitung regelt, ist etwas Selbstverständliches für elektronische Informationsverbünde, da solche Abstimmung und Kooperation erfordern. Die Zentralstelle bestimmt dabei prinzipiell die technischen Standards an denen sich die Bundesländer dann zu orientieren haben.[854] Satz 2 der Vorschrift gestattet schließlich in ausgewählten Fällen (§ 2 Abs. 5 Satz 1 Nr. 3 und 4 BKAG) eine Auftragsverarbeitung personenbezogener Daten durch das Bundeskriminalamt. Dabei sieht sich die Regelung Kritik ausgesetzt: Im Rahmen der Auftragsverarbeitung erfolgt keine Datenübermittlung, sondern nur eine Weitergabe der Daten (Art. 9 DSRL-JI; § 62 BDSG 2017/2018). Es werden von Seiten des Verantwortlichen Verarbeitungsaufgaben an den Auftragsverarbeiter delegiert, der die dabei übertragenen Daten in der Regel nur im Rahmen der Weisungen des Verantwortlichen verwenden darf (Art. 23 DSRL-JI). Bedenklich ist es insoweit, wenn das Bundeskriminalamt eine solche Auftragsverarbeitung für Länderpolizeien betreibt und davon Daten erfasst werden, die aus verfassungsrechtlichen Gründen nur auf Länderebene verarbeitet werden dürfen. Solche nicht bundesweit relevanten Daten können die von den jeweiligen Gesetzgebern festgelegte Aufgabenverteilung zwischen Bundes- und Länderpolizeien unter dem „Etikett der Auftragsverarbeitung" unterlaufen. *Petri* plädiert insofern dafür, § 2 Abs. 5 S. 2 BKAG Ausnahmecharakter zuzuerkennen.[855] Für *Barczak* kommt dieser Charakter schon dadurch zum Ausdruck, dass das BKA hier

852 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 35.
853 BT-Drs. 18/11163, S. 85.
854 So *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 47.
855 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 487f.

zum einen nicht eigeninitiativ, sondern nur auf ein entsprechendes Ersuchen und bei einer grundsätzlichen Pflicht zur Kostenerstattung hin tätig würde und sich zum anderen § 2 Abs. 5 S. 2 BKAG nach der ursprünglichen Intention des Normgebers von vorneherein auf Fälle beschränkt, in denen allein die Datenverarbeitungsanlagen und -anwendungen des BKA eine sachgerechte Verarbeitung der erhobenen Daten erwarten ließen.[856] Das mag zutreffen, nichtsdestotrotz begünstig diese normative Konstruktion eine weitere Aufwertung der informationellen Bedeutung und Kompetenzen des Bundeskriminalamts im polizeilichen Informationsverbund und forciert damit eine (weitere) Zentralisierung von Datenbeständen, wie es letztlich auch explizit als sicherheitspolitisches Projekt geplant ist.[857]

Schließlich hält auch Absatz 6 des § 2 BKAG für die vorliegende Untersuchung noch erwähnenswerte Aspekte bereit. Neben § 2 Abs. 6 Nr. 4 BKAG, der das Bundeskriminalamt verpflichtet, die technischen und organisatorischen Vorkehrungen zur Erfüllung der Datenschutzgrundsätzen zu treffen, ist vor allem Nr. 1 der Vorschrift von Bedeutung. Die Erstellung von strategischen und operativen kriminalpolizeilichen Analysen, Statistiken und Lageberichten sowie die dafür erforderliche Beobachtung und Auswertung der Kriminalität sind stark auf Datensammlungen und -verarbeitungen angewiesen. Es geht dabei vorrangig um die Identifizierung von Kriminalitätsphänomenen aller Art, um so insbesondere die Verhütung künftiger Straftaten zu ermöglichen.[858] Ein wesentlicher Teil der Zentralstellenaufgabe bezieht sich auf die allgemeine Auswertung und Analyse der gesammelten Informationen in operativer und strategischer Hinsicht; nur so kann das „unverzichtbare Hintergrundwissen" generiert werden, das zur Aufschlüsselung und kriminalstrategischen Bearbeitung der unterschiedlichen Kriminalitätsfelder notwendig ist. Dem Präsidenten des Bundeskriminalamtes, *Münch*, zufolge, gilt (auch) hier das Gebot, „aus bereits vorhandenen Daten die größtmögliche Aussagekraft für die polizeiliche Arbeit zu extrahieren und dieses Wissen mit anderen Polizei- und Sicherheitsbehörden zu teilen."[859] Vor dem Hintergrund des Massendatenparadigmas, nach dem vor allem schon bestehende große Datenbestände für noch granularere Einsichten angereichert werden sollen, ist anzunehmen, dass die zentrale

856 *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 73.
857 Siehe dazu unten S. 271 ff.
858 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 2 BKAG Rn. 52; *Barczak* in *Barczak* (Hrsg.), BKAG, § 2 Rn. 79.
859 *Münch*, A-Drs. 18(4)806 C S. 4.

Rolle des Bundeskriminalamtes im polizeilichen Informationswesen weiter an Bedeutung gewinnen wird.

2. Informationsverbund und Informationssysteme

Die tatsächlichen Strukturen des polizeilichen Informationswesens sind vor allem im BKAG auch teilweise rechtlich abgebildet. Mit der Novellierung des Gesetzes wurde hingegen, neben der Reaktion auf das BKAG-Urteil des Bundesverfassungsgerichts, auch die grundlegende Überarbeitung des Informationswesens angestoßen.[860] Die Entwicklung hin zu einem einheitlichen Verbundsystem mit zentraler Datenhaltung beim Bundeskriminalamt (sog. „gemeinsames Datenhaus der deutschen Polizei") ist weder technisch noch organisatorisch abgeschlossen.[861] Die folgenden Ausführungen sind daher nur eine Momentaufnahme in einem stark unter Wandlungsdruck stehenden System der polizeilichen Informationsverarbeitung. Nichtsdestotrotz scheinen mit der Neufassung des BKAG die normativen Rahmenbedingungen für die neue Informationsarchitektur auf mittelfristige Sicht gesetzt zu sein, da ein originärer gesetzgeberischer Wille für weitere Reformen gegenwärtig nicht vorhanden scheint. Insofern können die einschlägigen Vorschriften des BKAG als Grundlage für eine weitere Annäherung an das polizeiliche Informationswesen dienen. Zusätzlich werden hier im Zusammenhang mit den jeweiligen technischen Komponenten des Informationssystems rechtstatsächliche Aspekte dargestellt, weil sich nur über diese überhaupt die Bedeutung der jeweiligen Systeme, Dateien und so weiter erfassen lässt.

Wie bereits beschrieben trifft das Bundeskriminalamt im Rahmen der Zentralstellenfunktion aus § 2 Abs. 3 BKAG die Pflicht, einen einheitlichen polizeilichen Informationsverbund zu unterhalten. Diese Pflicht wird durch die §§ 29-31 BKAG näher ausgestaltet. An diesem Informationsverbund nimmt das Bundeskriminalamt wiederum gem. § 13 Abs. 1 BKAG mit seinem eigenen Informationssystem teil. Auch die übrigen Bundes- und Länderpolizeien unterhalten je eigene Informationssystemtypen für unterschiedliche polizeiliche Aufgabenfelder.

860 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G, Rn. 390.
861 Bundesministerium des Inneren, Polizei 2020 White Paper, S. 2, 11.

a) Der gegenwärtige Wandel des polizeilichen Informationsverbundes

Hauptelement des einheitlichen polizeilichen Informationsverbundes ist INPOL, das „polizeiliche Informationssystem",[862] wobei es sich um das gemeinsame, arbeitsteilige, elektronische Informationsverbundsystem der Polizeien des Bundes und der Länder zur Unterstützung vollzugspolizeilicher Aufgaben handelt, in dem informationstechnische Einrichtungen des Bundes und der Länder in einem Verbund zusammenwirken.[863] Während INPOL im neuen Gesetz auf § 29 BKAG fußen sollte, wurden alle beim Bundeskriminalamt bestehenden Dateien,[864] die INPOL derzeit ausmachen, auf nicht mehr geltenden Rechtsgrundlagen errichtet,[865] die den neuen Anforderungen an den Grundsatz der hypothetischen Datenneuerhebung und den damit verbundene Kennzeichnungspflichten nicht entsprechen.[866]

Die in INPOL vorgehaltenen Datenbestände sind (gegenwärtig noch) überwiegend in Dateien und Verarbeitungssystemen organisiert.[867] Es gliedert sich in ein zentrales System, INPOL-Z, das den zentralen Datenbestand enthält, und die Teilnehmersysteme, INPOL-Bund bzw. INPOL-Land (die INPOL-Land-Systeme haben mitunter Eigennamen), mit denen die Daten abgerufen und eingegeben werden können.[868] Dies soll im Zuge des IT-Großprojekts *Polizei 2020* unter anderem stark modifiziert werden, indem ein gemeinsamer Datenbestand mit verschiedenen Zugriffsrechten geschaffen werden soll.[869] In der ursprünglichen Konzeption, die INPOL durch die Ständige Konferenz der Innenminister und -senatoren der Län-

862 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 1.
863 BT-Drs. 13/1550, S. 28.
864 Unterschieden wird zwischen Amts- Zentral- und Verbunddateien. Verbunddateien sind solche Dateien im INPOL, in die die verschiedenen Teilnehmer in eigener Zuständigkeit dezentral Daten eingeben und abrufen können. Zentraldateien sind hingegen solche Dateien, die das Bundeskriminalamt führt und mit von anderen Polizeien im Rahmen seiner Zentralstellenfunktion angelieferten Daten befüllt, woraufhin diese Daten dann von beteiligten Stellen abgerufen werden können. Amtsdateien sind schließlich solche Dateien, die das Bundeskriminalamt zur Erfüllung der eigenen Aufgaben unterhält und worauf keine anderen Stellen Zugriff haben, siehe dazu Graulich in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 13 BKAG Rn. 2 ff.
865 BT-Drs. 19/15346, S. 3.
866 Siehe dazu auch unten S. 320 ff.
867 *Petri* in: *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 390.
868 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1199.
869 Siehe dazu unten S. 271 ff.

der (IMK) im Jahre 1990 in Form der „INPOL-Grundsätze" erhalten hatte, gehörten im Wesentlichen die Personen- und die Sachfahndung, der Kriminalaktennachweis, die Haftdatei, der Erkennungsdienst und die Daktyloskopie, Arbeitsdateien für besondere Kriminalitätsbereiche (PIOS[870]) Hinweis-/Spurendokumentation in Ermittlungsverfahren von länderübergreifender Bedeutung (SPUDOK) sowie die Polizeiliche Kriminalstatistik zum Verbund.[871] Das gegenwärtig in Betrieb befindliche polizeiliche Informationssystem, genannt INPOL-neu,[872] ist 2003 an den Start gegangen und weist gegenüber seinem Vorgänger einige Modifikationen auf.[873]

Normative Anknüpfungspunkte hierfür bietet indessen weniger das BKAG als vielmehr die erst[874] 2010 in Kraft getretene BKADV.[875] Diese ursprünglich auf Grundlage von § 7 Abs. 11 BKAG a.F. erlassene Verordnung gilt auch nach der Novellierung des BKAG weiterhin.[876] Sie dient der Konkretisierung der Datenarten und Dateiformen, die im polizeilichen Informationswesen verarbeitet und errichtet werden dürfen.[877] Problematisch ist in diesem Zusammenhang indessen der Umstand, dass die BKADV in ihrem Wortlaut noch immer auf die vorherige Fassung des BKAG verweist, obwohl im Normtext teils erhebliche Veränderung vorgenommen wurden. Es fehlt insoweit an einem „Übersetzungsschlüssel", der die BKADV für künftige Weiterverarbeitung von personenbezogenen Daten handhabbar macht.[878] Es ist zwar grundsätzlich denkbar, im Wege der Auslegung mit

870 PIOS steht für „Personen – Institutionen – Objekte – Sachen".

871 BT-Drs. 13/1550, S. 28; so auch *Zöller,* Informationssysteme, S. 140 ff.; zu weiteren damaligen Anwendungen im Bereich elektronischer Datenverarbeitung vgl. *Zöller*, a.a.O., S. 147.

872 In Abgrenzung zu „INPOL-aktuell", vgl. *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 8.

873 Siehe zu der diesbezüglichen historischen Entwicklung bereits oben S. 131 ff.

874 Zum langen Streit um die BKADV siehe *Kehr,* Datei Gewalttäter Sport, S. 191 ff. mwN.

875 *Spiecker gen. Döhmann/Kehr* Deutsches Verwaltungsblatt 2011, 930.

876 Einerseits ist anerkannt, dass das nachträgliche Erlöschen oder auch nur die nachträgliche Änderung ohne Einfluss auf den Rechtsbestand einer ordnungsgemäßen Rechtsverordnung ist, vgl. BVerfG, Beschluss vom 23. März 1977 – 2 BvR 812/74, Rn, 26; *Graulich,* Die Zustimmungsbedürftigkeit der Aufhebung, Verlängerung und Änderung von Gesetzen und Rechtsverordnungen, S. 146. Zudem trat aber gem. Art. 13 Abs. 2 des Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes v. 1.6.2017 I 1354 der neue § 20 BKAG bereits am Tag nach Verkündung in Kraft.

877 *Tetzlaff* Verwaltungsrundschau (vr) 57 (2011), 403.

878 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 20 BKAG Rn. 6.

der BKADV zu arbeiten,[879] schon zur Klarstellung und damit auch besseren Rechtswendung wäre indessen der Erlass einer angepassten BKADV dringend erforderlich.[880] Zudem hat das Bundesverwaltungsgericht bereits 2010 festgestellt, dass die Datenerhebung und -speicherung in den Dateien grundsätzlich so lange unzulässig ist, wie es an einer Rechtsverordnung i.S.d. § 7 Abs. 11 (vormals § 7 Abs. 6) BKAG a.F. fehlte.[881] Zwar ist fraglich, ob man die bis dato unterlassene Anpassung mit einem kompletten Fehlen gleichsetzen kann. Mit Blick auf das Urteil des Bundesverwaltungsgerichts zur Vorgängervorschrift der Verordnungsermächtigung des § 20 BKAG ließe sich das durchaus annehmen.[882] Das Untätigbleiben des Verordnungsgebers lässt sich aber vor allem auch als Sinnbild für das Verhältnis zwischen dem normativem Steuerungsanspruch des Rechts der polizeilichen Informationsverarbeitung und den faktischen Organisations- und Wirkweisen des polizeilichen Informationssystems lesen. Was faktisch getan wird, wird entweder in nicht unerheblichem Maße überhaupt nicht vom Recht erfasst oder findet in diesem in eher deskriptiver Weise seinen Niederschlag. Trotz des Stellenwertes, den Daten im gesellschaftlichen Bewusstsein mittlerweile haben, ist die BKADV weder mit Erlass des BKAG, noch zum geplanten Termin, Mitte 2020,[883] angepasst worden. Mit Blick auf den Umstand der geplanten Auflösung der Dateienstruktur scheinen die Anpassungsbedarfe zudem nicht lediglich redaktioneller Art zu sein. Zwar scheint es schon länger einen Entwurf zu geben,[884] der aber, soweit ersichtlich, nicht öffentlich zugänglich ist.

Die folgenden, an der BKADV orientierten Darstellungen der einzelnen INPOL-Bestandteile sind vor diesem Hintergrund zu lesen. Auch ist die normative Grundlage trotz der dazu in der BKADV enthaltenen Vorschrif-

879 So etwa die Wissenschaftliche Dienste des Bundestages, vgl. WD 3 - 3000 - 063/19, S. 6, Fn. 8.

880 Anders hingegen *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 20 BKAG Rn. 6, der die Umstellungen des neuen BKAG für so gravierend hält, „dass jedes Bemühen, mit einer sinnvollen Gesetzesauslegung den fehlenden Übersetzungsschlüssel ersetzen zu wollen, scheitern muss."; vgl. auch *Schenke/Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Einf. Rn. 4: „Die ehemalige BKADV bezieht sich auf das alte BKAG und hat deshalb keine Funktion mehr."

881 BVerwGE 137, 113-123, Rn. 20.

882 So *Bäcker*, A-Drs. 18(4)806 D, S. 4 Fn. 9.

883 Dieser Termin wurde dem Verfasser in einer schriftlichen Anfrage beim BMI genannt.

884 *Schenke/Graulich/Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Einführung A. Rn. 4.

ten schmal. Die Dateien werden nur knapp mit ihren Zweckausrichtungen benannt. Technische Strukturen, wie das ansatzweise für den polizeilichen Informationsverbund mit dem neuen BKAG geschaffen wurde, finden sich für die Dateien in der BKADV nicht. Hier hat also die normative Kraft des Faktischen einen weiten Wirkraum. Zudem ist sich immer zu vergegenwärtigen, dass die alte Dateienstruktur der Verrechtlichung der polizeilichen Informationsverarbeitung zeitlich vorgelagert ist, sodass sich neue Gesetze eher nach den bestehenden Strukturen als umgekehrt gerichtet haben und richten. Zu betonen ist in diesem Zusammenhang zudem, wie es auch die Verordnungsbegründung wiederholt tut, dass die Rechtsverordnung nicht die Voraussetzungen, unter denen die Daten im Einzelfall im Informationsverbund des Bundeskriminalamtes erfasst werden dürfen, definiert. Dies richtet sich nach wie vor nach den konkreten polizei- und strafverfahrensrechtlichen Erhebungsvorschriften.[885]

b) Komponenten von INPOL

aa) INPOL-Z und INPOL-Bund bzw. -Land

INPOL-Z ist nicht explizit geregelt. Rechtsgrundlage ist § 11 BKAG a.F. in Verbindung mit § 91 BKAG.[886] Enthalten sind die Grunddaten zur Person, die Fahndungsdateien, der zentrale Kriminalaktennachweis (KAN), erkennungsdienstliche Daten, personengebundene- und ermittlungsunterstützende Hinweise (PHW, EHW) sowie weitere Daten zu den gespeicherten Personen, womit es sich um die wesentliche technische Infrastruktur für den Datenaustausch der deutschen Polizeien handelt.[887] Dies ergibt sich auch nur mittelbar aus der BKADV, die „INPOL" als Bezeichnung aber nicht explizit nennt. Obwohl INPOL auf alten Rechtsgrundlagen errichtet wurde, richten sich Funktionsweise für alle Daten, die nicht unter die zweifelhafte Regelung des 91 BKAG[888] fallen, nunmehr nach den geltenden Bestimmungen des BKAG, sodass die Arbeit mit den größtenteils noch alten Komponenten, wie sie zuvor durch die alte Rechtslage angeleitet

885 Etwa BR-Drs. 329/10, S. 15.
886 BT-Drs. 19/15346, S. 3.
887 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1204.
888 Siehe dazu unten S. 275 ff.

wurde, nun mit der gegenwärtigen Rechtslage zum Informationsverbund in Übereinklang gebracht werden muss.

Der polizeiliche Informationsverbund dient gem. § 29 Abs. 2 Satz 1 BKAG der Erfüllung der in § 13 Abs. 2 BKAG genannten Grundfunktionen.[889] Teilnehmende Stellen können gemäß § 29 Abs. 3 Satz 1 BKAG neben dem Bundeskriminalamt und seinen Länderpendants prinzipiell alle sonstigen Polizeibehörden auf Bundes- und Landesebene sein, wobei das Bundeskriminalamt wegen der Parallelität der Grundfunktionen in seinem Informationssystem und im Informationsverbund „strukturbestimmend" ist.[890]

Die Grundfunktionen, zumal nur Regelbeispiele polizeilicher Tätigkeit bezüglich der Verarbeitung von Informationen, erlauben die Nutzung des Informationsverbundes in wenig beschränkter Weise. Eine strikte Zweckbindung sähe anders aus. Neben verfassungsrechtlichen Bedenken ergeben sich auch mit Blick auf die JI-Richtlinie Probleme: Während es sich bei den Grundfunktionen jeweils um strafjustizielle Zwecke im Sinne des Art. 1 Abs. 1 JI-Richtlinie handelt, fordert Art. 4 Abs. 1 lit. b JI-Richtlinie bei einer Verarbeitung zu neuen Zwecken, dass diese „festgelegt und eindeutig" sind, was als Zweckänderung nach verfassungsrechtlichen Vorgaben „hinreichend spezifische Verarbeitungsanlässe erfordert."[891]

In den Informationsverbund sollen – man muss wohl aufgrund des Umsetzungsgrades von *Polizei 2020*[892] sagen: zukünftig – nicht mehr Dateien, sondern Daten einbezogen werden, was Ausdruck des nunmehr gegenüber der technischen Zusammenfassung in Dateien vorrangigen Themenbezuges der Daten sein soll. So sollen etwa Dateien zur Personen- und Sachfahndung als abgegrenzte Datensilos im Informationsverbund wegfallen. Personen- und sachfahndungsrelevante Informationen würden jedoch weiterhin, entsprechend gekennzeichnet, bestehen und dann ohne ihre dateiförmige Strukturierung in die zentrale Datenbank des Bundeskriminalamtes eingestellt,[893] wo sie dann im Wege eines Rechte- und Rollenkonzepts

889 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 969; *Barczak* in *Barczak* (Hrsg.), BKAG, § 29 Rn. 11.
890 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 13 BKAG Rn. 1.
891 Vgl. *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 969 in Bezug auf BVerfGE 141, 220, 328 – Bundeskriminalamtgesetz.
892 Siehe dazu unten S. 465 ff.
893 BT-Drs. 18/11163, S. 109.

für verschiedene Akteur:innen in der Polizei unterschiedlich verfügbar wären.[894]

Ihre wesentliche Eingrenzung erfahren die im Informationsverbund zur Weiterverarbeitung zugelassenen Daten durch das Kriterium der „Verbundrelevanz" nach § 30 Abs. 1 BKAG. Das Kriterium, dem eine Schlüsselstellung im Verbund zukommt,[895] hat zwei Funktionen: Einerseits dient es dem Schutze des Informationsverbundes vor Überfrachtung mit irrelevanten Daten und soll so die Effektivität des Verbundes unterstützen. Vorbild für den Begriff der Relevanz im normativen Sinne war dabei das Recht der Nachrichtendienste, insbesondere § 5 Abs. 3 Satz 2 Nr. 1 BVerfSchG. Wie diese Norm findet auch in § 30 Abs. 1 BKAG eine Konkretisierung der datenschutzrechtlich stets zu beachtenden Erforderlichkeit statt, um durch die im Verbund aufgestellten, strikt einzuhaltenden Relevanzkriterien den Informationsfluss zu verbessern.[896] Andererseits soll mit der „Verbundrelevanz" die künftige, durch die Umstrukturierung der polizeilichen Informationsarchitektur bewirkte Irrelevanz des Instruments der Errichtungsanordnung kompensiert werden.[897]

Gemäß § 29 Abs. 3 BKAG haben die am polizeilichen Informationsverbund teilnehmenden Stellen das Recht, Daten zur Erfüllung der Verpflichtung nach § 32 BKAG im automatisierten Verfahren einzugeben und, soweit dies zur jeweiligen Aufgabenerfüllung erforderlich ist, abzurufen. Bisher wurde in Errichtungsanordnungen festgelegt, welcher Teilnehmer in welchem Umfang in welcher Datei personenbezogene Daten eingeben und abrufen darf.[898] Aufgrund des Wegfalls[899] der Errichtungsanordnungen für weite Teile des polizeilichen Informationsbestandes beim Bundeskriminalamt kommt es somit für die Eingabe auf die Verpflichtung nach § 32 BKAG sowie für den Abruf auf die jeweilig rechtlich bestimmten Aufgaben der einzelnen teilnehmenden Stellen an.[900] Dieses Berechtigungserfordernis soll gem. § 29 Abs. 4 Satz 1 BKAG vom Bundeskriminalamt

894 *Bundesministerium des Innern*, Polizei 2020.
895 *Barczak* in *Barczak* (Hrsg.), BKAG, § 30 Rn. 1.
896 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 30 BKAG Rn. 2, 4.
897 BT-Drs. 18/11163, S. 110.
898 BT-Drs. 13/1550, S. 28.
899 Da die Dateienstruktur aufgegeben wird, fällt auch das Instrument der Errichtungsanordnung auf langfristige Sicht weg. Diese Lücke soll unter anderem durch die unionsrechtlich vorgeschriebenen Datenschutzinstrumente aufgefangen werden, siehe dazu unter S. 361 ff.
900 *Barczak* in *Barczak* (Hrsg.), BKAG, § 32 Rn. 20.

durch organisatorische und technische Maßnahmen sichergestellt werden. Der Gesetzesbegründung zufolge ersetzt diese Vorschrift den § 11 Abs. 2 Satz 2 BKAG a.F., der aufgrund des Wegfalls der Errichtungsanordnungen überflüssig wird.[901] Diese Verpflichtung des Bundeskriminalamtes zur Implementierung organisatorischer und technischer Sicherungsmaßnahmen kompensiert letztlich ebenfalls die Abnahme normativer Konturen der polizeilichen Datenbestände. Über § 29 Abs. 4 Satz 2 BKAG gelten zudem die auch für das Bundeskriminalamt geltenden Verarbeitungsbestimmungen, insbesondere der Grundsatz der hypothetischen Datenneuerhebung sowie die zu seiner Implementierung erforderliche Kennzeichnung für die Datenspeicherung im Informationsverbund,[902] für alle anderen Teilnehmer des Verbundes.[903]

Aufgrund des Zusammentreffens verschiedener Datenquellen im Informationsverbund, muss die Befugnis zur Verarbeitung jedes einzelnen Datums festgelegt sein. Dies geschieht durch § 29 Abs. 5 BKAG. Dessen Satz 1 statuiert, dass nur diejenige Behörde, die die Daten eingegeben hat, befugt ist, diese zu ändern, zu berichtigen oder zu löschen. Dabei handelt es sich um das sogenannte Besitzerprinzip.[904] Als Besitzer gilt diejenige Stelle, die die Daten in den Verbund eingegeben hat. Wird ein so eingegebenes Datum von anderen Stellen in Vorgänge aufgenommen, sollen diese Stellen eine Besitzanwartschaft begründen, sodass bei Löschung durch den Erstbesitzer diejenige Stelle mit der ältesten Anwartschaft Besitzer wird. Vor allem mit Blick auf Löschungsansprüche von Betroffenen kann diese Praxis dazu führen, dass zu löschende Daten weiterhin im Informationswesen erhalten bleiben.[905] Mit dem Datenbesitz korreliert die datenschutzrechtlichen Verantwortung gemäß § 31 BKAG, was vor allem mit Blick auf individuellen Rechtsschutz relevant ist.[906] Gemäß § 29 Abs. 5 Satz 2 BKAG ist bei Anhaltspunkten über die Unrichtigkeit eines Datums jeder Teilnehmer des Verbundes verpflichtet, der gemäß Satz 1 zuständigen Behörde umgehend darüber Mitteilung zu machen. Die zuständige Behörde ist in einem solchen Fall verpflichtet, die in Frage stehenden Daten unverzüglich zu prüfen und erforderlichenfalls die Daten unverzüglich zu berichtigen, zu löschen

901 BT-Drs. 18/11163, S. 109.
902 Siehe dazu und zu Problemen in diesem Kontext unten S. 323 ff.
903 BT-Drs. 18/11163, S. 109.
904 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 31 BKAG Rn. 4.
905 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 915.
906 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 28; *Barczak* in *Barczak* (Hrsg.), BKAG, § 29 Rn. 25.

oder in ihrer Verarbeitung einzuschränken. Darüber hinaus ist in Satz 3 des § 29 Abs. 5 BKAG noch die Ergänzung von Daten geregelt: Sind personenbezogene Daten gespeichert, können von jeder teilnehmenden Stelle ergänzend Daten eingeben werden. Probleme kann dies allerdings verursachen, wenn mehrere verantwortliche Stellen Daten zu einer Person gespeichert haben. Neben der Frage nach der letztendlichen datenschutzrechtlichen Verantwortung ist dies vor allem der Fall, wenn eine Behörde ihren Datenbesitz löschen will, andere Stellen ihn jedoch erhalten wollen. In solchen Fällen kann der Datenbesitz auf die erhaltungswillige Stelle übergehen, wobei aber eine einzelfallspezifische rechtliche Bewertung hierüber zu treffen und zu dokumentieren ist. Aus der Parallelstruktur von INPOL-Z und INPOL-Land ergibt sich darüber hinaus die Pflicht, bei Löschungen in den Landessystemen für eine parallele Bereinigung in der Verbunddatei zu sorgen.[907] Mit einem stetig anschwellenden Datenvolumen in den Systemen, wie es Massendatendynamiken erwarten lassen, steht diese Form der Datenpflege vor gravierenden Herausforderungen, die sich vermutlich nur durch bestimmte Automatisierungslösungen adressieren lassen werden.

INPOL-Z stellt für den Datenumgang im Verbund keine eigene Benutzungsoberfläche bereit,[908] was sich mittelbar auch aus § 13 Abs. 3 BKAG ableiten lässt. Die verschiedenen Polizeiorganisationen nutzen vielmehr ihre eigenen Informationssysteme, mit denen sie an INPOL-Z teilnehmen. Konzeptuell spricht man von INPOL-Bund (§ 13 BKAG) und INPOL-Land. Tatsächlich sind die Systeme allerdings anders benannt. Am breitesten genutzt wird das System POLAS, das von allen Polizeibehörden, auch dem Bundeskriminalamt, dem Zollkriminalamt und der Bundespolizei, außer Nordrhein-Westfalen, (dort ViVa) Berlin (dort: POLIKS) und Rheinland-Pfalz (dort: POLIS) genutzt wird. Konturierende Rechtsvorschriften finden sich für diese Systeme kaum. Lediglich § 13 SOG LSA enthält noch eine dem § 13 BKAG vergleichbare Vorschrift. Ansonsten wird als Rechtsgrundlage in der Regel die Datenverarbeitungsgeneralklausel herangezogen werden (müssen), wie etwa in § 37 Abs. 1 S. 1 PolG BW: „Die Polizei kann personenbezogene Daten speichern, verändern und nutzen, soweit und solange dies zur Wahrnehmung ihrer Aufgaben erforderlich ist."

Dieser Befund ist mit Blick auf die Vielschichtigkeiten und Komplexitäten des Informationsumgangs in den Systemen einigermaßen ernüchternd.

907 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1209 f.

908 BT-Drs. 14/7734, S. 2.

Instruktiv wird er für die baden-württembergische POLAS-Version von *Kathke* geschildert[909]: POLAS BW ermöglicht einerseits den Zugang zu INPOL-Z, aber auch zu Auskunftssystemen externer Behörden. Anderseits fungiert POLAS BW für das Land Baden-Württemberg gleichfalls als regionales Verbundsystem für alle dortigen Polizeibehörden. Es ist dort „Landesdatenhaltungssystem und Auskunftssystem" für alle polizeilich gespeicherte Daten. Insofern fungiert POLAS BW „als Auskunfts- und Fahndungssystem zur repressiven und präventiven Kriminalitätsbekämpfung, zur Erfassung der für die PKS erforderlichen Daten und als Fallregistratur aller Anzeigen nicht geklärter Straftaten, die den Staatsanwaltschaften vorgelegt werden." Das Informationssystem besteht aus einer Auskunfts- und einer Änderungskomponente. Die Auskunftskomponenten steht allen Sachbearbeiter:innen über eine Webanwendung über eine Intranetseite zur Verfügung, wobei Suchen nach raumbezogenen Parametern (etwa regional oder national) angepasst werden können. Die Änderungskomponente ist weniger verfügbar. Sie ist „als Client-Server-Anwendung bei den Datenstationen der Polizeipräsidien als den zentral zuständigen Stellen lokalisiert." Nur hierüber können Daten manuell eingepflegt oder verändert werden, wobei dann eine automatische Plausibilitätsprüfung erfolgen soll.

Die Interaktion mit dem System erfolgt entlang drei verschiedener Entitäten, die so die polizeiliche Arbeit strukturieren: Personen, Sachen, Fälle. In den Entitäten sind die Daten wiederum in verschiedenen Gruppen organisiert, die untereinander miteinander verknüpft werden können und durch ihre Kategorisierung die Dateistruktur in INPOL-Z bilden, wie sie im Anschluss an diesen Unterabschnitt näher dargestellt wird. Für Personen enthält die Datengruppe „Rechtmäßige Personalien" (P-Gruppe) die personenbezogene Grunddaten, zudem können Daten aber auch als „Andere Personalien" und damit der A-Gruppe zugehörig referenziert werden, womit dann etwa die Aufnahme von Aliasnamen oder anderen Schreibweisen der Namen in die Datenbank ermöglicht wird. In der Datengruppe „Personenfahndung" (F-Gruppe) werden Ausschreibungen von Personen verwaltet, von Straftäter:innen über Zeug:innen bis hin zu vermissten Per-

909 Siehe zum Folgenden *Kathke*, Überlieferungsbildung aus, Fachverfahren Überlegungen zu POLAS BW der Polizei Baden-Württemberg, 2015, S. 12 ff.; es kann davon ausgegangen werden, dass trotz der oft erwähnten Heterogenität des polizeilichen Informationswesens die Informationssysteme, mit denen an INPOL-Z teilgenommen wird, im Wesentlichen dieselben Funktionalitäten aufweisen, sodass die Beschreibung von POLAS BW als repräsentativ angesehen werden darf, zumal POLAS von den meisten Polizeibehörden genutzt wird.

sonen. Die Datengruppe „Dokumente" (Q-Gruppe) erfasst Dokumente, die einen Personenbezug aufweisen, also etwa Haftbefehle oder strafverfahrensrechtliche Beschlüsse, nach einem Scan der Papierform digital. In der Datengruppe „Haftdatei" (H-Gruppe) werden die spezifischen Haftdaten von erfassten Personen gespeichert. Die Datengruppe „Erkennungsdienst" (E-Gruppe) enthält erkennungsdienstliche Daten. Daneben bestehen noch die L-Gruppe („Personenbeschreibung"), über die eine detaillierte Personenbeschreibung vorgenommen werden kann, sowie die W-Gruppe („Personenbezogene Hinweise") und Z-Gruppe („Zusätzliche Personeninformationen"), die detaillierte Informationen zu den verwalteten Personen enthalten, etwa die Einstufung als gewalttätig, links- oder rechtsextrem oder als Drogenkonsument:in sowie berufliche Ausbildungen und Tätigkeiten. *Kathke* zufolge sind die Daten der Gruppe „Unterlagen" (U-Gruppe) von besonderer Bedeutung für den Bereich der Personen, da sie den „Verweis auf die kriminalaktenführende Polizeidienststelle (KAN-Nachweis), das Aussonderungsprüfdatum der Unterlagen, die vorhandenen Fall- und Ereignisdaten, die Entscheidung bzw. die Mitteilung über den Verfahrensausgang und ein Verzeichnis der durchgeführten DNA-Maßnahmen enthält." Über diese Gruppe findet somit eine Vernetzung der aus Polizeiperspektive zentralen Daten statt, weil „über das Datenfeld Ereignisse eine Zuordnung von bekannten Fällen erfolgt, die Erfassung einer U-Gruppe Voraussetzung einer Erfassung von A-, E-, L- und W-Gruppe ist und der Dateninhalt maßgeblich für die Aufnahme von personenbezogenen Daten eines Tatverdächtigen in den Kriminalaktennachweis beim BKA ist." Insofern können über den Zugang zu dieser Gruppe neben einer tiefgehenden Analyse der Person, insbesondere über die Hinweise, auch alle Verbindungen der Person zu bekannten Taten dargestellt werden. Gemeinsam mit den Haftdaten lassen sich so kriminelle Karrieren rekonstruieren und darüberhinausgehende Zusammenhänge ableiten.

Weniger facettenreich ist POLAS BW mit Blick auf Sachdaten. Hier können Kennzeichen, Ausweisnummern, Banknoten, Waffen oder andere mit numerischen Zeichen versehene Gegenstände erfasst und abgefragt werden. Dazu werden die Sachfahndungsnotierung (N-Gruppe) und die Sachbeschreibung (S-Gruppe) gebildet: Die N-Gruppe enthält vorrangig Daten zu rechtlichen oder faktischen Personen-Sachen-Beziehungen, die S-Gruppe spezifische Informationen zur Sache.

Die letzte Entität, Fälle, enthält schließlich straftatenbezogene Einzelhinweise bezüglich geklärter wie ungeklärter Fälle. In der sog. T-Gruppe gespeichert werden Daten der Tat, Opferdaten und Deliktsdaten.

Nicht nur innerhalb einer Entität, sondern auch die Entitäten untereinander können miteinander verknüpft werden. So kann eine Person mit mehreren Fällen und ein Fall mit mehreren Personen verbunden sein. Diese Netzwerkstruktur spiegelt sich auch in den Suchmöglichkeiten wider. So ist „ein Wechsel von einer Personenrecherche zu einem verbundenen Fall und umgekehrt [...] innerhalb der Datenbank jederzeit möglich." Genauso verhält es sich mit Sachen und Fällen. Die Entität Fall ist somit zentral im Datenmodell von POLAS BW, da hier Personen und Sachen in polizeirelevanter Weise miteinander verklammert werden.

Die Daten für POLAS BW kommen aus dem Vorgangsbearbeitungssystem[910] der Polizei in Baden-Württemberg (ComVor). Wenn die Daten übertragen werden, erfolgt eine Prüfung und erforderlichenfalls eine Korrektur bei der zuständigen Datenstation. Anschließend erfolgt die Übertragung zu POLAS auf Knopfdruck. Eine vollautomatisierte Übertragung erfolgt gegenwärtig nicht. Auch müssen einige Datenarten noch manuell in POLAS BW erfasst werden, so etwa Sachfahndungsdaten oder auch von der Justiz übermitteltete Fahndungs- und Haftdaten. Einmal in POLAS angekommen, können die Daten dort noch weiter ergänzt werden, ein Rückfluss der Informationen nach ComVor ist hingegen nicht möglich. Sowohl das Vorgangsbearbeitungssystem als auch POLAS BW verfügen aber über eine Schnittstelle, über die Schnittstelle mit ComVor gibt es außerdem eine Verbindung zu X-Justiz, also insbesondere für strafverfahrensrechtliche Daten. Die weit wichtigere Schnittstelle – und hier schließt sich der Kreis zu INPOL-Z – ist jedoch die Teilnahme von POLAS BW (und allen anderen äquivalenten INPOL-Land-Systemen) an INPOL-Z. So sind Sach- und Personenfahndungsdaten parallel gespeichert, denn die Daten, die in POLAS gespeichert werden und Verbundrelevanz besitzen, werden an das vom Bundeskriminalamt geführte INPOL-Z weitergeleitet und von dort in die anderen Informationssysteme der 16 Bundesländer sowie die Systeme vom Bundeskriminalamt selbst, von Bundespolizei und Zollkriminalamt übertragen. Über die INPOL-Z-Schnittstelle liefert POLAS BW auch Daten in das Gesichtserkennungssystem (GES), das Automatische-Fingerabdruck-Informationssystem (AFIS), die DNA-Analyse-Datei International (DAD-i) sowie das nationale Schengener Informationssystem (NSIS), wo europaweite Fahndungen eingetragen werden. Umgekehrt können diese Datenbanken auch alle über POLAS BW für die polizeiliche Aufgabenerfüllung genutzt werden. Schließlich hält POLAS BW auch noch

910 Näher zu Vorgangsbearbeitungssystemen siehe unten S. 254 ff.

Schnittstellen zu nicht-polizeilichen öffentlichen Datenbanken wie zu MeldIT, dem Meldedatenbestand, dem Bundeszentralregister (BZR), dem Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV), dem Zentralen Verkehrsinformationssystem für die Polizei beim Kraftfahrbundesamt (ZEWIS) oder dem Ausländerzentralregister bereit.

Vor dem Hintergrund der vielfältigen Funktionalitäten von INPOL ließe sich zwar argumentieren, dass eine detailgetreue(re) Abbildung dieser Strukturen und Verarbeitungsmöglichkeiten im Gesetz die Rechtslage eher noch verworrener machen würde und auch, dass die BKADV doch eine Präzisierung des INPOL-Betriebes enthält. Neben dem Umstand, dass diese jedoch – wie bereits dargelegt – gegenwärtig veraltet ist, wurde sie zudem wie ein Großteil der geltenden Regelungen stets nach den technischen Strukturen erlassen, sodass selbst die präzisierende BKADV lediglich bereits Bestehendes und Praktiziertes abbildet, ohne in irgendeiner Weise einen eigenen rechtlichen Steuerungsanspruch zu entwickeln. Auf dieser Linie liegt auch weiterhin die Gesetzgebung. Das gilt einerseits, wenn sie lediglich Datenverarbeitungsgeneralklauseln für komplexe Informationssysteme schafft, die eine ganz andere Eingriffsintensität entfalten, als wenn Sachbearbeiter:innen lediglich mit Papierakten arbeiten würden – beide Arbeitsformen sollen aber anscheinend ihre Rechtsgrundlage in den Generalklauseln finden. Andererseits wird die mangelnde gesetzgeberische Eigeninitiative auch evident, wenn der Gesetzgeber versucht – wie das in 29 ff. BKAG geschehen ist – einen im Wesentlichen aus der Exekutive stammenden Innovationsimpuls, *Polizei 2020*, in Gesetzesform zu gießen.

bb) Personen- und Sachfahndungsdateien

Kernstück des gegenwärtigen INPOL-Verbundsystems sind die Personen- und Sachfahndungsdateien.[911] Die Befugnis des Bundeskriminalamtes zum Führen von Personenfahndungsdateien ergibt sich aus § 16 Abs. 2 Satz 1 BKAG.[912] Im Polizeialltag spielt sie eine übergeordnete Rolle. Zwar bezieht sich § 16 Abs. 2 Satz 1 BKAG seinem Wortlaut zufolge auf die Weiterverar-

911 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html (Stand: 01.10.2023); vgl. auch *Arzt* Neue Juristische Wochenschrift 2011, 352, S. 353, der von „Grundpfeilern" polizeilicher Datenverarbeitung spricht.

912 *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 13.

beitung im Informationssystem des Bundeskriminalamtes. Über § 29 Abs. 4 Satz 2 BKAG findet die Norm aber Anwendung auf den gesamten Informationsverbund. Die Datei enthält Daten über Personen, die von der Polizei aufgrund eines Haftbefehls, einer Ingewahrsamnahme, einer Aufenthaltsermittlung, einer Ausreiseuntersagung sowie bei Ausländer:innen wegen beabsichtigter Abschiebung oder Zurückweisung gesucht werden.[913] Zudem ermöglicht sie dem Bundeskriminalamt die Weiterverarbeitung von personenbezogenen Daten, soweit dies zur polizeilichen Beobachtung oder gezielten Kontrolle erforderlich ist.[914] Sowohl bei Personen- als auch bei Sachfahndungsdateien, die beide in der BKADV in § 9 Abs. 2 Nr. 1 konkretisiert werden, handelt es sich um Verbunddateien. Welche personenbezogenen Daten in der Personenfahndungsdatei gespeichert werden dürfen, wird umfänglich in § 6 Abs. 1 BKADV geregelt. Demgegenüber bestimmt § 6 Abs. 2 BKADV die Personen, von denen die in Absatz 1 genannten Daten verarbeitet werden dürfen. Dabei ist – wie auch bei allen anderen Datenspeichern, die personenbezogene Daten enthalten – ein hoher Anspruch an die Datenrichtigkeit zu stellen, wie er insbesondere durch die JI-Richtlinie nunmehr für das nationale Recht, etwa in § 75 Abs. 1 BDSG, postuliert wurde.[915] Denn die hohe Dynamik der datenverarbeitenden Operationen und damit die Dynamik des Informationswesens selbst eröffnen laufend Spielräume für Datenfehler, etwa in Form von Verwechslungen. Mit Blick auf die darin für Betroffene liegenden Gefahren[916] muss der Datenqualität ein höherer Stellenwert als ihrer Quantität eingeräumt werden.[917] Gegenwärtig[918] sind in der INPOL-Personenfahndungsdatei 274.894 Ausschreibungen zur Festnahme und 426.962 Ausschreibungen zur Aufenthaltsermittlung enthalten.[919]

913 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G., Rn. 424.

914 Zudem muss das Bundeskriminalamt oder die die Ausschreibung veranlassende Stelle nach dem für sie geltenden Recht befugt sein, die mit der Ausschreibung für Zwecke der Strafverfolgung, des Strafvollzugs, der Strafvollstreckung oder der Abwehr erheblicher Gefahr vorgesehene Maßnahme vorzunehmen oder durch eine Polizeibehörde vornehmen zu lassen.

915 Siehe dazu bereits oben S. 215 ff.

916 Siehe dazu bereits den Fall in Fn. 811.

917 So zutreffend *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1212.

918 Stand 01.10.2023.

919 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html (Stand: 01.10.2023).

Die Sachfahndungsdatei wird nicht in 16 Abs. 2 Satz 1 BKAG geregelt. Erwähnt wird sie in § 2 Abs. 4 Nr. 2, § 13 Abs. 2 Nr. 2 sowie 27 Abs. 2 BKAG. Während die beiden erstgenannten Normen keine Befugnisnormen wie etwa § 16 Abs. 2 Satz BKAG sind, setzt § 27 Abs. 2 BKAG die Sachfahndungsdatei vielmehr voraus, als sie zu regeln. Mangels Personenbezug ist für die Sachfahndungsdatei hingegen grundsätzlich keine besondere Befugnis erforderlich. In der BKADV findet sich in § 6 Abs. 3 eine Regelung für diejenigen Daten und Personen, die im Zusammenhang mit zur Fahndung oder zur polizeilichen Beobachtung ausgeschriebenen Sachen gespeichert werden dürfen, wo also doch ein Personenbezug der Sachen besteht. Gegenwärtig[920] sind etwa 16 Mio. Gegenstände erfasst, die wegen eines möglichen Zusammenhangs mit Straftaten gesucht werden.[921]

cc) Kriminalaktennachweis (KAN)

Im INPOL wird ein Kriminalaktennachweis (KAN) über Straftaten von erheblicher Bedeutung und überregional bedeutsame Straftaten,[922] also ein Indexsystem für die bei den Polizeien vorgehaltenen Kriminalakten, als Verbunddatei geführt. Erhebliche Straftaten sind Verbrechen gem. § 12 Abs. 1 StGB sowie die Katalogstraftaten des § 100a StPO. Die überregionale Bedeutung wird kasuistisch bestimmt.[923] So können beispielsweise auch Akten indexiert werden, deren Bedeutung per se unterhalb dieser Schwellen liegt, bei denen sich aber mittels Prognose ergibt, dass sie zur Verhütung von Straftaten mit länderübergreifender, internationaler oder (sonst) erheblicher Bedeutung beitragen können.[924] Die im KAN indexierten Kriminalakten stellen zudem kriminalpolizeiliche personenbezogene Sammlungen (KpS) dar. Da über die Rahmenbedingungen der KpS im Wesentlichen geregelt wird, was an Informationen überhaupt in Kriminalakten aufgenommen wird und damit auch potenziell im KAN verfügbar ist, besteht ein enger Konnex zwischen beiden Strukturen. KAN und KpS sind allerdings trotz dieses inhaltlichen Konnexes nicht zusammenhängend

920 Stand 01.10.2023.
921 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/ElektronischeFahndungsInformationssysteme/polizeilicheInformationssysteme_node.html (Stand: 01.10.2023).
922 § 9 Abs. 1 Nr. 2 BKADV.
923 Siehe *Zöller,* Informationssysteme, S. 141.
924 NdsLT-Drs. 16/2770, Anlage 5, S. 1.

geregelt. Während der KAN im Wesentlichen im BKAG und der BKADV geregelt ist, finden sich für die KpS verschiedene Richtlinien in den Ländern.

Zwar verweisen die KpS-Richtlinien darauf, dass Datenverarbeitungen zu kriminalpolizeilichen Zwecken nur auf Basis entsprechender Rechtsgrundlagen erfolgen dürfen. Allerdings dürften die KpS-Richtlinien aufgrund ihrer kohärenten Darstellung der Vorgaben zur Verarbeitung von Daten zu kriminalpolizeilichen Zwecken in der Praxis einen wesentlichen normativen Rahmen bei der formalen und auch inhaltlichen Ausgestaltung der kriminalpolizeilichen Datenverarbeitung spielen. So stellen die KpS-Richtlinien etwa an einem Ort zusammen, welche Personen oder welche Datentypen – etwa Verhaltensdaten – in die Sammlungen aufgenommen werden dürfen.[925] Es ist zwar zu begrüßen, dass den Polizeibeamt:innen ein kohärenter Leitfaden für die Arbeit mit kriminalpolizeilichen Daten an die Hand gegeben wird. Allerdings entstammen diese normativen Vorgaben nicht dem demokratischen Deliberationsprozess, sodass sich auch am neuralgischen Punkt der kriminalpolizeilichen Datenverarbeitung eine Entkoppelung der polizeilichen Institutionen von direkten legislativen Steuerungsimpulsen zeigt. Das ist mit Blick auf die Bedeutung der KpS für die polizeiliche Informationsverarbeitung problematisch: Sie gelten als „polizeiliches Gedächtnis" für Kriminalität und sind ein zentrales Instrument polizeilicher Informationsarbeit.[926]

Gesetzlich geregelt ist hingegen der KAN, über den Zugriff auf die kriminalpolizeilichen Daten hergestellt werden kann. Die den KAN vormals regelnden §§ 7 bis 9 BKAG a.F. sind unter anderem in § 18 BKAG aufgegangen.[927] Im Aktennachweissystem sind Grunddaten, die den Personendaten nach § 1 Abs. 1 BKADV entsprechen,[928] soweit erforderlich, andere zur Identifizierung geeignete Merkmale, die kriminalaktenführende Stelle und die Kriminalaktennummer sowie die nähere Bezeichnung der Straftat nach Tatzeiten, Tatorten und Tatvorwürfen enthalten. Bedeutsam sind dabei insbesondere die anderen zur Identifizierung geeigneten Merkmale gem. § 1 Abs. 2 BKADV, denen auch Informationen unterfallen, die eine

925 Siehe Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen (KpS-Richtlinien) KpS-Richtlinien vom 2. Oktober 2008 (Brem.ABl. 2008, S. 893).

926 So *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1215.

927 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 Rn. 1.

928 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 15.

Verhaltensbeurteilung der gespeicherten Person ermöglichen können oder sogar sollen.[929] Aufgrund unklarer Zugriffsberechtigungen wird der KAN in der Praxis nicht nur als Aktennachweis, sondern auch als Personenindex genutzt. Vor dem Hintergrund der zunehmenden Elektronisierung der Aktenbestände,[930] nimmt so auch die Intensität eines Eingriffs durch Speicherung im KAN zu, da die dort gespeicherten Informationen so zunehmend breit und schnell verfügbar sind. Die im KAN gespeicherten Daten, die in der Regel die wichtigsten Informationen der zugrundeliegenden Kriminalakte zusammenfassen, können in ihrer Komprimiertheit eine gewisse Voreingenommenheit erzeugen – vor allem, wenn eine detaillierte Auseinandersetzung mit der in Frage stehenden Person durch den jeweiligen Polizeibeamten durch den Abruf der Daten aus dem KAN unterbleibt.[931] Das ist umso gravierender, wenn auch Kontakt- und Begleitpersonen sowie Auskunftspersonen in den KAN gelangen.[932] Voraussetzung für die Aufnahme in den KAN ist eine Negativprognose, wie sie beispielsweise in § 18 Abs. 1 Nr. 4 BKAG für Anlasspersonen vorgeschrieben wird. Umfasst sind also solche Personen, bei denen ohne Verurteilung, Beschuldigung oder Verdacht (nur) tatsächliche Anhaltspunkte die Annahme zukünftiger Straftaten rechtfertigen. Aufgrund des Umstandes, dass die Weiterverarbeitung von personenbezogenen Daten des Personenkreises von § 18 BKAG im Ermessen der jeweiligen Behörde steht, das jedoch vom Gesetz in keinerlei Hinsicht angeleitet wird, hat *Bäcker* zudem weitere Eingrenzungen vorgeschlagen: So soll der Anwendungsbereich von § 18 Abs. 1 und 2 BKAG auf Straftaten von hinreichendem Gewicht beschränkt werden und die Weiterverarbeitung, die vor allem in der Bevorratung der Daten liegt, zeitlich begrenzt sowie der Verarbeitungsanlass dahingehend konkretisiert werden, dass konkrete Tatsachen auf die Begehung von Straftaten schließen lassen.[933]

929 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 406.

930 Siehe den Nachweis bei *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1215.

931 *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, 11. Edition, § 24 PolG NRW Rn. 33; *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 406.

932 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1216 Siehe näher zu diesen Personenkazegorien unten S. 324 ff.

933 *Bäcker*, Schriftsatz der Verfassungsbeschwerde im Verfahren 1 BvR 1160/19, S. 51 f., abrufbar unter: https://freiheitsrechte.org/home/wp-content/uploads/2019/10/2019-05-21-BKA-Gesetz-VB-anonymisiert.pdf (Stand: 01.10.2023).

Die im KAN gespeicherten Daten besitzen dabei aufgrund der praktischen Handhabung von Kriminalakten besondere Beharrungskräfte, denn die Polizei speichert die Daten auch über den reinen Abschluss der Ermittlungen oder Verfahren hinaus, wenn ein Restverdacht besteht, selbst wenn die betroffene Person wegen Beweismangels freigesprochen oder das Verfahren sanktionslos eingestellt worden ist.[934] Diese Praxis wird durch § 18 Abs. 5 BKAG bestätigt, der eine obligatorische Löschung nur für Fälle vorschreibt, in denen das Urteil explizit angibt, dass jemand eine Tat nicht oder nicht rechtswidrig begangen hat. Die Norm scheint indessen in einem Spannungsverhältnis zu verfassungs- und menschenrechtlichen Vorgaben zu stehen. Während das Bundesverfassungsgericht entschieden hat, dass es „nach einem Freispruch […] für die Annahme eines fortbestehenden Tatverdachts aber besonderer, von der speichernden Polizeibehörde darzulegender Anhaltspunkte [bedarf], die sich insbesondere aus den Gründen des freisprechenden strafgerichtlichen Urteils selbst ergeben können",[935] es also nur in Ausnahmefällen zu einer weiteren Speicherung kommen kann, ist der Europäische Gerichtshof für Menschenrechte insoweit strenger: „Tatsächlich gilt die Unschuldsvermutung nicht nur während eines laufenden Strafverfahrens. Damit sie praktisch und wirksam ist, dürfen Behörden und Gerichte im Fall der Einstellung eines Strafverfahrens oder des Freispruchs in den Gründen ihrer Entscheidung keinen Schuldvorwurf gegenüber dem Betroffenen äußern."[936] Daraus ergibt sich zumindest eine intensivere Prüfungspflicht für die der weiteren Speicherung zugrunde liegende Negativprognose, insbesondere in den Fällen des § 18 Abs. 5 BKAG. Da hierzu zunächst der Ausgang des Verfahrens als initiale Information benötigt wird, müssen die Staatsanwaltschaften gem. § 482 Abs. 2 S. 1 StPO in Verbindung mit Nr. 88 S. 2 RiStBV Mitteilung über den Ausgang machen, wobei aber nicht immer die Gründe für die Verfahrensbeendigung mitgeteilt werden, sodass die Verpflichtung zur automatisierten Mitteilung derselben in § 32 Abs. 2 BKAG zu begrüßen ist, wenngleich Zweifel hinsichtlich der technischen Umsetzbarkeit bestehen.[937]

934 *Bundesbeauftragter für Datenschutz und Informationssicherheit*, A-Drs. 18(4)806 A, S. 20 ff.

935 BVerfG, 16.05.2002 - 1 BvR 2257/01 (NJW 2002, 3231).

936 EGMR, Urteil vom 15.01.2015 - EGMR Aktenzeichen 48144/09 (NJW 2016, 3225).

937 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1221 Ausführlicher zum Verfahren rund um § 18 Abs. 5 BKAG auch unten S. 329 ff.

dd) Haftdatei

Ebenfalls starken kriminaljustiziellen Bezug hat die Haftdatei, die in § 18 Abs. 4 BKAG hinsichtlich der Verarbeitung geregelt und in § 9 Abs. 2 Nr. 2 BKADV hinsichtlich ihrer Struktur erwähnt ist. Sie dient dem Nachweis über Personen, die wegen rechtswidriger Straftat oder des Verdachts einer rechtswidrigen Straftat einer richterlich angeordneten Freiheitsentziehung unterliegen. Zweck sind die Verhinderung unnötiger Fahndungen, Alibiüberprüfungen und das Informiertsein über bevorstehende Haftentlassungen, sodass die Haftdatei vor allem der Vorsorge künftiger Strafverfolgung, aber auch der Gefahrenabwehr dient.[938] Voraussetzung für eine Verarbeitung in der Datei ist eine richterlich angeordnete Freiheitsentziehung anlässlich einer rechtswidrigen Tat. Die BKADV legt näher fest, welche Daten von der Polizei in entsprechenden Fällen verarbeitet werden dürfen.

ee) Erkennungsdienstliche Dateien und DNA-Analyse-Dateien (DAD)

Die schon seit den Anfängen der modernen Polizei bestehende Aufgabe der fehlerfreien Identifizierung von Personen hat in INPOL ihren strukturellen Niederschlag in Form der erkennungsdienstlichen Dateien gefunden. Die gespeicherten Daten, die gemäß § 16 Abs. 5 i.V.m. § 2 Abs. 4 BKAG zu repressiven und präventiven Zwecken verarbeitet werden dürfen, sollen eine möglichst präzise Identifizierung ermöglichen. Die BKADV sieht daher in § 9 Abs. 1 Nr. 4 in Verbindung mit § 5 Abs. 1 einen breiten Katalog an Datentypen vor, die diesem Zweck dienen. Gegenwärtig dürften in diesem Rahmen nach wie vor die daktyloskopischen Bestände und Systeme den größten praktischen Nutzen mit sich bringen. Hier gibt es unterschiedliche technische Lösungen wie die Automatisierten Fingerabdruck-Identifizierungssysteme für den polizeirechtlichen (AFIS-P) bzw. asylrechtlichen Bereich (AFIS-A), die dem Abgleich von Mustern dienen, sowie die Nationale Datenbank für digitalisierte Fingerabdrücke für Polizei (NatDB P) und Asyl (NatDB A), die als digitale Sammlung der vorhandenen Fingerabdruckblätter fungieren.[939] Zum zuletzt von Behördenseite aktualisierten Stand (April 2022) sind so 5,3 Millionen Personen und 440.000 Spuren

938 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 37; *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 18 Rn. 11.

939 BT-Drs. 17/14735, 17.

in den Datenbanken gespeichert.[940] Der informationelle Wert dieser Daten für die polizeiliche Arbeit steigt mit zunehmend verbesserter Identifizierungstechnologie. So gibt es bereits seit einigen Jahren die Möglichkeit Fingerabdrücke im Einsatz zu erfassen und digital in Echtzeit abzugleichen.[941] Mit fortschreitender Leistungsfähigkeit von sogenannter „intelligenter" Videotechnik[942] und der verbreiteten Nutzung von digitalen Kameras im Einsatz zur Personenidentifizierung innerhalb weniger Augenblicke[943] ist aber auch ein Bedeutungszuwachs der visuellen Daten, etwa von Lichtbildern und sonstigen besonderen körperlichen Merkmalen, zu erwarten.

Neben diesen klassischen Identifizierungsformen ist seit den 1990er-Jahren auch die Speicherung von DNA-Analyse-Mustern zum Zwecke der Identifizierung ein Thema von zunehmender Relevanz im polizeilichen Informationswesen. § 5 Abs. 5 BKADV regelt dazu, welche Muster und damit zusammenhängende oder dafür relevante Daten wie etwa hinsichtlich der dazugehörigen Tat in der in § 9 Abs. 1 Nr. 5 vorgesehenen DNA-Analyse-Datei gespeichert werden können, wo sie dann gemäß § 16 Abs. 5 Nr. 1 BKAG weiterverarbeitet werden dürfen. Ein Großteil der 836.000 Personen, die in der Datei gespeichert sind, dürfte auf § 81g StPO beruhen, der nunmehr aber auch von präventiven Landesregelungen flankiert wird. Daneben liegen zusätzlich 386.000 Spuren in der Datenbank vor (Stand: April 2022). In der DAD kann bei Spurenfunden dann auf Direkttreffer abgeglichen werden, ein Abgleich mit Beinahetreffern war hingegen 2018 weder möglich noch geplant.[944] Die polizeiliche Nutzung von Beinahetreffern („familial searching") bleibt somit zunächst auf DNA-Reihenuntersuchungen beschränkt (§ 81h Abs. 1 StPO), wobei aber die gegenwärtige Ausweitung von genetischen Ermittlungsbefugnissen der Polizei auch der DAD und der in ihr gespeicherten Daten einen weiteren Bedeutungszuwachs verschaffen könnte.[945]

940 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Erkennungsdienst/erkennungsdienst_node.html#doc19616bodyText3 (Stand: 01.10.2023).
941 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1174.
942 Siehe dazu etwa *Held,* Intelligente Videoüberwachung.
943 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1174.
944 BT-Drs. 19/4354, 6.
945 Siehe dazu (auch in anderen Staaten) *Butz* NK 33 (2021), 316.

ff) Delikts- und phänomenbezogene Dateien

Neben diesen integralen Bestandteilen von INPOL zeichnet sich nun schon seit einigen Jahrzehnten das Bedürfnis einer zumindest teilweisen Durchbrechung der logischen Trennung der Datenbestände ab, die durch die Zuordnung zu Datengruppen eingezogen werden. Mit einem zunehmenden Vorfeldfokus der Polizei, der sich als wesentliches Merkmal der auf Prävention bedachten Sicherheitsgesellschaft materialisiert hat, reicht es immer weniger aus, anlässlich eines Akts abweichenden Verhaltens zu prüfen, ob die in Frage stehende Person bekannt sein könnte. Mit Ausweitung und Intensivierung des polizeilichen Blicks im Namen der Prävention wird die Produktion von Wissen aus der Verknüpfung von datenförmig vorhandenen Informationen immer wichtiger. In der technischen Infrastruktur des polizeilichen Informationswesens spiegelt sich dieser Wandel in delikts- und phänomenbezogenen Dateien wider, die bestimmte soziale Interaktionsfelder, denen Devianz zugeschrieben wird, abzubilden versuchen.

Zu diesem Zweck wurden über die Jahre verschiedene Verbunddateien in INPOL eingerichtet, in denen der Datenaustausch zu verschiedenen Bereichen[946] – „Innere Sicherheit", „Gewalttäter Links", „Gewalttäter Rechts", „Gewalttäter Sport", „politische Ausländerkriminalität" oder auch „APOK" (Aufklärung / vorbeugende Bekämpfung von Straftaten der Organisierten Kriminalität) – stattfindet. Daneben gibt es auch deliktsspezifischere Dateien, wie Falldateien zum „Rauschgift", „Falschgeld" oder „ViCLAS" (Violent Crime Linkage Analysis System) für Gewaltdelikte.[947]

Die in diesen Informationsbeständen stattfindenden Datenverarbeitungen müssen durchweg als intensive Eingriffe gehandelt werden, da beim Kontakt der Betroffenen mit der Polizei regelmäßig eine alerte Reaktion der jeweiligen Polizist:innen ausgelöst werden soll und wird, was mit weiteren polizeilichen Maßnahmen verbunden sein kann.[948] Dem wird der Grad der rechtlichen Regulierung dieser informationellen Instrumente nur begrenzt gerecht. Rechtsgrundlage für fast alle diese Verbunddateien ist § 8 BKAG a.F., wobei stets eine Konkretisierung von Dateizweck und -funktionalitäten durch Errichtungsanordnungen erfolgt. Über IfSG-Anfragen konnten einige dieser nicht-öffentlichen Dokumente der Öffentlichkeit zugänglich

946 Kritisch zu den Gewaltäterdateien *Ruch/Feltes* NK 17 (2016), 62.
947 Siehe dazu die Übersicht bei BT-Drs. 17/14735, S. 9 ff.
948 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1257.

gemacht werden, womit Einblicke in die Rahmenbedingungen der Dateien möglich werden.[949] Auch die Errichtungsanordnungen begrenzen das polizeiliche Informationshandeln nur bedingt. So können in Phänomenbereichen etwa Daten zu Kontakt- und Begleitpersonen zum Zwecke der Straftatenverhütung oder -vorsorge gespeichert werden, was eine weitreichende, prinzipiell nur von polizeilicher Definitionsmacht begrenzte Befugnis ist, die es im Übrigen schon vor der großen Verrechtlichung polizeilichen Informationshandelns in dieser im Wesentlichen unbeschränkten Form gegeben hat.[950] Zudem ist über die Möglichkeit der Freitextfeldspeicherung der Weg offen für eine ungefilterte Abbildung polizeilicher Interpretationen und Zuschreibungen in den polizeilichen Informationsbeständen. Jahrelang wurden die Verbunddateien zudem ohne die konkretisierende Rechtsgrundlage der BKADV betrieben, die erst 2010 nach einem dreizehnjährigen Disput über deren rechtliche Erforderlichkeit im Anschluss an die Novellierung des BKAG 1997 erlassen wurde.[951] Allerdings verblasst die Bedeutung der Dateienstruktur mit dem gegenwärtigen Wandel des polizeilichen Informationswesens, wie er durch Projekte wie PIAV oder *Polizei 2020*[952] angestoßen wird. Damit verliert zwar die konkrete Frage nach den rechtlichen Rahmenbedingungen dieser Dateien an Relevanz. Das Problem präsentiert sich aber angesichts der Frage nach den normativen Konturen der geplanten technologischen Infrastruktur mit mindestens ebenso großer Dringlichkeit in neuem Gewand.

gg) Zusätzliche Datenakkumulation in INPOL durch Hinweise

Neben den Dateistrukturen, in denen sich dateizweckspezifische Daten ansammeln, hat sich in der polizeilichen Informationsverarbeitung über die Zeit hinweg ein Hinweissystem etabliert. Im Rahmen dieses Systems können zu bereits gespeicherten Personen – aus Perspektive der Polizei – sinnvolle Ergänzungen in die Informationsbestände aufgenommen werden. So werden polizeiliche Beobachtungen der Realität, vor allem aber auch

949 Siehe dazu und zum Folgenden etwa die Errichtungsanordnung zur Datei „Gewalttäter Links", https://fragdenstaat.de/dokumente/5281-ifg_bka_pmk-links_eao/ (Stand: 01.10.2023).

950 Siehe zur informationellen Durchleuchtung der sogenannten „Sympathisantenszene" im Zuge des RAF-Terrors oben S. 126 ff.

951 Siehe dazu *Arzt* Neue Juristische Wochenschrift 2011, 352.

952 Zu beiden Entwicklungen unten S. 268 ff.

Deutungen und Interpretationen derselben in Form sogenannter personengebundener (PHW) oder ermittlungsunterstützender (EHW) Hinweise, Teil der Datenakkumulationen zu einzelnen Personen. Das mag den Datendoubles[953] mehr Kontur und Greifbarkeit für die polizeiliche Arbeit verschaffen. Das Labeln mit solchen Hinweisen ist aber immer auch verkürzend und reproduziert eingeübte und stabilisierte Bilder, die die Polizei von ihren „Gegenübern" hat.

Die Rechtsgrundlage zur Verarbeitung für PHW und EHW ist nunmehr in § 16 Abs. 6 Nr. 1 und 2 BKAG geregelt. Die Hinzuspeicherung von Hinweisen kann anlasslos erfolgen, was mit Blick auf den Verhältnismäßigkeitsgrundsatz problematisch ist,[954] auch wenn § 16 Abs. 6 Nr. 1 BKAG sich auf Personen nach § 18 Abs. 1 BKAG bezieht.[955] Insbesondere § 16 Abs. 6 Nr. 2 BKAG ermöglicht zudem eine kaum eingegrenzte Speicherung von Hinweisen – auch über „Dritte", wenn auch zu deren Schutz – nach polizeilichem Ermessen und wird deshalb auch als aufgrund von Unverhältnismäßigkeit für verfassungswidrig gehalten.[956]

PHW werden in der BKADV in § 2 Abs. 1 Nr. 15 konkretisiert: Es sind solche Hinweise, die dem Schutz des Betroffenen dienen wie „Freitodgefahr" oder die die Eigensicherung der ermittelnden Bediensteten bezwecken wie „bewaffnet", „gewalttätig", „Explosivstoffgefahr". Dabei handelt es sich allerdings nur um beispielhafte Nennungen von Hinweisen. In der polizeilichen Praxis werden so etwa Hinweise verwendet wie: BEWA, Bewaffnet; GEWA, Gewalttätig; AUSB, Ausbrecher; ANST, Ansteckungsgefahr; GEKR, Geisteskrank; BTMK, BtM-Konsument; FREI, Freitodgefahr; PROS, Prostitution; VEMO, Straftäter verbotener militanter Organisation/Vereinigung/Partei/Gruppe; REMO, Straftäter rechtsmotiviert; LIMO, Straftäter linksmotiviert; AUMO, Straftäter politisch motivierter Ausländerkriminalität; EXPL, Explosivstoffgefahr; SEXT, Sexualtäter; HWAO, Häufig wechselnder Aufenthaltsort.[957] Deren Festlegung und die Kriterien für ihre Vergabe sind in einem nicht-öffentlichen PHW-Leitfaden niedergelegt.[958] Zur Vergabepraxis ist quasi nichts bekannt. Es soll bei Vergabe von Hin-

953 Siehe zu diesem Begriff bereits oben S. 55 ff.
954 *Bäcker*, A-Drs. 18(4)806 D, S.16.
955 *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 21.
956 So *Bäcker*, Schriftsatz der Verfassungsbeschwerde im Verfahren 1 BvR 1160/19, S. 62 f., abrufbar unter: https://freiheitsrechte.org/home/wp-content/uploads/2019/10/2019-05-21-BKA-Gesetz-VB-anonymisiert.pdf (Stand: 01.10.2023).
957 ULD, Tätigkeitsbericht 2010, S. 41.
958 WD 3 - 3000 - 063/19, S. 6.

weisen eine Einzelfallprüfung mit Blick auf Geeignetheit, Erforderlichkeit und Angemessenheit erfolgen.[959] Allerdings gibt es abweichende Praktiken bei der Verwendung bestimmter Hinweise,[960] was eine länder- und polizeispezifische Informationspraxis impliziert und auf die Grenzen normativer Steuerbarkeit polizeilicher Informationspraktiken durch opake Richtlinien hindeutet. So gibt es beispielsweise zusätzlich zu den oben genannten PHW in Sachsen noch JUNI, Jugendlicher Intensivtäter; LAST, Land- oder Stadtstreicher; SGRB, Sogenannter Reichsbürger; DROG, Konsument harter Drogen oder auch SPRY, Sprayer.[961] Solche länderspezifische Hinweise sind vor allem dann nicht unproblematisch, wenn Hinweise, wie es regelmäßig geschieht, aus den Ländern heraus in INPOL-Z gespeichert werden. Auf diese Weise können verschiedene Hinweispraktiken zu Diskrepanzen in der Kategorisierung führen, was unter Gerechtigkeitsgesichtspunkten, aber auch mit Blick auf die Richtigkeit von Daten – sofern man davon bei den stark interpretatorisch geprägten PHW überhaupt sprechen kann – kritikwürdig ist. Rechtlich einschlägig für viele der Hinweise oder der ihnen zugrundeliegenden Daten wäre auch § 48 BDSG, der die Vorgaben der JI-Richtlinie zur Verarbeitung besonderer Kategorien personenbezogener Daten umsetzen soll. Inwieweit das Kriterium der unbedingten Erforderlichkeit der Verarbeitung sowie die Garantien für die Rechtsgüter der Betroffenen eingehalten wurde bzw. umgesetzt worden sind, ist nicht bekannt – beides erscheint indessen mit Blick auf die langjährige Hinweispraxis zweifelhaft.

Zusätzlich sind PHW inhaltlichen Bedenken ausgesetzt: Hinweise wie „Häufig wechselnder Aufenthaltsort" lassen zudem vermuten, dass sich dort diskriminierende Polizeipraktiken gegenüber Minderheiten wie Sinti:zze und Rom:nja lediglich nominal verändert fortschreiben.[962] Noch 2017 wurde aber auch von ganz expliziten Hinweisen wie „Sinti", „Roma" oder sogar „Zigeuner" berichtet.[963] Die Problematik, dass es sich bei „HWAO" zudem um im Wesentlichen legales Verhalten handelt, trifft auch auf Hinweise wie „Ansteckungsgefahr", „Geisteskrank" oder „Prostitution" zu. Durch eine solche Gefahrenwahrnehmung, die einen prüfenden Blick auf legales Ver-

959 Hamburger Bürgerschaft-Drs. Drucksache 20/13106, S. 2.
960 Hamburger Bürgerschaft-Drs. Drucksache 20/13106, S. 1.
961 Sächs. LT-Drs. 6/16086, Anlage 1.
962 Ausführlicher dazu *Töpfer*, (Dis-)Kontinuitäten antiziganistischen Profilings im Zusammenhang mit der Bekämpfung „reisender Täter", Forschungsbericht zur Vorlage bei der Unabhängigen Kommission Antiziganismus, 2020.
963 *Mayer* Süddeutsche Zeitung v. 17. Juni 2021.

halten institutionalisiert, werden mehr Teile des Sozialen unter polizeiliche Aufsicht gestellt, als durch einen reinen Fokus auf strafrechtlich relevantes Verhalten.[964] Dass PHW zudem Interaktionen zwischen gespeicherten Personen und der Polizei eskalativ vorstrukturieren können, legt der polizeiliche Umgang mit psychisch kranken und gestörten Personen nahe, bei dem es in der Vergangenheit immer wieder auch zum Tod der Betroffenen kam.[965] Ähnliche Wirkungen dürften alle PHW haben, die eine gewisse personeninhärente Gefährlichkeit implizieren.

Ermittlungsunterstützende Hinweise werden in § 2 Abs. 1 Nr. 16 BKADV konkretisiert: Es handelt sich um solche, die Ermittlungsunterstützung dienen wie „Sexualstraftäter", „Straftäter politisch links motiviert" oder „Straftäter politisch rechts motiviert". Auch hierbei handelt es sich nur um Beispiele. Verwendet werden Hinweise wie BTKU, BTM-Handel (Kurier); BTMA, BTM-Handel (Abnehmer); BTMH, BTM-Handel (Händler); BTML, BTM-Handel (Lieferant); BTMP, BTM-Handel (Produzent); EINB, Einbrecher; GEFB, Gefährdung (Brandstifter); GEFH, Gefährdung (Häusliche Gewalt); GEFS, Gefährdung (Stalker); IDDO, Identität (Dokumentenbeschaffer); IDEN, Identität; IDPA, Identität (Passüberlasser); INTS, Intensivtäter (Sportveranstaltungen); JIHA, Reisender in/aus Jihad-/Krisengebiet; KFZD, Kraftfahrzeug-Dieb; MENA, Menschenhandel (Anwerber); MENS, Menschenhandel (Schleuser); MENV, Menschenhandel (Vermieter); MENZ, Menschenhandel (Zuhälter); PMKA, Politisch motivierter Straftäter (PMK -ausländische Ideologie-); PMKL, Politisch motivierter Straftäter (PMK -links-); PMKN, Politisch motivierter Straftäter (PMK -nicht zuzuordnen-); PMKR, Politisch motivierter Straftäter (PMK -rechts-); PMRE Politisch motivierter Straftäter (PMK -religiöse Ideologie-); REIB, Reichsbürger/Selbstverwalter; REIT, Reisender Täter; ROCK, Rocker; SCHM, Schmuggler; SEXT, Sexualtäter; TDIE, Trick-/Taschendieb[966] oder neuerdings auch CLAN, Clankriminalität und CLAN-UMFELD, Clankriminalität Umfeld.[967]

Bei diesen EHW sind Überschneidungen mit einigen PHW zu beobachten (etwa REIT und HWAO). Bei den EHW ist indessen (noch) weniger deutlich, welchem polizeilichen Zweck die Hinweise dienen sollen. So

964 *Kretschmann* in Legnaro/Klimke (Hrsg.), Kriminologische Diskussionstexte II, 139 (155).
965 *Derin/Singelnstein,* Die Polizei: Helfer, Gegner, Staatsgewalt, 152 f.
966 Diese Hinweise werden ersichtlich aus Sächs. LT-Drs. 6/18032, Anlage 1.
967 Bln. AH-Drs. 18/24342, S. 1.

findet sich beispielsweise die Ansicht, EHW seien „Hinweise auf Besonderheiten einer natürlichen Person, die primär dazu geeignet sind, einen polizeilichen Kontext zu verdeutlichen, polizeiliches Handeln zielgerichteter zu steuern bzw. zu unterstützen, oder die dem Schutz Dritter dienen. Sie sind darüber hinaus auch geeignet, Datenbestände für Ermittlungen zu kennzeichnen bzw. zu selektieren."[968] Da auch die EHW anhand einer nicht-öffentlichen Richtlinie vergeben werden, ist diese Form der Datenverarbeitung aufgrund der schwächer ausgeprägten Zweckbestimmung der EHW im Vergleich zu den PHW problematisch, ein Zustand, der durch die anscheinend geplante Umwandlung von PHW in EHW[969] verschärft wird. Insofern ist *Arzt* zuzustimmen, der anlässlich der EHW von „eine[r] rechtlich schwer abzugrenzende[n] und normenklar einzuhegende[n] Gemengelage" spricht.[970]

hh) Der Polizeiliche Informations- und Analyseverbund

Eine besondere und jüngere Entwicklung des polizeilichen Informationswesen in seinen verbundmäßigen Ausformungen stellt das Projekt des Polizeilichen Informations- und Analyseverbundes (PIAV) dar. PIAV kann als Antwort auf eine empfundene Trägheit des polizeilichen Informationswesens gelesen werden. Die eher starre Struktur konnte auch durch die verschiedenen delikts- und phänomenbezogenen Dateien nicht in einer befriedigenden Weise dynamisiert werden, sodass als Lösung der PIAV konzipiert wurde, in welchem übergreifende, auf bestimmte Kriminalitätsphänomene bezogene Dateien – nach Relevanzprüfung – einschlägige Informationen und personenbezogene Daten zusammenfassen.[971] Es handelt sich nach Angaben des Bundesministeriums des Innern um einen Informationsverbund zur länderübergreifenden Kriminalitätsanalyse, der aus einer operativen und einer strategischen Komponente besteht und technisch durch das BKA bereitgestellt wird. Zweck des Verbundes ist es, einen medienbruchfreien und durchgängigen Informationsaustausch zwischen den Teilnehmern zu ermöglichen, um Tat-Tat, Tat-Täter- und Täter-

968 BT-Drs. Drucksache 18/5659, S. 18.
969 BT-Drs. Drucksache 18/5659, S. 18.
970 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1248.
971 BT-Drs. 16/12600, S. 56.

Täter-Zusammenhänge delikt- und phänomenübergreifend zu erkennen.[972] Strukturell ähnelt der PIAV dem INPOL-Verbund: Der Informationsverbund besteht aus dem PIAV-Zentralsystem und den 19 Teilnehmersystemen von Bund (Bundeskriminalamt, Zollkriminalamt und Bundespolizei) und Ländern. PIAV gilt als „das derzeit bedeutsamste föderale Software- und Organisationsentwicklungsvorhaben zur Fortentwicklung der Polizeiarbeit in Deutschland" und „hat den Anspruch, die Auswertungs- und Ermittlungsarbeit im Verbund zu stärken und die Informationszusammenarbeit der Polizeien des Bundes und der Länder auf eine technisch, fachlich und organisatorisch zeitgemäße Basis zu stellen."[973]

Neben der strukturellen Verbesserung des Informationsflusses im polizeilichen Informationswesen soll PIAV auch der Verbesserung des nicht mehr ganz zeitgemäßen Kriminalpolizeilichen Meldedienstes (KPMD) dienen.[974] Dieses alte Informationsinstrument[975] soll dafür sorgen, dass Polizeidienststellen bei Delikten, bei denen der Verdacht auf überregionale Relevanz besteht, Meldung an ihr jeweiliges Landeskriminalamt machen können, das dann wiederum nach Prüfung der Relevanz an das Bundeskriminalamt weiterleiten kann, wo die Daten dann gesammelt zur Verfügung gestellt werden können.[976] Vor allem diese Meldewege sowie die häufig notwendigen Mehrmalerfassungen, die durch den KPMD bedingt werden, sollen durch den PIAV wesentlich verbessert werden. Die Verbundstruktur des PIAV soll hier Abhilfe schaffen, indem die Daten zentral gesammelt und dann einem „transbehördlichem Zugriff" freigegeben werden.[977] Im Anschluss sollen die Daten über eine gemeinsame webbasierte Oberfläche durchsuchbar sein.[978] In der operativen Komponente des PIAV (PIAV-O) werden so Module, ähnlich den dadurch gleichfalls abzulösenden alten INPOL-Falldateien, zu bestimmten Phänomenbereichen eingerichtet. So sind die Bereiche "Waffen- und Sprengstoffkriminalität", „Rauschgiftkriminalität" und „Gewaltdelikte/gemeingefährliche Straftaten"

---

972 BT-Drs. 19/15346, S. 8.
973 Bundesministerium des Inneren, White Paper Polizei 2020, S. 28.
974 https://police-it.net/category/polizeiliche-informationssysteme/polizeiliche-bund-laender-informationssysteme/piav-polizeilicher-informations-und-analyseverbund (Stand: 01.10.2023).
975 Siehe dazu bereits oben S. 112 ff.
976 Amtsblatt für Brandenburg – Nr. 9 vom 28. Februar 2001, S. 190.
977 *Egbert* in Hunold/Ruch (Hrsg.), Polizeiarbeit zwischen Praxishandeln und Rechtsordnung, 77 (85).
978 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (19).

seit 2016 bzw. 2018 aktiv. Die Umsetzung von „Cybercrime", „Dokumentenkriminalität", „Schleusung/Menschenhandel/Ausbeutung", „Sexualdelikte" und „Eigentumskriminalität/Vermögensdelikte" erfolgte 2020.[979] Weitere Komponenten, wie „Politische motivierte Kriminalität", „Organisierte Kriminalität" und „Wirtschaft- und Umweltkriminalität" sollten 2021 in den Wirkbetrieb gehen.[980] Diese Komponenten werden über Schnittstellen mit den Fall- bzw. Vorgangsbearbeitungssystemen[981] der jeweiligen Polizeien mit den jeweils freigegebenen Daten gespeist.[982]

Die operative Komponente ergänzen soll PIAV-S, also die strategische Nutzung der Daten im PIAV. PIAV-S soll dabei helfen, Schwerpunkte zu setzen und die polizeilichen und politischen Führungs- und Entscheidungsebenen zu beraten. Dafür soll es ausgewählte Personen-, Fall- und Sachdaten aus den Vorgangs- oder Fallbearbeitungssystemen der Polizeibehörden bereitstellen und eine tagesaktuelle, orts- und personenbezogene Zählung von Straftaten ermöglichen. Da die dabei verwendeten Daten nach Ansicht des Bundesbeauftragten für Datenschutz und Informationssicherheit nur pseudonymisiert sind und somit weiterhin Personenbezug bestünde, würde die Verarbeitung von Daten in PIAV-S derzeit ohne eigentlich erforderliche Rechtsgrundlage erfolgen.[983]

Überhaupt werden die Konturen des PIAV, soweit bisher ersichtlich, vor allem durch die konzeptuellen Grundlagen und tatsächliche technische Umsetzungsbemühungen gezogen. Worauf der Verbund rechtlich fußt, ist nicht eindeutig klar. Denkbar wäre es, dass PIAV einen rechtlichen Ankerpunkt ebenfalls in § 29 BKAG hat, da INPOL durch den neuen Verbund eine gewisse Ergänzung erfahren soll. Auch eine Errichtungsanordnung, wie sie zumindest für andere Verbundsysteme vorliegt, scheint für PIAV jedoch zu fehlen. In einer IfSG-Anfrage wird vom Bundeskriminalamt im Zusammenhang mit PIAV auf die Errichtungsanordnungen der Quelldateien verwiesen.[984] Diese Errichtungsanordnungen können aber keinen, quasi mosaikhaften, rechtlichen Rahmen für den PIAV bilden. Die Bun-

979 BT-Drs. 19/27083, S. 7.
980 BT-Drs. 19/15346, S. 8.
981 Zu beiden Systemtypen siehe unten S. 254 ff. sowie S. 259 ff.
982 BT-Drs. 19/15346, S. 8.
983 BfDI, Tätigkeitsbericht für das Jahr 2020 (29. Tätigkeitsbericht), BT-Drs. 19/26681, S. 56 f.
984 https://fragdenstaat.de/anfrage/errichtungsanordnungen-im-zusammenhang-mit-polizei-analyse-system-piav/17859/anhang/20140613antwort-bka.jpg (Stand: 01.10.2023).

desregierung scheint davon auszugehen, dass die Teilkomponenten der PIAV-Teilnehmerbehörden im Wesentlichen auf polizeirechtliche Generalklauseln und die strafverfahrensrechtlichen Vorschriften (§§ 438 ff. StPO) zur Datenverarbeitung gestützt werden können.[985] Mit Blick auf die beabsichtigte informationelle Schlagkraft des PIAV sind diese angenommenen Rechtsgrundlagen nicht ausreichend. In der Folge scheint dieses so relevante neue Verbundsystem der Polizei gegenwärtig keine hinreichende Rechtsgrundlage aufzuweisen. Damit wird das hergebrachte Verhältnis zwischen technologischer Entwicklung des polizeilichen Informationswesens und diesbezüglicher legislativer Steuerungsverantwortung – erst entwickeln, dann rechtlich (unzureichend) abbilden – auch bei gegenwärtigen Entwicklungen für die Zukunft fortgeschrieben.

c) Vorgangsbearbeitungssysteme

Neben den bundesweiten polizeilichen Datennetzen wie INPOL und neuerdings auch PIAV haben die Bundes- und Landespolizeiorganisation zudem alle Vorgangsbearbeitungssysteme,[986] die jeweils absolut integraler Bestandteil des polizeilichen Informationshandelns und damit der polizeilichen Alltagsarbeit in den entsprechenden Organisationen sind. Die administrativ anmutende Bezeichnung dieser Informationssysteme ist dabei indessen nur teilweise treffend. Administrative Tätigkeiten wie die Vorgangsverwaltung und Dokumentation sind Teil des Funktionsumfangs, aber die Systeme dienen darüber hinaus vor allem der polizeilichen Aufgabenerfüllung im Allgemeinen, womit die beiden klassischen Zwecke der Strafverfolgung und Gefahrenabwehr mit ihren jeweiligen Unterfällen, aber auch die Strafverfolgungsvorsorge und Straftatenverhütung als Vorfeldbefugnisse angesprochen sind. Auch Ordnungswidrigkeiten werden mitunter in den Vorgangsbearbeitungssystemen untergebracht. Kurz: „In polizeilichen Vorgangsbearbeitungssystemen werden alle polizeilich relevanten Vorgänge

985 So zumindest für die PIAV-Komponenten der Bundespolizei, vgl. BT-Drs. 19/15436, S. 24 ff.

986 Zu den verschiedenen Bezeichnungen siehe *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1180 mwN; in ihren Funktionalitäten sollen sich diese hingegen nur wenig unterscheiden, siehe *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 5.

aus dem operativen Kernbereich der polizeilichen Arbeit erfasst und geführt."[987] Als Informationsinstrument weisen die Vorgangsbearbeitungssysteme also eine hohe Multifunktionalität auf, was sich auch in der von den Polizeien für sie angenommenen Rechtsgrundlagen[988] ablesen lässt: Neben den strafverfahrensrechtlichen Vorschriften der §§ 161, 163, 483 ff. StPO sind vor allem diejenigen Vorschriften in den jeweiligen Polizeigesetzen einschlägig, die die Datenverarbeitung generell zur Aufgabenerfüllung nach jeweiligem Polizeigesetz, aber auch zu anderen Zwecken wie der Dokumentation, der Vorgangsverwaltung, der Datenschutzkontrolle oder zur Datensicherung freigeben. Während hierbei auch Aspekte der Kontrolle polizeilichen Handelns angesprochen sind, ergibt sich mit einem Verweis auf die gesetzliche Aufgabenerfüllung und die regelmäßig in Polizeigesetzen enthaltene Befugnis, strafverfahrensrechtlich relevante Daten auch zum Zwecke der Gefahrenabwehr weiterzuverarbeiten, ein breites Feld an gesetzlich freigegebenem Datenumgang, das mit Blick auf das verfassungsrechtliche Zweckbindungsprinzip wenig beschränkt erscheint. Hinzu kommt, dass es keine die Systeme als technische Infrastruktur ordnenden Vorschriften gibt, wie es beispielsweise mit §§ 29 ff., 13 BKAG für INPOL-Z und INPOL-Bund der Fall ist.[989] Auch die Vorgangsbearbeitungssysteme werden aber mitunter noch weiter durch Errichtungsanordnungen konkretisiert.[990]

Um die Polizeien bei der Erfüllung ihrer Aufgaben zu unterstützen, sind in den Vorgangsbearbeitungssystemen in großem Umfang auch personenbezogene Daten über Beschuldigte, Geschädigte, Zeug:innen und andere, wie etwa Kontakt- und Anlasspersonen enthalten, wobei die unterschiedlichen Verarbeitungsvoraussetzungen zu beachten sind. Umfassend werden auch Sachverhalte zu Gefahrenabwehr- oder Strafverfolgungsvorgängen aufgenommen, sodass für sämtliche polizeilich erfassten Vorgänge der jüngeren Zeit zahlreiche Datenpunkte zu Personen, Objekten und

987 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

988 Siehe dazu beispielhaft die Rechtsgrundlagen von Nivadis, dem niedersächsischen Vorgangsbearbeitungssystem, NdsLT-Drs. 16/2770, Anlage 1, S. 3.

989 Ausnahme ist § 13c SOG LSA, der aber im Wesentlichen nur § 13 BKAG kopiert und damit vor allem einen normativen Anknüpfungspunkt für die INPOL-Land-Komponente aus Sachsen-Anhalt bietet dürfte, nicht hingegen für das dortigen Vorgangsbearbeitungssystem.

990 Siehe etwa Errichtungsanordnung ViVA, https://fragdenstaat.de/dokumente/3242-verfahren-zur-integrierten-vorgangsbearbeitung-und-auskunft/ (Stand: 01.10.2023).

Vorgängen vorliegen. Mit mehreren hundert festgelegten Datenkategorien[991] und zusätzlichen Freitext-Speicherungen[992] bieten die Vorgangsbearbeitungssysteme die Möglichkeit zur granularen Wirklichkeitserfassung. Mit ihrem breiten Informationsfundament bilden die Systeme auch eine Grundlage für Ermittlungsakten der Polizeien, wobei hier auch häufig zusätzlich noch mit Fallbearbeitungssystemen[993] gearbeitet wird. Die vorgangsbezogene Struktur der Systeme wird in einem solchen Fall durch eine parallele personenbezogene Struktur ergänzt, womit die Führung der (elektronischen) Kriminalakte nach der bereits erwähnten KpS-Richtlinie im selben System ermöglicht wird.[994] Geht bereits diese Funktionalität streng genommen über die reine Vorgangsbearbeitung hinaus,[995] so vereinen einige Vorgangsbearbeitungssysteme unter einer Oberfläche neben der Vorgangsbearbeitung noch weitere Komponenten, wie INPOL-Land, und verzahnen beides dann mit Schnittstellen zu anderen Informationssystemen wie INPOL-Z, staatsanwaltschaftlichen Systemen, Fallbearbeitungssystemen und sonstigen Datenspeichern, die zu polizeilichen Analyse-, Dokumentations- und Informationszwecken genutzt werden können.[996] Die Verarbeitung von personenbezogenen Daten zur Aufgabenerfüllung in den polizeilichen Vorgangsbearbeitungssystemen kann vor dem Hintergrund der Vielfalt möglicher Datenpunkte als zumindest potentiell sehr eingriffsintensiv eingestuft werden. Umso mehr gilt dies in Fällen, in denen wiederum „besondere Kategorien personenbezogener Daten" betroffen sind, denn auch die Vorgangsbearbeitungssysteme enthalten das zuvor besprochene Hinweissystem[997] und arbeiten darüber hinaus mit festgelegten Da-

991 NdsLT-Drs. 16/2770, Anlage 1, S. 4 ff.

992 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

993 Dazu sogleich unter S. 259 ff.

994 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

995 So *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 11.

996 Siehe Errichtungsanordnung ViVA, S. 1 f., https://fragdenstaat.de/dokumente/3242-verfahren-zur-integrierten-vorgangsbearbeitung-und-auskunft/ (Stand: 01.10.2023).

997 Siehe dazu oben S. 247 ff.

tenpunkten, die Kategorien des § 48 BDSG berühren, etwa im Kontext von Staatschutzdelikten oder von als ausländisch klassifizierten Täter:innen.[998]

Neben den originären polizeilichen Zwecken dienen die Vorgangsbearbeitungssysteme, wie bereits erwähnt, auch noch weiteren, eher administrativen Zwecken. Ist die Aufgabenerfüllung einmal abgeschlossen, sollten die dazu verarbeiteten Daten nicht mehr zu repressiv- oder präventivpolizeilichen Zwecken zur Verfügung stehen. Nach einem Statuswechsel sollten die Vorgänge in einen durch technisch-organisatorische Maßnahmen abgegrenzten Bereich gelangen, der nicht mehr ohne Weiteres für die alltägliche Informationsarbeit zur Verfügung steht, sondern nur noch für Zwecke der Vorgangsverwaltung, Dokumentation oder Datenschutzkontrolle genutzt werden kann.[999] Vorgangsverwaltung meint dabei das Auffinden von Vorgängen zur Dokumentation und Überprüfung, dass polizeiliches Handeln rechtmäßig war, insbesondere im Zusammenhang mit verwaltungsgerichtlichen Klagen.[1000] Allerdings gestatten die Polizeigesetze regelmäßig einen Durchbruch dieser eher archivisch-administrativen Zweckbindung zu Zwecken der Aufgabenerfüllung, also für Gefahrenabwehr und Strafverfolgung. In der Regel erfolgt allerdings eine Beschränkung der neuen alten Zwecke auf Maßnahmen, die dem Schutz von Leib, Leben oder Freiheit bzw. der Verhütung schwerer, in der Regel „terroristischer" Straftaten dienen. Dabei ist die Möglichkeit, die Daten wieder zur – wenn auch im Umfang beschränkten – originären polizeilichen Aufgabenerfüllung verarbeitbar zu machen, nicht trivial: So speichert etwa die Bundespolizei in ihrem Aktennachweis etwa 40 Millionen Datensätze zu mehr als 830.000 Personen.[1001] Wenn solche Daten, die grundsätzlich nur noch zu Zwecken der Vorgangsverwaltung und Dokumentation verarbeitet werden dürfen, für eine Personensuche in den polizeilichen Systemen genutzt werden können, konterkariert das die bestehende Zweckbindung in erheblichem Ausmaß – das gilt auch, wenn nur sichtbar gemacht werden kann, dass die betroffene Person in irgendeiner Weise mit bestimmten Sachverhalten in Verbindung steht, weil die Daten im Wesentlichen gesperrt sind. Denn bereits hieraus ergeben sich Anhaltspunkte für polizeiliches Handeln, zumal gesperrte Daten mitunter – je nach technischer Ausgestaltung – über zweckdurchbre-

998 NdsLT-Drs. 16/2770, Anlage 1, S. 4 ff.
999 NdsLT-Drs. 16/2770, Anlage 1, S. 2.
1000 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1192.
1001 BT-Drs. 19/15346, S. 23.

chende Maßnahmen wieder sichtbar gemacht werden können.[1002] In der Vergangenheit wurde aber auch schon von Vorgangsbearbeitungssystemen berichtet, die diese Trennung überhaupt nicht kannten, was eine unrechtmäßig zweckdurchbrechende Verarbeitung durch die Polizei befördert.[1003] Auch zeitlich zweküberschreitende Verarbeitungen gibt es häufig in den Vorgangsbearbeitungssystemen, was nicht zuletzt an der Vielfalt der möglichen Verarbeitungszwecke liegt. Zwar gibt es sogenannte Aussonderungsprüffristen, nach denen überprüft werden muss, ob bestimmte Daten noch benötigt werden – das sind grundsätzlich fünf Jahre bei Erwachsenen.[1004] Allerdings fehlt es einerseits mitunter an klaren Regelungen zu solchen Prüf- und damit potenziell auch Löschfristen[1005] und andererseits können die damit beabsichtigten temporalen Begrenzungen der Speicherung im Vorgangsbearbeitungssystem durch sogenannte Mitziehautomatiken ausgehebelt werden. Dabei handelt es sich um Regelungen, die bei jeder Speicherung eines neuen Datenpunkts – etwa auch im Rahmen der Anzeige eines Bagatelldelikts – zu einer Person die Speicherfrist hinsichtlich aller gespeicherter Daten wieder auf Anfang setzt.[1006] Diese – treffend auch als „Jungbrunnen" bezeichnete – Regelung begünstigt strukturell ein zunehmendes Anwachsen der Datenbestände der Polizeien, was insgesamt im Widerspruch zu den normativen Postulaten von Erforderlichkeit, Datensparsamkeit und Datenminimierung steht.[1007]

Zudem verkomplizieren die Multifunktionalität der mit den Vorgangsbearbeitungssystemen verknüpften Quell- und Zielsysteme und die Vielfältigkeit der sich in den Systemen überlagernden Zwecke die Einhaltung dieser rechtlichen Vorgaben und machen aufwändige technisch-organisatorische Maßnahmen erforderlich, mit denen die Daten und ihre Verarbeitung auf ihre Rechtmäßigkeit hin überprüft und gegebenenfalls gelöscht werden können. Die wenigen, aber dafür häufig breiten und unübersichtlichen

1002 OVG Lüneburg 11. Senat, Urteil vom 11.07.2017, 11 LC 222/16, ECLI:DE:OVGNI:2017:0711.11LC222.16.00, Rn. 38.

1003 So der BfDI zum Vorgangsbearbeitungssystem der Bundespolizei, 26. Tätigkeitsbericht 2015/2016, S. 133 f. und auch zum System des Bundeskriminalamts, 28. Tätigkeitsbericht 2019, S. 55 f.

1004 Siehe dazu etwa die Erläuterung des Verfahrens durch den TLfDI, 11. Tätigkeitsbericht zum Datenschutz: öffentlicher Bereich 2014/2015, S. 231.

1005 BfDI, 28. Tätigkeitsbericht 2019, S. 56.

1006 *Bundesbeauftragte für Datenschutz und Informationssicherheit*, A-Drs. 18(4)806 A, S. 13 ff.

1007 So zutreffend *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1194.

Normen, die die Vorgangsbearbeitung regeln sollen, führen also zu einem nur wenig regulierten Datenumgang in den Vorgangsbearbeitungssystemen. Vor dem Hintergrund der in ihnen gespeicherten Datenvolumina[1008] gibt dieser Umstand Anlass zu Besorgnis, insbesondere mit Blick auf das zu erwartende weitere Anwachsen der Datenbestände des polizeilichen Informationswesens und auf die vielfältigen schnittstellenbasierten Vernetzungen der Vorgangsbearbeitungssysteme mit den übrigen Teilen des Informationswesens.[1009]

d) Kriminalpolizeiliche Informationsinstrumente: Strafverfolgungsdateien und Fallbearbeitungssysteme

Neben den bisher beschriebenen Verfahren und Systemen, die prinzipiell polizeirechtlich fundiert sind, existieren auch informationstechnische Instrumente, die in erster Linie der kriminalpolizeilichen und damit strafverfahrensrechtlichen Aufgabenerfüllung dienen.

Nach den Kriminalakten ist die nächstgrößte informationstechnische Einheit der Strafverfolgungsbehörden die Strafverfahrensdatei gem. § 483 ff. StPO. Die Grundnorm des § 483 StPO gibt dafür die Errichtung von Dateien recht breit – für Zwecke des Strafverfahrens – und niedrigschwellig – soweit es für diese erforderlich ist[1010] – frei, womit ein flexibles Informationsinstrument für die Strafverfolgungsbehörden, also auch die Polizei, besteht. Auch hinsichtlich der Datentypen besteht keinerlei Beschränkung. Der Gesetzgeber hatte auf eine solche Festlegung mit Blick auf die polizeiliche und auch staatsanwaltschaftliche Praxis bewusst verzichtet, wobei er davon ausging, dass die möglichen und erforderlichen Daten sowie die Spannbreite der notwendigen Datenfelder im Hinblick auf die jeweiligen

1008 So waren etwa in Sachsen 2018 9,1 Millionen Personen in 3,4 Millionen Datensätzen erfasst, SächsLT-Drs. 6/11770, Anlage, S. 1. In Niedersachsen waren 2010 3,8 Millionen Personen im dortigen Informationssystem erfasst, NdsLT-Drs. 16/2770, Anlage 1, S. 3. Diese Zahlen sind umso frappierender, wenn man bedenkt, dass die Vorgangsbearbeitungssysteme „landesbezogen" und „auf das Land […]" beschränkt sein sollen, a.a.O., S. 1.

1009 Siehe dazu etwa S. 439 ff.

1010 Gemeint ist hier die Erforderlichkeit der Verarbeitung in Dateisystemen, also eine Erforderlichkeit, die über die zur Datenverarbeitung in herkömmlicher Weise – regelmäßig gegenwärtig noch in Akten – hinausgeht. Das kann etwa aus Gründen der Wirtschaftlichkeit oder sonstigen Effizienz der Fall sein, vgl. Weßlau/Deiters in *J. Wolter* (Hrsg.), SK-StPO, § 483 Rn. 7.

fall- bzw. deliktspezifischen Bedürfnisse der speichernden Stelle sehr unterschiedlich sind, weswegen eine gesetzliche Eingrenzung nicht möglich sei.[1011] Insofern kann eine Kriminalakte komplett in einer solchen Datei abgebildet werden.[1012] Einschränkungen können und sollen sich aber für einzelne Dateien aus ihren jeweiligen Errichtungsanordnungen gem. § 490 StPO ergeben.[1013] Nichtsdestotrotz besteht hier mangels einer der BKADV vergleichbaren datenkonkretisierenden Verordnung eine normative Leerstelle, die vor allem durch die faktischen Datenverarbeitungspraktiken der Strafverfolgungsbehörden gefüllt werden dürfte.

In der Praxis verbreitete Dateitypen sind etwa solche zur Spurendokumentation, sogenannten „Spudok"-Dateien, in großen Verfahren. In Wirtschaftsstrafverfahren kommen zur Auswertung von Bilanzen, Buchhaltung und Finanzfluss eines Wirtschaftsunternehmens sogenannte intelligente Programme zur Anwendung, die Analysen und Verknüpfungen aufgrund einprogrammierter Suchkriterien vornehmen. Dateien können auch maßnahmenspezifisch etwa zur Auswertung im Anschluss an massenhafte Datengewinnung im Rahmen von Telekommunikationsüberwachungsmaßnahmen nach § 100a StPO oder Verkehrsdatenabfragen nach § 100g StPO errichtet werden. Zudem werden in Strafverfahren der Massenkriminalität zur arbeitsökonomischen Erledigung Dateien eingerichtet, um mit Textverarbeitungsprogrammen mit Eingabemasken automatisiert Schriftstücke zu erstellen.[1014] Dabei können die hier als getrennt beschriebenen Dateizwecke und weitere Funktionen auch mit Systemen zur dateiübergreifenden Arbeit verbunden werden.[1015] Die Möglichkeit zur stärkeren informationellen Verknüpfung der in einer Strafverfahrensdatei gespeicherten Daten bietet auch die Möglichkeit der Lokalisierung der Datei in einem polizeilichen Informationssystem gemäß § 483 Abs. 1 S. 2 StPO. Da eine solche Verknüpfung mit Blick auf die prinzipielle Bindung der Daten an den Zweck eines spezifischen Strafverfahrens aber zunächst möglichst zu unterbinden ist, legt § 483 Abs. 1 S. 3 StPO fest, dass die Daten entsprechend ihrer konkreten Strafverfahrensbindung zu konkretisieren sind (Nr. 1), ein Zugriffsberech-

1011 BT-Drs. 14/1484, S. 31.
1012 *Kersten* in *Abel,* Datenschutz in Anwaltschaft, Notariat und Justiz, S. 188.
1013 BT-Drs. 14/1484, S. 31.
1014 Als wenig geklärt gilt allerdings, inwiefern bestimmte Teile von und auch Metainformationen über Strafverfolgungsdateien zu den staatsanwaltschaftlichen Strafakten genommen werden müssen, vgl. etwa *Weßlau/Deiters* in *J. Wolter* (Hrsg.), SK-StPO, § 483 Rn. 9.
1015 *Weßlau/Deiters* in *J. Wolter* (Hrsg.), SK-StPO, § 483, Rn. 6.

tigungskonzept zu implementieren ist (Nr. 2) und Löschungsprüffristen festzulegen sind (Nr. 3). Dieser Versuch, die Zweckbindung normativ abzusichern, wird indessen bereits in § 483 Abs. 2 StPO relativiert, der die Datenverarbeitung auch für andere Strafverfahren freigibt, wobei begrenzend die für Übermittlung (§ 487 StPO) bestehenden Kautelen zu beachten sind – freilich nur, wenn für die zweckändernde Nutzung eine Übermittlung überhaupt erforderlich ist. Auch die Möglichkeit zum automatisierten Abruf gem. § 488 StPO schwächt die Zweckbindung, da eine Einzelfallprüfung der Übermittlungsvoraussetzungen entfällt. Zudem ist der Steuerungsanspruch der Strafprozessordnung mit § 483 StPO für Dateien, die in Informationssystemen der Polizei angesiedelt sind und auch Daten auf polizeirechtlicher Grundlage verarbeiten, relativiert, da hier auch für die strafverfahrensrechtlichen Daten nunmehr das Recht der Polizeien gilt. Der Einwand, der Bundesgesetzgeber behalte ohnehin über das BKAG erhebliche Regelungsmöglichkeiten,[1016] greift nur sehr bedingt durch: Einerseits ist diskutabel, inwieweit das dem BKAG unterfallende INPOL-System normativ tatsächlich durch das BKAG hinreichend konturiert wird. Andererseits gilt das BKAG gerade nicht für die rechtlich nur wenig geregelten Vorgangsbearbeitungssysteme, in denen aber auch Daten zu konkreten sowie künftigen Strafverfahren verarbeitet werden.[1017] Das prinzipielle Postulat der Zweckbindung von Strafverfahrensdaten, die regelmäßig als sensibel gelten dürften, erweist sich mithin schon aufgrund der gegenwärtigen Regelungslage als illusionär.[1018]

Neben den Vorgangsbearbeitungssystemen, die die polizeiliche Arbeit – wie beschrieben – sehr breit stützen, haben sich im strafverfahrensrechtlichen bzw. kriminalpolizeilichen Kontext ebenfalls breitere Informationssysteme, die sogenannten Fallbearbeitungssysteme, herausgebildet. Sie dienen der Unterstützung von kriminalpolizeilichen Ermittlungsverfahren, ermöglichen die vernetzte Darstellung und Auswertung von Ermittlungserkenntnissen und kommen mitunter auch im Bereich der Kriminalprävention zum Einsatz. In Fallbearbeitungssystemen werden einzelne Datenpunkte aus polizeilichen Ermittlungen gespeichert wie etwa Person, Adresse, Beruf, Straftaten, Veranstaltung, Firma, Waffe, et cetera. Diese Einzelinforma-

1016 *Weßlau/Deiters* in *J. Wolter* (Hrsg.), SK-StPO, § 483 Rn. 16.

1017 So etwa in @rtus-Bund, dem Vorgangsbearbeitungssystem der Bundespolizei, vgl. BT-Drs. 19/15346, S. 22.

1018 In ähnlichen Worten so bereits *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1287.

tionen können dann miteinander verknüpft werden. Zusätzlich können andere mediale Datenformate wie Fotografien, Filme oder Dokumente in die Datenbank geladen werden und sind wiederum verknüpfbar.[1019] Fallbearbeitungssysteme arbeiten dabei in erster Linie ereignisorientiert. Die vorhandenen personenbezogenen Daten werden also mit einem Ereignis verknüpft, das seinerseits mit weiteren Personen, Ereignissen, Institutionen oder Sachen verknüpft werden kann. Die Zahl der Verknüpfungsebenen ist nicht begrenzt, sodass die zu einer Person gespeicherten Daten zunehmend in größeren Datenbeständen diffundieren.[1020] Die Systeme dienen komplexeren Ermittlungen wie in bestimmten Phänomenbereichen oder Fällen mit umfassenden Sachverhalten. Entsprechend umfangreich sind die in den Systemen vorgehaltenen Daten. Es werden allerdings nicht nur Daten in den Systemen selbst vorgehalten. Vielmehr können bei entsprechenden Ermittlungen über Schnittstellen verschiedene polizeiliche Auskunftssysteme angesprochen werden und die Trefferdaten als neue Objekte in die Bearbeitung übernommen werden. Dabei richtet sich die Rechtsgrundlage der Systeme danach, wie die Fallbearbeitungssysteme konkret zur Ermittlungsunterstützung genutzt werden.[1021] Mangels konkreter Vorschriften ist die Rechtsgrundlage der Fallbearbeitungssysteme im allgemeinen Regelungskonzept der Strafprozessordnung zur Verarbeitung von Daten, den §§ 483 ff., zu suchen. Hier gilt dasselbe, wie auch für Strafverfolgungsdateien – als im Vergleich zu Fallbearbeitungssystemen eher untergeordnete informationstechnologische Einheit: Rechtlich möglich sind Ausgestaltung rein auf strafverfahrensrechtlicher Basis oder als Informationssysteme nach polizeirechtlichen Regelungen.[1022] Zur rechtlichen Konkretisierung kommen zudem auch Errichtungsanordnungen zum Einsatz,[1023] von denen allerdings, soweit ersichtlich, keine einzige veröffentlicht ist. Auf Grundlage der gesetzlichen Vorgaben ist es insofern – wie es für polizeiliche Informationssysteme typisch ist – nur begrenzt möglich, Aussagen über die Fallbearbeitungssysteme zu treffen. Bekannt ist aber, dass sie üblicherweise bei ge-

1019 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 15.

1020 BfDI, 26. Tätigkeitsbericht 2015/2016, S. 110.

1021 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 15.

1022 Siehe auch BfDI, 26. Tätigkeitsbericht 2015/2016, S. 110 f.

1023 BT-Drs. 17/8544 (neu), S. 32.

nerell umfangreichen und komplexen Ermittlungsverfahren, bei Mord- und Branddelikten in Sonderkommissionen, bei Serienstraftaten, in besonderen Phänomenbereichen (etwa Organisierte Kriminalität oder politisch motivierte Kriminalität) sowie bei Gefahrenabwehrlagen mit massenhaft anfallenden Informationen genutzt werden. Damit sind Fallbearbeitungssysteme eine informationstechnologische Weiterentwicklung der analogen kriminalpolizeilichen Karteikartensammlungen, Spurenakten und Handakten.[1024] Sind die polizeilichen Ermittlungen abgeschlossen, werden die Ergebnisse, die die Hauptspur der Ermittler stützen, in (wohl gegenwärtig überwiegend noch) analoger Form an die Staatsanwaltschaft übergeben. Diese Akte für die Staatsanwaltschaft enthält dann regelmäßig die wesentlichen Ermittlungsergebnisse, was nicht alle Inhalte aus dem Fallbearbeitungssystem miteinschließt. Neben nicht verfolgten Spuren finden etwa Massendaten wie etwa DNA-Proben, TKÜ-Daten, telefonische Abfragen oder andere digitale oder digitalisierte Daten, die mittels Schnittstelle oder Schreibkraft in das Fallbearbeitungssystem importiert wurden, normalerweise keinen Aktenrückhalt.[1025]

Neben der retrospektiven Ermittlungsarbeit bei begangenen Straftaten werden Fallbearbeitungssysteme aber auch prospektiv zum Zwecke der Kriminalprävention genutzt. Konkret geht es dabei zumeist um die Überwachung bestimmter Phänomenbereiche. Die Fallbearbeitungssysteme werden in diesem Kontext zur Speicherung und Analyse von Daten zum Zwecke der Beobachtung devianter Organisationen und Strukturen und zur Verhinderung der daraus drohenden Straftaten genutzt.[1026] Für die Speicherung von Personen zu diesem Zweck ist stets eine Negativprognose wie etwa in § 18 Abs. 1 Nr. 3 BKAG[1027] erforderlich, das heißt die betroffene Person muss einer Straftat verdächtig sein und wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkennt-

1024 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1025 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1026 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1027 Die Vorschriften des BKAG, die in diesem Absatz zitiert werden, stehen beispielhaft für vergleichbare Regelungen in den Polizeigesetzen.

nisse muss Grund zu der Annahme bestehen, dass zukünftig Strafverfahren gegen sie zu führen sind. Daneben können aber auch Anlasspersonen – das sind Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (§ 18 Abs. 1 Nr. 4 BKAG), mit in kriminalpräventive Datensammlungen aufgenommen werden.[1028] Dasselbe gilt auch für Kontaktpersonen gem. § 19 Abs. 1 Nr. 3 BKAG, wobei es sich um Personen handelt, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie mit in § 18 Abs. 1 Nr. 1-3 BKAG bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken. Darüber hinaus existiert auch die Praxis sogenannter Prüffälle, in denen eine vorsorgliche Speicherung zur vorbeugenden Kriminalprävention erfolgt, mit anderen Worten also erst noch geprüft werden muss, ob die ohnehin eher vagen und in der Praxis nicht immer beachteten Voraussetzungen[1029] einer Negativprognose oder die noch weiter heruntergefahrenen Voraussetzungen für die Bejahung einer Anlasspersoneneigenschaft vorliegen. Zwar sind diese Daten nur begrenzt verarbeitbar (siehe etwa § 18 Abs. 3 BKAG), stehen aber dennoch für die polizeiliche Arbeit im Kontext von vermuteter devianter Neigung und damit in stigmatisierender Weise zur Verfügung, ohne dass eine stichhaltige Tatsachengrundlage – verlässliche tatsächliche Anhaltspunkte fehlen in solchen Fällen gerade – vorläge.[1030] Konkret werden die Daten, die im Rahmen der Ermittlungen erhobenen wurden, zum Zweck der Kriminalitätsverhütung unterschiedlichen Phänomenbereichen zugeordnet (Rauschgift, Falschgeld, Organisierte Kriminalität, Staatsschutz etc.) und mit weiteren Ermittlungsinformationen der jeweils zuständigen Dienststellen angereichert, neu verknüpft und strukturiert. Im Gegensatz zum reinen Ermittlungsbereich können die Daten – je nach Rechtemodell

1028 Mit Einwilligung können auch die in § 19 Abs. 1 Nr. 1, 2, 4 BKAG genannten Personen in entsprechende Datensammlungen aufgenommen werden.

1029 HmbLfDI, 26. Tätigkeitsbericht 2016/2017, S. 33.

1030 Die zuvor ungeregelte und damit rechtswidrige Praxis, Personen mit dem Ziel der „Anreicherung" der Daten zu speichern (so und kritisch dazu BfDI, 24. Tätigkeitsbericht 2011/2012, S. 97; 26. Tätigkeitsbericht 2015/2016, S. 111) ist mit dem neuen § 18 Abs. 3 BKAG in begrenzter Form legalisiert worden.

– verfahrensübergreifend auf Landesebene ausgewertet werden. Allerdings kann es bei Bestehen von lokalen Kriminalitätsstrukturen aus polizeilicher Sicht sinnvoll sein, dass die diesbezüglichen Informationen auch von den lokalen Polizeiorganisationen bearbeitet werden.[1031] Der Umstand, dass eine solche Datenverarbeitung zu Zwecken der strukturellen Kriminalprävention dazu führt, dass Informationen weit über das einzelne anlassgebende Ermittlungsverfahren hinaus behalten werden, macht auch Fallbearbeitungssysteme zu invasiven Informationsinstrumenten.

e) Sonstige Informationssystemtypen

Darüber hinaus arbeiten die Polizeien in Bund und Ländern mit einer – mitunter als verwirrend bezeichneten[1032] – Vielzahl weiterer elektronischer Anwendungen und Systemen. Neben den bereits beschriebenen Komponenten des polizeilichen Informationswesens gibt es noch drei informationstechnische Fachverfahren, welche zentral für die polizeiliche Arbeit sind: Einsatzleit-, Einsatzprotokoll- und Lageinformationssysteme.

Einsatzleitsysteme ermöglichen in den Einsatzleitstellen der deutschen Polizeien die Koordinierung der Einsatzkräfte in den aktuellen Einsätzen und ermöglichen so einen Echtzeit-Überblick über laufende Einsätze und die darin eingesetzten Kräfte. Zu den einzelnen Einsätzen werden bestimmte Daten dokumentiert. Hierzu gehören der Einsatzanlass, die Einsatzmittel (etwa Funkrufname und Kategorisierung der eingesetzten Fahrzeuge), der Status („frei auf Wache“ oder „Einsatz übernommen“), die Einsatzobjekte (inkl. Gefahrenhinweise, Anfahrtshinweise, Hinweise zu Ansprechpartnern) sowie Geodaten zum Anzeigen von Einsatzorten in einem Geoinformationssystem. Es handelt sich dabei überwiegend um nicht-personenbezogene Daten. Für diejenigen Daten, die einen Personenbezug zulassen, gibt es in den Polizeigesetzen vereinzelte Rechtsgrundlagen, die die Aufzeichnung der Büger:in-Polizei- und Polizei-Polizei-Kommunikation im Kontext der Einsätze gestatten (vgl. etwa § 20 Abs. 11 HSOG). Die Daten

1031 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 16.

1032 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 5.

werden wenige Monate im Einsatzleitsystem gespeichert und dann automatisch gelöscht. Entwickelt sich jedoch aus einem Einsatz ein Ermittlungsvorgang, werden die relevanten Daten aus dem Einsatzleitsystem in das Vorgangsbearbeitungssystem und gegebenenfalls in das Fallbearbeitungssystem übernommen (vgl. etwa § 20 Abs. 11 S. 3 HSOG). Bei besonderen Einsatzlagen kann ein Löschverbot für alle mit dem Ereignis verbundenen Daten ausgesprochen werden. Die Einsatzleitsysteme sind temporäre Spiegelbilder des polizeilichen Alltagsgeschäfts. Hier gehen verschiedenste Meldung zu allen Fallarten ein und werden für eine gewisse Zeit gespeichert. So entsteht eine Momentaufnahme derjenigen gesellschaftlichen Problemlagen, die die Bevölkerung als polizeirelevant einstuft.[1033] Aufgrund der nur kurzen Speicherung und weil die Daten bei Relevanz in die genannten Informationssysteme diffundieren, ist die sehr oberflächliche Regelung dieser Systeme in den Polizeigesetzen für sich genommen akzeptabel. In den unterschiedlichen Informationssystemen angekommen, treten jedoch die bereits beschriebenen rechtlichen Problemlagen auf.

Einsatzprotokollsysteme (auch Einsatzdokumentationssysteme genannt) werden von den Polizeibehörden von Bund und Ländern bei der Bewältigung und Dokumentation größerer Einsätze eingesetzt, die einer Besonderen Aufbauorganisation bedürfen. Mit ihnen wird der Informationsfluss zwischen Einsatzführung und Einsatzkräften gewährleistet und protokolliert, so dass alle Beteiligten über alle benötigten Informationen verfügen.[1034]

Daneben treten schließlich noch die Lageinformationssysteme. Eine Lage im polizeilichen Sinne meint eine Situation, in der polizeiliches Handeln erforderlich ist, um der gesetzlichen Aufgabenerfüllung der Gefahrenabwehr und der Strafverfolgung nachzukommen. Lagen können angesichts vielfältiger Einsatzrealitäten sehr unterschiedlich aussehen. Eine grundsätzliche Unterscheidung besteht zwischen einsatzorientierten Lagen und eher größer dimensionierten Kriminalitätslagen oder Speziallagen. Letztere beschreiben große umfassende Phänomene und werden zumeist in Lagebildern erfasst (etwa Lagebild Rauschgiftkriminalität, Lagebild Organisierte

1033 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 10.

1034 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 13.

Kriminalität, Lagebild Cybercrime). Einsatzorientierte Lagen beziehen sich dagegen auf konkrete Einsatzsituationen und beschreiben Ausgangssituation und Geschehen vor Ort. Die Einsatzkräfte vor Ort übermitteln Lagemeldungen an die Einsatzführung. Die so zustande kommenden Lagebilder sind die Voraussetzung für ein zielgerichtetes polizeiliches Handeln und dienen dem Erkennen, der Analyse und der Prognose relevanter Ereignisse und Entwicklungen. Eine weitere spezielle und für das polizeiliche Handeln wichtige Form ist die sogenannte Tageslage (auch: tägliches Lagebild, Präsidiallage, Landeslage). Diese umfasst mindestens die wesentlichen Einsatzaktivitäten der vergangenen 24 Stunden. Mit Blick auf die Tageslage können alle Polizist:innen, v.a. aber auch die Polizeiführer:innen, einen schnellen Überblick über das jüngste Einsatzgeschehen ihrer Polizeibehörde erhalten, womit die Kontinuität der polizeilichen Aufgabenerfüllung gewährleistet wird. Die Tageslage ist zumeist in unterschiedliche Bereiche wie Einsatzlage, Kriminalitätslage und Verkehrslage gegliedert, womit eine Übersicht über bekannte Störungen des gesellschaftlichen Lebens – etwa in Form von Bränden, Wohnungseinbrüchen oder Verkehrsunfällen – im Zuständigkeitsbereich der jeweiligen Polizeiorganisation ermöglicht wird. Die Tageslage wird weiter durch Informationen wie Fahndungen, Festnahmen und Ähnliches ergänzt. Alle konkreten Lageinformationen beschreiben kurz das Geschehen sowie den Einsatz der Polizei. Lagen können bei der Polizei durch sogenannte Lageinformationssysteme elektronisch erstellt werden. Diese Funktionalität kann auch ins Vorgangsbearbeitungssystem integriert sein. Aus Einsatzleitsystem und Vorgangsbearbeitungssystem, in denen alles Einsatzhandeln dokumentiert ist, werden bestimmte Daten automatisiert in das Lageinformationssystem übernommen. Dort werden die Geschehnisse mit einer kurzen Beschreibung in chronologischer und/oder geographischer Ordnung dargestellt, wobei häufig die Möglichkeit der Kartendarstellung implementiert ist. Je nach polizeilichem Bedarf können Lagen gefiltert dargestellt werden. Ungeachtet des traditionellen Begriffs der Tageslage können Lageinformationssysteme auch Zeiträume von mehr als 24 Stunden abdecken und somit über größere Zeiträume das Einsatzgeschehen nachhalten. Die Tageslagen werden wenige Monate im System gespeichert und dann automatisiert gelöscht.[1035] Ähnlich wie auch andere neuere Systeme dienen Lageinformationssysteme der Dynamisierung der

1035 *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 14.

polizeilichen Informationsbestände und damit einer Nutzung der vorgehaltenen Daten zur möglichst optimalen Aufgabenerfüllung durch die Polizeien in ihren jeweiligen Tätigkeitsfeldern.

Neben diesen einsatzunterstützenden Systemen wurden in jüngerer Zeit und im Kontext von Massendatentechnologien zudem sogenannte Analysesysteme entwickelt, die zunehmend in der Polizei zur bestmöglichen Informationsgewinnung aus den weitläufigen Datenbeständen eingesetzt werden, die der Polizei zur Verfügung stehen. Da diese Systeme jedoch paradigmatisch für den Wandel des polizeilichen Informationswesens stehen, werden sie auch im Rahmen dieser nun zu behandelnden Entwicklung dargestellt.

3. Die neue Informationsarchitektur der Polizei

Als Agglomeration von Datenbeständen, Informationssystemen und sonstigen informationstechnischen Anwendungen sowie unterschiedlichen Informationspraktiken ist das polizeiliche Informationswesen ein aus vielen beweglichen Teilen zusammengesetztes Ganzes – und als solches ist es ständig in Bewegung und im Wandel begriffen. Gegenwärtig durchläuft es jedoch eine Entwicklung – so ist es auch die der Arbeit zugrundeliegende Annahme – neuer Qualität, die gleichzeitig erzwungen wird, aber auch gewollt ist. Erzwungen wird der Wandel einerseits, weil das medienevolutive Massendatenphänomen, das informationstechnologisch angestoßen wurde und bereits jetzt mit vielfältigen sozialen Prozessen verzahnt ist, sich als makrostrukturelles Kraftfeld in den menschlichen Gesellschaften weder revidieren noch ignorieren lässt. Insofern zwingt es gesellschaftlich mächtige Akteure, wie die Polizei, zu reagieren. Andererseits ist der Wandel des polizeilichen Informationswesens auch von menschlicher Intentionalität getragen, denn innerhalb des massendatenbedingten Reaktionszwangs gibt es Handlungs- und Gestaltungsspielräume, die sicherheitspolitisch beeinflussbar sind. Insofern sind die vielfältigen, mittlerweile großteilig unter der Ägide des *Projekts 2020* versammelten Bemühungen zur technologiegemäßen Ausgestaltung des polizeilichen Informationswesens auch Ausdruck einer gewollten Evolution polizeilicher Informationsverarbeitung im Rahmen eines überwiegend technologiebegeisterten Sicherheitsdiskurses.

a) Rechtspolitische Ausgangslage

Die beschriebenen, sich gegenwärtig noch in Benutzung befindlichen Dateien im INPOL-Verbund sollen in den nächsten Jahren ihre klaren Grenzen verlieren und im Wesentlichen in einen großen polizeilichen Datenbestand überführt werden, um die Schaffung einer gemeinsamen, modernen, einheitlichen Informationsarchitektur zu ermöglichen. Seinen konkreten politischen Ursprung hat dieses Projekt in der sogenannten Saarbrückener Agenda, einem Papier der „Innenministerkonferenz" (IMK).[1036] Dieser den Logiken des Massendatenparadigmas entsprechende Schritt wurde hingegen im dazugehörigen Gesetzgebungsprozess als rechtspolitisch zwingend notwendiges Projekt präsentiert. Der Entwurf zur Gesetzesreform des BKAG nennt vorrangig das Urteil des Bundesverfassungsgerichts zum BKAG[1037] als primären Grund für die geplante Umstrukturierung der IT-Infrastruktur des Bundeskriminalamtes.[1038] Ob die Umstrukturierung nur aufgrund des verfassungsgerichtlichen Urteils alternativlos ist, lässt sich bezweifeln.[1039] Das Argument der verfassungsrechtlich bedingten Notwendigkeit der Umstrukturierung wirkt auch vor dem Hintergrund der historischen Entwicklung des Informationswesens vorgeschoben: Bereits die gegenwärtige Ausführung von INPOL, die mal als INPOL-neu geplant wurde und die bis dahin (2003) bestehende ursprüngliche Ausführung von INPOL („INPOL-alt") ablöste, war einmal sehr ähnlich zu gegenwärtigen Planungen konzipiert. Beamt:innen sollten von den an ihren Arbeitsplätzen verfügbaren Vorgangsbearbeitungssystemen je nach Berechtigung auf sämtliche Polizeidaten zugreifen können. Das Projekt scheiterte jedoch mit seinen konzeptuellen Ansprüchen wegen der vielfältigen Inkompatibilitäten der bis dahin wildgewachsenen Systeme auf Bundes- und Landesebene und

1036 *Innenministerkonferenz*, Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit, 2016.

1037 BVerfGE 141, 220 – 378 – Bundeskriminalamtgesetz.

1038 BT-Drs. 18/11163, S. 1 f.

1039 Siehe etwa *Bäcker*, Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz, https://verfassungsblog.de/der-umsturz-kommt-zu-frueh-anmerkungen-zur-polizeilichen-informationsordnung-nach-dem-neuen-bka-gesetz/ (Stand: 01.10.2023), demzufolge es nicht ohne weiteres ersichtlich sei, „warum es nicht auch auf der Grundlage der hergebrachten Dateistruktur möglich sein soll, die Informationsbestände von Bund und Ländern zu vernetzen und Querbezüge zwischen unterschiedlichen Kriminalitätsfeldern zu erkennen" und die Grundrechte nicht dazu zwängen, „die hergebrachte Dateistruktur generell aufzugeben, wie es die Gesetzesbegründung nahelegt".

wurde in abgewandelter, oben beschriebener Form umgesetzt.[1040] Als Idee ist die bessere Vernetzung und Nutzbarkeit der polizeilichen Daten in Form eines gemeinsamen Datenbestandes jedoch lebendig geblieben und hat mit zunehmender Präsenz des Massendatenphänomens und anwachsender gesellschaftlicher Bedeutung von Sicherheit[1041] wieder neue Auftriebskraft erhalten, die auch durch zwei weitere konkrete rechtspolitische Ansprüche an die polizeiliche Informationsverarbeitung verstärkt wurde: Einerseits war das Ergebnis des NSU-Untersuchungsausschusses des Deutschen Bundestages in die Informationsverarbeitung zu implementieren.[1042] Eine zentrale Forderung des Ausschusses betraf dabei die Forderung nach Herstellung von Interoperabilität der Datensysteme, die „zügig zu einem guten, verfassungsrechtlich einwandfreien" Abschluss gebracht werden sollten.[1043] Und andererseits war die infolge der Europäischen Datenschutzreform erlassene JI-Richtlinie vom Gesetzgeber umzusetzen. In dieser rechts- und sicherheitspolitischen Gemengelange konnte das Konzept zur Vereinheitlichung, Konsolidierung und Effektivierung des polizeilichen Informationswesens ein neues legitimierendes Substrat finden, aus dem heraus sich die gegenwärtig laufende Umstrukturierung der informationstechnologischen Strukturen der deutschen Polizeien entwickelte. Vorrangiges Ziel ist und bleibt dabei aber die Homogenisierung und stärkere Integration des als zu heterogen empfundenen polizeilichen Informationswesens.[1044]

Legislativ entschloss sich der Bundesgesetzgeber, die komplexen und mitunter widersprüchlichen Vorgaben – Interoperabilität der Datensysteme ist etwa datenschutzrechtlichen Belangen nicht ohne weiteres zuträglich – im Wesentlichen in einem einzigen Gesetzesvorhaben, der Novellierung des BKAG, umzusetzen. Auch in den Stellungnahmen im Innenausschuss wurde mit deutlichen Worten Kritik daran geübt. *Bäcker* sprach in Bezug auf die Informationsordnung von dem „anspruchsvollsten Teil des Ent-

1040 Siehe dazu sowie zum gesamten Entwicklungsprozess bis 2003, *H. Busch* Bürgerrechte & Polizei (CILIP) 25 (2003), 12.

1041 *Legnaro/Klimke* in Legnaro/Klimke (Hrsg.), Kriminologische Diskussionstexte II, 89.

1042 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 3.

1043 BT-Drs. 17/14600, S. 862.

1044 Siehe etwa Bundesministerium des Inneren, White Paper Polizei 2020, S. 5, 9, 20; diese Einschätzung bezüglich der Heterogenität findet sich auch in *Konferenz der Leiterinnen und Leiter der Archivverwaltungen des Bundes und der Länder*, Bewertung von Fachverfahren der Polizeibehörden von Bund und Ländern, Abschlussbericht, (Version 1.1, 2020), S. 5.

wurfs“[1045] und empfahl die Zurückstellung dieses Vorhabens.[1046] Diesem Appell wurde nicht entsprochen, sodass der gegenwärtig bestehende, oben bereits in Teilen erläuterte Rechtsrahmen[1047] der polizeilichen Informationsarchitektur die Umstrukturierung des Informationswesens normativ tragen und absichern soll.

b) Polizei 2020: Aspekte der neuen informationstechnologischen Architektur und Umsetzungsverlauf

Die Umstrukturierung der polizeilichen Informationsarchitektur erfolgt durch das IT-Großprojekt und Organisationsentwicklungsvorhaben[1048] „Polizei 2020“,[1049] mit dem die Polizei die digitale Transformation bewältigen soll.[1050] Ein zentrales Anliegen des geplanten Umbaus ist dabei das „gemeinsame Datenhaus der deutschen Polizei“, also die bereits angesprochene Abschaffung der bisher bestehenden Dateienlandschaft zugunsten eines gemeinsamen Datenbestandes, wobei der Zugriff „zielgerichtet über ein dynamisches und modernes Zugriffsmanagement geregelt“ werden soll. Verbundrelevante Informationen sollen allen Teilnehmern zur Verfügung stehen. Die Verantwortung verbleibt aber beim Datenbesitzer. Daten ohne Verbundrelevanz sollen hingegen nur für die jeweiligen Datenbesitzer einsehbar sein.[1051] So müssen „Anpassungen für das Verbundsystem […] nur einmal vorgenommen und nicht 19 Mal (in den Systemen der 16 Länder

1045 *Bäcker*, A-Drs. 18(4)806 D, S.4.
1046 *Bäcker*, A-Drs. 18(4)806 D, S. 2, 10.
1047 Siehe dazu oben S. 230 ff.
1048 Die Bundesregierung weist darauf hin, dass es sich beim Polizei 2020 nicht primär um ein IT-Großprojekt handle, da ebenfalls „die die entsprechenden fachlichen und technischen Prozesse sowie die föderalen Bedarfe“ zu berücksichtigen seien, BT-Drs. 19/25651, S. 2. Gerade diese vielfältigen Bedarfe machen das im Kern informationstechnologische Projekt aber zu einem großen. Dass es auch organisationale Komponenten aufweist ist auch nichts Ungewöhnliches bei IT-Projekten, die zumeist auch auf Umstrukturierung von organisatorischen Prozessen abzielen. Zu den einzelnen Komponentprojekten siehe BT-Drs. 19/27083, S. 4 f.
1049 Mittlerweile wird es offiziell auch P20 genannt, siehe https://www.bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html (Stand: 01.10.2023). „Polizei 2020“ ist jedoch die weitaus verbreitetere Bezeichnung.
1050 BT-Drs. 19/25651, S. 2.
1051 Bundesministerium des Inneren, White Paper Polizei 2020, S. 11 f.; vgl. auch BT-Drs. 18/11163, S. 84 f.

sowie den Polizeien des Bundes) nachvollzogen werden."[1052] Neben einer verbesserten Verfügbarkeit polizeilicher Informationen soll dadurch auch die Wirtschaftlichkeit polizeilicher Datenverarbeitung erhöht und der Datenschutz durch Technikgestaltung verbessert werden können.[1053] Relevant soll in Zukunft damit „nicht mehr die technische Zusammenfassung von Informationen in Dateien, sondern der Themenbezug der Information sein."[1054] Über den technisch gesteuerten Zugriff soll auch der Grundsatz der hypothetischen Datenneuerhebung umgesetzt werden können. Dazu muss die Eingriffstiefe der jeweils vorhandenen Daten bestimmt werden.[1055] Die Protokollierung dieser Zugriffe an zentraler Stelle wird ebenfalls als Verbesserung des Datenschutzes angeführt.[1056] Daneben soll die Rolle des Bundeskriminalamtes als dienstleistungsorientierte Zentralstelle gestärkt werden, was insbesondere bedeutet, dass das Amt den anderen Polizeibehörden Anwendungen und Dienste für die polizeiliche Arbeit bereitstellen wird.[1057] Außerdem soll „moderne und zukunftsfähige Technologie" zum Einsatz kommen.[1058] Neben der geplanten INPOL-Modernisierung sind auch der bereits seit 2008 geplante[1059] Polizeiliche Informations- und Analyseverbund (PIAV),[1060] der einen bruchlosen Datenaustausch zur Aufklärung länder- oder phänomenübergreifender Tatzusammenhänge ermöglichen soll,[1061] sowie die Entwicklung eines für die Bundespolizeibehörden vereinheitlichten Fallbearbeitungssystems (einheitliches Fallbearbeitungssystem – eFBS) als Teilprojekte in das Polizei 2020-Vorhaben integriert worden.[1062]

Neben diesen beiden wichtigen Teilprojekten und der zentralen Modernisierung von INPOL sind unter dem Dach von Polizei 2020 gegenwärtig noch 23 weitere Projekte zur abgestimmten Bearbeitung versammelt. Angegliedert sind dort etwa die elektronische Akte in Strafsachen, der Gesamtansatz Auswertung und Analyse, die Anbindung der Staatsanwaltschaften

1052 BT-Drs. 18/11163, S. 84.
1053 Bundesministerium des Inneren, White Paper Polizei 2020, S. 8 ff.
1054 BT-Drs. 18/11163, S. 109.
1055 Bundesministerium des Inneren, White Paper Polizei 2020, S. 12.
1056 Bundesministerium des Inneren, White Paper Polizei 2020, S. 10.
1057 Bundesministerium des Inneren, White Paper Polizei 2020, S. 13.
1058 Bundesministerium des Inneren, White Paper Polizei 2020, S. 14.
1059 BT-Drs. 16/12600, S. 56.
1060 Siehe dazu bereits oben S. 251 ff.
1061 *Aden/Fährmann* Zeitschrift für Rechtspolitik 2019, 175177.
1062 Bundesministerium des Inneren, White Paper Polizei 2020, S. 6.

an INPOL, ein Projekt zur Konzeptionierung der mobilen Verfügbarkeit der Fachanwendungsmodule durch mobile Anwendungen oder ein Projekt zur automatisierten Erkennung Kinderpornografischen Materials mittels eines KI-basierten Verfahrens. Dies unterstreicht den Charakter von Polizei 2020 als tiefgreifendes Transformationsprogramm, das zudem weiter offen für die bedarfsmäßige Integration neuer Projekte bleibt.[1063]

Für den Erfolg von Polizei 2020 sind aber insbesondere das eFBS und mehr noch ein einheitliches Vorgangsbearbeitungssystem,[1064] da durch letztere ein Großteil der polizeilich verwertbaren Daten generiert wird, denn aus jedem Einsatz und aus jeder Strafanzeige wird zunächst ein Vorgang.[1065] Ohne die Einbindung eines einheitlichen Vorgangsbearbeitungssystems in das Projekt ist das angestrebte Ziel der Einmalerfassung der Daten nicht erreichbar.[1066] Denn ein gemeinsames polizeiliches Informationssystem, wie es die INPOL-Modernisierung in Form des gemeinsamen Datenhauses vorsieht, funktioniert nur dann effektiv, wenn die Quellsysteme bei allen beteiligten Behörden einheitlich funktionieren.[1067] Vor dem Hintergrund großer Heterogenität bei den polizeilichen Vorgangsbearbeitungssystemen liegt darin eine große Hürde des gesamten Projekts. Gegenwärtig scheinen Bedarfe und Bestände in den Teilnehmerländern und den teilnehmenden Behörden ermittelt zu werden. Auf Grundlage dieser Prüfungsergebnisse sollen zunächst drei Interims-Vorgangsbearbeitungssysteme festgelegt werden. Ein viertes soll sich zudem noch in Prüfung befinden. Die Entscheidung für die Ausgestaltung des jeweiligen Vorgangsbearbeitungssystems ist dabei nicht trivial, da sie die Art der Sachbearbeitung für die kommenden Jahre maßgeblich beeinflussen wird.[1068]

Konkreter scheinen die Pläne zum eFBS zu sein, das für die Homogenisierung der kriminalpolizeilichen Datenerfassung zentral ist und somit ebenfalls mit über den Erfolg von Polizei 2020 entscheiden dürfte. Das System wurde durch das Programm im Mai 2020 in den Wirkbetrieb überführt. Insgesamt soll das eFBS derzeit durch sechs Teilnehmer von Bund und Ländern (BKA, Bundespolizei, Baden-Württemberg, Branden-

1063 Siehe zur vollständige Liste BT-Drs. 19/27083, S. 4 f.
1064 Zu Vorgangsbearbeitungssystemen siehe bereits oben S. 254 ff.; zur Bedeutung der Vorgangsbearbeitungssysteme für die gescheiterte INPOL-neu-Konzeption siehe oben S. 131 ff.
1065 *Geerdts* Moderne Polizei: Magazinreihe 2021, 6 (6).
1066 Behördenspiegel zitiert nach *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (21).
1067 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (20).
1068 *Geerdts* Moderne Polizei: Magazinreihe 2021, 6 (6 f.).

burg, Hamburg, Hessen) genutzt werden, wobei die Zuschaltung weiterer Teilnehmer geplant ist.[1069] Auch die Protokollierung von Anlass und Zweck der Abfragen soll schon zentral auf einem Server beim Bundeskriminalamt erfasst werden können.[1070] Die Vereinheitlichung solcher Systeme erfolgt über die Beachtung des „Informationsmodell Polizei" bei der Programmierung, womit dann Informationen in identischer Weise Daten- und Objektkategorien zugewiesen würden. Nur so können Daten nach Übermittlung in ein zentrales System von anderen angeschlossenen Behörden einheitlich abgefragt und verwendet werden.[1071]

Die Umsetzung des Gesamtprojekts ist dementsprechend noch lange nicht abgeschlossen, viele der Schritte, von denen berichtet wird, wirken wie eher vage Konzeptionierungsarbeiten oder kleinteilige Schritte im Rahmen der einzelnen Teilprojekte.[1072] Auch wird von Widerständen aus den Länderpolizeien berichtet, weil Systeme aufgegeben werden sollen, die teilweise selbst entwickelt wurden und auch individueller an die jeweiligen fachlichen Vorgaben angepasst sind.[1073]

Die historisch gewachsene IT- sowie Prozesslandschaft der Polizeien in Bund und Ländern beweist hinsichtlich ihrer Vielfältigkeit und Heterogenität einige Beharrungskräfte. Auch in den nächsten Jahren werden die Herausforderungen bezüglich der Umsetzung des Projekts vor allem in der Harmonisierung und Konsolidierung der unterschiedlichen Ist-Zustände der einzelnen Teilnehmer und der Erarbeitung gemeinsamer Standards liegen. Gleichzeitig ist Polizei 2020 Projektarbeit an einem laufenden System. Die laufende polizeiliche Informationsarbeit soll möglichst wenig gestört werden. Deshalb erfolgt die Umsetzung modul- und phasenweise. Zunächst sollen daher die verschiedenen in Bund und Ländern bestehenden Einzelsysteme, sogenannte Monolithen, so weit wie möglich reduziert werden, um dann ausgehend von einem einheitlicheren Zwischenstand des polizeilichen Informationswesens die Transformation in die schlussendliche Zielarchitektur zu bewerkstelligen.[1074] Das Projekt, dem ein Zeitrahmen von mehr als 10 Jahren zugesprochen wird[1075] und für das kein Abschlusszeit-

1069 BT-Drs. 19/25651, S. 3.
1070 BT-Drs. 19/25651, S. 6.
1071 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (20).
1072 BT-Drs. 19/25651, S. 4.
1073 *Burczyk* Bürgerrechte & Polizei (CILIP) 2020, 16 (21).
1074 BT-Drs. 19/27083, S. 13.
1075 BfDI, 28. Tätigkeitsbericht 2019, S. 50.

punkt festgesetzt wurde,[1076] wird die Polizei und ihr Informationssystem also im kommenden Jahrzehnt maßgeblich beschäftigen und prägen.

c) Normativität und Faktizität

Die strukturellen Neuerungen, die der Umbau des polizeilichen Informationswesens mit sich bringen wird, sind rechtlich in erster Linie im neuen BKAG und dort vor allem in §§ 12-19 sowie §§ 29-32 abgebildet. Angesichts der nicht unbeträchtlichen Umwälzungen, die mit Polizei 2020 einhergehen, wirken diese rechtlichen Konturen indessen eher blass.[1077] Geändert wurde im Zuge der das Projekt begleitenden Gesetzgebung auch nichts am bestehenden Problem der unzureichenden Einhegung vieler Komponenten des Informationswesens. Zudem fährt das neue BKAG die rechtliche Rahmung der neuen zentralen Datenhaltung beim Bundeskriminalamt auch an anderer Stelle zurück: Für die gegenwärtige Dateien-Struktur der polizeilichen Informationsverarbeitung konkretisieren Errichtungsanordnungen den zulässigen Umfang und rechtlichen Rahmen bei der Verarbeitung personenbezogener Daten. Da die Errichtungsanordnung den Zweck der Dateien näher bezeichnet, ist eine Verarbeitung zu in ihr nicht vorgesehenen Zwecken nicht gestattet.[1078] Künftig werden diese – mit Ausnahme von gemeinsamen projektbezogenen Dateien nach § 17 BKAG[1079] – jedoch wegfallen, wie es dem neuen Konzept eines gemeinsamen Datenbestandes entspricht und beispielsweise auch in § 91 BKAG indirekt zum Ausdruck kommt. Gibt es keine abgrenzbaren Dateien mehr, sind Errichtungsanordnungen überflüssig. An ihre Stelle treten die von §§ 80 BKAG

1076 BWLT-Drs. 16/7932, S. 4.

1077 So *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 4, der zum rechtlichen Rahmen der neuen IT-Architektur des Bundeskriminalamtes im Wesentlichen sogar nur §§ 12 und 29 BKAG zählt.

1078 Siehe etwa AbgHBln-Drs. 17/14375, S.

1079 Errichtungsanordnungen finden weiter im Rahmen sog. projektbezogener gemeinsamer Dateien Anwendung, vgl. § 17 Abs. 6 S. 1 BKAG. Damit soll jedoch vor allem der Besonderheit und Bedeutung der Zusammenführung von Erkenntnissen und der gemeinsamen Verarbeitung von personenbezogenen Daten von Polizeien, Nachrichtendiensten und Zollkriminalamt Rechnung getragen werden, vgl. BT-Drs. 18/11163, S. 98. Für den davon insoweit abzugrenzenden Bereich der ausschließlich polizeilichen Informationsverarbeitung gilt das Erfordernis einer Errichtungsanordnung nach der Neukonzeption des BKAG also gerade nicht mehr.

i.V.m. 70 BDSG in Umsetzung der JI-Richtlinie vorgeschriebenen Verarbeitungsverzeichnisse,[1080] die jedoch nicht dieselbe normative Ordnungskraft entwickeln.[1081] Sind die Errichtungsanordnungen auch „nur" Verwaltungsvorschriften,[1082] so verringert ihre Abschaffung in wesentlichen Bereichen zweifellos die Konturenschärfe der normativen Grenzen des zukünftigen „Datenhauses der deutschen Polizei". Dies schien auch dem Gesetzgeber bewusst gewesen zu sein, der mit dem neueingefügten § 30 BKAG den Versuch einer ausgleichenden Konkretisierung unternimmt. Danach haben die am Informationsverbund teilnehmenden Stellen nunmehr festzulegen, welche Straftaten als verbundrelevant im Sinne des § 30 Abs. 1 Nr. 1 BKAG gelten sollen. Das ist indessen ein eindeutig niedrigerer Anspruch an Konkretisierung, denn Errichtungsanordnungen legen demgegenüber mit einiger Detailliertheit fest, welche Datenkategorien von wem zu welchen Zwecken verarbeitet werden dürfen.[1083] Von rechtsstaatlicher Warte aus betrachtet lässt sich diese Entwicklung kaum anders denn als Rückschritt bewerten: Statt die rechtliche Flankierung des gemeinsamen Datenhauses zu verstärken, wie es die Abschaffung der Dateistruktur und damit die weitere Relativierung der Zweckbindung von Daten geboten hätten, wird mit dem Konzept der Verbundrelevanz ein gegenüber der bisherigen Rechtslage schwächeres Begrenzungsinstrument gewählt. Ohne Errichtungsanordnungen ist die polizeiliche Informationsverarbeitung in Zukunft noch stärker normativer Anknüpfungspunkte beraubt.[1084] Insgesamt wird der rechtliche Regelungsanspruch damit gegenüber der normativen Kraft der tatsächlichen informationstechnischen Strukturen und der an ihnen eingeübten polizeilichen Informationspraktiken zurückgefahren. Ob sich dieses Ungleichgewicht durch einen Datenschutz prozeduraler Färbung ausgleichen lässt, wie es insbesondere im Wege der JI-Richtlinie erfolgen soll, muss sich erst noch zeigen.[1085]

1080 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 458.
1081 Siehe dazu unten S. 401.
1082 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 91 BKAG Rn. 1.
1083 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 459.
1084 Ähnlich *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 4.
1085 Siehe näher zum Datenschutz im neuen Informationswesen S. 361 ff.

d) Neues Recht und alte Dateienlandschaft nach § 91 BKAG: Verfassungsrecht und Polizeiwirklichkeit

Der Primat des Faktischen in der polizeilichen Informationsverarbeitung wird gerade auch im Übergang von alter zu neuer Architektur deutlich. Denn während INPOL-Z noch auf Grundlage alten Fassung des BKAG betrieben wird, ist die Arbeit im polizeilichen Informationsverbund durch neue Normen geregelt, die andere rechtliche Anforderungen an den Datenumgang im Informationsverbund stellen.[1086] Diesen potenziellen Konflikt hat auch der Gesetzgeber gesehen und mit der Übergangsregelung des § 91 BKAG zu lösen versucht. Die Vorschrift erlaubt dem Bundeskriminalamt eine Weiterverarbeitung seiner Datenbestände nach den Bestimmungen der für die Daten am 24. Mai 2018 jeweils geltenden Errichtungsanordnung nach § 34 a.F. BKAG in der bis zum 24. Mai 2018 geltenden Fassung. Diese Errichtungsanordnungen gelten bis zur vollständigen Umsetzung von Polizei 2020 fort.[1087] Diese legislative Entscheidung ist aus verfassungsrechtlicher Perspektive höchst problematisch.

Nachdem das verfassungsrechtliche Prinzip der Zweckbindung in Form des Grundsatzes der hypothetischen Datenneuerhebung konkretisiert wurde, muss dieser nun gem. § 12 Abs. 5 BKAG durch technische und organisatorische Vorkehrungen sichergestellt werden. Diese Verpflichtung ist einfachgesetzlich wiederum in den §§ 14, 15 BKAG ausgestaltet, die die Kennzeichnung von Daten sowie die Regelung von Zugriffsberechtigungen in einer Art und Weise erfordern, die die Einhaltung der Vorgaben des § 12 BKAG gewährleisten. Die dafür erforderlichen Änderungen in der bundeskriminalamtlichen IT-Architektur konnten indessen, aufgrund ihres nicht unerheblichen Aufwandes, mit dem Ablauf der im BKAG-Urteils vorgegebenen Frist nicht umgesetzt werden.[1088] Die infolgedessen bestehende Diskrepanz zwischen gesetzlicher Vorgabe, wie sie in den §§ 14, 15 BKAG zum Ausdruck kommt, und tatsächlicher Situation in der IT-Architektur soll nach Vorstellung des Gesetzgebers durch geeignete Maßnahmen[1089] seitens des Bundeskriminalamtes behoben werden. Grundsätzlich soll das Problem

1086 Siehe dazu bereits oben S. 230 ff.
1087 BT-Drs. 19/5923, S. 7, 9 f.; BT-Drs. 19/15346, S. 3.
1088 *Schenke/Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Einf. Rn. 18.
1089 Damit sind ausweislich der Gesetzesbegründungen Maßnahmen gemeint, die ein hohes Maß an Beachtung des Grundsatzes der hypothetischen Neuerhebung gewährleisten, gleichzeitig jedoch nicht dazu führen, dass – gerade auch vor dem Hintergrund der zeitaufwändigen Prozesse innerhalb des derzeitigen INPOL-Ver-

aber durch § 91 BKAG neutralisiert werden. Die Norm statuiert eine Ausnahme von der Weiterverarbeitungssperre des § 14 Abs. 2 BKAG von nicht gekennzeichneten, personenbezogenen Daten, wenn die Bestimmungen der für die Daten am 24. Mai 2018 jeweils geltenden Errichtungsanordnung nach § 34 BKAG in der bis zum 24. Mai 2018 geltenden Fassung eingehalten werden. Damit soll unumstritten die Weiterverarbeitungsmöglichkeit der bereits in den Dateien gespeicherten Altdaten in der Transitionsphase von alter Dateienlandschaft zu neuem einheitlichen Informationsbestand lückenlos gewährleistet werden.[1090] Offengelassen wurde, ob die Ausnahme auch für nach dem 24.5.2018 gespeicherte Daten gilt. Dagegen sprechen jedenfalls der Wortlaut der Übergangsregelung und die verfassungsrechtlichen Vorgaben, auf deren Grundlage man die Verfassungsmäßigkeit von § 91 BKAG insgesamt bezweifeln muss.

Auf diese Weise werden die Vorgaben des Bundesverfassungsgerichts zwar textlich im Gesetz implementiert. Die im Urteil gesetzte Umsetzungsfrist von zwei Jahren bis Mai 2018 wird aber durch § 91 BKAG faktisch missachtet. Da im derzeitigen INPOL-Z auch für neu zu speichernde Daten zumindest Ende 2019 eine Kennzeichnungspflicht nicht umgesetzt werden konnte,[1091] ist die tatsächliche Umsetzung des vom Bundesverfassungsgericht aufgestellten Grundsatz der hypothetischen Datenneuerhebung zunächst auf einen unbekannten Zeitpunkt in der Zukunft vertagt.[1092] Denn für die Praxis polizeilicher Datenverarbeitung heißt dies mit Blick auf § 12 Abs. 2 BKAG: Ist ein Datum nicht nach § 14 Abs. 1 gekennzeichnet, wird sich nur begrenzt feststellen lassen, ob eine Weiterverarbeitung über den Grundsatz der hypothetischen Datenneuerhebung möglich ist. Eine solche Nichtbeachtung des Grundsatzes der hypothetischen Datenneuerhebung verletzt das verfassungsrechtliche Verhältnismäßigkeitsprinzip, dessen Ausfluss der Zweckbindungsgrundsatz im Kontext der informationellen Selbstbestimmung ist.[1093] Mangels einer der gesetzlichen Lage entsprechenden IT-Architektur ist unklar, ob oder inwieweit die gesetzlichen und insbesondere verfassungsrechtlichen Vorgaben im Bereich polizeilicher Informationsverarbeitung gegenwärtig Beachtung finden.[1094] Auch dieser Vorgang ist

bundes, für den die Vorschrift gemäß § 29 gilt – die technische Implementierung behindert oder verzögert wird, BT-Drs. 11163, S. 95.

1090 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 91 BKAG Rn. 1 ff.

1091 BT-Drs. 19/15346, S. 10.

1092 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 14 BKAG Rn. 1.

1093 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 14 BKAG Rn. 1.

1094 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 14 BKAG Rn. 6.

ein eindrucksvoller Beleg für die Schwächen des Rechts (und seiner legislativen Akteure) bei der verfassungsgemäßen Regulierung des polizeilichen Informationswesens.

e) Informationstechnologische Evolutionen mit rechtlichem Niederschlag

Neben den zentralen Projekten von Polizei 2020 bildet das polizeiliche Informationswesen auch weitere, seinen Wandel indizierenden informationstechnologische Strukturen aus, die als Reaktionen auf das Massendatenphänomen aufgefasst werden müssen. Die konkreten Ausformungen des technischen Wandels sind dabei mehrzweigig und betreffen unterschiedliche Bereiche des polizeilichen Tätigkeitsfelds.

aa) Predictive Policing

Für die möglichst optimale Nutzung der eigenen Datenbestände rücken Systeme, mit denen sich die Daten algorithmisch analysieren lassen, immer stärker in die polizeiliche Informationsverarbeitung. Viele der technologischen Anwendungen werden dabei unter dem aus dem englischsprachigen Raum importierten Begriff des Predictive Policing versammelt,[1095] was für den deutschsprachigen Diskurs häufig mit „vorausschauender Polizeiarbeit" übersetzt wird.[1096] Wenn auch verschiedene Begriffsverständnisse zirkulieren, scheint ein gemeinsamer definitorischer Nenner zu sein, dass es sich um computergestützte Anwendungen handelt[1097] deren primäres Ziel darin besteht, aus Daten der Vergangenheit und der Gegenwart räumlich-zeitlich möglichst exakte Vorhersagen für das Auftreten von Ereignissen zu generieren.[1098] Dabei ermöglicht die informationstechnologische Fundierung die Verarbeitung großer Datenvolumina, wie sie rein menschlicher Infor-

1095 Viel zitiert und einflussreich im englischsprachigen Diskurs etwa *Perry/McInnis/Price* ua, Predictive policing.
1096 *Gluba* Die Polizei 107 (2016), 53 (53).
1097 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 3.
1098 *Gluba* Die Polizei 107 (2016), 53 (53).

mationsverarbeitung versagt wäre.[1099] Neu ist insofern vor allem die vom Menschen losgelöste Analyseleistung.

Unterschieden wird klassischerweise zwischen raumbezogenem und personenbezogenem Predictive Policing.[1100] In der ersten Spielart dieser neuen Form der Polizeiarbeit werden der Polizei zur Verfügung stehende Daten mit Blick auf das Aufkommen von abweichendem Verhalten an einem speziellen Ort ausgewertet, um dann auf dieser Grundlage die Häufigkeit von diesem Verhalten am untersuchten Ort zu einem zukünftigen Zeitpunkt zu prognostizieren. Es ist diejenige Variante, die weltweit am stärksten verbreitet ist.[1101] In Deutschland kommt vorausschauende Polizeiarbeit dementsprechend auch bisher quasi ausschließlich in ihrer raumbezogenen Dimension zum Einsatz, wobei deliktisch der Fokus auf Wohnungseinbrüchen liegt.[1102] Dabei wird prinzipiell darauf geachtet, dass keine personenbezogenen Daten verarbeitet werden,[1103] wobei sich der Personenbezug je nach eingesetzter Software anscheinend durchaus wieder herstellen lassen könnte.[1104] Insofern gelten Anwendungen raumbezogenen Predictive Policings als rechtlich weniger bedenklich und finden wegen des fehlenden Personenbezuges auch derzeit keinen gesetzlichen Niederschlag. Anders ist dies allerdings bei der personenbezogenen Variante gelagert.[1105] Dabei geht es darum, das Risiko für die Begehung oder auch Opferwerdung von Straftaten über die Analyse der zur Verfügung stehenden Daten zu prognostizieren und polizeilich nutzbar zu machen.[1106] In Deutschland wird eine solche Form des Predictive Policing explizit nicht praktiziert, wenngleich auch das vom Bundeskriminalamt genutzte Prognoseinstrument RADAR-

1099 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 3.

1100 *Sommerer,* Personenbezogenes Predictive Policing, 36 ff.

1101 *Egbert/Krasmann*, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis., Projektabschlussbericht, 2019, 20 f.

1102 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 1; zu den eingesetzten Systemen s. den Überblick bei Arzt in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1300.

1103 *Gerstner,* Predictive Policing als Instrument zur Prävention von Wohnungseinbruchdiebstahl, S. 3.

1104 BWLfDI, 32. Tätigkeitsbericht 2014/2015, S. 44.

1105 Grundlegend *Sommerer,* Personenbezogenes Predictive Policing.

1106 *Egbert/Krasmann*, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis., Projektabschlussbericht, 2019, 12 f.

iTE (Regelbasierte Analyse potenziell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus) oder auch die Fluggastdatenspeicherung als diesem Kontext unterfallend diskutiert werden.[1107]

bb) Analysesysteme

Neben diesen Formen des Predictive Policing ist in letzter Zeit noch ein weiterer informationstechnologischer Verfahrenstyp aufgekommen, um die Datenbestände des polizeilichen Informationswesens besser nutzbar zu machen. Anders als raum- oder personenbezogenes Predictive Policing, das regelmäßig mit Risikoscores arbeitet[1108] und damit – auch bei Risikoskalen – häufig ein binäres Ergebnis (eingriffsrelevante Risikoschwelle überschritten: ja oder nein) liefert, wodurch das anschließende polizeiliche Handeln prinzipiell vorstrukturiert wird, arbeiten diese Systeme offener. Dazu gehört etwa die „Automatisierte Anwendung zur Datenanalyse" in § 25a HSOG, die „Automatisierte Anwendung zur Auswertung von Daten" in § 49 HmbPolDVG oder auch das „System zur Datenbankübergreifenden Analyse und Recherche" (DAR) in Nordrhein-Westfalen gemäß § 23 Abs. 6 PolG NRW.[1109] Mit diesen Systemen werden die in heterogenen Datenspeichern vorgehaltenen Daten der Polizei virtuell in einer Analyseplattform vereinigt. Diese greift auf die grundsätzlich voneinander getrennte INPOL-Auskunftskomponente, das Vorgangsbearbeitungs- sowie das Fallbearbeitungssystem zu und macht die Daten, die in diesen für die polizeiliche Informationsarbeit wichtigsten Quellsysteme vorgehalten werden, zur datenbankübergreifenden Recherche, Verknüpfung und Analyse verfügbar.[1110] Durch die Anwendungen werden die heterogenen Datenbestände virtuell homogenisiert und lassen sich damit einfacher und schneller durchsuchen

1107 Siehe etwa *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1302, 1330.

1108 Vgl. *Egbert/Krasmann*, Predictive Policing. Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis., Projektabschlussbericht, 2019, 20, 29, 31, 33.

1109 Auch Bayern hat einen Rahmenvertrag mit dem Unternehmen Palantir geschlossen, der es anderen Ländern erlaubt, das ausgewählte Produkt, eine verfahrensübergreifende Recherche- und Analyseplattform (VeRA), ohne Vergabeverfahren selbstständig abzurufen, s. BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 15.

1110 HessLT-Drs. 20/660, S. 1 ff.

und vernetzen. Zudem können weitere Datenquellen integriert werden.[1111] Mit den Systemen ist folglich eine enorme Steigerung des informationellen Gehalts der polizeilichen Datenbestände beabsichtigt. Analysesysteme stehen emblematisch für die polizeiliche Informationsverarbeitung im Massendatenkontext und sollen aufgrund dieser Relevanz hier eingehender mit Blick auf ihre rechtlichen Implikationen analysiert werden.

(1) Das Urteil des Bundesverfassungsgerichts vom 16. Februar 2023

Alle vorgenannten Anwendungen setzen maßgeblich auf komplexere informationstechnische Algorithmen, die teilweise automatisiert auf die Rechercheimpulse ihrer Nutzer:innen reagieren. Mittlerweile ist bekannt, welche Problemlagen der gesellschaftliche Einsatz von Algorithmen mit sich bringen,[1112] woraus sich ein besonderes rechtliches Anforderungsprogramm bei der Regulierung von Algorithmen ergibt.[1113] Auch der Erste Senat des Bundesverfassungsgerichts hat sich nunmehr mit einem Urteil vom 16. Februar 2023 zu den Rechtsgrundlagen der Anwendungen zur automatisierten Datenanalyse in Hamburg und Hessen geäußert und beide Vorschriften in ihrer gegenwärtigen Form für verfassungswidrig erklärt. Bereits zuvor hatte das Gericht begonnen, im Kontext des nachrichtendienstlichen Informationsrechts Leitlinien für die Nutzung von Datenanalyse-Instrumenten zu entwickeln. Diese sollen hier kurz nachgezeichnet werden, um darauf aufbauend das Urteil zur polizeilichen automatisierten Datenanalyse darzustellen.

Zunächst hatte das Gericht in der BND-Entscheidung in diesem Kontext Regelungen insbesondere bezüglich der Sicherstellung der grundsätzlichen Nachvollziehbarkeit für unabhängige Kontrolle für erforderlich gehalten.[1114] Wichtiger, weil ausführlicher, waren für polizeiliche Analysesysteme aber insofern die Ausführungen des Gerichts in seinem zweiten Urteil zum ATDG. In der Entscheidung hatte das Bundesverfassungsgericht unter anderem zu klären, ob die sogenannte erweiterte projektbezogene Datennutzung der Antiterrordatei den Anforderungen des Rechts auf informatio-

1111 HessLT-Drs. 19/6864, S. 18.
1112 *O'Neil,* Weapons of math destruction; *Pasquale,* The Black Box Society; *Noble,* Algorithms of oppression.
1113 Siehe grundlegend dazu *Martini,* Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, 27 ff.
1114 BVerfGE 154, 152 (260) – BND: Ausland-Ausland-Fernmeldeaufklärung.

nelle Selbstbestimmung genügte. Eine solche Datennutzung meint gemäß § 6a Abs. 5 S. 1 ATDG das Herstellen von Zusammenhängen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen, der Ausschluss von unbedeutenden Informationen und Erkenntnissen, die Zuordnung eingehender Informationen zu bekannten Sachverhalten sowie die statistische Auswertung der gespeicherten Daten. Darin wird vom Gericht ein typischer Fall des „Data-Mining" gesehen, was nach einer Definition der Bundesregierung vorläge, wenn Verfahren und Methoden eingesetzt werden, „mit deren Hilfe bereits vorhandene große Datenbestände, zumeist auf statistisch-mathematischen Verfahren basierend, selbständig auf Zusammenhänge analysiert werden, um auf diesem Wege neues Wissen zu generieren." Da eine solche Verknüpfung von Daten etwa mehrstufige Analysen ermögliche, die neue Verdachtsmomente erst erzeugen, sowie weitere Analyseschritte oder auch daran anschließende operative Maßnahmen denkbar mache, gehen von der Maßnahme erhebliche Beeinträchtigungswirkungen aus.[1115] Neben der hier auszuklammernden Frage, wie sich die Verschränkung der Informationsbestände von Polizeien und Nachrichtendiensten in diesem Kontext konkret auswirkt, war vor allem das das eigentliche Verfahren der Verknüpfung gespeicherter Daten zur Erzeugung neuer Erkenntnisse und Zusammenhänge verfassungsrechtlich zu bewerten. Dieses könne eine erhebliche Persönlichkeitsrelevanz aufweisen, wobei das Eingriffsgewicht noch weiter erhöht ist, wenn die neuen Erkenntnisse und Zusammenhänge sodann auch durch die Polizeien operativ nutzbar gemacht werden können.[1116] Mit diesem Urteil knüpft das Bundesverfassungsgericht an eine Idee am ursprünglichen konzeptuellen Fundament der informationellen Selbstbestimmung an: Die informationstechnologischen Verarbeitungs- und Verknüpfungsmöglichkeiten begründen überhaupt erst die Notwendigkeit des Schutzes von Daten und bestimmen ganz maßgeblich über die Eingriffstiefe mit.[1117] Allerdings war bereits das zweite Urteil zur Rasterfahndung davon ausgegangen, dass angesichts der Menge und Vielfalt der personenbezogenen Daten, die heute über nahezu jede Person vorhanden sind, die Rasterfahndung nahe an die von der Verfassung verbotene Praxis der Erstellung von teilweisen oder vollständigen Persönlich-

1115 BVerfGE 156, 11 (40) – Antiterrordateigesetz II.
1116 BVerfGE 156, 11 (52) – Antiterrordateigesetz II.
1117 BVerfGE 65, 1 (44) – Volkszählung.

keitsbildern rücke.[1118] Insofern bestehen auch für das Data-Mining hohe Hürden für eine verfassungsrechtliche Zulässigkeit.

Für die Nutzung solcher Verfahren durch die auch operativ tätigen Polizeien sah das Gericht vor allem die zu schützenden Rechtsgüter und die diesbezüglichen Eingriffsschwellen als neuralgischen Punkt für die verfassungsrechtliche Bewertung.[1119] So ist sicherheitsbehördliches Data-Mining grundsätzlich zum Schutze besonders gewichtiger Rechtsgüter wie Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zulässig.[1120] Allerdings sind weiterhin spezifische Anforderungen an die Eingriffsschwelle zu stellen. Geht es um die Abwehr von Gefahren muss eine „wenigstens hinreichend konkretisierte Gefahr in dem Sinne (…) [gegeben sein], dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr vorliegen."[1121] Dabei „genügt es nicht, wenn das Gesetz allein verlangt, dass Tatsachen vorliegen, die die Annahme rechtfertigen, dass eine Straftat begangen werden soll, weil dies nicht ausschließt, dass sich die behördliche Prognose allein auf Erfahrungssätze stützt."[1122] Die Behörde muss vielmehr ein „wenigstens seiner Art nach konkretisiertes und absehbares Geschehen" erkennen oder erkennen, „dass das individualisierte Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in absehbarer Zeit terroristische Straftaten begeht."[1123] Während darin keine Verschärfung des herkömmlichen Gefahrerfordernisses liegt, ist das Bundesverfassungsgericht im repressiven Bereich strenger. Ein einfacher Tatverdacht genügt nicht, vielmehr muss die etwaige Rechtsgrundlage verlangen, dass bestimmte, den Verdacht begründende Tatsachen vorliegen", also „dass insoweit konkrete und in gewissem Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorhanden" sind.[1124]

Diese Vorgaben hat das Bundesverfassungsgericht in seinem Urteil vom 16. Februar 2023 nunmehr aktualisiert und spezifiziert. Der Prüfungsgegenstand des Urteils beschränkte sich dabei auf die Eingriffsschwelle in

1118 BVerfGE 115, 320 (350 f.) – Rasterfahndung II.
1119 BVerfGE 156, 11 (49) – Antiterrordateigesetz II.
1120 BVerfGE 156, 11 (56) – Antiterrordateigesetz II.
1121 BVerfGE 156, 11 (54) – Antiterrordateigesetz II.
1122 BVerfGE 156, 11 (61) – Antiterrordateigesetz II.
1123 BVerfGE 156, 11 (61) – Antiterrordateigesetz II.
1124 BVerfGE 156, 11 (55) – Antiterrordateigesetz II.

§ 25a HSOG, § 49 HmbPolDVG;[1125] im Übrigen waren die Verfassungsbeschwerden als unzulässig verworfen worden. Explizit ausgeklammert war damit die Frage, „ob die Gesetzgeber verfassungsrechtlich ausreichende Regelungen zu den durch die Datenanalyse oder -auswertung nach § 25a HSOG und § 49 HmbPolDVG zu schützenden Rechtsgütern getroffen haben." Auch wurde nicht überprüft, „ob die für Transparenz und Rechtsschutz sorgenden Verfahrens- und Organisationsregelungen verfassungsrechtlichen Anforderungen genügen, ob insbesondere auch mit Blick auf komplexe Formen automatisierten Datenabgleichs bis hin zu selbstlernenden Systemen hinreichende verfahrensrechtliche Sicherungen bestehen." Ferner wurde nicht verfassungsrechtlich überprüft, „ob der verfassungsrechtliche Grundsatz der Zweckbindung bereits erhobener personenbezogener Daten gewahrt ist, ob also insbesondere auch hinreichend begrenzt ist, inwiefern Daten, die unter Eingriff in Art. 13 Abs. 1 GG oder Art. 10 Abs. 1 GG erhoben worden sind, weiter genutzt werden dürfen. Auch gelten die Ausführungen des Urteils nur für den Einsatz der Datenanalyse zu Zwecken der vorbeugenden Straftatbekämpfung." Die Befugnis zur Abwehr von Gefahren blieb also von den Ausführungen des Gerichts unberührt.[1126]

(2) Verfassungsrechtliche Anforderungen an Analysesysteme

Die dem Verfahren zugrundeliegenden[1127] Vorschriften ermöglichen grundsätzlich zwei Formen des Informationseingriffes, mit je eigenem Eingriffsgewicht[1128]: Einerseits liegt in der automatisierten Auswertung der gespeicherten Daten eine weitere Nutzung, d.h. eine erneut nach dem Grundsatz der Zweckbindung rechtfertigungsbedürftige Datenverarbeitung. Darüber hinaus liegt ein Grundrechtseingriff „nicht nur in der weiteren, zusammenführenden Verwendung vormals getrennter Daten, sondern [auch] in der Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die

1125 Siehe dazu und zu den folgenden zitierten Passagen BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 48.

1126 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 49.

1127 Die Ausführungen beanspruchen indessen Geltung für andere Datenanalyse-Rechtsgrundlagen bzw. -verfahren.

1128 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 54.

automatisierte Datenanalyse oder -auswertung geschaffen werden kann."[1129] Als insofern erforderlichen legitimen Zweck für den Erlass der Vorschriften hat das Gericht den Zweck anerkannt, „vor dem Hintergrund informationstechnischer Entwicklung die Wirksamkeit der vorbeugenden Bekämpfung schwerer Straftaten zu steigern, indem Anhaltspunkte für bevorstehende schwere Straftaten gewonnen werden, die im Datenbestand der Polizei ansonsten unerkannt blieben."[1130] Dies sei der Fall, da – wie es die hessische Landesregierung dargelegt habe – „die Polizeibehörden […] infolge der insbesondere in den Bereichen terroristischer und extremistischer Gewalt sowie der organisierten und schweren Kriminalität zunehmenden Nutzung digitaler Medien und Kommunikationsmittel mit einem ständig anwachsenden und nach Qualität und Format zunehmend heterogenen Datenaufkommen konfrontiert [seien]."[1131]

Wie jeder Informationseingriff sind auch Rechtsgrundlagen für die Datenanalyse zunächst an den Rechtfertigungsanforderungen zu messen, die der Grundsatz der Zweckbindung und Zweckänderung aufstellt. Insofern ist die im Urteil zum Bundeskriminalamtsgesetz entwickelte Dogmatik der zweckwahrenden und zweckändernden Weiternutzung zu beachten.[1132] Das Gericht fordert im Rahmen der „zweckwahrenden" Weiternutzung von Daten für die Wahrung der Zweckbindung grundsätzlich[1133] nicht, dass erneut die Anlassschwelle (etwa in Form eines Anfangsverdacht) der Datenerhebungsnorm erfüllt ist, sodass eine Nutzung als bloßer Spurenansatz auch im Rahmen der Verarbeitung im Wege der automatisierten Datenanalyse denkbar ist.[1134] Auch für die zweckändernde Weiternutzung ergeben sich im Kontext der automatisierten Datenanalyse insofern keine über das Urteil zum Bundeskriminalamtsgesetz hinausgehenden Besonderheiten.[1135] Da die

1129 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 50.
1130 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 52.
1131 Ebd.
1132 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 55; siehe dazu bereits oben S. 164 ff.
1133 Anders ist dies nach wie vor für Daten aus Wohnraumüberwachungen und Online-Durchsuchungen, siehe BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 59.
1134 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 58.
1135 Vgl. BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 60 ff.

Vorschriften aus Hamburg und Hessen beide Weiterverarbeitungsmodalitäten zulassen, ist aus bundesverfassungsrechtlicher Sicht die Kennzeichnung der Daten zentral, um die Einhaltung der Zweckbindungsregeln überhaupt überprüfen zu können.[1136]

Neben diesen Aspekten, bei denen es im Wesentlichen um das Eingriffsgewicht der einer Datenanalyse vorangegangenen Datenerhebungen geht, stellt das Bundesverfassungsgericht weitere befugnisspezifische Rechtfertigungsanforderungen auf, die in den der automatisierten Datenanalyse per se inhärenten Belastungseffekten begründet liegen. Dabei ist das Eingriffsgewicht der Datenanalyse als solche nicht statisch, sondern hängt variabel von der näheren Ausgestaltung der Befugnis – und damit auch der Anwendung – ab.[1137] Die automatisierte Datenanalyse kann dabei ein über die ursprüngliche Erhebung hinausgehendes Eingriffsgewicht haben. Denn sie ist darauf gerichtet, neues Wissen zu generieren, indem – wie es die dem Verfahren zugrundeliegenden Vorschriften ermöglichen sollten – Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt werden. Damit – so das Gericht – kann die „handelnde Behörde aus den zur Verfügung stehenden Daten mit praktisch allen informationstechnisch möglichen Methoden weitreichende Erkenntnisse abschöpfen sowie aus der Auswertung neue Zusammenhänge erschließen. Die Verknüpfung von Daten ermöglicht etwa mehrstufige Analysen, die neue Verdachtsmomente erst erzeugen, sowie weitere Analyseschritte oder auch daran anschließende operative Maßnahmen."[1138] Zwar ist dies grundsätzlich ein Bestandteil polizeilicher Kerntätigkeiten.[1139] Gerade die Ermöglichung der Verarbeitung komplexer Informationsbestände ist jedoch neu. Die Maßnahme „erschließt die in den Daten enthaltenen Informationen […] intensiver als zuvor." Insofern können nicht nur verborgene Informationen über eine Person zutage gefördert werden, sondern es findet eine Annäherung an Profiling-Verfahren (Art. 4 Nr. 4 DS-GVO) statt, da „sich softwaregestützt neue Möglichkeiten einer Vervollständigung des Bildes von einer Person ergeben [können], wenn Daten

1136 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 65.

1137 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 66.

1138 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 67.

1139 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 68.

und algorithmisch errechnete Annahmen über Beziehungen und Zusammenhänge aus dem Umfeld der Betroffenen einbezogen werden."[1140] Zudem kann „auch die Kombination personenbezogener und nicht personenbezogener Daten und gegebenenfalls die algorithmentypische Berücksichtigung bloßer Korrelationen neue, sonst nicht sicht- oder ermittelbare persönlichkeitsrelevante Aufschlüsse geben."[1141] Das besondere Eingriffsgewicht der automatisierten Datenanalyse ergibt sich für das Bundesverfassungsgericht – in konsequenter Aktualisierung der schon im Volkszählungsurteil angelegten Grundgedanken – in der Überwindung der tatsächlichen Kapazitäts- bzw. praktischen Erkenntnisgrenzen der bisherigen informationellen Polizeiarbeit. Es kann insoweit aus der Sicht des Gerichts zu einer entscheidenden Veränderung von Arbeitsweise und Erkenntnismöglichkeiten der Polizei kommen, der dann allein mit dem verfassungsrechtlichen Grundsatz der Zweckbindung nicht mehr Rechnung getragen werden kann.[1142]

Anlässlich dieser neuen Eingriffsqualität der automatisierten Datenanalyse als informationelle Maßnahme hat das Bundesverfassungsgericht generelle Maßstäbe für die Bestimmung des – aufgrund der vielen Ausgestaltungsmöglichkeiten gesetzlicher Vorschriften variierenden – Eingriffsgewichts festgelegt.[1143] Grundsätzlich gilt, dass bei einer Begrenzung der Befugnis auf schlichte Formen des Abgleichs einer begrenzten Zahl von Daten näher eingegrenzter Herkunft nur ein geringes befugnisspezifisches Eingriffsgewicht anzunehmen ist. Es nimmt umgekehrt zu, je weiter die Möglichkeiten durch die gesetzliche Ausgestaltung reichen; dann reicht auch der Grundsatz der Zweckbindung für sich genommen zunehmend weniger zur Rechtfertigung aus.[1144] Bei schweren Informationseingriffen durch Anwendungen der automatisierten Datenanalyse – etwa die Erstellung von genaueren Bewegungs-, Verhaltens- oder Beziehungsprofilen oder Einbeziehung von Personen, die objektiv nicht zurechenbar in das relevante Geschehen verfangen sind – gelten die Voraussetzungen für eingriffs-

1140 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 69.
1141 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 69.
1142 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 70.
1143 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 71.
1144 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 72.

intensive heimliche Überwachungsmaßnahmen.[1145] Grundsätzlich finden insofern die bereits bekannten Faktoren für die Bestimmung des Eingriffsgewichts Anwendung.[1146] Im Kontext der automatisierten Datenanalyse betont das Bundesverfassungsgericht neben dem Ausmaß des persönlichkeitsrelevanten Wissens sowie der Frage, ob eine Person durch ihr Verhalten zurechenbar Anlass für eine sie treffende Datenanalyse und daran anschließende operative Maßnahmen gegeben hat, vor allem auch den Umfang von Diskriminierungsrisiken – diese sind umso weniger hinzunehmen, „je mehr sich die Wirkungen der automatisierten Datenanalyse […] einer nach Art. 3 Abs. 3 GG unzulässigen Benachteiligung annähern können."[1147]

Vor allem Art und Umfang der Daten – wie es generell für polizeiliche Informationseingriffe und ganz besonders für die elektronische Datenverarbeitung gilt – bestimmen das Eingriffsgewicht einer automatisierten Datenanalyse.[1148] Hier sind verschiedene Variierungen möglich, die sich auf die informationelle Intensität einer Datenanalyse auswirken können: Denkbar ist, die Datenherkunft zu begrenzen, etwa auf von der Polizei (eines Bundeslandes) oder einer inländischen Behörde selbst erhobene Daten, oder Daten aus sozialen Netzwerken auszuschließen.[1149] Eine Eingrenzung kann auch mit Blick auf die „Umstände der Ersterhebung gesetzlich nach Art und Menge" insofern erfolgen, als – in der Regel durch technisch-organisatorische Sicherungen – gewährleistet wird, dass Daten nur gemäß ihrer rechtlichen Verwendbarkeit verarbeitet werden; in der Sache geht es also um eine strikte Beachtung der Zweckbindung.[1150] Allerdings ist auch eine aufgabenbezogene[1151] (etwa: „Terrorismusbekämpfung") oder stark auf die

1145 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 73; letztlich handelt es sich bei der automatisierten Datenanalyse auch um eine heimliche Überwachungsmaßnahme; siehe grundlegend dazu *Schwabenbauer,* Heimliche.

1146 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 76; siehe dazu bereits oben S. 156 ff. sowie BVerfGE 156, 11 48 f. mwN.

1147 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 77.

1148 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 78.

1149 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 79.

1150 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 80.

1151 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 82.

Erforderlichkeit[1152] fokussierende Eingrenzung der einzubeziehenden Daten denkbar. Verfassungsrechtlich ist eine Begrenzung nach den Eingriffsmodalitäten besonders dort zu beachten, wo Daten aus besonders schwerwiegenden Grundrechtseingriffen stammen, wobei hier ohnehin bereits die insofern entwickelten anlass- und zweckbezogenen Schwellen des sicherheitsbehördlichen Informationsverfassungsrechts für solche eingriffsintensiven Maßnahmen zu beachten sind.[1153] Eingriffsmildernd soll zudem eine Beschränkung der verwendeten Daten dahingehend sein, dass diese von Anlass- oder Kontaktpersonen stammen.[1154] Auch über Aufbewahrungs- und Löschfristen lässt sich die Intensität der Datenanalyse modulieren – hier gelten vor allem im Zusammenhang mit der Einbeziehung von Verkehrsdaten erhöhte Anforderungen mit Blick auf die Begrenzung der erfassbaren Datenmengen sowie die Höchstspeicherungsdauer.[1155] Ferner ist der Automatisierungsgrad der Anwendung von Relevanz. Müssen Dateien für jeden Analysevorgang händisch hinzugezogen werden, schwächt es die informationelle Intensität des Eingriffs; umgekehrt wirkt beispielsweise eine Anbindung ans Internet eingriffsverstärkend.[1156] Ähnlich wirkt die technisch-organisatorische Ausgestaltung des Betriebs der automatisierten Datenanalyse: Darf diese nur von einem begrenzten Mitarbeiter:innen-Kreis verwendet werden, so ist das Eingriffsgewicht geringer, denn „[j]e weniger Personen Zugriff auf das Analyseinstrument haben und je zielgenauer der Zugriff erfolgt, umso weniger Analyse- und Auswertungsvorgänge dürften tendenziell in Gang gesetzt und werden und umso weniger Daten werden verarbeitet."[1157] Bezüglich der Datenarten gilt schließlich: Je beschränkter die einbeziehbaren Dateiformate (etwa Bilder-, Video- oder

1152 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 83

1153 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 81.

1154 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 84; das Gericht verwendet nicht genau diese Terminologie (siehe näher dazu unten S. 324 ff.), meint aber letztlich dasselbe.

1155 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 85.

1156 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 88.

1157 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 89.

Audioaufnahmen oder biometrische Daten), desto weniger eingriffsintensiv die Rechtsgrundlage.[1158]

Daneben sind die durch die gesetzliche Regelung zugelassenen Methoden der Datenanalyse maßgebend. Generell gilt hier, dass der Komplexitätsgrad der Methode bestimmend ist, denn die Methode ist „umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können."[1159] Das Bundesverfassungsgericht zieht hier als wenig(er) eingriffsintensive Vergleichskategorie die Maßnahme des Datenabgleichs[1160] heran, bei dem regelmäßig Daten eines Betroffenen an gespeicherten Daten vorbeigeführt werden, um Übereinstimmungen festzustellen, oder aber Daten eines Bestandes in einen anderen überführt werden. Das Eingriffsgewicht ist hier vor allem an die Zahl der vorprogrammierten, also ohne menschliches Zutun veranlassten, Abgleichschritte und Verknüpfungen gekoppelt.[1161] Umgekehrt wirkt dementsprechend die zunehmende Offenheit eines Suchvorgangs, der nur begrenzt „durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster" strukturiert ist, eingriffsintensivierend.[1162] Das gilt vor allem wenn – wie im Kontext der vorbeugenden Straftatenbekämpfung in besonderer Weise der Fall – ohne konkreten Sachverhaltsbezug durch die Analyse überhaupt erst Anhaltspunkte für polizeiliches Tätigwerden generiert werden, insbesondere dann, wenn es um die Identifizierung von statistischen Auffälligkeiten in den Datenmengen und deren (automatisierte) weitere Verknüpfung mit bestimmten Datenbeständen zur Generierung vollkommen neuer, zuvor außerhalb des polizeilichen Suchfokus liegender Informationen geht.[1163] Ferner gewinnt der Informationseingriff an Gewicht, „wenn Suchvorgänge nicht auf näher

1158 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 87.
1159 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 90.
1160 Siehe näher dazu unten S. 351 ff.
1161 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 91.
1162 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 93.
1163 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 93.

umschreibbare Personen ausgerichtet sind und keine sachliche Verbindung zwischen dem gefährdeten Rechtsgut und den von der automatisierten Anwendung Betroffenen vorausgesetzt wird", da ein Personenbezug dann überhaupt erst durch die Maßnahme hergestellt wird und damit das Risiko steigt, „dass Personen in weitere polizeiliche Maßnahmen einbezogen werden, die dafür keinen zurechenbaren Anlass gegeben haben."[1164] Die mit einer offenen Suche verbundenen Gefahren können aber durch eine „anspruchsvoll gestaltete Eingriffsschwelle verringert" oder „durch eine Einschränkung der Datenverarbeitungsmethode gesenkt werden". Verfassungsrechtlich unzulässig ist jedenfalls „[e]ine weder im Einzelfall durch einen konkreten Anlass getragene noch durch Vorgaben zur Verarbeitungsmethode inhaltlich eingeschränkte automatisierte Durchsuchung großer Bestände personenbezogener Daten auf bislang unbekannte Gesetzmäßigkeiten und gefahrenabwehrrechtlich bedeutende Zusammenhänge hin".[1165] Im Kontext der Auswertung großer Datenmengen, insbesondere auf statistische Zusammenhänge hin, statuiert das Gericht ferner eine Pflicht zur Sicherstellung ausreichender Datenqualität sowie zum Treffen von Vorkehrung dagegen, „dass die Auswahl der einbezogenen Daten unangemessen verzerrende, diskriminierende Wirkungen entfalten kann."[1166] Eine weitere grundlegende Weiche für das Eingriffsgewicht ist das Erkenntnisobjekt – das Bundesverfassungsgericht spricht hier von der „Art von Suchergebnissen":[1167] Weniger eingriffsintensiv ist die Erkennung gefährlicher oder gefährdete Orte,[1168] besonders eingriffsintensiv hingegen, „wenn Ergebnis der automatisierten Anwendung personenbezogene Erkenntnisse sind und dieses Ergebnis maschinelle Sachverhaltsbewertungen enthält, die also über die bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten hinausgehen", wobei insbesondere eingriffsintensivierend wirkt, „wenn im Sinne eines „predictive policing" maschinell

1164 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 94.
1165 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 95.
1166 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 95.
1167 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 96.
1168 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 97.

Gefährlichkeitsaussagen über Personen getroffen werden."[1169] Dabei kann der Informationseingriff, der in der Generierung neuen Wissens durch eine Anwendung automatisierte Datenanalyse besteht, dadurch abgemildert werden, dass eine weitere Schwelle für die Weiterverwendung entsprechender Erkenntnisse eingezogen wird.[1170] Für das Eingriffsgewicht von besonderer Bedeutung ist schließlich die Frage, ob lernfähige Systeme, also Anwendungen Künstlicher Intelligenz, Verwendung finden.[1171] Deren spezifische Gefahren liegen nach Auffassung des Verfassungsgerichts im Bereich der polizeilichen Datenanalyse darin, dass Erkenntnismuster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden, wodurch besonders weitgehende Informationen und Annahmen über Personen erzeugt, diese regelmäßig aber zugleich nur unter erschwerten Bedingungen nachgeprüft werden können; derartige selbstlernende, aber bei entsprechender Komplexität auch deterministische,[1172] Systeme dürfen in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau etwa vor Diskriminierungseffekten oder – bei Verwendung einer von privaten entwickelten Software – vor Manipulation sowie unbemerktem Zugriff auf Daten durch Dritte aufweisen.[1173] Damit eng verknüpft ist auch die generelle Fehleranfälligkeit der eingesetzten Technologien sowie die Möglichkeit, problematische Abläufe zu identifizieren – je schwieriger dies ist, desto eingriffsintensiver wird die Datenanalyse.[1174]

Das informationelle Gewicht einer Rechtsgrundlage zur automatisierten Datenanalyse wird neben den soeben dargelegten befugnisspezifischen Belastungseffekten zudem noch durch korrespondierende Eingriffsvoraussetzungen bestimmt. Das Gebot der Verhältnismäßigkeit im engeren Sinne statuiert insofern Anforderungen an das mit der Maßnahme zu schützende

1169 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 98.
1170 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 99.
1171 Siehe dazu bereits oben S. 77 ff.
1172 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 101.
1173 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 100.
1174 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 102.

Rechtsgut wie auch an die Eingriffsschwelle, also den Anlass der Maßnahme.[1175] Ist die Befugnis zur Datenverarbeitung in einer nach den genannten Kriterien sehr belastenden Weise ausgestaltet, so sind hohe Anforderungen an die Rechtsgüter – erfasst sind nur der Schutz vor und die Verhütung von Straftaten im Kontext von besonders gewichtigen Rechtsgütern wie Leib, Leben und Freiheit der Person sowie Bestand des Bundes oder eines Landes, aber auch Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist[1176] – und Eingriffsanlass – erforderlich ist eine hinreichend konkretisierte Gefahr[1177] – zu stellen.[1178] Darunter erfolgt eine Abstufung: Auf mittlerer Stufe stehen durch Einschränkung von Art und Umfang der Daten sowie Verarbeitungsmethode begrenzte „weniger gewichtigen Eingriffen", bei denen es genügt, wenn die gesetzliche Ermächtigungsnorm eine konkretisierte Gefahr oder den Schutz von Rechtsgütern von zumindest erheblichem Gewicht voraussetzt.[1179] Noch darunter stehen Maßnahmen, bei denen Art und Umfang der einbeziehbaren Daten sowie die Verarbeitungsmethoden in einer Weise eingeschränkt sind, „dass eine auf die Befugnis gestützte Maßnahme nicht zu tieferen Einsichten in die persönliche Lebensgestaltung der Betroffenen führt als sie die Behörde, wenngleich aufwendiger und langsamer, auch ohne automatisierte Anwendung realistisch erlangen könnte"; dasselbe gilt, wenn „die Befugnis von vornherein nur darauf [zielt], gefährliche oder gefährdete Orte zu identifizieren, ohne dabei personenbezogene Informationen zu generieren" – hier kann dann bereits die Einhaltung des Grundsatzes der Zweckbindung ausreichen, um die weitere Verarbeitung der Daten in einer automatisierten Anwendung zu rechtfertigen.[1180] Neben diesen Eingriffsvoraussetzungen fließen aus dem Verhältnismäßigkeitsgrundsatz im Rahmen der automatisierten Datenanalyse schließlich Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle, wobei insbesondere einer

1175 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 103.

1176 Sofern hier ein enges Verständnis zugrundegelegt (das Bundesverfassungsgericht spricht von „Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen").

1177 Siehe dazu bereits oben S. 177 ff.

1178 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 104 ff.

1179 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 107.

1180 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 108.

sachgerechten Ausgestaltung der Kontrolle große Bedeutung zukommt. Neben der Befassung der (unabhängigen und behördlichen) Datenschutzbeauftragten ist für das Bundesverfassungsgericht dabei „unerlässlich", „dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden."[1181] Steigt der Komplexitätsgrad der eingesetzten Software sind zudem „Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit erforderlich, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann."[1182]

Hinsichtlich der abstrakten verfassungsrechtlichen Vorgaben für die Regulierung der automatisierten Datenanalyse führt das Bundesverfassungsgericht zudem noch aus, dass auf die Schwelle einer wenigstens konkretisierten Gefahr für besonders gewichtige Rechtsgüter – wie etwa im Bereich der vorbeugenden Bekämpfung von Straftaten regelmäßig der Fall – auch verzichtet werden kann, allerdings nur, „wenn die zugelassenen Analysemöglichkeiten normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahme erheblich gesenkt ist."[1183] Hier muss der Gesetzgeber grundsätzlich den Wesentlichkeitsvorbehalt beachten, kann aber aufgrund „der besonderen Technizität und der raschen Fortentwicklungsbedürftigkeit der hier zur Milderung des Eingriffs benötigten Regelungen […], soweit eine tiefergehende gesetzliche Normierung nicht praktikabel erscheint, die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen", wobei er aber „sicherstellen [muss], dass im Zusammenwirken der gesetzlichen Vorgaben mit den Regelungsermächtigungen und -verpflichtungen der Verwaltung Art und Umfang der Daten und die Verarbeitungsmethoden insgesamt inhaltlich ausreichend, normenklar und transparent begrenzt sind."[1184] Egal wie die Konkretisierung durch die Verwaltung in einem solchen Fall ausgestaltet wird, muss gesetzlich sichergestellt werden, dass die Verwaltung ihre

1181 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 109.

1182 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 109; nähere Ausführungen zum flankierenden Schutz tätigt das Gericht nicht, da dies nicht Gegenstand des Verfahrens war.

1183 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 110.

1184 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 112.

Konkretisierungen und Standardisierungen der gesetzlichen Regelung in einer vom Gesetzgeber vorgeschriebenen Weise nachvollziehbar dokumentiert und veröffentlicht; diese Transparenzanforderungen sind vor allem deshalb geboten, „weil die Durchführung einer automatisierten Datenanalyse oder -auswertung in der Regel von den Betroffenen nicht wahrgenommen wird und sich die Konkretisierung der gesetzlichen Vorgaben damit kaum im Wechselspiel von Verwaltungsakt und gerichtlicher Kontrolle vollzieht", womit „ein zentraler Mechanismus notwendiger Begrenzung konkretisierungsbedürftiger Befugnisnormen weitgehend [ausfällt]."[1185] Auf diese Weise sollen vor allem die Datenschutzbeauftragten in die Lage versetzt werden, die Anwendung der Befugnis durch die Polizeien zu kontrollieren.[1186] Zu den wesentlichen Aspekten, die der Gesetzgeber aber in einem solchen Fall jedenfalls selbst regeln muss, gehört die Frage, welche Datenbestände einbezogen werden dürfen und inwiefern dies automatisiert erfolgen darf, wobei auch hier wieder eine das Eingriffsgewicht erhöhende oder senkende Flexibilisierung der Regelung möglich ist.[1187] Erfolgt keine inhaltliche und mengenmäßige „sehr eng[e]" Begrenzung, ist eine mitarbeiter:innenbezogene Einschränkung der Zugriffsmöglichkeiten gesetzlich festzuschreiben und über technisch-organisatorische Maßnahmen abzusichern.[1188] Ebenfalls durch das Gesetz zu regeln sind die Einbeziehung von Daten aus schwerwiegenden Grundrechtseingriffen – wobei Daten aus Online-Durchsuchung und Wohnraumüberwachung nicht mit in die Datenanalyse zur vorbeugenden Bekämpfung von Straftaten einbezogen werden dürfen – und die technisch-organisatorischen Maßnahme – etwa Kennzeichnungspflichten – zur Absicherung dieser Regelungen.[1189] Auch die Methode einer Datenanalyse zur vorbeugenden Bekämpfung von Straftaten muss vorab normenklar und hinreichend bestimmt gesetzlich festgelegt werden: Neben dem Ausschluss des Einsatzes selbstlernender System muss der Gesetzgeber grundlegende Maßgaben zur Begrenzung des Auto-

1185 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 113.
1186 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 113.
1187 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 115 f.
1188 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 117.
1189 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 118 f.

matisierungsgrades, der Suchfunktionalitäten und den Analyseergebnissen – wie etwa den Ausschluss maschineller Sachverhaltsbewertungen, die über die Anzeige von Übereinstimmungen zwischen Suchkriterien und durchsuchten Datenbeständen hinausgehen, oder Gefährlichkeitsaussagen über Personen – treffen und darf die Ausgestaltung nicht dem faktischen Vollzug durch die Polizeien überlassen.[1190]

Vor diesem Hintergrund hat das Bundesverfassungsgericht § 49 Abs. 1 Alt. 1 HmbPolDVG für nichtig und § 25a Abs. 1 Alt. 1 HSOG – da, anders als für die Hamburger Polizei der Fall, die hessische Polizei bereits auf Grundlage der Landesvorschrift eine Anwendung der automatisierten Datenanalyse betrieb – für unvereinbar mit der Verfassung erklärt, da die in den Vorschriften enthaltenen Befugnisse der automatisierten Datenanalyse zur vorbeugenden Bekämpfung von Straftaten aufgrund ihrer daten- und methodenoffenen Formulierung ein sehr hohes Eingriffsgewicht aufwiesen, ohne dabei zugleich mit den von Verfassungs wegen insofern erforderlichen strengen Eingriffsvoraussetzungen versehen worden zu sein. Vor Ablauf der Übergangsfrist am 30.09.2023 hat der hessische Gesetzgeber eine umfassende Umgestaltung der Vorschrift vorgenommen, die voraussichtlich Vorbild für weitere Gesetzgebungsvorhaben in Bund und Ländern sein wird.

(3) Gegenwärtige Regelungslage und kritische Würdigung

Die Novellierung des § 25a HSOG hat die Vorschrift konkretisiert und erweitert. Im Ersten Absatz wird die automatisierte Datenanalyse als polizeiliches Informationswerkzeug abstrakt-generell beschrieben, der zweite Absatz enthält die Eingriffsvoraussetzungen, d.h. die prinzipiellen Zweckrichtungen, die geschützten Rechtsgüter bzw. erfassten Straftaten sowie die jeweiligen Eingriffsschwellen. Im dritten bis fünften Absatz werden im Wesentlichen Regelung für Verfahren und Kontrolle im Kontext der automatisierten Datenanalyse getroffen.

Der erste Absatz erlaubt es der Polizei, rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenzuführen. Unter Beachtung der übrigen Regelungsaspekte der Sätze 3 bis 6 und der Abs. 2 bis 5 dürfen die hessischen Polizeibehörden – dies ist die eigentliche Beschreibung der automatisierten Datenanalyse – die zu-

1190 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 120 f.

sammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden. Dies ist die Legaldefinition der automatisierten Anwendung zur Datenanalyse. Nach Angaben des Gesetzgebers besteht die automatisierte Datenanalyse somit aus „zwei logisch aufeinander aufbauenden, aber praktisch zeitgleich stattfindenden Schritten, nämlich dem Zusammenführen unterschiedlicher „Datentöpfe" auf der Analyseplattform und der sich daran anschließenden Recherche innerhalb des so zusammengeführten Datenbestands".[1191] Der erste Schritt solle „das strukturelle Problem, dass in den Beständen der Polizei Daten in unterschiedlichen Formaten und disparaten Dateien gespeichert und damit nicht im selben Bearbeitungskontext gleichzeitig verfügbar sind, [überwinden], der zweite führt zu der verfassungsrechtlich relevanten Frage, was genau die Polizei mit den so zusammengeführten Daten machen darf und was nicht."[1192] Satz 3 konkretisiert dies noch etwas näher dahingehend, dass die automatisierte Anwendung zur Datenanalyse ein technisches Hilfsmittel ist, das es den Polizeibehörden bei der Erfüllung ihrer Aufgaben nach Maßgabe der folgenden Absätze ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen. Damit solle sichergestellt werden, „dass immer – und natürlich immer auch in all seiner Fehlerhaftigkeit – der Mensch am Anfang und am Ende des Entscheidungsprozesses steht."[1193] Die Analyseplattform dürfe „die Arbeitsweise der Polizei also nicht „entscheidend verändern", sondern sie soll helfen, ihre bewährte Arbeitsweise zu verbessern, nämlich Informationen aus verschiedenen Quellen zusammenzustellen und sie zu bewerten."[1194] Damit soll ausgeschlossen werden, „dass etwa eine polizeiliche Sachbearbeiterin bei Dienstbeginn das Analysetool gleichsam befragt, was heute denn zu tun sei." [1195] Die automatisierte Datenanalyse – so schreibt es Satz 4 vor – erfolgt immer anhand anlassbezogener und zielgerichteter Suchkriterien. Hiermit soll gewährleistet werden, „dass eine Analysesoftware nicht etwa ein wie immer geartetes Eigenleben oder gar eigene Gesetzmäßigkeiten entwickelt, sondern dass sie bleibt, was sie derzeit

1191 HessLT-Drs. 20/11235, S. 7.
1192 HessLT-Drs. 20/11235, S. 7.
1193 HessLT-Drs. 20/11235, S. 7.
1194 HessLT-Drs. 20/11235, S. 7.
1195 HessLT-Drs. 20/11235, S. 7.

schon ist, nämlich ein bloßes Hilfsinstrument."[1196] Ferner (Satz 5) ist sie manuell auszulösen und soll regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ablaufen. Spezifiziert wird dies dahingehend, dass der Analysevorgang „aus einer Reihe simultan ausgelöster und miteinander in Verbindung gesetzter, auf Wenn-Dann-Operatoren beruhender Suchaktionen über den zuvor zusammengeführten Datenbestand [besteht]. Als regelbasierte oder, gleichbedeutend, deterministische Datenanalyse folgt sie einem klar definierten, unveränderlichen Ablauf und erzeugt deshalb auch konsistente und reproduzierbare Ergebnisse, die einer Gegenkontrolle leichter zugänglich sind als die Datenanalyse unter Einbeziehung selbstlernender Systeme."[1197] Satz 6 schließt zudem eine direkte Anbindung an Internetdienste aus. „Erforderlichenfalls", so die Gesetzesbegründung, „können aber die bei der Bearbeitung eines konkreten Fallkomplexes gezielt ermittelten und zuvor von den Polizeibehörden gespeicherten Daten, die bei einer Internetrecherche angefallen sind, in die automatisierte Datenanalyse einbezogen werden."[1198]

Damit greift Abs. 1 Einiges aus dem Urteil des Bundesverfassungsgerichts aus. Offen ist auch nach der Umformulierung aber, ob die hessische Anwendung der automatisierten Datenanalyse die gesetzlichen Vorgaben faktisch entspricht, was zu überprüfen vor allem der Kontrolle durch den hessischen Landesdatenschutzbeauftragten anheimgestellt werden muss. Dabei könnte eine Schwierigkeit darin bestehen, dass Begrifflichkeiten wie „anlassbezogene und zielgerichtete Suchkriterien" oder eine „vom Menschen definierte Abfolge von Analyse- und Verarbeitungsschritten" Raum für interpretierende Ausgestaltung seitens der Verwaltung lassen, sodass hiermit die Datenverarbeitungsmethode nur begrenzt bestimmt beschrieben ist. Auch die Abgrenzung zwischen einer „Analyseplattform" und einer „automatisierten Anwendung zur Datenanalyse" ist unklar. Zu begrüßen ist der Ausschluss einer direkten Anbindung an Internetdienste. Hier stellt sich aber die Frage, ob bzw. inwiefern eine indirekte Anbindung an Internetdienste erfolgt. Daten von Internetdiensten werden jedenfalls von der Polizei im Rahmen ihrer Aufgabenerfüllung regelmäßig erhoben werden. Falls das Verfahren der Speicherung von solchen Daten im polizeilichen Informationsbestand eher automatisiert erfolgt – etwa im Rahmen von

1196 HessLT-Drs. 20/11235, S. 7.
1197 HessLT-Drs. 20/11235, S. 7.
1198 HessLT-Drs. 20/11235, S. 7.

Online-Wachen[1199] oder sonstigen potenziellen virtuellen Meldestellen – und derartige Informationen als dann Daten aus dem polizeilichen Informationsbestand mit in die automatisierte Datenanalyse einbezogen werden, könnte sich eine solche indirekte Anbindung einer direkten Anbindung durchaus annähern.

Nach § 25a Abs. 2 Satz 1 ist die Weiterverarbeitung von rechtmäßig[1200] gespeicherten personenbezogenen Daten erlaubt, wenn (Nr. 1) dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, erforderlich ist (nunmehr legaldefiniert als „Abwehr konkreter Gefahren"), wenn (Nr. 2) tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten mit erheblicher Bedeutung begangen werden und dies zur Verhinderung dieser Straftaten erforderlich ist (nunmehr legaldefiniert als „Abwehr konkretisierter Gefahren") sowie wenn (Nr. 3) tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass schwere oder besonders schwere Straftaten begangen werden sollen, und die Weiterverarbeitung erforderlich ist, um diese Straftaten zu verhüten (nunmehr legaldefiniert als „Vorbeugende Bekämpfung von Straftaten"). In Satz 2 werden die in die Analyse einbeziehbaren Datenbestände bestimmt; einbezogen werden können Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch. Gemäß Satz 3 können zudem Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen ergänzend in die Datenanalyse miteinbezogen werden. Satz 3 zufolge ist der Einbezug von Verkehrsdaten in Maßnahmen nach § 25 Abs. 2 Satz 1 Nr. 3 nicht gestattet.

Dem Gesetzgeber zufolge überträgt Abs. 2 das in Abs. 1 Satz 2 normierte „Prinzip der Anlass-, Fall- und Zielbezogenheit der automatisierten Daten-

1199 Siehe dazu S. 461 et passim.

1200 Abs. 2 enthält anders als Abs. 1 nicht mehr den Zusatz der „rechtmäßig" gespeicherten Daten. Da nach Abs. 1 aber nur rechtmäßig gespeicherte Daten auf einer Analyseplattform zusammengeführt werden dürfen, ist davon auszugehen, dass auch eine Weiterverarbeitung nur rechtmäßige Daten erfassen darf.

analyse in die Polizeirechtsdogmatik."[1201] Die drei Tatbestandsvarianten des Abs. 2 sollen dabei dem „verfassungsrechtliche[n| Erfordernis einer gleichsam auf dem Hintergrund unterschiedlicher Ebenen, Sektoren und Skalen auszudifferenzierenden Rechtsgrundlage für ein und dasselbe Instrument" Rechnung tragen, wobei [w]egen der dem Gefahrenbegriff eigentümlichen Wechselwirkung zwischen Schadenshöhe und Eintrittswahrscheinlichkeit jede der drei Varianten einen Korridor, dessen Grenzen schon für sich beweglich sind," beschreibe.[1202] Zudem geht die Gesetzesbegründung davon aus, dass diese „Korridore" nicht trennscharf nebeneinander stehen, sondern einander überlappen und ineinander übergehen können. Die grundlegende Überlegung bei dieser Beschreibung scheint zu sein, dass ein Sachkomplex im Laufe seiner Entfaltung nacheinander die verschiedenen „Korridore" durchlaufen kann und mit dieser Progression eine Intensivierung der informationellen Durchleuchtung des Sachkomplexes vorgenommen werden soll. Zugleich hat es der Gesetzgeber ausweisliche der Begründung unternommen, die aus dem Grundsatz der Zweckbindung fließenden Anforderungen sowie das rechtsstaatliche Gebot, die Rechte Unbeteiligter zu schützen, mit im Kontext der Eingriffsgrundlagen in Abs. 2 zu regeln, wobei sich insbesondere zu letzterem Aspekt auch in Abs. 3 wesentliche Regelungsgehalte finden. Der Schutz Unbeteiligter wird dem Gesetzgeber zufolge vor allem durch die Ausklammerung der Nutzung von Verkehrsdaten, in denen regelmäßig viele Daten Unbeteiligter enthalten sind, bei Maßnahmen im Rahmen der vorbeugenden Straftatenbekämpfung gewährleistet.[1203] Der ansonsten nach Abs. 2 Satz 2 kaum begrenzte Einbezug von „Datentöpfen"[1204] in die automatisierte Datenanalyse soll wohl durch das Rechte- und Rollenkonzept aus Abs. 3 kompensiert werden. Der Gesetzesbegründung zufolge soll die „gebotene Reduzierung der Datenmenge und damit die Verringerung der Eingriffsintensität […] deshalb schwerpunktmäßig funktional [erfolgen], indem unter Berücksichtigung und Fortentwicklung bewährter arbeitsteiliger Organisations- und Rechtsformen […] die Schaffung zeitgemäßer, an situativen Anforderungen ausgerichteter Rollen- und Rechtekonzepte durch die Verwaltung verbindlich vorgeschrieben wird mit der Folge, dass die im Einzelfall jeweils zu verarbeitende Datenmenge immer nur ein – mehr oder weniger großer –

1201 HessLT-Drs. 20/11235, S. 8.
1202 HessLT-Drs. 20/11235, S. 8.
1203 HessLT-Drs. 20/11235, S. 8.
1204 Zu den einzelnen Datenbeständen siehe die Ausführungen S. 230 ff.

Ausschnitt des auf der Plattform zusammengeführten und damit potentiell verfügbaren Datenbestandes ist." Weiter heißt es: „Die Datentöpfe sind also zwar vorhanden. Ihr Inhalt darf aber jeweils nur in Teilen entnommen werden. Weil der Gesetzgeber in seinem an die Verwaltung adressierten Regelungsauftrag hierfür nur übergeordnete Ziele, abstrakte Maßstäbe und beispielhafte Kriterien vorgibt, ist es der Verwaltung nicht verwehrt, in Fällen dringender Gefahren für höchstrangige Rechtsgüter – etwa bei einem drohenden Terroranschlag – erforderlichenfalls auch das „volle Programm" zuzulassen, also einzelnen Anwendern den Zugriff auf den vollständigen Inhalt aller Datentöpfe zu erlauben."[1205] Die Eingriffsvoraussetzungen selbst, wie sie in den Nr. 1 bis 3 des Abs. 2 Satz 1 festgelegt sind, sind bereits durch die Rechtsprechung des Bundesverfassungsgerichts konturiert.[1206] Beachtenswert sind insofern noch die gesetzgeberischen Ausführungen zu Abs. 2 Satz 3, wonach es sich bei Datensätzen aus Internetquellen „vor allem um die Ergebnisse polizeilicher Recherchen in für jedermann offenen sozialen Netzwerken" handelt.[1207]

Sehr umfangreich und im Regelungsinhalt einigermaßen komplex ist Abs. 3 geraten. Satz 1 erklärt zunächst – klarstellend – die Geltung des Zweckbindungsgrundsatzes (§ 20 Abs. 1 und 2 HSOG) im Kontext der automatisierten Datenanalyse, was gemäß Satz 2 durch eine zu veröffentlichende Verwaltungsvorschrift sicherzustellen ist. Konkretisiert wird deren Inhalt durch die folgenden Regelungsgehalte: Satz 3 verlangt ein Rechte- und Rollenkonzept sowie ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten. Diese Komponenten werden in den Nr. 1 und 2 des Abs. 3 sodann spezifiziert. Zuvor legt Satz 4 allerdings noch fest, dass sich diese Konzepte unter Berücksichtigung der in Abs. 2 Satz 1 nach Schutzgütern und Eingriffsschwellen unterschiedenen Lagebilder an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter orientieren; legaldefiniert wird dies als funktionale Reduzierung der Eingriffsintensität. Nr. 1 statuiert sodann, dass das Rollen- und Rechtekonzept die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen regelt. Nach Satz 2 sind Maßstab für dieses Konzept das Gewicht der zu schützenden Rechtsgüter und der Grad der Dringlichkeit des poli-

1205 HessLT-Drs. 20/11235, S. 9.
1206 Siehe HessLT-Drs. 20/11235, S. 9 ff für entsprechende Nachweise.
1207 HessLT-Drs. 20/11235, S. 14.

zeilichen Einschreitens. Weiter ist es nach dem Prinzip auszugestalten, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform zusammengeführten Daten haben dürfen. Satz 4 schreibt schließlich vor, dass im Konzept mindestens die einzelnen Phänomenbereiche, ihre Gewichtung und ihr Verhältnis zueinander umschrieben und die dienstrechtliche Stellung der Berechtigten, ihre Funktion und ihre spezifische Qualifizierung bezogen auf den Umfang der jeweiligen Berechtigung festgelegt werden müssen. Nr. 2 konkretisiert das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten. Dieses regelt anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen. In lit. a) wird weiter ausgeführt: Der Maßstab für dieses Konzept ist zum einen der sachliche Bezug der von der Analyse betroffenen Personen zum jeweiligen Phänomenbereich, legaldefiniert als sog. „Veranlassungszusammenhang". Dies folgt dem Prinzip, wonach eine automatisierte Datenanalyse umso komplexer sein darf, je gewichtiger der Veranlassungszusammenhang ist, und dass sie umso einfacher sein muss, je weniger gewichtig der Veranlassungszusammenhang ist. Nach Satz 3 ist Ausgangspunkt die Differenzierung nach verurteilten, beschuldigten, verdächtigen Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen einerseits und unbeteiligten Personen andererseits. Zum Schutz Unbeteiligter werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Auch hier regelt das Nähere eine Verwaltungsvorschrift, die insbesondere für Verkehrsdaten eine Speicherfrist von regelmäßig zwei Jahren in der Analyseplattform vorsieht. Eine weitere Konkretisierung erfolgt sodann noch in lit. b). Danach ist Maßstab für das in Abs. 3 Nr. 2 geregelte Konzept neben dem Veranlassungszusammenhang die Kategorisierung personenbezogener Daten nach der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung bei ihrer Erhebung, legaldefiniert als Grundrechtsrelevanz. Diese Grundrechtsrelevanz erfordert, dass abstrakte Regelungen getroffen werden müssen, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen, und es muss durch technisch-organisatorische Vorkehrungen sichergestellt werden, dass diese Regelungen praktisch wirksam werden. Schließlich werden in die automatisierte Anwendung zur Datenanalyse keine personenbezogenen Daten einbezogen, die aus Wohnraumüberwachung und Online-Durchsuchung gewonnen wurden.

Der in Abs. 3 enthaltene regulatorische Ansatz verknüpft ausweislich der Gesetzesbegründung die Folgerungen aus dem verfassungsrechtlichen Zweckbindungsgrundsatz mit Regelungen über materielle Rechtfertigungsanforderungen und gelangt auf diese Weise zu einer „Kombination aus organisatorischen und materiellen Elementen, die […] als funktionale Reduzierung der Eingriffsintensität bezeichnet wird."[1208] Dabei soll Abs. 3 einerseits das Zweckbindungsprinzip mit „dem auf einem zeitgemäßen und flexiblen, die Funktionalität einer Analyseplattform unterstützenden, an vorhandene Organisationsstrukturen anschließbaren Rollen- und Rechtekonzept" verschränken. Andererseits soll der Absatz eine „eingriffsreduzierenden Vorauswahl [vorschreiben], nämlich [eine] Kategorisierung und Kennzeichnung personenbezogener Daten anhand der materiellen Kriterien des Veranlassungszusammenhangs und der Grundrechtsrelevanz, die dazu führt, dass bestimmte grundrechtssensible Daten von vornherein nur in begrenztem Umfang oder überhaupt nicht in die automatisierte Datenanalyse einbezogen werden dürfen."[1209] Ziel dieses Ansatzes ist die Reduzierung des Datenvolumens, die Angemessenheit der Analysemethode sowie Schutz Unbeteiligter.[1210] Mit den ersten beiden Aspekten greift die Regelung die zentralen Eingriffsgewichtstopoi aus dem Urteil des Bundesverfassungsgerichts auf und auch der Schutz Unbeteiligter, der letztlich auch an die Datenart aus dem Urteil anknüpft, ist wesentlich in der Argumentation des Gerichts. Das Rollen- und Rechtekonzept[1211] wirkt der Dynamik der automatisierten Datenanalyse zur Zusammenführung von Daten auf einer Plattform der Gesetzesbegründung nach entgegen, „weil es dazu führt, dass im normalen Polizeialltag sozusagen niemand in alle der zusammengeführten Datentöpfe schauen kann, sondern immer nur einen Ausschnitt der zusammengeführten Daten sieht."[1212] Die Ausgestaltung des Rollen- und Rechtekonzepts soll sich am Gewicht der zu schützenden Rechtsgüter und der Dringlichkeit der Sache ausrichten, wobei die drei Tatbestandsvarianten des Abs. 2 Satz 1 als abstrakter Maßstab, die kriminologischen Phänomenbereiche, denen innerhalb einer Behörde die verschiedenen Sachbearbeiter:innen zugeordnet sind, als konkreter Anknüpfungspunkt für Rechte

1208 HessLT-Drs. 20/11235, S. 14.
1209 HessLT-Drs. 20/11235, S. 14 f.
1210 HessLT-Drs. 20/11235, S. 15.
1211 Siehe dazu unter anderem unten S. 366 ff.
1212 HessLT-Drs. 20/11235, S. 15.

und Rollen fungieren soll.[1213] Der Gesetzgeber sieht insofern vor, dass etwa „nur wenige und besonders geschulte Berechtigte Zugriff auf Verkehrsdaten oder Daten aus Asservaten haben, weil es sich dabei um große Datenmengen handelt, die typischerweise viele personenbezogene Daten Unbeteiligter beinhalten und deshalb mit besonderer Sensibilität zu behandeln sind", wobei die nähere Ausgestaltung einer Verwaltungsvorschrift überlassen bleibt.[1214] Ferner soll das Rechte- und Rollenkonzept auch dokumentiert und technisch – insbesondere durch eine Zugangskontrolle – abgesichert werden.[1215] Die zweite Stellschraube zur Minimierung der Eingriffsintensität ist in der gesetzgeberischen Konzeption die nähere Kategorisierung der einzubeziehenden Daten und der damit einhergehende Ausschluss bestimmter Datenarten. Hier arbeitet das Gesetz einerseits mit dem sogenannten Veranlassungszusammenhang, was letztlich an die Terminologie der relevanten Personen etwa im BKAG[1216] anknüpft und verlangt, dass einzubeziehende Daten von Personen stammen, die verurteilt, beschuldigt oder verdächtigt sind oder als sonstige Kontakt- oder Anlasspersonen nach § 15 Abs. 2 Nr. 4 HSOG gelten. Daten von Unbeteiligten sollen hingegen „gewissermaßen unsichtbar gemacht werden, obwohl sie in den Quellsystemen, etwa einem Vorgangsbearbeitungssystem, noch auffindbar sind."[1217] Der Schutz dieser Personen sei „dadurch gewährleistet, dass mangels spezifischer Erfassung dieser Daten im Quellsystem ihre elektronische Verknüpfung und somit auch ihre automatisierte Weiterverarbeitung nicht möglich ist."[1218] Hier soll eine menschliche Bewertungsebene vor einer weiteren Verarbeitung eingezogen werden. In der Gesetzesbegründung heißt es: „Der polizeiliche Sachbearbeiter kann also das entsprechende Dokument und darin enthaltene Namen zwar lesen. Er kann diese Namen aber nicht automatisch weiterverarbeiten, ohne zuvor eine überprüfbare Bewertung darüber abgegeben zu haben, dass die betreffende Person nunmehr als Anlassperson (oder als Begleitperson einer Anlassperson) einzustufen ist."[1219] Zur Verringerung der Eingriffsintensität arbeitet der Gesetzgeber andererseits mit Begrenzung oder sogar Ausschluss von personenbezogenen Daten aus schwerwiegenden Grundrechtseingriffen. Verfassungsrechtlich ausge-

1213 HessLT-Drs. 20/11235, S. 15.
1214 HessLT-Drs. 20/11235, S. 15.
1215 HessLT-Drs. 20/11235, S. 16.
1216 Siehe dazu S. 324 ff., 331 ff.
1217 HessLT-Drs. 20/11235, S. 16.
1218 HessLT-Drs. 20/11235, S. 16.
1219 HessLT-Drs. 20/11235, S. 16.

schlossen sind Daten aus Online-Durchsuchungen und Wohnraumüberwachungen.[1220] Alle Daten aus Eingriffen, die bezüglich der Eingriffsintensität darunter liegen, sollen regelmäßig weiter – wenn die verfassungsrechtlichen Voraussetzungen wie etwa das Vorliegen eines konkreten Ermittlungsansatzes erfüllt sind – in die Datenanalyse mit einbezogen werden können, wobei in der Gesetzesbegründung darauf hingewiesen wird, es sei Aufgabe der Verwaltung, „Ausnahmekonstellationen zu identifizieren und sie gegebenenfalls normativ zu erschließen.[1221]

In Abs. 4 hat der Gesetzgeber „Regelungen zur Gewährleistung von Kontrolle, Transparenz, Richtigkeitsvergewisserung und Rechtsschutz aufgenommen."[1222] Satz 1 statuiert eine Zugangskontrolle zur automatisierten Anwendung zur Datenanalyse, wobei Zugriffe nach Satz 2 der ständigen Protokollierung unterliegen. Zudem ist jeder Fall der automatisierten Anwendung zur Datenanalyse von der Anwenderin oder dem Anwender zu begründen, was der Selbstvergewisserung und der nachträglichen Kontrolle dienen soll. Näheres regelt eine Verwaltungsvorschrift. Schließlich ermächtigt Satz 6 behördliche Datenschutzbeauftragte zur Durchführung stichprobenartiger Kontrollen. Die Zugriffskontrolle ist letztlich eine Absicherung des Rechte- und Rollenkonzepts, die etwa eine technische Sperrung für nicht autorisierte Personen vorsieht.[1223] Die nach Satz 5 durch eine Verwaltungsvorschrift zu konkretisierende Begründungspflicht soll nach den gesetzgeberischen Vorstellungen jedenfalls ein Freitextfeld enthalten, um die verfassungsrechtlichen Anforderungen – „eigenständig ausformulierte Begründungen"[1224] – zu erfüllen.[1225]

Die Regelung in Abs. 5 schließlich entspricht dem bisherigen Abs. 3 und schreibt einen (nicht ganz strikten) Behördenleiter:innen-Vorbehalt sowie die Anhörung des oder der hessischen Datenschutzbeauftragten vor.

Grundsätzlich erscheint die neue Regelung der Anwendung zur automatisierten Datenanalyse – insbesondere im Kontrast zu ihrer Vorgängerregelung – ein Fortschritt zu sein, was gesetzgeberische Auseinandersetzung mit dem Regelungsgegenstand angeht; dies schlägt sich auch in einer prinzipiell ausdifferenzierten und entsprechend anspruchsvollen Vorschrift

1220 HessLT-Drs. 20/11235, S. 16.
1221 HessLT-Drs. 20/11235, S. 17.
1222 HessLT-Drs. 20/11235, S. 17.
1223 HessLT-Drs. 20/11235, S. 17.
1224 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 109.
1225 HessLT-Drs. 20/11235, S. 17.

nieder, deren Stärken vor allem in der verfahrensrechtlichen Absicherung der Maßnahme liegen. Allerdings bleibt abzuwarten, ob hier eine Regelung gelungen ist, die den praktischen Datenumgang im Rahmen der automatisierten Datenanalyse in einer Weise zu steuern vermag, welche den verfassungsrechtlichen Anforderungen an diese neue Form der informationellen Polizeiarbeit entspricht. Hier ist vor allem der oder die unabhängige Datenschutzbeauftragte, sind aber auch die behördlichen Datenschutzbeauftragten der damit befassten Polizeibehörden, gefragt, durch eine minutiöse Kontrolle regulative Fehlleistungen zu identifizieren und der weiteren rechtspolitischen Diskussion zuzuleiten. Dabei sollten vor allem auch die teilweise recht präzisen Vorstellungen des Gesetzgebers hinsichtlich des Umgangs mit der Maßnahme der automatisierten Datenanalyse bei den Kontrollen berücksichtigt werden.

Allerdings konnte die Neuregelung einige, bereits zuvor in der Diskussion geäußerte Problemaspekte nicht wirklich ausräumen. So enthält die Vorschrift nach wie vor – wie es zugegebenermaßen auch vom Bundesverfassungsgericht dem Grunde nach bestätigt wurde – den Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, als schützenswertes Rechtsgut. Das Verfassungsgericht versteht darunter wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.[1226] Der Infrastruktur-Begriff taucht in der Verfassungsrechtsprechung insbesondere im Kontext der Terrorismusabwehr auf und steht dabei etwa im Zusammenhang mit „Brücken" und „Behörden".[1227] Es geht dabei nicht um den Schutz des Eigentums oder Sachwerte als solcher.[1228] Ob sich dieses Verständnis auch in der polizeilichen Praxis niederschlagen wird, bleibt abzuwarten. Mit der durch den Bundesgerichtshof anerkannten Wertgrenze von 750 Euro[1229] für Sachen von bedeutendem Wert fallen darunter beispielsweise schon Parkbänke oder Geräte auf Kinderspielplätzen.[1230] Daneben könnten beispielsweise auch die aus der Sprayer:innen-Szene drohenden Sachbeschädigungen in Form von Graffitis an entsprechenden Sachen durch den Einsatz von Datenanalysen als Gefahren abgewehrt werden. Es wäre insofern zu begrüßen,

1226 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 105.
1227 BVerfGE 133, 277 (303) – Antiterrordateigesetz.
1228 BVerfGE 133, 277 (364) – Antiterrordateigesetz.
1229 BGH NStZ 2011, 215.
1230 *Golla* Neue Juristische Wochenschrift 74 (2021), 667 (671).

wenn das Schutzgut, das dem Bundesverfassungsgericht zufolge funktional zu verstehen ist, entsprechend durch eine gesetzliche Formulierung enger gefasst würde. Zudem hat der Gesetzgeber das Schutzgut der Umwelt mit aufgenommen und insoweit qualifiziert, als dass „gleichwertige Schäden" für diese zu erwarten sein müssen. Hier ist völlig offen, was damit genau gemeint ist. In der Zusammenschau mit dem Veranlassungszusammenhang könnte man zumindest annehmen, dass nur Umweltstraftaten davon erfasst sein sollen, was aber – auch mit Blick auf nebenstrafrechtliche Bestimmungen – den Kreis erfasster Verhaltensweisen nicht wirklich präzise eingrenzt. Letztlich hat auch die Neufassung der Eingriffstatbestände in § 25a Abs. 2 S. 1 Nr. 1 bis 3 HSOG nur wenig Begrenzung bezüglich des Einsatzes der Maßnahme gebracht. Nach wie vor ist mit der vorbeugenden Bekämpfung von Straftaten eine Phase vor jeder konkreten oder konkretisierten Gefahr (und jedem konkreten Tatverdacht) angesprochen, sodass *Bäuerles* Feststellung nach wie vor treffend ist, dass nach dem Wortlaut bereits niedrigschwellige und diffuse Anhaltspunkte für mögliche Gefahren oder Straftaten ausreichen könnten. Insofern könnten schon „Tatsachenlagen, die durch eine hohe Ambivalenz der Bedeutung einzelner Beobachtungen gekennzeichnet sind", zum Anlass für eine Datenanalyse genommen werden, obwohl noch nicht verlässlich festgestellt werden kann, ob überhaupt von den dann konkret betroffenen Personen in irgendeiner Weise Gefährdungspotenzial ausgeht.[1231] Zwar ist der Anwendungsbereich auf schwere oder besonders schwere Straftaten, also solche mit einer Höchststrafe von mindestens fünf[1232] bzw. zehn[1233] Jahren, begrenzt. Neben dem Umstand, dass unter die erstere Kategorie bereits eine Vielzahl strafrechtlicher Delikte fällt, ist auch im Bereich der besonders schweren Straftaten mit Delikten wie § 89a StGB und § 129a StGB eine hohe Tatbestandsambivalenz nach wie vor Teil der Eingriffsvoraussetzungen. Das Bundesverfassungsgericht hatte hierzu ausgeführt, dass sich „allein aus der Gefahr der Verwirklichung eines Vorfeldtatbestands […] nicht notwendigerweise bereits solche Gefahren für Rechtsgüter [ergeben]", es aber gerade „auf eine Gefahr für die geschützten Rechtsgüter" ankomme.[1234] Dies spiegelt sich nicht in der Vorschrift wider.

1231 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25a Rn. 37 ff.
1232 BVerfGE 129, 208 (243) – TKÜ-Neuregelung.
1233 BVerfGE 109, 279 (348) – Großer Lauschangriff.
1234 BVerfG-Urteil des Ersten Senats vom 16. Februar 2023 (Automatisierte Datenanalyse), Rn. 170.

Zudem zieht die Erstreckung der Maßnahme auf Anlasspersonen sowie – ausweislich der Gesetzesbegründung – auch auf Begleitpersonen[1235] der Anlasspersonen den Kreis potenziell Betroffener nach wie vor weit.[1236]

Davon abgesehen hat die Regelung aber auch weiterhin grundsätzliche Probleme, die allerdings weniger in der gesetzestechnischen Ausarbeitung selbst begründet sind. Vielmehr ergeben sie sich aus dem Konflikt, der aus der Konzeption der automatisierten Datenanalyse als solcher und dem Zweckbindungsgrundsatz als einem der Grundpfeiler der informationellen Selbstbestimmung erwächst. Denn die Datenanalysen ermöglicht nach wie vor einen wenig beschränkten Umgang mit Daten.[1237] Zwar muss insoweit auch gesehen werden, dass in bestimmten Kriminalitätsbereichen aufgrund des Gewichts der in Rede stehenden Rechtsgüter ohnehin auch „normalerweise" eine zweckändernde Nutzung der meisten oder sogar aller bei der Polizei verfügbarer Daten möglich wäre. Jedoch erscheint mit Blick auf die verfassungsrechtliche Dogmatik der informationellen Selbstbestimmung bei der automatisierten Datenanalyse vor allem problematisch, dass zweckändernde Datenverarbeitungen im Wege dieses informationellen Instruments weiter normalisiert, verfestigt und auf Dauer gestellt werden. Insofern ist es auch nach wie vor zutreffend, von „Zweckänderungsautomaten"[1238] zu sprechen. Letztlich sollte auch nicht vergessen werden, dass in der Regelung auch nach ihrer Neufassung ein altes sicherheitspolitisches Muster präsent bleibt: Es wird versucht ein bereits geplantes oder bestehendes informationstechnologisches Projekt, rechtlich abzubilden, damit – zumindest bis zur nächsten verfassungsgerichtlichen Entscheidung – Daten mit der neuen Anwendung (weiter)verarbeitet werden können.[1239] Wie bereits dargelegt bleibt nunmehr zu beobachten, ob die Eingriffsschwellen, Transparenzpflichten und das Kontroll- und Aufsichtsregime inklusive umfassender Datenprotokollierung zu einem rechtsstaatlich eingehegten Nutzungsverhalten der Polizeien führen. Darüber hinaus erscheint auch, wie von *Golla* vorgeschlagen, eine unabhängige Instanz[1240] zur Kontrolle der

1235 HessLT-Drs. 20/11235, S. 16.
1236 Siehe zu Anlasspersonen unten S. 324 ff.
1237 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25a Rn. 9.
1238 *Will* in Nolte/Poscher/H. Wolter (Hrsg.), Die Verfassung als Aufgabe von Wissenschaft, Praxis und Öffentlichkeit, 429.
1239 So erfolgte die Einführung des § 25a HSOG in Hessen erst nachdem das damit geregelte Verfahren bereits personenbezogene Daten verarbeitet hat, s. HessLT-Drs. 19/6864, Teil B, S. 6 f.
1240 *Golla* Neue Juristische Wochenschrift 74 (2021), 667 (672).

technischen Dimension von Befugnissen zum polizeilichen Einsatz komplexer Informationstechnologie sowie die Sicherstellung der Datenqualität und stete Durchführung einer Datenschutz-Folgenabschätzung sinnvoll.[1241]

Schließlich bleibt im Rahmen solcher Analysesysteme stets auch das unionsrechtliche Verbot automatisierter Einzelfallentscheidungen aus Art. 11 JI-Richtlinie zu beachten. Die in Bundes- und Landesdatenschutzgesetze übernommene Norm untersagt prinzipiell jede ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt. Die Vorschrift des § 25a HSOG hat insoweit versucht Abhilfe zu schaffen, indem ein menschliches Handlungselement im Normtext verankert wurde. Nichtsdestotrotz muss auch hier genau geschaut werden, ob es nicht doch schlicht zur menschlichen Bestätigung eines automatisierten Verarbeitungsvorgangs ohne inhaltliche Überprüfung – ob intentional oder aufgrund eines Automation Biases[1242] – kommt. Dabei handelt es sich um ein Szenario, für das die Entwicklung von (rechtlichen) Kontrollmöglichkeiten noch am Anfang steht.[1243]

cc) Digitalisierung der Informationsträger: Elektronische Strafakte

Eine weitere Innovation, die das polizeiliche Informationswesen der näheren Zukunft tangiert, ist die elektronische Strafakte. Mit ihr sollen die papiernen Strafakten bei Polizei und Staatsanwaltschaft durch eine digitalisierte Form der Informationsträger ersetzt werden. Die Einführung einer elektronischen Akte ist dabei Voraussetzung für einen Medienwechsel, der den technischen Fortschritt nachvollzieht und die Strafjustiz modernisiert.[1244] Neben einer beabsichtigten Vereinfachung und Beschleunigung des Rechtsverkehrs ist mit der sogenannten E-Akte auch die Vereinfachung der Verfügbarkeit und Übermittlung der Dokumente sowie eine einfachere und schnellere Durchsuchung, Filterung oder Verknüpfung von Daten angestrebt.[1245] Um die zuweilen kritisierte[1246] IT-Infrastruktur hierfür zu

1241 *Golla* Kriminologisches Journal 52 (2020), 149 (159).
1242 Siehe dazu etwa *Butz/Christoph/Sommerer* ua Bewährungshilfe 68 (2021), 241 (254 f.).
1243 *Golla* Neue Juristische Wochenschrift 74 (2021), 667 (672).
1244 BT-Drucks. 18/9416, S. 1.
1245 *Puschke* in *J. Wolter* (Hrsg.), SK-StPO, § 496 Rn. 2.
1246 Claus, jurisPR-StrafR 2/2018 Anm. 1.

schaffen oder auszubauen haben sich drei Entwicklungsverbünde gebildet, die jeweils Softwarelösungen entwickeln. Dabei müssen die E-Akten-Softwarelösungen auch Schnittstellen zu den bisherigen staatsanwaltschaftlichen Fachverfahren (MEDSTA und web.sta) enthalten.[1247] Insofern besteht hier IT-architektonisch ähnlich wie im polizeilichen Informationswesen ein gewisses Heterogenitätspotenzial, das sich in Kompatibilitätsproblemen äußern könnte.

Geregelt sind Einführung und Handhabung der elektronischen Strafakten in den §§ 32 ff., § 496 ff. StPO. So war im Zuge der Einführung etwa zu klären, wie sich die bisherige analoge Akte in eine digitale Form überführen lässt, also insbesondere welche Inhalte die E-Akte haben kann und soll und in welcher Form diese dargestellt werden können und sollen.[1248] Herausforderungen betreffen die Gewährleistung von Aktenwahrheit, Aktenklarheit und Aktenvollständigkeit sowie Zugangsmöglichkeiten der Verfahrensbeteiligten.[1249] Vor allem die datenschutzrechtlichen Implikationen der elektronischen Strafakte sind weitreichend, da ein zunehmend digitalisierter Aktenbestand durch die darin bestehenden Recherche- und Verknüpfungsmöglichkeiten eine hohe informationelle Durchdringung von Sachverhalten ermöglichen kann, was durch die Multimedialität einer digitalisierten Akte prinzipiell noch gesteigert wird. Insofern war eine rechtliche Sicherung gegenüber derart ausufernden Informationsmaßnahmen zu schaffen.[1250] Das hat der Gesetzgeber mit § 498 Abs. 2 StPO getan, der einen maschinelle Abgleich personenbezogener Daten mit elektronischen Akten oder elektronischen Aktenkopien gemäß § 98c StPO untersagt, es sei denn, er erfolgt mit einzelnen, zuvor individualisierten Akten oder Aktenkopien.[1251]

Allerdings treffen die Neuerungen rund um die elektronische Strafakte die Polizeien mehr indirekt. Denn mit den tatsächlichen E-Akten arbeiten nur Gerichte und Staatsanwaltschaften, die Polizeien, wenn sie die Vorgänge nicht ohnehin in ihren Vorgangs- oder Fallbearbeitungssystemen haben, sollen regelmäßig nur die sogenannten Repräsentate bekommen.[1252]

1247 *Mitterer* in Anders/Graalmann-Scheerer/Schady (Hrsg.), Innovative Entwicklungen in den deutschen Staatsanwaltschaften, 353 (355 f.).
1248 Vertiefend dazu *Growe/Gutfleisch* Neue Zeitschrift für Strafrecht 40 (2020), 633.
1249 *Puschke* in *J. Wolter* (Hrsg.), SK-StPO, § 496 Rn. 3.
1250 *Singelnstein* in *Knauer/Hartmut Schneider* (Hrsg.), Münchener Kommentar zur Strafprozessordnung Bd. 3: §§ 333-500 StPO, Vorb. zu § 496 Rn. 4.
1251 *Puschke* in *J. Wolter* (Hrsg.), SK-StPO, § 498 Rn. 4.
1252 BR-Drs. 633/19, S. 7 f.

Nichtsdestotrotz dürfte es die polizeiliche Arbeit, insbesondere ihre Effektivität, dadurch verändern, dass Daten bei flächendeckender Nutzung der E-Akte schneller und eventuell auch umfassender zwischen Polizeien und Staatsanwaltschaften zirkulieren. Inwieweit dadurch polizeiliche Informationen zügiger durch das Strafjustizsystem be- und verarbeitet werden können, wird sich zeigen – es ist allerdings anzunehmen. Effizienzsteigerungen sind immerhin eines der expliziten Ziele der Aktendigitalisierung. Wo die Polizeien auch tangiert sein könnten, ist der Bürger:innenkontakt. So ermöglicht es § 32c S. 2 StPO, in einer Rechtsverordnung die Einreichung bestimmter Daten in strukturierter maschinenlesbarer Form vorzuschreiben. Dadurch soll eine durchgehende IT-gestützte Vorgangsverarbeitung ermöglicht und häufig auftretende Verfahrensabläufe – etwa die Einreichung einer Strafanzeige, eines Strafantrags, eines Zeugenentschädigungsantrags oder eines Einspruchsgegen einen Strafbefehl – effizienter gestaltet werden.[1253] Soweit ersichtlich, ist dies noch nicht geschehen, sodass gegenwärtig nicht absehbar ist, an welche Stelle etwa Strafanzeigen geleitet und wie sie dort verarbeitet werden würden.

dd) Mobile Ausformungen des polizeilichen Informationssystems

Digitaltechnik zeichnet sich nebst anderem insbesondere auch durch die Miniaturisierung von Geräten und Instrumenten aus, was ein Mehr an und größere Mobilität von informationstechnischem Gerät in Polizeieinsätzen bedeutet. Emblematisch ist hier zunächst das Smartphone, das gegenwärtig flächendeckend bei deutschen Polizeien ausgerollt wird.[1254] Es kann eine Plattform für verschiedene appsystembasierte Polizeianwendungen bieten und als Aufnahmegerät für verschiedene Medienformate dienen. So sind etwa Messenger-Dienste für Kommunikation zwischen Beamt:innen, Auskunftsapps zum Abgleich mit dem polizeilichen Datenbestand und ein Dokumentenscanner mit KI-getriebener Bilderkennungssoftware denkbare Anwendungen. Daneben sollen in naher Zukunft – zumindest kleinere – Vorgänge vollständig digital erfasst oder etwa Fingerabdrücke digital abgeglichen werden könne.[1255] Damit wird es voraussichtlich zu einer nicht unerheblichen Steigerung der Effektivität informationeller Vorgänge kommen.

1253 BT-Drs. 18/9416, S. 50.

1254 Siehe dazu unten S. 471 ff.

1255 So die konkreten Pläne in NRW, https://www.im.nrw/smartphone-loesung-fuer-die-nrw-polizei (Stand: 01.10.2023).

Zudem ist eine durch die Technizität der Geräte und durch die eingesetzten Softwares bedingte Opazität des polizeilichen Handelns für Betroffene denkbar. Trotz dieser Aspekte, von denen man wohl eine intensitätssteigernde Wirkung behaupten könnte, gibt es keine Rechtsgrundlagen für den Einsatz von Smartphones. Es ist zugegebenermaßen auch fraglich, welchen substanziellen Mehrwert eine solche für ein Informationsinstrument bringen würde, das massenhaft eingesetzt werden soll. Ein prozeduraler Grundrechtsschutz ist indessen möglich. Die Geräte müssen dementsprechend durch technische und organisatorische Maßnahmen eingehegt und auch ansonsten datenschutzrechtlich eng kontrolliert werden.

Ebenfalls vermehrt im Einsatz sind mobile Formen der Videoüberwachung, was vor allem in Form sogenannter Bodycams auch zunehmend im alltäglichen Streifendienst der Fall wird. Diese werden von Polizeibeamt:innen an den Uniformen getragen und zeichnen Bild- und Tondaten im Rahmen des Einsatzes auf, können aber Personen in einem räumlich immer weiteren Umfeld erfassen. Der Aufzeichnungsmodus kann dabei unterschiedlich ausgestaltet sein. Häufig gibt es aber das Erfordernis der Aktivierung durch die Einsatzkräfte, wobei allerdings ein anlassloses Pre-Recording stattfindet. Die Kamera ist also quasi im Dauerbetrieb, überschreibt aber alle 30 oder 60 Sekunden die bis dahin erhobenen Daten. Über diese Zeitspanne hinaus erfasst wird dann nur bei Aktivierung der Bodycam.[1256] Rechtlich zugelassen[1257] sind diese Sonderformen der Videoüberwachung regelmäßig nur in der Öffentlichkeit und nur dann, wenn Polizeibediensteten oder Dritten eine Gefahr für Leib, Leben oder Freiheit droht, wobei die Tatbestandsvoraussetzungen und Ausgestaltungen mitunter divergieren. Ausweitungstendenzen zeichnen sich aber bereits ab, etwa in Form des Einsatzes der Bodycam auch in privaten Wohnräumen.[1258] Daneben müssen Bodycams auch als videotechnische Plattform begriffen werden, die etwa mit Gesichts- oder Verhaltenserkennungssoftware kombiniert werden könnten, wie es in einigen – auch demokratischen – Staaten

1256 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 693.

1257 § 27a BPolG; § 44 Abs. 5 BWPolG; Art. 33 Abs. 4 BayPAG; § 24c ASOG; § 33 BremPolG; § 18 Abs. 5 HmbPolDVG; § 14 Abs. 6 HSOG; § 32a SOG M-V; § 15c PolG NRW; § 31 Abs. 1 POGRP; § 27 Abs. 3 SPolG; § 16 Abs. 3 SOG LSA; § 184 Abs. 3 SchlHLVwG.

1258 Siehe dazu etwa *Lehmann*, Stellungnahme Einsatz Bodycam in privaten Wohnräumen (SPolG), Gesetz zur Neuregelung der polizeilichen Datenverarbeitung im Saarland (Drucksache 16/1180), 2020.

bereits entwickelt wird.[1259] Ob eine solche Konfiguration der Bodycams, die neben einer besonders invasiven Gefahrenabwehr auch eine massive Intensivierung von Fahndungen bedeuten könnte, überhaupt mit der Verfassung vereinbar ist, erscheint zweifelhaft, da dies einen flächendeckenderen Einsatz voraussetzt, der sich stark einer anlasslosen Vorratsdatenspeicherung annähern würde.[1260]

Eine Mobilisierung der Erkenntnisquellen des polizeilichen Informationssystems erfolgt zudem auch durch mobile Formen der automatisierten Kennzeichenkontrolle, wie sie sei einigen Jahren eingesetzt und ausgeweitet wird. Die Maßnahme, die sowohl in den Polizeigesetzen als auch in der StPO (§ 163g) geregelt ist, ermöglicht punktuelle aber dafür intensive Überwachung wichtiger Verkehrsströme. Die Regelungen sind verfassungsrechtlich nicht unproblematisch[1261] und es bleibt abzuwarten, inwiefern polizeiliche Verkehrsüberwachung ausgeweitet werden wird.

ee) Private Datenbestände als latente Datenquellen der Polizei

Die gleichen Merkmale, die das Internet im Allgemeinen und soziale Medien im Besonderen für Massenkommunikation so attraktiv machen – große Reichweite und vielfältige Vernetzungsebenen – machen sie ebenso attraktiv als Überwachungstechnologie. Insofern hat die Polizei Informationspraktiken entwickelt, um die im Internet verfügbaren (personenbezogenen) Daten nutzbar zu machen. Diese werden unter den Begriffen der Online-Streife und Online-Rasterfahndung sowie Open Source Intelligence (OSINT) besprochen. Geregelt sind diese Verfahren nur unzureichend. Zwar sind konkrete, häufig schwerwiegende Maßnahmen wie die Online-Durchsuchung oder die Quellen-Telekommunikationsüberwachung nach den verfassungsrechtlichen Vorgaben reguliert. Während es noch denkbar wäre, oberflächliche und sporadische Online-Streifen auf die Datenerhebungsgeneralklausel zu stützen, bedarf es für systematische Auswertungen

1259 Etwa in Israel, siehe *Cheslow* Times of Israel v. 22. Januar 2022; auch in den USA, *Westrope*, Wolfcom Embraces Body Cam Face Recognition Despite Concerns, https://www.govtech.com/biz/wolfcom-embraces-body-cam-face-recognition-despite-concerns.html (Stand: 01.10.2023).

1260 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 692.

1261 *Arzt* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1164.

der virtuellen Kommunikationssphären des Internets, etwa in Form von zielgerichteten verdeckten Ermittlungen oder dem systematischen Zusammentragen von Informationen aus sozialen Medien, konkrete Rechtsgrundlagen, die bereichsspezifisch verfassungsrechtliche Anforderungen umsetzen.[1262]

Streng genommen handelt es sich dabei jedoch um Datenerhebungsmaßnahmen, die nicht zum primären Fokus der vorliegenden Arbeit gehören. Als sich zunehmend etablierende Informationspraktiken weisen sie jedoch auf eine strukturelle Ausprägung des polizeilichen Informationswesens hin, die bisher nur wenig in der Diskussion um polizeiliche Datenbestände thematisiert wurde: Die Nutzung privater Datenbestände im Rahmen der polizeilichen Aufgabenerfüllung. Zwar ist dieses Phänomen im Kern nicht neu. Rasterfahndung, Telekommunikationsüberwachung und Online-Durchsuchung sind für ihren Erfolg häufig auf die Kooperation mit privatwirtschaftlichen Akteuren angewiesen. Aber die Nutzbarmachung der massiven Datenbestände der Datenökonomie, die ihrerseits – worauf *Zubroff* hingewiesen hat – über inhärente Überwachungsdynamiken verfügt,[1263] scheint noch am Anfang zu stehen. In welcher Form sich eine Verschränkung von polizeilichen und privaten Akteuren, insbesondere den Betreibern von großen Social Media-Plattformen, auf die von der Polizei ausgeübte Sozialkontrolle auswirken wird, ist dabei noch nicht im Detail abzusehen.

Allerdings ist die Polizei bereits heute stark auf eine Beweisfindung und -sicherung im Digitalen angewiesen, sodass die Plattformbetreiber insofern eine wichtige Vermittlerrolle einnehmen und die Strategien, die sie zur Inhaltsmoderierung einsetzen, Einfluss auf die Arbeit der Polizei haben.[1264] So wurden vor allem in Europa besondere Stellen bei vielen Polizeien eingerichtet, um auf Rechtsverletzungen im Internet auch angemessen strafverfolgend reagieren zu können.[1265] In Deutschland ist diese Kopplung zwischen Plattformen und Polizeien für den Fall eventuell strafrechtsrelevanter Online-Kommunikation mit § 3a Abs. 2 NetzDG zentral beim Bundeskriminalamt verankert. Betreiber sozialer Netzwerke müssen diesem zum Zwecke der Ermöglichung der Verfolgung von Straftaten Inhalte über-

1262 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 705 mwN.

1263 *Zuboff,* The age of surveillance capitalism.

1264 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (103).

1265 Siehe dazu etwa *Chang* COLUM. HUM. RTS. L. REV. 49 (2018), 114.

mitteln, die dem Anbieter in einer Beschwerde über rechtswidrige Inhalte gemeldet worden sind, die der Anbieter entfernt oder zu denen er den Zugang gesperrt hat und bei denen konkrete Anhaltspunkte dafür bestehen, dass sie mindestens einen der Tatbestände der §§ 86, 86a, 89a, 91, 126, 129 bis 129b, 130, 131 oder 140 des Strafgesetzbuches, des § 184b des Strafgesetzbuches oder des § 241 des Strafgesetzbuches in Form der Bedrohung mit einem Verbrechen gegen das Leben, die sexuelle Selbstbestimmung, die körperliche Unversehrtheit oder die persönliche Freiheit erfüllen und nicht gerechtfertigt sind. Darüber hinaus sind Metadaten des entsprechenden Inhalts gem. § 3a Abs. 4 NetzDG zu übermitteln. Nach einem Urteil des Verwaltungsgerichts Köln ist § 3a NetzDG jedoch zunächst aufgrund von Unvereinbarkeit mit dem Unionsrecht für unanwendbar erklärt worden.[1266]

Allerdings ist damit mitnichten das letzte Wort in der Verschränkung von Digitalökonomie und Strafverfolgungsbehörden gesprochen, vielmehr ist es der Auftakt der Ausgestaltung dieses Verhältnisses. Die bereits abzusehenden und recht sicher zu erwartenden Dynamiken in dieser Beziehung hat *Bloch-Wehba* bereits konturiert. Einerseits weiten die Strafverfolgungsbehörden ihren Einfluss auf die Plattformbetreiber aus. Nicht nur Meldepflichten wie in § 3a NetzDG, sondern auch die generellen Belange der Strafverfolgungsbehörden veranlassen Plattformbetreiber dazu, ihre Moderierung entsprechend anzupassen. Zudem spiegeln die technischen Infrastrukturen der Inhaltsmoderation – in dem Maße, in dem Plattformunternehmen auf Automatisierung und „künstliche Intelligenz" setzen, um ihre Bemühungen zur Bekämpfung schädlicher Online-Inhalte zu verstärken – zunehmend die Einflüsse von staatlichen Sicherheitsentscheidungen wider.[1267] Umgekehrt sind jedoch auch die Strafverfolgungsbehörden einem Einfluss seitens der Plattformbetreiber unterworfen. Die technische Affordanzstruktur der jeweiligen Plattformen und sozialen Netzwerke bestimmt entschieden darüber mit, was etwa Polizeien bei ihren Online-Streifen als mögliche Beweise für eine vorgefallene Straftat sehen und sichern können. Werden Inhalte vorher gelöscht, ist auch das Delikte mitunter nicht mehr aufklärbar, wenn keine Instrumente zur Wiederherstellung der Daten bestehen.[1268] Gerade bei der Überwachung von und Ermittlung in devianten

1266 VG Köln, Beschluss vom 1.3.2022 – 6 L 1277/21 – Google = MMR 2022, 330.

1267 *Bloch-Wehba* Cornell Int'l L.J. 53 (2020), 41 (69 f.); *Fourcade/Gordon* JLPE 1 (2020) sprechen insoweit treffend von "dataist statecraft".

1268 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (104 f.).

Gruppierungen, die regelmäßig über einen längeren Zeitraum erfolgen, kann es für die Polizeien wichtig sein, dass Inhalte nicht möglichst schnell verschwinden.[1269] Insofern spielen inhaltsbezogenen Entscheidungen der Plattformen eine zunehmend größere Rolle für Strafverfolgungsbehörden – private und staatliche Akteure sind insofern beidseitig und komplex miteinander verflochten.[1270] Auch könnte der Prozess der Inhaltsmoderation selbst zu einem immer attraktiveren Ziel für die Strafverfolgungsbehörden werden, wenn die Plattformen zunehmend proaktiv und automatisiert filtern. Setzen Plattformen automatische Moderationsverfahren ein, erhalten sie regelmäßig Zugang zu einer großen Menge an Inhalten, die entweder tatsächlich gegen das Gesetz verstoßen oder diesen Anschein erwecken. Denn die Technik ist häufig noch nicht ausgereift genug, nur tatsächlich strafrechtliche Inhalte zu identifizieren und mit Blick auf die normative Natur strafrechtlicher Normen ist auch zweifelhaft, ob eine fehlerfreie Identifizierung überhaupt möglich ist. Deshalb sind die automatisierten Techniken oft zwangsläufig zu umfassend und erfassen mehr Inhalte, als beabsichtigt war.[1271] Neben dieser vorrangig digitalen Sphäre kommt durch das Internet der Dinge aber auch der digital augmentierte analoge Raum (auch: Onlife[1272]-Sphäre) in einen – durch die jeweiligen Unternehmen der Digitalökonomie vermittelten – Fokus der Polizei. Statt eine Wohnung tatsächlich in Raum und Zeit zu durchsuchen, könne eine retrospektive Durchsuchung über eine Reihe von vernetzen Haustechnologien erfolgen.[1273]

Insofern lassen sich Entwicklungstendenzen erkennen, die reichhaltigen Datenbestände der Digitalökonomie (auch) zu latenten polizeilichen Datenspeichern umzufunktionieren: Die vorgehaltenen Daten sind nicht direkt Teil des polizeilichen Informationswesens, sondern fungieren als Ressource im Leerlauf, die bei Bedarf oder durch gesetzlichen Impuls als informationelle Quelle in die polizeiliche Arbeit eingebunden werden kann. Neben der bedenklichen Informationsfülle, die dadurch „an den Fingerspitzen" der Polizeien liegt, wirft eine umfassendere Zusammenarbeit zwischen Strafverfolgungsbehörden und Plattformen zusätzlich schwierige

1269 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (117 f.).
1270 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (118).
1271 *Gorwa/Binns/Katzenbach* Big Data & Society 7 (2020), 1-15 (5).
1272 *Floridi,* The 4th revolution, passim.
1273 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (136).

Fragen darüber auf, wie integrale Bestandteile des Rechtsstaats wie Rechenschaftspflicht und Transparenz am besten in diesem verflochtenen Feld umgesetzt werden können.[1274]

III. Die einfachgesetzliche Normierung polizeilicher Informationspraktiken

Nachdem nun das Recht der Infrastrukturen des polizeilichen Informationswesens dargestellt und erläutert wurde, soll dies nun in einem zweiten Schritt auch für den normativen Rahmens der im Informationswesen ausgeübten Informationspraktiken erfolgen. Die Darstellung ist dabei nochmals zweigeteilt und geht zunächst auf Datenverarbeitungen im polizeilichen Informationsverbund ein. Danach erfolgt noch eine Auseinandersetzung mit Datenverarbeitungen in den polizeibehördeneigenen Systemen. Die Fülle an nicht unerheblichen Divergenzen in den Polizeirechtsordnungen der Länder- und Bundesbehörden erschweren jedoch eine umfassende Gesamtdarstellung, weshalb der Fokus stattdessen auf zentrale Strukturprinzipien gelegt wird.[1275]

1. Polizeiliche Datenverarbeitung im Informationsverbund

Zentral für die (rein) polizeiliche Datenverarbeitung im Informationsverbund sind die §§ 16, 18 und 19 BKAG, deren Beachtung über § 29 Abs. 4 S. 2 BKAG im Wesentlichen auch für alle anderen Polizeibehörden, die am Verbund teilnehmen, vorgeschrieben ist. Die Vorschriften sind dabei auch – wie bereits dargelegt[1276] – für bestimmte Ausformungen des Informationsverbundes relevant, etwa für Fahndungs-, Haft- und erkennungsdienstliche Dateien. Im Folgenden soll hingegen auf die konkreten Verarbeitungsmöglichkeiten geschaut werden, die die Normen ermöglichen. Dabei adressieren die §§ 16, 18 und 19 BKAG in ihrer direkten Anwendung das Bundeskriminalamt und dessen Datenweiterverarbeitungen im eigenen Informationssystem nach § 13 BKAG. Nicht ganz klar ist, welche Bedeu-

1274 *Bloch-Wehba* Law & Society: Private Law - Intellectual Property eJournal 2021, 102 (107).

1275 So auch *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 578, siehe dort auch Fn. 1419.

1276 Siehe dazu bereits oben S. 230 ff.

tung die drei Vorschriften für die teilnehmenden Polizeibehörden konkret haben, die Gesetzesbegründung ist insoweit unverständlich.[1277] Zwar lässt sich sagen, dass die Normen dem Informationsverbund zugrunde liegen,[1278] aber gleichzeitig findet sich die Berechtigung für Eingabe und Abruf von Daten im Informationsverbund durch die teilnehmenden Stellen gesondert in § 29 Abs. 3 BKAG geregelt. Als relativ sicher kann insofern allerdings wohl gelten, dass die in § 29 Abs. 4 S. 2 BKAG genannten Vorschriften des 2. Unterabschnitts im 2. Abschnitt des BKAG für die Eingabe und den Abruf durch die am Informationsverbund beteiligten Behörden zu beachten sind. Da – was *Bäcker* eindrücklich für seine Stellungnahme anlässlich der Gesetzesberatungen zum BKAG herausgearbeitet hat – bereits die direkte Anwendung der §§ 16, 18 und 19 BKAG im Rahmen der bundeskriminalamtlichen Datenverarbeitung mit erheblichen Problemen behaftet sind, beschränkt sich die nachfolgende Darstellung auf diesen Anwendungsfall, da eine Beschäftigung mit der entsprechenden Anwendung einer strukturell defizitären, änderungswürdigen Rechtslage kaum Erkenntnisgewinne verspricht.

a) Verarbeitung personenbezogener Daten durch das Bundeskriminalamt nach § 16 BKAG

Gemäß § 16 Abs. 1 BKAG kann das Bundeskriminalamt personenbezogene Daten unter Berücksichtigung des § 12 BKAG im Informationssystem ver-

1277 Danach entspricht Satz 2 „dem bisherigen § 11 Absatz 1 Satz 3, wobei die Verweise der neuen Rechtslage angepasst werden. Durch den Verweis in Satz 3 auf die §§ 12, 14 und 15 wird sichergestellt, dass der Grundsatz der hypothetischen Datenneuerhebung und die zu dessen Implementierung erforderliche Kennzeichnung für die Eingaben im INPOL-Verbund für alle Teilnehmer Geltung besitzt." Der alte § 11 Abs. 1 S. 3 BKAG schreibt lediglich vor, dass § 36 BKAG a.F. unberührt bleibt; die Vorschrift betrifft eine für das alte BKAG geltende Verordnungsermächtigung. Denkbar ist, dass es sich dabei um einen inhaltlichen Fehler in der Gesetzesbegründung handelt und eigentlich § 11 Abs. 2 S. 3 gemeint war, der für die Eingabe durch die teilnehmenden Behörden im „alten" Informationsverbund die §§ 7-9 BKAG a.F. für anwendbar erklärt. Strukturell ist dieser Verweis näher an § 29 Abs. 4 S. 2 BKAG n.F., der wiederum Datenverarbeitungsregeln im „neuen" Informationsverbund für entsprechend anwendbar erklärt. Auch die bisher einzige Kommentierung zu § 29 Abs. 4 S. 2 BKAG erschließt die Vorschrift nur bedingt, denn sie bezieht sich unter anderem auf § 29 Abs. 2 S. 4 BKAG, vgl. Graulich in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 Rn. 26.

1278 So *Bäcker*, A-Drs. 18(4)806 D, S. 3 ebenfalls auf § 29 Abs. 4 S. 2 BKAG verweisend.

arbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und das BKAG keine zusätzlichen besonderen Voraussetzungen vorsieht. Das Bundeskriminalamt ist damit berechtigt, im Zusammenhang mit bestimmten gesetzlichen Aufgaben angefallene Daten auch für die Erfüllung einer anderen Aufgabe zu nutzen. So können etwa im Rahmen der Zentralstellenaufgabe angefallene Daten auch für die Aufgabenerfüllung nach §§ 4 bis 8 BKAG genutzt werden. Im Zuge einer solchen Zweckänderung ist, worauf § 16 Abs. 1 BKAG explizit verweist, der Grundsatz der hypothetischen Datenneuerhebung einzuhalten.[1279] Der Begriff der Verarbeitung ist im Sinne des § 46 Nr. 2 BDSG weit zu verstehen und beinhaltet damit jeden Umgang mit Daten, der nicht Datenerhebung ist.

aa) Verfassungsrechtliche Bedenken bzgl. § 16 Abs. 1 BKAG i.V.m. der Figur der zweckwahrenden Weiternutzung

Im Gegensatz zur bisherigen Rechtslage, die § 16 Abs. 1 BKAG nur abbilden soll,[1280] ermöglicht die Norm neuerdings jedoch auch weitreichende Weiterverarbeitungen im Rahmen einer ursprünglichen Aufgabe („zweckwahrende Weiternutzung“[1281]), wie *Bäcker* am Beispiel der Terrorismusabwehr gemäß § 5 BKAG darlegt: Im Rahmen dieser Aufgabe sind regelmäßig hochrangige Rechtsgüter bedroht, was den Einsatz eingriffsintensiver Datenerhebungsmaßnahmen ermöglicht und so typischerweise besonders sensible Daten in die Sphäre des Bundeskriminalamtes gelangen lässt. Die Weiterverarbeitung innerhalb derselben Aufgabe erfordert dabei mangels Zweckänderung nicht, dass die Voraussetzungen des Grundsatzes der hypothetischen Datenneuerhebung, also insbesondere ein konkreter Ermittlungsansatz, vorliegen. Darüber hinaus ist Voraussetzung für die Weiterverarbeitung lediglich noch, dass diese zur Aufgabenerfüllung erforderlich ist. Dabei handelt es sich um eine niedrigschwellige Voraussetzung.[1282] Das Bundeskriminalamt kann unter diesen Voraussetzungen etwa einmal im Rahmen der Terrorismusabwehr erhobene Daten langfristig bevorraten, um die gegebenenfalls später innerhalb derselben Aufgabe zu nutzen. Einschränkend wirkt dabei nur die nach wie vor nicht an die neue Rechtslage

1279 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 16 BKAG Rn. 6.
1280 BT-Drs. 18/11163, S. 97.
1281 Siehe dazu bereits oben S. 164 ff.
1282 *Bäcker*, A-Drs. 18(4)806 D, S. 4.

angepasste BKADV[1283], die die zu speichernden Datenarten konkretisiert. Restriktivere Speicherungsanlässe zur Bevorratung von Daten innerhalb einer Aufgabenzuweisung sieht das BKAG nicht vor. Auch die Verwertung der so anfallenden und bevorrateten Daten wäre als Unterfall des Weiterverarbeitungsbegriffes im Rahmen derselben Aufgabe auf § 16 Abs. 1 BKAG zu stützen und hinge damit allein von der Erforderlichkeit zur jeweiligen Aufgabenerfüllung ab. Hinzu kommt, dass die in § 79 Abs. 1 S. 1, 1. HS BKAG anlässlich Zweckerreichung aufgestellte Löschungspflicht gem. § 79 Abs. 1 S. 1, 2. HS BKAG nicht für nach den Vorschriften des Abschnitts 1, Unterabschnitt 2 verarbeiteten Daten gilt, worunter unter anderem die Weiterverarbeitung nach § 16 Abs. 1 BKAG fällt.[1284] Insofern ist § 16 BKAG als Bevorratungsermächtigung zu lesen, die sich an den dafür bestehenden verfassungsrechtlichen Vorgaben messen lassen muss. Die Breite und tendenzielle Sensibilität der erfassbaren Daten haben eine hohe Grundrechtsbelastung zur Folge. Mithilfe der bevorrateten Daten ist eine granulare Abbildung der hinter den Daten stehenden Personen möglich.[1285] Eine so eingriffsintensive Bevorratungsermächtigung bedarf eines hinreichenden Anlasses[1286] und erfordert, dass dem Eingriffsgewicht der Bevorratung auf Ebene der Datenverwertung Rechnung getragen wird. Dem wird § 16 Abs. 1 BKAG mit seinem einfachen Erforderlichkeitskriterium nicht gerecht.[1287] Hier zeigt sich auch ein Problem in der unreflektierten Übernahme der unionrechtlichen Datenschutz-Terminologie. Indem mit dem Weiterverarbeitungsbegriff operiert wird, werden alle möglichen Datenverarbeitungsschritte tatbestandlich vermengt, obwohl ihnen unterschiedliches Eingriffsgewicht zukommen kann, zumal auch die unionsrechtliche Dogmatik eine anlass- und unterschiedslose Speicherung insbesondere von sensiblen Daten nicht erlaubt.[1288] Auch der Verweis auf eine verfassungskonforme Auslegung, wie man ihn im polizeilichen Informationsrecht anlässlich gesetzgeberischer Unterregulierung immer wieder findet,[1289] kann für § 16 Abs. 1

1283 Siehe dazu bereits oben S. 227 ff.
1284 *Bäcker*, A-Drs. 18(4)806 D, S. 4 f.
1285 Siehe *Bäcker*, A-Drs. 18(4)806 D, S. 5, Fn. 15 zu „maßgeblichen Intensitätskriterien".
1286 BVerfGE 133, 277, 339 ff. – Antiterrordatei; EuGH, 21.12.2016 - C-203/15, C-698/15 – Tele2 Sverige u.a., 96 ff.; EGMR, 04.12.2008 - 30562/04, 30566/04 – S. und Marper gegen Vereinigtes Königreich, Rn. 101 ff.
1287 Vgl. *Bäcker*, A-Drs. 18(4)806 D, S. 5 f.
1288 Siehe dazu, auch mwN., *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 11.
1289 *Schenke* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 45 BKAG Rn. 26, 33; *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Po-

BKAG nicht ernsthaft in Erwägung gezogen werden, dafür ist die Norm zu zentral für das System der Datenverarbeitung im polizeilichen Informationswesen.[1290]

bb) Spezielle Datenverarbeitungsformen nach § 16 BKAG

Neben der Weiterverarbeitungsgeneralklausel, die an den beschriebenen Mängeln leidet und damit das Informationshandeln des Bundeskriminalamts als wichtigstem Akteur im polizeilichen Informationsverbund normativ unzureichend einhegen, geschweige denn steuern kann, enthält § 16 BKAG noch spezielle Verarbeitungsbefugnisse. Sie erlauben die Verarbeitung der Daten in den wichtigen Dateien bzw. zukünftig den durch Zugriffsrechte abgegrenzten Teilen des „gemeinsamen Datenhauses". Geregelt ist dort die Verarbeitung zu Fahndungs-, Strafverfolgungsvorsorge- und erkennungsdienstlichen Zwecken sowie die Verarbeitung von Hinweisen. Auch hier ist gegenwärtig die fehlende Konkretisierung durch die BKADV ein Problem. Welche Daten genau verarbeitet werden dürfen, lässt sich insoweit nicht sagen.

Daneben erlaubt § 16 Abs. 4 S. 1 BKAG Datenabgleiche, wenn Grund zu der Annahme besteht, dass dies zur Erfüllung einer Aufgabe erforderlich ist. Der Datenabgleich ermöglicht die Feststellung, ob zu einer Person bereits eine Speicherung in einer polizeilichen Datei bzw. im „gemeinsamen Datenhaus der Polizei" enthalten ist. Der Maßnahme wird nur eine geringe Eingriffsintensität zugesprochen,[1291] was angesichts der umfangreichen Datenbestände der Polizeien nicht ohne Weiteres einleuchtet, zumal im Trefferfall denkbar ist, dass sich weitere Maßnahmen anschließen, die allerdings auch ihre eigenen Eingriffsschwellen haben. Dennoch ist fraglich, ob angesichts des Anwachsens der polizeilichen Datenbestände, wie es in Folge der Datafizierung halbwegs sicher zu erwarten ist, bei der Kategorisierung von Datenabgleichen als wenig eingriffsintensiv stehen geblieben werden kann.

---

lizeirechts, G. Rn. 618, 961; *Schenke* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, E. Rn. 404.

1290 Siehe zur verfassungsrechtlichen Problematik des § 16 Abs. 1 BKAG auch die Ausführungen bei *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 16 Rn. 7 ff.

1291 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 16 BKAG Rn. 36; kritisch zur Eingriffsintensität etwa *Golla* Kriminologisches Journal 52 (2020), 149 (158).

b) Datenverarbeitung durch das Bundeskriminalamt und im Informationsverbund nach §§ 18, 19 BKAG

Neben § 16 BKAG sind die §§ 18, 19 BKAG integrale Normen für die Verarbeitung von personenbezogenen Daten im bundeskriminalamtlichen Informationssystem und im Informationsverbund. Neben der Zentralstellenaufgabe (§ 18 Abs. 1 i.V.m. § 2 Abs. 1 bis 3 BKAG) darf die Verarbeitung, über § 16 Abs. 3 BKAG, vor allem auch zu Zwecken der Strafverfolgungsvorsorge erfolgen. Es geht hierbei also um die wichtige Frage, zu welchen Personen Daten im polizeilichen Informationsverbund bevorratet werden dürfen.

Das Gesetz unterscheidet insofern zwischen (Nr. 1) Verurteilten, (Nr. 2) Beschuldigten, (Nr. 3) Personen, die einer Straftat verdächtig sind, sofern die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, und (Nr. 4) Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffene Person in naher Zukunft Straftaten von erheblicher Bedeutung begehen wird (sog. Anlasspersonen). Dieser „personenbezogene Eingriffstatbestand“,[1292] den es auch vorher bereits gab, ist nunmehr auch unionsrechtlich erforderlich und setzt insofern Art. 6 JI-Richtlinie um, der die Mitgliedstaaten verpflichtet, die personenbezogenen Daten unterschiedlicher Personenkategorien unterscheidbar zu machen.[1293] Diese Vorgabe ergibt sich aus Erwägungsgrund 31 der JI-Richtlinie, wonach es bei der Verarbeitung personenbezogener Daten im Rahmen der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit naturgemäß um betroffene Personen verschiedener Kategorien geht.

1292 So *Bäcker*, Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz, https://verfassungsblog.de/der-umsturz-kommt-zu-frueh-anmerkungen-zur-polizeilichen-informationsordnung-nach-dem-neuen-bka-gesetz/ (Stand: 01.10.2023), für §§ 18, 19 BKAG.

1293 BT-Drs. 18/11163, S. 99.

aa) Personenkategorien nach § 18 BKAG

Eine erste Gruppe ist die der Verurteilten, die gegenüber der Vorgängerregelung neu aufgenommen wurde. Eine Erweiterung der Befugnisse soll damit nicht einhergehen.[1294] Verurteilte im Sinne der Norm sind gemäß § 4 BZRG diejenigen, bei denen ein deutsches Gericht (§ 4 Nr. 1 BZRG) wegen einer rechtswidrigen Tat auf Strafe erkannt, (Nr. 2) eine Maßregel der Besserung und Sicherung angeordnet, (Nr. 3) jemanden nach § 59 des StGB mit Strafvorbehalt verwarnt oder (Nr. 4) nach § 27 JGG die Schuld eines Jugendlichen oder Heranwachsenden festgestellt hat.[1295] Der Begriff des Beschuldigten ist dem Strafverfahrensrecht entlehnt.[1296] Darunter fallen diejenigen Tatverdächtigen, gegen die das Verfahren als Beschuldigte betrieben wird. Um diese Eigenschaft zu begründen, bedarf es eines Willensakts der zuständigen Strafverfolgungsbehörde.[1297] Ebenfalls erfasst sind die unterschiedlichen, von der jeweiligen Phase des Strafverfahrens abhängigen, Formen des Beschuldigtenstatus.[1298] Die Kategorien von verurteilten und beschuldigten Personen verweisen folglich auf formale Stadien des Strafverfahrens; dieser Formalisierungsgrad gilt hingegen bereits nicht mehr bei der Kategorie der Verdächtigen gem. Nr. 3, obgleich es auch hier einen strafprozessualen Konnex gibt.[1299] Denn der Begriff des Verdächtigen stammt zwar aus dem Strafverfahrensrecht, ist dort aber nicht präzise definiert. Entscheidend ist, dass der strafprozessual relevante Verdacht hinsichtlich einer Tat sich auf bestimmte Tatsachen stützen muss, bloße Vermutungen reichen hingegen nicht aus.[1300] Neben der Verdächtigeneigenschaft ist noch das Bejahen der in § 18 Abs. 1 Nr. 3 BKAG genannten Prognose (sogenannte Negativprognose) für eine zulässige Weiterverarbeitung erforderlich. Die Prognose ist – wie in § 16 Abs. 1 und 5 BKAG – gerichtlich überprüfbar.[1301] Die letzte Personenkategorie, für die § 18 Abs. 1 Nr. 4 BKAG die Weiterverarbeitung gestattet, ist die der Anlassperson. Das

1294 BT-Drs. 18/11163, S. 99.
1295 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 3.
1296 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 4.
1297 *Diemer* in *Hannich* (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, § 136 Rn. 4.
1298 Angeschuldigte:r und Angeklagte:r.
1299 Eichenhofer in *Barczak* (Hrsg.), BKAG, § 18 Rn. 7.
1300 *Kölbel* in *Hartmut Schneider* (Hrsg.), Münchener Kommentar zur Strafprozessordnung, § 170 Rn. 15.
1301 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 5.

Erfordernis der tatsächlichen Anhaltspunkte für die Begehung einer Straftat von erheblicher Bedeutung durch die von der Verarbeitung betroffene Person ist sehr niedrigschwellig. Vor allem im direkten Vergleich zu Nr. 3 der Vorschrift, die eine Verarbeitung neben der Verdächtigeneigenschaft noch an weitere täter- oder tatbezogene Voraussetzungen knüpft, ist die Norm zu unbestimmt. Dass die betroffene Person in der Vergangenheit beschuldigt oder verdächtig war, ist nicht erforderlich, sodass personenbezogene Daten von bisher an Straftaten völlig unbeteiligten Personen verarbeitet werden können.[1302] Zudem ist das Erfordernis der tatsächlichen Anhaltspunkt für die Begehung einer Straftat von erheblicher Bedeutung gesetzlich nicht weiter definiert, was die Unbestimmtheit der Norm zusätzlich erhöht.[1303] Wie dieses Erfordernis durch die polizeiliche Datenverarbeitungspraxis entgrenzt werden kann, haben *Ruch und Feltes* am Beispiel der Gewalttäterdateien dargelegt.[1304] Inhaltlich handelt es sich bei der Prognose nach § 18 Abs. 1 Nr. 4 BKAG um eine Einzelfallprüfung nach kriminalistischen Erfahrungsgrundsätzen,[1305] bei der „von dem speichernden Beamten eine alle Umstände des Einzelfalls berücksichtigende Individualprognose erwartet wird, die einer […] schematischen Darstellung nicht zugänglich ist. Je nach Lebenssachverhalt und je nach Datei kommen beispielsweise Ankündigungen einer Straftat, Offenbarungen gegenüber Dritten oder andere Hinweise in Betracht. Der wesentliche Unterschied zu Verdächtigen und Beschuldigten ist damit nicht das Merkmal einer vermeintlichen Beliebigkeit, sondern dass die Straftat, um die es geht, noch nicht begangen wurde."[1306] Die Regelung hat keinen strafprozessualen Anknüpfungspunkt mehr und dient daher rein präventiven Zwecken.[1307] Während die Datenverarbeitung in diesem Kontext in der Vergangenheit noch durch die für die jeweiligen Dateien erforderlichen Errichtungsanordnungen konkretisiert wurde,[1308] fehlt diese ermessensleitende Begrenzung nunmehr. Unter all diesen Gesichtspunkten ist der Auffangtatbestand des § 18 Abs. 1 Nr. 4 BKAG verfassungsrechtlich schwer tragbar, da bei polizeilicher Betrachtung

1302 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 6.
1303 Vgl. *Arzt* Neue Juristische Wochenschrift 2011, 352, 354 für die Vorgängerversion des § 18 Abs. 1 Nr. 4 BKAG (§ 8 Abs. 5 BKAG a.F.).
1304 *Ruch/Feltes* NK 17 (2016), 62 (71 f.).
1305 BT-Drs. 16/13563, S. 8, zur Vorgängerversion des § 18 Abs. 1 Nr. 4 BKAG (§ 8 Abs. 5 BKAG a.F.).
1306 BT-Drs. 17/2803, S. 4.
1307 *Eichenhofer* in *Barczak* (Hrsg.), BKAG, § 18 Rn. 7.
1308 BT-Drs. 17/2803, S. 4.

individueller Lebenspraktiken wohl nicht selten Anhaltspunkte auftreten können, die eine entsprechende Annahme rechtfertigen können und so die Gefahr für Betroffene bergen, zum polizeilichen „Informationsobjekt" zu werden.[1309] Das gilt insbesondere in den Bereichen des Strafrechts, die stark von dessen kriminalpräventiven Neujustierung betroffen sind, wie etwa §§ 89a, 129a StGB. Auch eine sehr enge Ermessenspraxis, wie es *Graulich* zur verfassungsrechtlichen Bewahrung der Norm vorschlägt,[1310] ist mit Blick auf den Wesentlichkeitsgrundsatz eher abzulehnen: Eine exekutive Selbstprogrammierung in einem derart sensiblen Bereich kann – vor allem auch mit Blick auf die Geschichte der normativen Einhegung polizeilicher Informationsverarbeitung[1311] – nicht (mehr) hingenommen werden.

Ferner gestattet § 18 Abs. 3 BKAG es dem Bundeskriminalamt, sogenannte Prüffälle zu verarbeiten,[1312] also zu schauen, ob bei ihm eingegangene Erkenntnisse und Angaben zu Personen, die bisher unbekannt waren, dazu führen, dass die betroffene Person einer der in Abs. 1 genannten Kategorien unterfällt. Das Bundeskriminalamt muss dann zunächst feststellen, ob die personenbezogenen Daten für seine Aufgabenerfüllung erforderlich sind und, wenn dies zu bejahen ist, welcher Personenkategorie sie zugeordnet werden müssen.[1313] Die Daten sind gesondert im Informationssystem zu speichern, § 18 Abs. 3 S. 2 BKAG. Die Löschung hat gemäß Satz 3 nach Abschluss der Prüfung, spätestens jedoch nach zwölf Monaten zu erfolgen, wobei der Gesetzgeber zur Begründung dieser nicht unerheblichen Verarbeitungsdauer auf die vorhandenen Erfahrungen im internationalen Dienstverkehr und erhebliche Dauer von Strafverfahren im In- und Ausland verweist.[1314] Damit ist die Möglichkeit eröffnet, noch unter dem personenbezogenen Eingriffstatbestandes der sogenannten Anlassperson Daten zu speichern und zu verarbeiten, wenn auch – zumindest rechtlich – nur begrenzt.

1309 *Zöller,* Informationssysteme, S. 164.
1310 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 11.
1311 Siehe dazu bereits oben S. 119 ff.
1312 Siehe dazu bereits oben S. 259 ff.
1313 BT-Drs. 18/11163, S. 99 f.
1314 BT-Drs. 18/11163, S. 100.

bb) Datenarten im Rahmen der Personenkategorien des § 18 BKAG

Die Arten der personenbezogenen Daten, die von den in § 18 Abs. 1 BKAG genannten Personen verarbeitet werden können, werden in § 18 Abs. 2 BKAG genannt und durch die BKADV konkretisiert. Demnach kann das Bundeskriminalamt (Nr. 1) von Personen nach Abs. 1 Nr. 1 bis 4 (lit. a) die Grunddaten, (lit. b) soweit erforderlich, andere zur Identifizierung geeignete Merkmale, (lit. c) die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer, (lit. d) die Tatzeiten und Tatorte und (lit. e) die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten weiterverarbeiten. Darüber hinaus (Nr. 2) kann es von Personen nach § 18 Abs. 1 Nr. 1 und 2 BKAG weitere personenbezogenen Daten verarbeiten, soweit die Weiterverarbeitung erforderlich ist, weil wegen der Art oder der Ausführung der Tat, der Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind. Dasselbe gilt auch für Personen nach § 18 Abs. 1 Nr. 3 und 4 BKAG, wobei hier keine solche Prognose durchzuführen ist, § 18 Abs. 2 Nr. 3 BKAG.

Diese noch recht weiten Beschreibungen der Arten personenbezogener Daten müssen durch die BKADV weiter eingegrenzt werden. Mangels aktueller und tatsächlich auf Grundlage von § 20 BKAG erlassener BKADV findet eine solche Eingrenzung gegenwärtig wohl nur auf Grundlage der alten BKADV statt. Eine Limitierung bewirkt zudem die für die Verarbeitung vorausgesetzten Erforderlichkeitsgründe des § 18 Abs. 2 Nr. 2. Diese sind strafrechtsakzessorisch auszulegen, wofür insbesondere spricht, dass § 18 Abs. 2 BKAG über § 16 Abs. 3 BKAG der Strafverfolgungsvorsorge dient und nicht der Gefahrenabwehr.[1315] „Art oder Ausführung der Tat" beinhaltet insofern, angelehnt an die Auslegung des § 46 Abs. 2 StGB, die Tat begleitende oder sie sonst prägende Aspekte, also etwa Tatmodaliäten von Zeit, Ort, Dauer und Mitteln.[1316] Um für die Datenverarbeitung erforderlich zu sein, müssen Merkmale der Persönlichkeit des Betroffenen in Zusammenhang mit dem bisherigen Verhalten stehen. Elemente der Lebensführung, die in keinerlei Zusammenhang zu dem Tatvorwurf stehen, können nicht als relevant berücksichtigt werden.[1317] Darüber hinaus können auch „sonstige Erkenntnisse" die Erforderlichkeit der Datenverarbeitung von

1315 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 24.
1316 *Bußmann* in *Matt/Renzikowski,* Strafgesetzbuch: StGB, § 46 Rn. 17.
1317 *Kühl* in *Lackner/Kühl* (Hrsg.), Strafgesetzbuch, § 46 Rn. 36, 47.

Personen nach § 18 Abs. 1 Nr. 1 und 2 BKAG begründen. Dieser Auffangtatbestand räumt bei der Bestimmung des Verarbeitungsanlasses – ähnlich wie auch § 18 Abs. 1 Nr. 4 BKAG – in verfassungsrechtlich problematischer Weise einen normativ kaum gesteuerten Spielraum ein. So steht etwa zu befürchten, dass bestehende Erkenntnisse zu Personen – es geht um Verurteilte und Beschuldigte – den Bedarf an weiterer Datenverarbeitung aus sich selbst heraus legitimieren und so die datengestützten Einschätzungen bezüglich der Betroffenen perpetuieren.[1318]

Ist zumindest eine dieser Erforderlichkeitsvoraussetzungen erfüllt muss darüber hinaus noch Grund zu der Annahme bestehen, dass Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind. Der Gesetzesbegründung zufolge muss die durchzuführende Prognose neben der Persönlichkeit des Betroffenen alle Umstände des Einzelfalls berücksichtigen. Dabei muss es konkrete Anhaltspunkte für einen Verarbeitungsanlass geben, wofür aber ausreichen soll, wenn als Ergebnis einer summarischen Prüfung anhand der entsprechenden Anhaltspunkte nach allgemeinen Erfahrungswerten, wie etwa kriminalistischer Erfahrung, die Möglichkeit besteht, dass gegen den Betroffenen künftig Strafverfahren zu führen sein werden.[1319] Nötig ist dementsprechend eine Wiederholungsgefahr,[1320] wobei diese bei erstmalig Beschuldigten i.S.d. § 18 Abs. 1 Nr. 2 BKAG auch für ein erwiesenermaßen relevantes Verhalten in der Vergangenheit nicht ohne Weiteres – quasi schematisch – bejaht werden darf. Diese Prognose ist gerichtlich überprüfbar.[1321] Auch hier besteht indes ein weiter Deutungsspielraum bei den Polizeien.

Die Verarbeitung weiterer personenbezogener Daten ist gemäß § 18 Abs. 2 Nr. 3 BKAG zudem auch für die Personen nach Abs. 1 Nr. 3 und 4 gestattet. Da hier bereits für die Zuordnung zu einer der beiden Personenkategorie jeweils eine Prognose erforderlich ist, ist diese Voraussetzung im Rahmen des Abs. 2 Nr. 3 BKAG nachvollziehbarerweise nicht noch einmal genannt, wie in § 18 Abs. 2 Nr. 2 BKAG. Dennoch ist es nicht ohne Weiteres einsichtig, weshalb auch für die in Abs. 1 Nr. 3 und 4 genannten Personen ohne Weiteres die Verarbeitung weitere personenbezogener Daten möglich sein soll. Während sich argumentieren ließe, dass der Unterschied zwischen Beschuldigten und Tatverdächtigen eher formaler Natur

1318 So *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 27.
1319 BT-Drs. 13/1550, S. 25.
1320 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 28.
1321 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 28.

ist, ist doch jedenfalls für die Anlasspersonen von einem eher kategorischen Unterschied zu den restlichen Personenkategorien auszugehen, da – wie bereits ausgeführt wurde[1322] – ein breiter Personenkreis von der Regelung erfasst werden kann. Die bereits im Kontext des § 18 Abs. 1 BKAG problematische Gleichbehandlung setzt sich mithin auch in Abs. 2 fort. Das Gesetz gestattet damit nicht nur, dass überhaupt Daten zu Anlasspersonen gespeichert werden können, sondern ermöglicht auch die informationell tiefergehende Verarbeitung weiterer personenbezogener Daten.

Ähnlich wie § 16 BKAG enthält § 18 BKAG in seinem vierten Absatz eine Verarbeitungsermächtigung für die Haftdatei oder im geplanten „gemeinsamen Datenhaus" haftrelevante Daten. Er ersetzt den vormaligen § 9 Abs. 2 BKAG a.F., der die Haftdatei regelte.[1323]

cc) Weiterverarbeitungssperre im Rahmen des § 18 BKAG

Gemäß § 18 Abs. 5 BKAG ist die Weiterverarbeitung unzulässig, wenn der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wird und sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat. Bei fehlender Schuld und Strafausschließungsgründen ist einzelfallbezogen zu prüfen, ob die Prognose dennoch zu bejahen ist.[1324] Zudem sind die Daten nach den allgemeinen Löschungsregeln der §§ 77 ff. BKAG zu löschen, wenn sie nicht mehr erforderlich sind.[1325] Bei nicht ausreichendem Tatverdacht kann die Verarbeitung hingegen weitergeführt werden.[1326] Die Regelung ist mithin sehr relevant für die Grenzen kriminalpolizeilicher Datenverarbeitung.

Zentral für die Beurteilung der Unzulässigkeit der Weiterverarbeitung ist, dass sich aus den Gründen der Entscheidung positiv ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat. Ergibt sich diese positive Feststellung nicht aus der Entscheidung, ist dem Bundesverwaltungsgericht zufolge der Tatbestand des § 18 Abs. 5 BKAG

1322 Siehe dazu oben S. 324 f.
1323 Siehe zur Haftdatei bereits oben S. 244.
1324 BT-Drs. 13/1550, S. 25.
1325 Siehe dazu unten S. 370 f.
1326 BT-Drs. 13/1550, S. 25.

nicht erfüllt. Die positive Bestätigung eines Restverdachts durch die jeweilige Entscheidung ist für die Zulässigkeit der Weiterverarbeitung nach dem Gesetz demzufolge nicht notwendig. Dem Bundesverwaltungsgericht nach ist dies auch nicht als Verstoß gegen die in Art. 6 Abs. 2 EMRK verbürgte Unschuldsvermutung zu werten, da die „Berücksichtigung von Verdachtsgründen, die auch nach einer Verfahrensbeendigung durch Freispruch oder Einstellung fortbestehen können, keine Schuldfeststellung oder -zuweisung [darstellt], wenn und soweit sie bei Wiederholungsgefahr anderen Zwecken, insbesondere der vorbeugenden Straftatenbekämpfung, dient."[1327] Wie bereits dargelegt, erscheint diese Ansicht zweifelhaft.[1328] Zudem ist dieses Verständnis mit Blick auf die Konstellation der Verfahrenseinstellung nach § 170 Abs. 2 StPO problematisch. Die staatsanwaltschaftliche Begründung richtet sich in diesem Fall nach den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV), in deren Nr. 88, „Mitteilungen an den Beschuldigten", vorgesehen ist, dass bei einer Einstellung nach § 170 Abs. 2 StPO die Gründe der Einstellung der beschuldigten Person nur auf Antrag und dann auch nur soweit bekannt zu geben sind, als kein schutzwürdiges Interesse entgegensteht. Hat sich die Unschuld herausgestellt oder besteht kein begründeter Verdacht mehr, so ist dies ebenfalls mitzuteilen. Obwohl die Begründung des § 170 Abs. 2 StPO auch im Rahmen des § 18 Abs. 5 BKAG relevant wird, hat es der Gesetzgeber unterlassen, kompatible Kategorien zu schaffen. Aus der Mitteilung der Staatsanwaltschaft ergibt sich somit nicht unmittelbar, ob Beschuldigte die Tat nicht oder nicht rechtswidrig begangen haben, wie es für § 18 Abs. 5 BKAG erforderlich wäre. Das Bundesverwaltungsgericht spricht sich anlässlich dieser Rechtslage für eine „Anpassung der Begrifflichkeiten in § 170 StPO, Nr. 88 RiStBV, § 8 Abs. 3 BKAG und § 484 Abs. 2 Satz 2 StPO" aus, um „die Folgen der Einstellung eines strafrechtlichen Ermittlungsverfahrens für die Befugnis zur Datenspeicherung aus Gründen der vorbeugenden Verbrechensbekämpfung oder der Strafverfolgungsvorsorge normklarer zu gestalten."[1329] Gleichzeitig zieht es allerdings nicht die Konsequenz, die Verarbeitungsvoraussetzungen wegen der inkompatiblen Kategorien zu verneinen.[1330] Vielmehr will das Gericht die Entscheidung über die Unzulässigkeit der Weiterverarbeitung auf die Mittelung der Staatsanwaltschaft an die Polizeibehörde, die im Rah-

1327 Vgl. BVerwGE 137, 113, Rn. 26 zu der Vorgängerregelung § 8 Abs. 3 BKAG a.F.
1328 Siehe dazu bereits oben S. 243 f.
1329 BVerwGE 137, 113, Rn. 29.
1330 So wohl *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 51.

men des polizeilichen Informationssystems die datenschutzrechtliche Verantwortung für die beim Bundeskriminalamt gespeicherten Daten gemäß § 16 Abs. 2 trägt, stützen. Nach § 482 Abs. 2 StPO hat die Staatsanwaltschaft die mit der Angelegenheit befasste Polizeibehörde über den Ausgang des Verfahrens zu unterrichten. Grundsätzlich geschieht dies durch Mitteilung der Entscheidungsformel, kann aber erforderlichenfalls auch durch die mit Gründen versehene Einstellungsentscheidung erfolgen. Auch soll die entsprechende Polizeibehörde gegebenenfalls bei der Staatsanwaltschaft um eine solche begründete Entscheidung nachsuchen, bevor sie über weitere Datenverarbeitungen entscheidet.[1331]

Damit ergibt sich indessen ein etwas inkonsistenter Zustand im Rahmen der Rechtsanwendung des § 18 Abs. 5 BKAG: Bei Freispruch oder Nichteröffnung des Hauptverfahrens ist die Verarbeitung nach der Vorschrift unzulässig. Bei einer Einstellung nach § 170 Abs. 2 StPO, für die erforderlich ist, dass bei Durchführung der Hauptverhandlung ein Freispruch wahrscheinlicher ist als eine Verurteilung, ist dies jedoch nach Rechtsprechung des Bundesverwaltungsgerichts nicht der Fall. Trotz des Umstandes also, dass die drei Varianten des § 18 Abs. 5 BKAG in ihrer Implikation für das Vorliegen einer Straftat vergleichbar sind, werden sie unterschiedlich gehandhabt. Zudem besteht für den Betroffenen aufgrund der positiven Wirkung des § 170 Abs. 2 StPO keine Möglichkeit eine Einstellungsentscheidung im oben genannten Sinne herbeizuführen.[1332] Im Ergebnis bedeutet dies für die Praxis polizeilicher Informationsverarbeitung, dass personenbezogene Daten von einem wohl nicht unerheblichen Teil der Beschuldigten auch nach Beendigung des Strafverfahrens im Wege der Einstellung weiterverarbeitet werden dürfen.

dd) Datenverarbeitungen nach § 19 BKAG

Der „personenbezogene Eingriffstatbestand“[1333] des § 19 BKAG gestattet über die Kategorien des § 18 BKAG hinaus Daten zu anderen Personen zu verarbeiten. Auch § 19 BKAG Abs. 1 S. 1 BKAG nennt in Umsetzung des Art. 6 lit. d JI-Richtlinie abgegrenzte Personengruppen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass (Nr. 1) sie bei einer zukünftigen Strafverfolgung als Zeugen in Betracht kommen, (Nr. 2) bei einer künftigen

1331 BVerwGE 137, 113, Rn. 30.
1332 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 18 BKAG Rn. 51.
1333 Siehe dazu bereits Fn. 1292.

Straftat als Opfer in Betracht kommen, (Nr. 3) sie mit in § 18 Abs. 1 Nr. 1 bis 3 BKAG bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken, oder (Nr. 4) es sich um Hinweisgeber und sonstige Auskunftspersonen handelt.

Auch hier müssen im Rahmen der Erforderlichkeitsvoraussetzung des Tatbestandes konkrete Anhaltspunkte vorliegen, dass die Verarbeitung der personenbezogenen Daten zur Verhütung von Straftaten oder Strafverfolgungsvorsorge notwendig ist; allgemeine Nützlichkeitserwägungen sind nicht ausreichend.[1334] Der Wortlaut des § 19 Abs. 1 S. 1 BKAG drückt durch die Nennung von Verhütung von Straftaten, die im Polizeirecht wurzelt, und Strafverfolgungsvorsorge, die aus dem Strafrecht herrührt, ein kompetenzrechtliches Verständnis der Verschränkung beider Bereiche aus, was unter dem Gesichtspunkt der legislatorisch grundsätzlich getrennten Verantwortung problematisch ist. Dies trägt zur Vermischung von Präventiv- und Repressivdaten bei. Ferner ist in § 16 Abs. 3 BKAG nur der Verweis auf die Strafverfolgungsvorsorge enthalten, sodass sich § 19 Abs. 1 S. 1 BKAG innerhalb des BKAG widersprüchlich verhält.[1335] Der Begriff der erheblichen Straftat ist identisch mit dem in § 2 Abs. 1 BKAG. Die Prognose diesbezüglich folgt demselben Schema wie im Rahmen des § 18 Abs. 1 Nr. 4 BKAG.[1336] Da personeller Anknüpfungspunkt die zukünftige Straftat eines Dritten ist, muss diese erläutert und überprüfbar festgehalten werden, damit der Verarbeitungszweck erkennbar wird und bleibt.[1337] Auffällig ist zudem die Eingriffsschwelle der „tatsächliche[n] Anhaltspunkte", die dem Recht der Nachrichtendienste entlehnt ist und keine Berührungspunkte mit den Eingriffsschwellen der konkreten Gefahr der Gefahrenabwehr bzw. des Anfangsverdachts der Strafverfolgung hat. Die demgegenüber niedrigere Schwelle im nachrichtendienstlichen Kontext kann mit Blick auf die regelmäßig weniger eingriffsintensiven Maßnahmen der Dienste gerechtfertigt

1334 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 19 BKAG Rn. 4.
1335 *Zöller,* Informationssysteme, S. 165 zum insoweit identischen § 20 BKAG a.F.
1336 Siehe dazu bereits oben S. 324 ff.
1337 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 19 BKAG Rn. 6.

werden, ist allerdings im Rahmen der polizeilichen Datenverarbeitung problematischer.[1338]

Liegen die Tatbestandsvoraussetzungen vor, so kann das Bundeskriminalamt personenbezogene Daten der vier genannten Personenkategorien verarbeiten, wobei für Zeug:innen, Opfern und Hinweisgeber:innen zudem noch deren Einwilligung erforderlich. Bei Kontakt- oder Begleitpersonen nach § 19 Abs. 1 Nr. 3 BKAG handelt es sich um Auffangkategorien. Nachdem die Vorgängerregelung des § 8 Abs. 4 BKAG a.F. nach heutigen verfassungsrechtlichen Maßstäben, wie sie im Antiterrordatei-Urteil zum Ausdruck gekommen sind,[1339] keinen Bestand mehr hätte, hat sich der Gesetzgeber bei der Novellierung des BKAG für den Zusatz entschieden, dass Tatsachen die Annahme rechtfertigen müssen, dass die Kontakt- oder Begleitpersonen maßgebliche Kenntnis der Straftaten besitzen oder daran mitgewirkt haben müssen. Der Begründung zufolge entspricht dies wesentlichen verfassungsrechtlichen Vorgaben und stellt einen „objektiven Tatbezug" her.[1340] Das ist hinsichtlich der einer jeden Prognose innewohnende Unsicherheit allerdings nur bis zu einem gewissen Grad der Fall.[1341] Der Bestimmtheitsgrad dieser Kategorie ist dementsprechend zumindest kritisierbar.

Die Arten der personenbezogenen Daten sind allerdings gemäß § 19 Abs. 1 S. 2 BKAG gegenüber dem insofern extensiveren § 18 Abs. 1 BKAG eingeschränkt: Die Weiterverarbeitung ist demnach beschränkt auf die in § 18 Abs. 2 Nr. 1 lit. a bis lit. c BKAG bezeichneten Daten sowie auf die Angabe, in welcher Eigenschaft der Person in Bezug auf welchen Sachverhalt die Speicherung der Daten erfolgt. Das Fehlen einer aktualisierten BKADV wirkt sich auch hier auf die Konkretisierung der Datenverarbeitung aus.

Die in § 19 Abs. 1 S. 1 Nr. 3 BKAG genannten Personen müssen dabei mit einer Personenkategorie des § 18 Abs. 1 BKAG in Verbindung gebracht werden, wobei nur Verurteilte, Beschuldigte und Tatverdächtige taugliche Anknüpfungspersonen sein können, Der damit zum Ausdruck kommende Ausschluss von Anlasspersonen gemäß § 18 Abs. 1 Nr. 4 BKAG ist aufgrund der unbestimmten personellen Reichweite dieser Norm verfassungsrechtlich zu begrüßen. Eine Datenverarbeitung wäre ansonsten von einer doppelten personenbezogenen Prognose abhängig, deren Hintereinanderschal-

1338 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 19 BKAG Rn. 7.
1339 BVerfGE 133, 277, 347 ff. – Antiterrordateigesetz.
1340 BT-Drs. 18/11163, S. 100.
1341 Siehe etwa *Schöch* in Hans Schneider (Hrsg.), Grundlagen der Kriminologie, 359 (S. 361).

tung erhebliches Potenzial für Falschpositive mit sich brächte. Allerdings bedeutet die Einbeziehung von Tatverdächtigen (und, in abgeschwächter Form auch von Beschuldigten) ebenfalls eine Verkettung zweier Prognosen, denn auch bei dieser Personenkategorie ist noch nicht sicher, ob sie tatsächlich eine Straftat begangen haben.

Wie bereits § 18 Abs. 3 BKAG hat auch § 19 BKAG in seinem Abs. 3 eine insoweit identische Prüffallregelung. Diese ist mit Blick auf die mitunter unsichere Tatsachengrundlage für Datenverarbeitungen nach § 19 Abs. 1 Nr. 3 BKAG problematisch, denn eine Prüfung dahingehend, ob eine Person in der tatbestandlich relevanten Weise mit (potenziell) delinquenten Personen gemäß § 18 Abs. 1 Nr. 1-3 BKAG in Verbindung steht, kann theoretisch bei allen Personen durchgeführt werden, die irgendwie in Kontakt mit einer Person aus den Kategorien des § 18 Abs. 1 Nr. 1-3 BKAG gekommen sind.

ee) Konstruktionsfehler in der neuen Informationsarchitektur?

Wie *Bäcker* herausgearbeitet hat, tun sich – wie bei § 16 BKAG – auch im Rahmen der §§ 18, 19 BKAG strukturelle Probleme auf, die aus dem Zusammentreffen der novellierten Gesetzessystematik und den verfassungsrechtlichen Anforderungen herrühren[1342]: Das unklare Verhältnis der beiden personenbezogenen Eingriffstatbestände der §§ 18, 19 BKAG zu § 16 Abs. 1 BKAG und damit mittelbar zu § 12 BKAG verursacht Schwierigkeiten bei der Auslegung: Dem Wortlaut des § 16 Abs. 1 BKAG zufolge sind Verarbeitungen nach dieser Datenverarbeitungsgeneralklausel möglich, „soweit dieses Gesetz keine zusätzlichen besonderen Voraussetzungen vorsieht." Da die §§ 18, 19 BKAG die Datenverarbeitung jedoch an andere Voraussetzungen als die Erforderlichkeit des § 16 Abs. 1 BKAG knüpfen, gehen diese beiden Normen dem § 16 Abs. 1 BKAG „soweit" vor. Nun verweist § 16 Abs. 1 BKAG über seine eigenen Voraussetzungen hinaus auch auf § 12 BKAG, der den verfassungsrechtlichen Grundsatz der hypothetischen Datenneuerhebung einfachgesetzlich abbildet. Einen entsprechenden Verweis findet man in den §§ 18, 19 BKAG indessen nicht. Bei Speicherungen von Daten nach §§ 18, 19 BKAG kommt es allerdings regelmäßig zu einer Zweckände-

1342 Siehe zu den weiteren Ausführungen die äußerst instruktive Stellungnahme *Bäckers* vor dem Innenausschuss des Deutschen Bundestages, *ders.*, A-Drs. 18(4)806 D, S. 6 ff.

rung, wenn Daten nunmehr der bundeskriminalamtlichen Zentralstellenfunktion unterfallen sollen. Anlässlich einer solchen Zweckänderung wäre prinzipiell erforderlich, dass die Voraussetzungen der hypothetische Datenneuerhebung, wie sie in § 12 BKAG zum Ausdruck kommen, gegeben sind. Die Datenverarbeitungsgeneralklausel des § 16 Abs. 1 BKAG scheint ihrem Wortsinn nach ebenfalls davon auszugehen, insofern dort die Rede davon ist, dass Subsidiarität nur insoweit eintritt, als „zusätzliche" Erfordernisse aufgestellt werden. Der Gesetzgeber spricht hingegen davon, dass „spezifische Weiterverarbeitungsbefugnisse" dem § 16 Abs. 1 „vorgehen"[1343] und legt damit eher eine totale Subsidiarität nahe. Zudem findet sich im Wortlaut der §§ 18, 19 BKAG keinerlei Verweis auf § 12 BKAG.

Die gesetzliche Systematik lässt damit zwei Auslegungsalternativen zu: Entweder findet der Grundsatz der hypothetischen Datenneuerhebung auch im Rahmen der §§ 18, 19 BKAG Anwendung, oder eben nicht. Während die Notwendigkeit zur Gesetzesauslegung prinzipiell kein Problem, sondern dem Recht vielmehr inhärent ist, ist die Situation im Rahmen der §§ 18, 19 BKAG problematisch, weil beide Auslegungsalternativen gänzlich unerwünschte Ergebnisse liefern.

In der ersten Auslegungsvariante – über den nur teilweise subsidiären § 16 Abs. 1 BKAG findet der in § 12 BKAG verkörperte Grundsatz der hypothetischen Datenneuerhebung im Rahmen der §§ 18, 19 BKAG Anwendung – wäre eine polizeipraktisch ungünstige Situation das Ergebnis. Die §§ 18, 19 BKAG dienen dem Bundeskriminalamt dazu, personenbezogene Daten für künftige Verfahren vorzuhalten. Die Befugnis dazu knüpft an die strafprozessuale Rolle einer Person oder an eine auf bestimmte Tatsachen gestützte Prognose einer zukünftigen Rolle der Person an. Die damit verbundenen Erwartungen sind hingegen rein personenbezogen und sehen keine situationsbezogene Schadensprognose im Einzelfall vor. Hingegen fordert die hypothetische Datenneuerhebung, dass ein „konkreter Ermittlungsansatz" vorliegt, wenn Daten zweckändernd weiterverarbeitet werden sollen.[1344] Dieses relativ neue verfassungsrechtliche Erfordernis ist vom Gesetzgeber insoweit konkretisiert worden, dass der Ermittlungsansatz zu bejahen ist wenn „sich eine Gefahr für mindestens vergleichbar bedeutsame Rechtsgüter, zu deren Schutz die ursprüngliche Datenerhebung vorgenommen wurde, nicht nur abstrakt, sondern vielmehr als eine in ersten Um-

1343 BT-Drs. 18/11163, S. 94.
1344 Siehe dazu bereits oben S. 168 f.

rissen absehbare und konkretisierte Möglichkeit eines Schadenseintrittes für ein solches Rechtsgut darstellt."[1345] Wäre dies nun im Rahmen von zweckändernden Datenverarbeitungen im Bereich der §§ 18, 19 BKAG zu beachten, wäre bei jeder Datenverarbeitungshandlung, also bereits bei der initialen Datenspeicherung, ein konkreter Ermittlungsansatz erforderlich. Ein solcher lässt sich jedoch nicht bereits aus einer gemäß §§ 18, 19 BKAG anzustellenden rein personenbezogenen Prognosen ableiten; gleiches gilt für den Umstand, dass jemand in der Vergangenheit verurteilt oder beschuldigt worden ist. Vielmehr bedürfte es einer darüberhinausgehenden Schadensprognose, um ein einzelnes Datum überhaupt erst zu speichern. Damit hätte der Gesetzgeber die Verarbeitungsbefugnisse des Bundeskriminalamtes gegenüber der vorherigen Rechtslage eingeschränkt. Die Intention, einen umfassenden Informationsbestand für noch nicht absehbare Lagen zu schaffen, würde konterkariert und die Aufgabe des Bundeskriminalamtes, als Zentralstelle im Informationsverbund zu fungieren, wäre erheblich beeinträchtigt, was die polizeiliche Informationsverarbeitung insgesamt empfindlich treffen würde.

Folgt man hingegen der zweiten Auslegungsalternative– § 16 Abs. 1 BKAG tritt gegenüber §§ 18, 19 BKAG vollständig subsidiär zurück – entstehen verfassungsrechtliche Probleme. Der Grundsatz der hypothetischen Datenneuerhebung gemäß § 12 BKAG käme im Rahmen der § 18, 19 BKAG nie zur Anwendung. Damit wären Datenverarbeitungen in diesem Bereich lediglich daran geknüpft, dass die personenbezogenen Eingriffstatbestände erfüllt sind, die letztlich nur Prognosen über zukünftiges Verhalten sind. Einmal auf diese Weise gespeicherte Daten könnten beliebig verarbeitet werden. Mit Blick auf die bundesverfassungsrechtliche Rechtsprechung zur Verarbeitung personenbezogener Daten ist dies widersprüchlich: Wenn schon für zweckändernde Verarbeitungen, die sich unmittelbar an die Erhebung anschließen, der Grundsatz der hypothetischen Datenneuerhebung gilt, muss dies erst recht gelten, wenn die Daten zwischenzeitlich im Informationsbestand vorgehalten worden sind. Ein solcher grenzenloser Umgang mit einmal gespeicherten Daten würde den Grundsatz der Zweckbindung für die in Frage stehenden Verarbeitungsformen mithin auch in rechtlicher Hinsicht abschaffen.

Eine dritte, sinnvollere Auslegungsvariante, etwa dass der Grundsatz der hypothetischen Datenneuerhebung nicht bei der Datenspeicherung nach

1345 BT-Drs. 18/11163, S. 91.

§§ 18, 19 BKAG, sondern erst bei der dann folgenden Verwertung Anwendung findet – ebenfalls ein Vorschlag *Bäckers* – lässt sich mit dem gegebenen Regelungen indessen nicht konstruieren, da in Anlehnung an den Begriff der Weiterverarbeitung von Daten, wie ihn die JI-Richtlinie kennt, unterschiedslos jeder Umgang von Daten von der insoweit indifferenten Terminologie des BKAG erfasst wird, mithin keine Trennung zwischen Speicherung und Verwertung möglich ist.[1346]

Insgesamt ist *Bäckers* Kritik an den zentralen Normen der neuen Informationsarchitektur des Bundeskriminalamtes zuzustimmen: Die Novellierung hat den Versuch unternommen, verfassungs- und unionsrechtliche Vorgaben möglichst sparsam und kompakt in das bisherige Gesetz einzupassen und hat damit eine für die vorgesehene Praxis der polizeilichen Datenverarbeitung unpassende normative Struktur geschaffen. Um den problematisch ausufernden Anwendungsbereich des § 16 Abs. 1 BKAG[1347] einzugrenzen, ist die inhaltliche Begrenzung des Begriffs der „weiteren Nutzung" dahingehend sinnvoll, dass nur Datennutzungen erfasst werden, die sich unmittelbar an das polizeiliche Verfahren anschließen, aus dem die Daten stammen. Werden die Daten über das Verfahren hinaus nicht mehr gebraucht, ist aus Verhältnismäßigkeitsgesichtspunkten eine Löschung vorzunehmen. Das bedeutet nicht, dass eine Speicherung ausgeschlossen wäre, aber sie sollte an andere Voraussetzungen geknüpft werden, als diejenigen, die für die weitere Nutzung ausschlaggebend sind. Auch Datenspeicherung und Datenverwertung scheinen kaum zusammengefasst unter dem Begriff der Weiterverarbeitung regelbar zu sein, wie die vorangegangenen Ausführungen zu §§ 18, 19 BKAG und ihr Verhältnis zu § 16 Abs. 1 in Verbindung mit § 12 BKAG gezeigt haben sollten. *Bäcker* schlägt hier eine Trennung der jeweiligen Phasen der Datenverarbeitung vor.[1348] Die Datenspeicherung ließe sich dementsprechend, wie es bereits zuvor angeklungen ist und auch der gegenwärtigen Rechtslage entspricht, auf die personenbezogene Prognose stützen. Die Datenverwertung hingegen bedürfte dann einer eigenen Verwertungsbefugnis, die bestimmte Anlässe festlegt oder allgemein auf den Grundsatz der hypothetischen Datenneuerhebung verweist. Dabei ist insgesamt zu beachten, dass Datenspeicherung und -verwertung miteinander in rechtlicher Wechselwirkung stehen: Je niedrigschwelliger der Speicherungsanlass, desto höher müssen die Voraussetzungen an die

1346 *Bäcker*, A-Drs. 18(4)806 D, S. 9 f.
1347 Siehe dazu bereits oben S. 320 ff.
1348 *Bäcker*, A-Drs. 18(4)806 D, S. 10.

sich anschließende Verwertung sein, und umgekehrt. Demnach müssen in unterschiedlichen Konstellationen diese beiden Formen des Datenumgangs in einer austarierten Weise aufeinander eingestellt werden. Die undifferenzierte Regelungsweise des BKAG schafft ein solches Austarieren, wie es für die verschiedenen Datenverarbeitungsbereiche des Bundeskriminalamtes notwendig wäre, nicht, sondern versucht die polizeiliche Datenverarbeitung in eine datenrechtliche Einheitsgröße zu zwängen. Das ist umso bedenklicher, als es nicht nur darum geht, eine bestehende Praxis rechtlich neu einzukleiden, sondern der Weg für einen neuen Modus der Informationsverarbeitung geebnet werden soll. Mit der Abschaffung der Dateien und der Errichtung eines einheitlichen Informationsbestandes, der „rechtlich primär durch den Grundsatz der hypothetischen Datenneuerhebung gesteuert werden" soll[1349] , wurde eine ambitionierte Zielvorstellung für das polizeiliche Informationswesen gesetzt. Die Umsetzung, so zeigen die vorstehenden Ausführungen, ist nicht nur technisch, sondern auch rechtlich so komplex, dass *Bäcker* zufolge eine „rechtlich tragfähige Fundierung" für die Neugliederung der Informationsordnung derzeit noch nicht in Sicht ist. Zwar wird die vage und vor allem fehlerbehaftete Normierung des Vorhabens vor diesem Hintergrund verständlich.[1350] Die Oberflächlichkeit und fehlende Stringenz der legislativen Befassung, die in den rechtlichen Mängeln der §§ 16, 18, 19 BKAG zum Ausdruck kommen, zeigen jedoch erneut den peripheren Stellenwert des Rechts im Rahmen der polizeilichen Informationsverarbeitung auf äußerst bedenkliche Weise.

c) Datenübermittlung im Rahmen des Informationsverbundes: Eingabe und Abruf

Der Informationsaustausch zwischen den deutschen Polizeien, der neben der Errichtung eines einheitlichen polizeilichen Datenbestandes die Hauptfunktion des Informationsverbundes ist, geschieht durch Eingabe und Abruf von Daten, wobei es sich rechtlich um Datenübermittlungen handelt.

1349 *Bäcker*, A-Drs. 18(4)806 D, S. 10.

1350 Ähnlich *Bäcker*, A-Drs. 18(4)806 D, S. 10, der eindringlich dazu riet, den die Informationsordnung betreffenden Teil des Gesetzesvorhabens zurückzustellen und eventuell auch die alte Dateienstruktur mit Blick auf die verfassungsrechtlichen Vorgaben normativ zu modernisieren. Der Gesetzgeber hat keine seiner Anmerkungen und Vorschläge aufgegriffen.

aa) Datenübermittlung an den polizeilichen Informationsverbund

Die Übermittlung der Daten an das Bundeskriminalamt zur Speicherung im Informationsverbund ist im Wesentlichen durch § 32 BKAG geregelt. Dessen Abs. 1 Satz 1 verpflichtet zunächst die einzelnen Landeskriminalämter, dem Bundeskriminalamt nach Maßgabe der Rechtsverordnung nach § 20 BKAG die zur Erfüllung seiner Aufgaben als Zentralstelle erforderlichen Informationen zu übermitteln. Die in der Vorschrift in Bezug genommene Rechtsverordnung ist die BKADV[1351], welche die Datenarten konkretisieren soll. Die Landeskriminalämter sind damit wesentlich für den polizeilichen Informationsaustausch mitverantwortlich.[1352] Neben den Landeskriminalämtern kann die Verpflichtung zur Datenübermittlung auch von anderen Polizeibehörden des Landes erfüllt werden, § 32 Abs. 1 Satz 2 BKAG. Gemäß § 32 Abs. 1 Satz 3 BKAG legt das Bundeskriminalamt zudem im Benehmen mit den Landeskriminalämtern Einzelheiten der Informationsübermittlung fest. Damit wird eine Koordination der Informationsübermittlung, insbesondere formal und inhaltlich, ermöglicht.[1353] Um Einzelheiten überhaupt zu festlegen zu können, ist zunächst eine Konkretisierung durch die BKADV als Grundlage erforderlich,[1354] von der es gegenwärtig keine auf die aktuelle Rechtslage angepasste Version gibt. Mit der Verpflichtung aus § 32 korrespondiert für die am polizeilichen Informationsverbund teilnehmenden Stellen nach § 29 Abs. 3 Satz 2 BKAG das Recht, Daten zur Erfüllung der Verpflichtung nach § 32 BKAG im automatisierten Verfahren einzugeben. Besondere Regelung für die Einrichtung von automatisierten Datenabrufen ist verfassungsrechtlich geboten, weil sich Verfahrensstruktur gegenüber herkömmlichen Übermittlungen unterscheidet, was für Betroffene zusätzliche informationelle Risiken birgt: Raum-zeitliche Schranken des Datenzugriffs bestehen nicht mehr, die Daten sind für potenzielle Datenempfänger jederzeit verfügbar. Zudem erfolgt beim Online-Zugriff regelmäßig keine Prüfung der Rechtmäßigkeit vor der jeweiligen Datenübermittlung durch die übermittelnde Stelle, sondern die empfangende Stelle entscheidet durch ihren Abruf, ob und wann es zu einer Übermittlung kommt.[1355]

1351 Siehe dazu bereits oben S. 227 ff.
1352 BT-Drs. 13/1550, S. 30.
1353 BT-Drs. 13/1550, S. 30.
1354 OVG Lüneburg NdsVBl. 2009, 135 Rn. 17.
1355 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, H. Rn. 467.

Einen weiteren zentralen Aspekt der Datenübermittlung regelt § 32 Abs. 2 BKAG. Während in dessen Satz 1 eine grundsätzliche und unverzügliche Mitteilungspflicht der Justiz- und Verwaltungsbehörden der Länder gegenüber dem jeweils zuständigen Landeskriminalamt bezüglich Unterbrechungen und Beendigungen von Freiheitsentziehungen statuiert, die durch ein Gericht wegen des Verdachts oder des Nachweises einer rechtswidrigen Tat angeordnet worden sind, ist es vor allem § 32 Abs. 2 Satz 2 BKAG, der in der polizeilichen Informationsarchitektur eine wichtige Funktion einnimmt: Danach teilen die Justizbehörden des Bundes und der Länder bei Mitteilungspflicht nach Abs. 1 dem jeweils zuständigen Landeskriminalamt unverzüglich und, soweit technisch möglich, automatisiert mit, ob die beschuldigte Person rechtskräftig freigesprochen wurde (Nr. 1 lit. a), die Eröffnung des Hauptverfahrens unanfechtbar abgelehnt wurde (Nr. 1 lit. b) oder das Verfahren nicht nur vorläufig eingestellt wurde (Nr. 1 lit. c). Nach § 32 Abs. 2 Satz 2 Nr. 2 BKAG sind zudem die tragenden Gründe der Entscheidung mitzuteilen. Dieser Zusatz im Rahmen der Mitteilungspflicht ist neu durch das BKAG von 2018 eingefügt worden und soll sicherstellen, dass die Polizeien des Bundes und der Länder in die Lage versetzt werden, Speicherungen in ihren Informationssystemen und im Informationsverbund nach Abschluss des justiziellen Verfahrens auf die Notwendigkeit der weiteren Speicherung hin zu überprüfen, die entsprechenden Löschungen vorzunehmen und hierdurch ungerechtfertigte Speicherungen, also Datenverarbeitungen Unschuldiger,[1356] zu vermeiden. Gegenwärtig ist das Meldeverhalten der Justizbehörden beschränkt und uneinheitlich, was die Überprüfung erschwert oder verhindert.[1357]

Neben den Landeskriminalämtern und -polizeibehörden sind gemäß § 32 Abs. 3 BKAG auch Bundespolizeibehörden dem Abs. 1 entsprechend verpflichtet, sofern die Informationen Vorgänge betreffen, die sie in eigener Zuständigkeit bearbeiten. Gleiches gilt für das Bundeskriminalamt und seine nach den §§ 3 bis 8 BKAG gewonnenen Informationen. Neben den direkt erlangten Informationen handelt es sich dabei um aus vorhandenen Daten neu abgeleitete Informationen, wobei nicht erforderlich ist, dass es sich um ein Produkt automatisierter Datenverarbeitung handelt.[1358]

1356 *Barczak* in *Barczak* (Hrsg.), BKAG, § 32 Rn. 14.
1357 BT-Drs. 18/11163, S. 110.
1358 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 32 BKAG Rn. 16.

bb) Datenübermittlungen aus dem Informationsverbund

Datenübermittlungen aus dem Informationsverbund heraus erfolgen regelmäßig[1359] in Form des (automatisierten) Abrufs, zu dem teilnehmenden Stellen nach § 29 Abs. 3 Satz 2 BKAG berechtigt sind, soweit dies zur jeweiligen Aufgabenerfüllung erforderlich ist. Dies bezieht sich auf die generelle Aufgabenzuweisung eines INPOL-Teilnehmers. Da die Dateistruktur zunächst weiter Bestand hat, wird bisher noch durch Errichtungsanordnungen festgelegt, welcher Teilnehmer in welchem Umfang Daten eingeben und abrufen darf.[1360] In Zukunft wird dies weniger trennscharf durch das Kriterium der Verbundrelevanz gesteuert werden.[1361] Zentral für eine verfassungsgemäße Ausgestaltung ist die Beachtung der in § 29 Abs. 4 Satz 2 BKAG erwähnten Regulative wie der Grundsatz der hypothetischen Datenneuerhebung (§ 12 Abs. 2–5 BKAG), die dafür nötigen Kennzeichnungspflichten (§ 14 BKAG), die Bindung an die Erforderlichkeit der Kenntnis der Daten für mehr oder weniger konkretisierte Aufgaben und Pflichten (beispielsweise § 15 Abs. 1 Nr. 2 BKAG) sowie sachlich oder personell mehr oder weniger differenzierte Schwellen für die Datenverarbeitung (§§ 16, 18 und 19 BKAG), deren Einhaltung das Bundeskriminalamt organisatorisch und technisch sicherzustellen hat.[1362]

Neben diesen Übermittlungen aus dem Verbund kann auch das Bundeskriminalamt, das vom Verbund getrennte Datenbestände unterhält, an andere Polizeien Daten übermitteln. Neben der grundsätzlichen Übermittlungsbefugnis in § 25 Abs. 1 BKAG enthält § 25 Abs. 7 zudem ebenfalls die Möglichkeit, ein automatisiertes Abrufverfahren für die Datenbestände in eigenen Informationssystemen, also insbesondere Zentraldateien, einzurichten. Der Kreis der abrufberechtigten Behörden ist beschränkt auf die Behörden, die vollzugspolizeiliche Aufgaben wahrnehmen.[1363]

Normen, die den Datenaustausch zwischen Polizeibehörden unterschiedlicher Bundesländer bzw. den beiden föderalen Ebenen ermöglichen,

1359 Es wird für INPOL-Teilnehmer grundsätzlich angenommen, dass sie aufgrund der Vielzahl der Datenübermittlungen und der Eilbedürftigkeit regelmäßig die Berechtigung zum Abruf im automatisierten Verfahren haben, BT-Drs. 13/1550 S. 28.

1360 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 29 BKAG Rn. 23.

1361 Siehe dazu bereits oben S. 232 ff.

1362 *Barczak* in *Barczak* (Hrsg.), BKAG, § 29 Rn. 22.

1363 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 37.

also die andere „Tür" in der Doppeltür-Dogmatik darstellen,[1364] finden sich in allen Polizeigesetzen.[1365] Der Datenaustausch zwischen diesen unterschiedlichen Polizeien ist dabei indes nicht so unproblematisch, wie man es angesichts der scheinbar übereinstimmenden Zwecke der Behörden annehmen könnte: Bundesebene, insbesondere das Bundeskriminalamt, und Landesebene haben unterschiedliche Aufgaben und auch unter den Bundesländern ist die Reichweite der polizeilichen Aufgabenkreise mitunter nicht identisch.[1366] Zudem ist seit dem BKAG-Urteil des Bundesverfassungsgerichts jede Übermittlung von Daten aus eingriffsintensiven Erhebungsmaßnahmen an andere Sicherheitsbehörden regelmäßig als Zweckänderung anzusehen.[1367] Sollen solche Daten zu einem anderen Zweck verarbeitet werden, so muss dies zumindest dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich eine Neuerhebung mit vergleichbar schwerwiegenden Mitteln gerechtfertigt hätte.[1368] Auch unionsrechtlich verlangt der Übermittlungsvorgang mit Blick auf Art. 4 Abs. 2 JI-Richtlinie die Beachtung besonderer Anforderungen.

Insoweit ist – auch wenn sie prinzipiell den Logiken und Dynamiken des Massendatenparadigmas entspricht – die Einrichtung von automatisierten Abrufverfahren, wie es die Regel im polizeilichen Informationswesen ist, stets auch kritisch zu hinterfragen. Polizeiliche Interessen an einem solchen ubiquitären Zugriff auf die verschiedenen Datenbestände können nur dann die Betroffeneninteressen überwiegen, wenn gewichtige Vorteile durch die Automatisierung bestehen, etwa weil besonders schnell oder besonders große Mengen Daten benötigt werden.[1369] Zudem müssen in entsprechender Anwendung des § 81 Abs. 2 BKAG der Zeitpunkt, die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Zugriff verantwortliche Stelle vom Bundeskriminalamt protokolliert werden.[1370] Im Zusammenhang mit automatisierten Abrufsystemen ist eine Protokollierung seitens der übermittelnden Stelle geboten, die Verarbeitungskategorie, Anlass, Inhalt, Empfänger und Datum der Übermittlung

1364 Siehe dazu bereits oben S. 170 ff.
1365 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 950.
1366 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 951.
1367 BVerfGE 141, 220, 336 f. – Bundeskriminalamtgesetz.
1368 BVerfGE 141, 220, 328 – Bundeskriminalamtgesetz.
1369 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 42.
1370 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht § 25 BKAG Rn. 43.

erfasst.[1371] Zudem ist aufseiten der empfangenden Stelle eine Vollprotokollierung geboten, da die zugreifende Stelle voll verantwortlich für die Rechtmäßigkeit des Datenabrufs ist.[1372] Nur eine solch umfassende Protokollierung, die auch den zugreifenden Rechner erfassen sollte,[1373] ermöglicht eine nachträgliche Feststellung möglicher Rechtsverstöße, etwa in Form von Abrufen durch Polizeibedienstete ohne entsprechende dienstliche Berechtigung, wobei es sich um eine Straftat handeln kann.[1374]

2. Polizeiliche Datenverarbeitung in den polizeibehördeneigenen Informationssystemen

Neben der Datenverarbeitung im Informationsverbund findet ein weiterer großer Teil des Informationsumgangs in den polizeibehördeneigenen Informationssystemen statt. Dabei lässt sich zunächst – wie bei Datenerhebungen – zwischen strafverfahrensrechtlicher und polizeirechtlicher Datenverarbeitung unterscheiden. Dementsprechend können für alle Polizeibehörden – je nach konkreter Aufgabengestaltung einzelner Organisationsteile – sowohl das jeweilige Polizeigesetz als auch die Strafprozessordnung bei ihrer informationellen Arbeit zu beachten sein. Insofern besteht eine gewisse Parallelität zwischen den Gesetzesmaterien, wobei dennoch auch weiter Diskrepanzen zwischen den einzelnen Rechtsordnungen existieren, sowohl im Verhältnis zwischen repressiver Strafprozessordnung und den präventiven Polizeirechtsordnungen als auch im Verhältnis der Polizeirechtsordnungen untereinander. In der Folge beschränken sich die Ausführungen auf die grundsätzlichen Strukturen der behördeneigenen Datenverarbeitung im polizeilichen Informationswesen.[1375]

Einmal in den behördenspezifischen Bereich des polizeilichen Informationswesens gelangt – im Wege der Datenerhebung oder Übermittlung durch staatliche oder auch nicht-staatliche Stellen – bedarf es spezifischer Rechtgrundlagen, um den daran anschließenden Umgang mit Daten zu erlauben. Dafür ist nunmehr das unionsrechtliche Konzept der Weiterverarbeitung

1371 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 883.
1372 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 47.
1373 *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 25 BKAG Rn. 47.
1374 Siehe dazu etwa *Golla* Legal Tribune Online v. 16.08.2019.
1375 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 577.

maßgeblich. Wenn einige Polizeigesetze noch mit der alten Terminologie von Datenspeicherung, Datenveränderung, Datenberichtigung, Datennutzung und so weiter operieren, so sind darin Teilaspekte des weiten Weiterverarbeitungsbegriffes zu sehen. Mit diesem Begriff sollen dann, wie Art. 3 JI-Richtlinie und die nationalen Umsetzungsnormen zeigen, zunächst einmal alle denkbaren Datenverarbeitungsprozessschritte erfasst sein.[1376] Da sich für bestimmte Datenumgänge spezielle verfassungsrechtliche Anforderungen ergeben, sind diese durch die jeweiligen Gesetzgeber im Bundes- oder Landesrecht spezifisch zu regeln. Dazu gehören die Datenübermittlung, der Datenabgleich und neuere Formen der Datenanalyse.[1377] Zudem sind Datenumgänge, die den mit der Informationsverarbeitung verbundenen Grundrechtseingriff abschwächen oder aufheben, sowie die Einschränkung der Verarbeitung oder die Löschung separat geregelt.

a) Datenverarbeitungsgeneralklausel

Zentral für den Datenumgang nach Datenerhebung durch oder -übermittlung an die Polizeien sind Datenverarbeitungsgeneralklauseln, die wahlweise mit den alten, aufgegliederten Begrifflichkeiten oder der neuen Weiterverarbeitungsterminologie arbeiten. Entsprechende Vorschriften finden sich sowohl in den Polizeirechtsordnungen als auch in der Strafprozessordnung.

Im Polizeirecht[1378] wird die generelle Befugnis zur Datenverarbeitung regelmäßig an die Erforderlichkeit der Verarbeitung zur Aufgabenerfüllung, den Zweckbindungsgrundsatz sowie die Rechtmäßigkeit der Erhebung geknüpft. Während es sich beim Rechtmäßigkeitserfordernis noch um die beharrlichste Verarbeitungsschranke handelt, findet eine Begrenzung des Datenumgangs durch Erforderlichkeit und Zweckbindung nur oberflächlich statt. Der Erforderlichkeitsgrundsatz stellt im Rahmen der Generalklauseln zunächst sicher, dass Daten nicht anlasslos und zeitlich unbegrenzt gespeichert oder sonst wie verarbeitet werden können. Im konkreten Da-

1376 Siehe zu den einzelnen Bedeutungen der Unterbegriffe *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 594.

1377 Siehe dazu bereits oben S. 281 ff.

1378 Vgl. § 16 BKAG; § 29 BPolG; § 15 BWPolG; Art. 53 BayPAG; § 42 ASOG Bln; § 39. BbgPolG; § 36a BremPolG; § 36 HmbPolDVG; § 20 HSOG; § 36 SOG M-V; § 38 NPOG; § 23 PolG NRW; § 52 RP POG, § 21 SPolDVG; § 22 SOG LSA; § 80 SächsVDG; § 188 SchlHLVwG; § 40 TPAG.

tenumgang bedeutet Erforderlichkeit hingegen keine hohe Hürde, sondern verlangt zunächst nur, dass ein Bedarf an der Verarbeitung bestimmter Daten zur Erfüllung der Aufgaben besteht. Die Breite der Aufgaben macht aber eine weitere Limitierung durch den Zweckbindungsgrundsatz erforderlich. Auch dieser ist einfachgesetzlich durchweg in den Polizeigesetzen normiert, dasselbe gilt aber auch für seine Durchbrechung in Form von Zweckänderungen oder von Ausnahmen vom Zweckbindungsgrundsatz.

Die wichtigste Ausnahme dürfte mittlerweile die sogenannte zweckwahrende Weiternutzung sein, die eine weitere Nutzung von Daten im Rahmen derselben Aufgabe und zum Schutz vergleichbarer Rechtsgüter ohne weitere Anforderungen an den Eingriffsanlass gestattet. Die darin liegende schlichte Übernahme der verfassungsrechtlichen Vorgaben ist jedoch aus verschiedenen Gründen problematisch. So ist etwa nicht klar, wie weit eine weitere Nutzung reichen soll. Während Anschlussverfahren gefahrenabwehr- oder strafverfahrensrechtlicher Art dem wohl unterfallen, wäre eine längerfristige Bevorratung im Rahmen einer Aufgabe nicht auf die die Datenverarbeitungsgeneralklausel zu stützen, sondern bedarf spezifische Regelungen, die dem Eingriffsgewicht von Datenbevorratung Rechnung tragen.[1379] Diese Situation kann durch sehr weite Aufgabenbeschreibungen verschärft werden. So haben etwa Bundeskriminalamt und Bundespolizei vergleichsweise enge Aufgabenbeschreibungen, die allerdings durch gesetzgeberische Interpretation aufgeweicht werden können. So will der Gesetzgeber bei der Novellierung des BPolG unter den Aufgaben der Bundespolizei die Gefahrenabwehr und die Strafverfolgung verstanden wissen und nicht die Einzelaufgaben der Bundespolizei, wie beispielsweise Grenzschutz, Sicherheit von bestimmten Verkehrsanlagen usw.[1380] Auf diese Weise interpretiert franst die ohnehin schon durch die Figur der zweckwahrenden Weiternutzung aufgeweichte Zweckbindung im polizeilichen Datenumgang weiter aus.[1381] Ein solch weites Verständnis der Aufgabenbereiche ist jedoch sogar explizit gesetzlich verankert, wenn die zweckwahrende Weiternutzung als grundsätzliches Prinzip der Verarbeitung in allgemeine

1379 *Bäcker*, A-Drs. 18(4)806 D, S. 3 ff.

1380 *Bundesministeriums des Innern und für Heimat*, Gesetzesentwurf zur Neustrukturierung des Bundespolizeigesetzes und Änderung anderer Gesetze (Referentenentwurf), S. 125, abrufbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/B1/ref-neustrukturierung-bundespolizeigesetz.pdf?__blob=publicationFile&v=5 (Stand: 01.10.2023).

1381 Kritisch und instruktiv dazu bereits *Arzt*, A-Drs. 19(4)772 B, S. 15 f.

Polizeirechtsordnung aufgenommen wird.[1382] Denn hier ist der Verweis auf die Aufgaben dann tatsächlich im Sinne des maximal weiten Verständnisses von präventiver und repressiver polizeilichem Tätigwerden samt den jeweiligen Vorfeldaufgaben zu lesen. Damit wirkt dann lediglich das Erfordernis der Rechtsgutsidentität, wie es die zweite Voraussetzung der zweckwahrenden Weiternutzung ist, einschränkend.[1383] Insofern ist unterhalb der Zweckänderungsschwelle ein Freiraum für Datenverarbeitungen geschaffen worden, von dem zwar fraglich ist, wie er konkret polizeipraktisch genutzt werden wird. Eine Steuerung des polizeilichen Datenumgangs wird er jedoch nicht mit sich bringen.

Das ist umso bedenklicher, als dass auch die im Rahmen der Zweckänderung zu beachtenden Erfordernisse nur sehr eingeschränkt die ihnen zugedachte Einhegung der polizeilichen Datenverarbeitung bewirken können. Denn die Zweckänderung wird in allen Polizeigesetzen nach dem Grundsatz der hypothetischen Datenneuerhebung gestattet, sodass die Polizeien präventiv erlangte Daten zu anderen Gefahrenabwehrzwecken nutzen können, soweit sie diese Daten auch zu diesen Zwecken hätten erheben können. Hinzukommt, dass auch strafverfahrensrechtlich erlangte Daten regelmäßig zweckändernd für präventiv-polizeiliche Zwecke umgewidmet werden können, was § 481 Abs. 1 StPO von bundesrechtlicher Seite aus möglich macht. Auch umgekehrt können gem. § 161 Abs. 3 StPO Daten ins Strafverfahren überführt werden. Eine etwas höhere Hürde besteht lediglich bei eingriffsintensiven Maßnahmen, wo neben Rechtsgutsidentität zwischen altem und neuem Zweck nunmehr auch ein konkreter Ermittlungsanlass erforderlich ist.[1384] Zwar sind diese Öffnungsvorschriften zur Vornahme von zweckändernden Datenverarbeitungen größtenteils keinen erheblichen rechtstechnischen Einwänden ausgesetzt, aber die recht breite einfachgesetzliche Freigabe der zweckändernden Datenverarbeitung lässt von der Zweckbindung, die als Prinzip einen Regelcharakter haben sollte, schon einfachgesetzlich wenig übrig. Es ist deshalb durchaus treffend, wenn *Petri* anlässlich dieser Regelungslage urteilt, der Zweckbindungsgrundsatz werde gesetzlich lediglich „vorgetäuscht".[1385]

1382 Siehe etwa § 20 HSOG.
1383 Siehe dazu *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 12 BKAG Rn. 10.
1384 Siehe dazu bereits S. 168 ff.
1385 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 855.

Neben diesen strukturellen Problemen der polizeirechtlichen Datenverarbeitungsgeneralklauseln zeichnet sich zudem die problematische Entwicklung zumindest für manche Polizeigesetze ab, unreflektiert die unionsrechtliche Terminologie der Weiterverarbeitung zu übernehmen. Die schlichte Übernahme einer Begriffsbestimmung in eine Rechtsgrundlage ist jedoch – worauf *Arzt* richtigerweise hingewiesen hat – mit den verfassungsrechtlichen Vorgaben von Normenbestimmtheit und -klarheit nicht vereinbar, da durch die Verwendung der Weiterverarbeitungsterminologie nicht klar ist, welche Datenverarbeitungsschritte genau zulässig sind.[1386]

Auch für den kriminalpolizeilichen Datenumgang finden sich generalklauselartige Datenverarbeitungsvorschriften in den §§ 161 Abs. 3 und 4 sowie 483 StPO. Während § 483 StPO mit seiner Formulierung, auch für den strafprozessualen Teil der polizeilichen Datenverarbeitung, die Grundsätze der Erforderlichkeit und Zweckbindung aufstellt, findet sich in § 161 Abs. 3 und 4 StPO der Grundsatz der hypothetischen Datenneuerhebung, wenn auch nicht in der expliziten Form wie zunehmend im Polizeirecht. Die grundsätzliche Bindung der repressiv erlangten Daten ans Strafverfahren wird indessen durch § 481 StPO und daran anknüpfende polizeirechtliche Regelungen stark relativiert. Zudem verlangt der Grundsatz der hypothetischen Datenneuerhebung bei der zweckändernden Weiterverarbeitung nicht die Erfüllung der ursprünglichen, bei der Datenerhebung zu erfüllenden prozeduralen Sicherungen, wie beispielsweise einen Richter:innenvorbehalt, sodass eine externe Kontrolle insofern nicht erfolgt. Um dies zu kompensieren, wird eine strenge Erforderlichkeitsprüfung für die Weiterverarbeitung – auch für die Nutzung als sogenannter Spurenansatz – verlangt, um die Verhältnismäßigkeit im Einzelfall zu wahren.[1387] Damit bleibt es allerdings bei einer polizeilichen Definition von Erforderlichkeitsschwellen. Eine nähere Überprüfung wäre zwar über die Protokollierungen von Verarbeitungsschritten, wie etwa Datenabfragen, möglich, hängt aber in ihrer Effektivität stark vom generellen Stand insbesondere der innerbehördlichen Datenschutzkontrolle ab. Ob zudem auch rechtswidrig erlangte Daten strafprozessual (nach einer entsprechenden Verhältnismäßigkeitsprüfung) weiterverarbeitet werden können, ist nach wie vor umstritten.[1388]

1386 *Arzt*, A-Drs. 19(4)772 B, S. 14 f.

1387 Siehe dazu mwN *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 828.

1388 Die Möglichkeit zur Verwendung zumindest bejahend als gegenwärtige Rechtslage beschreibend *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.),

Damit ergibt sich für den generellen Datenumgang rund um die vollzugspolizeilichen Vorgangsbearbeitungssysteme und die kriminalpolizeilichen Fallbearbeitungssysteme ein Bild wenig beschränkter Datenverarbeitungsmöglichkeiten. Ausnahmen betreffen vor allem Daten aus eingriffsintensiven Maßnahmen, die tief in die Privatsphäre von Betroffenen eingreifen. Darüber hinaus ist – der hierarchischen und spezialisierten Struktur der Polizei entsprechend – der Datenzugang nicht für alle Polizeibediensteten derselbe. Der Streifenpolizist hat weniger Zugriff und damit auch weniger Datenverarbeitungsmöglichkeiten als die Staatsschützerin. Im Rahmen der Verfügbarkeiten erlauben die gegenwärtigen Vorschriften aber einen grundsätzlich flexiblen Datenumgang, wie es zwar auch in Grundzügen für eine „moderne" Polizei in einer sich selbst zunehmend datafizierenden Gesellschaft sinnvoll erscheint, was jedoch an den beschriebenen verfassungsrechtlichen und rechtsstaatlichen Defiziten des polizeilichen Informationswesens nichts ändert.

b) Datenverarbeitung zum Zweck der Bevorratung strafprozessualer Daten

Ein im vorliegenden Kontext ebenfalls noch relevante Form des Datenumgangs ist die Bevorratung von strafverfahrensrechtlich erlangten Daten zu präventiv-polizeilichen Zwecken, also zur Bevorratung – insbesondere zur vorbeugenden Straftatenbekämpfung – wie sie bereits in den Ausführungen zum KAN als strukturellem Bestandteil des polizeilichen Informationswesens zur Sprache gekommen ist.[1389] Die Möglichkeit hierzu wird über den soeben bereits erwähnten § 481 Abs. 1 S. 1 StPO eröffnet, die von allen Polizeirechtsordnungen durch eine entsprechend spiegelnde Vorschrift genutzt wird. Datenverarbeitungen zur vorbeugenden Bekämpfung von Straftaten setzen voraus, dass wegen der Art, Ausführung oder Schwere der Tat und der Persönlichkeit des Betroffenen die Besorgnis der Begehung weiterer Straftaten besteht. Sie beziehen sich also auf Wiederholungstäter:innen. Neben dieser spezifischen Ausprägung des Verhältnismäßigkeitsgrundsatzes verbietet dieser zudem, die erstmalige Begehung von Bagatelldelikten zum Anlass für eine Bevorratung zu nehmen. Ferner ist bei jeder Speicherung

Handbuch des Polizeirechts, G. Rn. 830; explizit dagegen etwa *Singelnstein* in *Knauer/Hartmut Schneider* (Hrsg.), Münchener Kommentar zur Strafprozessordnung Bd. 3: §§ 333-500 StPO, § 483 Rn. 7.

1389 Siehe dazu bereits oben S. 240 ff.

zu prüfen, ob diese mit Blick auf das Ziel der Strafverfolgungsverhütung überhaupt im Einzelfall zweckmäßig ist.[1390] Auch hier ist den speichernden Beamt:innen ein nicht unerheblicher Ermessensspielraum zugeteilt. Selbst bei Freispruch oder Einstellung des Ermittlungsverfahrens nach § 170 Abs. 2 StPO können Daten im Rahmen der Bevorratung ausnahmsweise weiterverarbeitet werden, wenn es Verdachtsmomente und eine Wiederholungsgefahr gibt,[1391] wobei dies konkret geprüft und dargelegt werden muss.[1392] In diesen Kontext fällt auch das Problem der Mitteilung vonseiten der Staatsanwaltschaften an die Polizeibehörden.[1393] Eine vergleichbare Abwägungssituation besteht auch im Rahmen der Einstellung nach § 153 oder § 153a StPO, wo die Geringfügigkeit der Schuld eine Speicherung trotz bestehenden Restverdachts nicht ohne Weiteres erlauben kann. Während bei Ersttäter:innen im Falle von Bagatellkriminalität auch hier meistens eine Bevorratung nicht angemessen sein wird, kann es etwa anders aussehen, wenn eine Person bereits einige Male nachweislich straffällig geworden ist und die Daten aus dem einzustellenden Verfahren „das Gefährderprofil des Beschuldigten" abrunden können.[1394] Auch hier lassen sich wieder einige Unschärfen in den Beurteilungsmöglichkeiten erkennen, die zumindest in der Vergangenheit zu einer extensiven Anwendung der Bevorratungsermächtigungen geführt haben.[1395] Um die Ermessensausübung pragmatisch zu vereinfachen verzichten einige Polizeigesetze auf entsprechende Beurteilungsspielräume wie die Wiederholungsgefahr und setzen Speicherhöchstfristen ein, innerhalb derer sich wohl klären soll, ob es sich um Täter:innen handelt, die erneut straffällig werden.[1396] Damit wird zwar eine

1390 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 840.

1391 BVerfG, 16.05.2002 - 1 BvR 2257/01 = NJW 2002, 3231.

1392 VGH Hessen, 01.02.2017 - 8 A 2105/14.Z = NVwZ 2017, 982.

1393 Siehe dazu bereits oben S. 243 f.

1394 *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 877.

1395 So berichtet es etwa *Petri* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch, G. Rn. 880; s. auch BayLfD 24. Tätigkeitsbericht, 2010, 3.5.3.

1396 Sieh etwa § 75 Abs. 3 BWPolG wonach eine „Speicherung personenbezogener Daten bis zu einer Dauer von zwei Jahren [erforderlich ist], wenn aufgrund tatsächlicher Anhaltspunkte der Verdacht besteht, dass die betroffene Person eine Straftat begangen hat", es sei denn es die betroffene Person im Strafverfahren rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen sie unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wurde und sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Straftaten nicht oder nicht rechtswidrig begangen hat. Ähnlich ermöglicht § 37 Abs. 2 S. 1 SOG M-V, dass eine Speicherung zunächst für drei Jahre erfolgen darf, wenn

etwas unsichere Verwaltungspraxis vereinheitlicht, gleichzeitig bewirken solche Bevorratungsvorgaben aber selbstverständlich eine Ausweitung der gespeicherten Personen und Daten, da hierdurch die Möglichkeit, trotz Strafverfahrens nicht zu speichern, quasi aufgehoben wird.

c) Datenübermittlung

Aufgrund der föderalen und auch sonst nochmals zergliederten Struktur der deutschen Polizeien ist das polizeiliche Informationswesen für seine Funktionsfähigkeit in einem hohen Maße auf Datenübermittlungen[1397] angewiesen. Grundsätzlich müssen Übermittlungsrechtsgrundlagen – wie alle Datenverarbeitungsschritte – dem Grundsatz der Zweckbindung Rechnung tragen, auch ansonsten die Verhältnismäßigkeit wahren und besonders sensible Daten schützen. Obwohl in der Übertragung bereits eine Zweckänderung liegt,[1398] erfordert der Zweckbindungsgrundsatz, dass die empfangende Stelle an den ursprünglichen Zweck gebunden ist. Hiervon machen die Polizeigesetze allerdings, wie im Rahmen der generalklauselartigen Datenverarbeitungsermächtigungen, weitreichende Ausnahmen, sodass die empfangende Stelle die erhaltenen Daten regelmäßig zweckändernd weiterverarbeiten kann, soweit diese Daten auch zu diesem Zweck hätten übermittelt werden dürfen. Mit dieser „hypothetischen Datenneuerhebung" soll ein erneuter Übermittlungsvorgang an die Stelle, die die Daten ohnehin bereits besitzt, überflüssig gemacht werden.[1399] Übermittlungsvorschriften zwischen den Polizeibehörden und zwischen der Strafjustiz und den Polizeien ermöglichen dementsprechend einen flexiblen Datenaustausch zu präventiv-polizeilichen und repressiv-polizeilichen Zwecken sowie zwischen beiden Zweckdomänen.[1400]

---

zum Speicherungszeitpunkt der Verfahrensausgang nicht bekannt ist. Auch in diese Richtung erlaubt § 20 Abs. 6 S. 2 HSOG bei Tatverdächtigen die Speicherung solange, wie der Tatverdacht nicht ausgeräumt worden ist, was – mit Blick auf Einstellungen etwa nach §§ 153, 153a aber auch § 170 Abs. 2 StPO regelmäßig zur Bevorratung von Daten führen kann.

1397 Siehe zu den verfassungsrechtlichen Anforderungen bereits oben S. 170 f. ff. sowie zum Begriff S. 205 ff.

1398 BVerfGE 141, 220 (341) – BKAG-Urteil.

1399 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 871.

1400 § 482 Abs. 1 S. 2 StPO; § 25 Abs. 1 BKAG, § 32 Abs. 1 BPolG; Länder: § 59 BW PolG; Art. 56 Abs. 1 Nr. 1 BayPAG; § 44 Abs. 1 ASOG; § 42 Abs. 1 BbgPolG; § 36c ff.

Ein Großteil der für die polizeiliche Informationsarbeit erforderlichen Datenübermittlungen erfolgt dabei wie bereits dargelegt innerhalb des Informationsverbundes nach § 29 BKAG im automatisierten Abrufverfahren. Dabei ist eine Überprüfung und Steuerung der Datenverwendung durch die übermittelnde Stelle nicht möglich.[1401] Der Bedeutung dieser Form der Teilnahme entsprechend finden sich entsprechende Rechtsgrundlagen sowohl in der Strafprozessordnung als auch in allen Polizeigesetzen des Bundes und der Länder.[1402] Aufgrund der fehlenden rechtlichen Prüfung, die bei einer „händischen" Übermittlung zumindest ansatzweise noch von der übermittelnden Stelle zu leisten wäre, ist die Rechtmäßigkeit zunächst maßgeblich vom Abrufverhalten abhängig, das in der Vergangenheit durch Missachtung der Abrufrahmenbedingungen aufgefallen ist.[1403] Da indessen eher zu erwarten ist, dass automatisierte Abrufverfahren noch größere Bedeutung für die Polizeien im Angesicht des Massendatenphänomens erlangen werden, muss vor allem eine lückenlose Protokollierung der massenhaften Eingaben und Abrufe erfolgen wie etwa in § 81 BKAG für den Informationsverbund vorgeschrieben ist. Sodann kann über das interne Datenschutzkontrollregime und gegebenenfalls die Aufsichtsbehörden eine Identifizierung und Korrektur von unrechtmäßigen Datenübermittlungen erfolgen.

d) Datenabgleich

Zunehmende Bedeutung in einem immer weiter digitalisierten Informationswesen gewinnt zudem das Instrument des Datenabgleichs, der in al-

---

BremPolG; § 40 HmbPolDVG; § 22 Abs. 1 HSOG; § 39b Abs. 1 SOG M-V; § 41 NPOG; § 27 Abs. 1 PolG NRW; § 57 Abs. 1 RH POG; § 84 SächsPVDG; § 27 Abs. 1 SOG LSA; § 192 Abs. 1 SH LVwG; § 41 Abs. 1 TPAG.

1401 Siehe dazu bereits oben S. 341 f.

1402 § 488 StPO; § 29 BKAG; § 33 Abs. 7 und 8 BPolG; § 22 AZRG; §§ 30a, 30b StVG; Länder: § 59 Abs. 5 BWPolG; Art. 63 BayPAG; § 46 ASOG Bln; § 49 BbgPolG; § 36c BremPolG; § 62 HmbPolDVG; § 24 HSOG; § 42 SOG M-V; § 42 NPOG; § 70 Abs. 2 DSG NRW iVm § 6 Abs. 1 DSG NRW; § 64 RH POG; § 46 SPolDVG; § 7 DSG LSA, § 85 SächsPVDG; § 194 SH LVwG; § 42 ThürPAG.

1403 *92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf - Konsequenzen für polizeiliche Datenverarbeitung notwendig, 2016.

len einschlägigen Rechtsordnungen eine Rechtsgrundlage findet.[1404] Beim Datenabgleich werden die der Polizei bekannt gewordenen Daten einer Person – etwa im Rahmen einer polizeilichen Kontrolle – verwendet, um zu überprüfen, ob in den polizeiinternen Datenbeständen bereits (weitere) Daten zu ihr vorliegen. Abzugrenzen ist die Maßnahme insofern von der Rasterfahndung, die polizeiexterne Datenbestände zum Abgleich heranzieht. Der Datenabgleich gilt häufig als wenig intensives informationelles Instrument.[1405] Dem ist zu widersprechen. Der Datenabgleich gestattet – je nach Ausgestaltung – die Nutzbarmachung eines nicht unerheblichen Teils der polizeilichen Datenbestände im konkreten Bürger:innenkontakt und mobilisiert gerade durch die Überprüfung, ob oder was an Daten bereits zu einer Person vorhanden ist, einen wesentlichen Aspekt der informationellen Macht polizeilicher Datenbestände. Zwar werden strenggenommen keine neuen Daten erhoben, aber für die Polizeibediensteten in der konkreten Situation ist der Datenabgleich ein Erkenntnisinstrument, das anderswo vorhandene Daten für die aktuelle lebensweltliche Situation verfügbar macht und zu ihrer informationellen Neubewertung mit potenziell nachteiligen Folgen in Form von Folgemaßnahmen für Betroffene führen kann.[1406] Dabei ist die Datengrundlage, insbesondere im Bereich von insoweit besonders problematischen Dateien, wie den Gewalttäterdateien, häufig nicht verlässlich.[1407] Zudem ist die handlungsleitende Verwendung von eventuell im Informationswesen vorhandenen, auf Datenverknüpfungen beruhenden Datendoubles gerade konträr zur Prinzip der informationellen Selbstbestimmung im zwischenmenschlichen Kontakt.[1408]

1404 § 98c StPO; § 16 Abs. 4 BKAG; § 34 Abs. 1 BPolG; Länder: § 47 BWPolG; Art. 61 BayPAG; § 28 ASOG; § 40 BbgPolG; § 36h BremPolG; § 48 HmbPolDVG; § 25 HSOG; § 43 SOG M-V; § 45 Abs. 1 NPOG; § 25 PolG NRW; § 65 RH POG; § 28 SPolDVG; § 30 SOG LSA; § 87 SächsPVDG; § 195 SH LVwG; § 43 TPAG.

1405 So etwa Schmidbauer in *W. Schmidbauer/Steiner,* Polizeiaufgabengesetz, Polizeiorganisationsgesetz, Art. 61 PAG Rn. 1; auch *Aulehner* in *Möstl/Schwabenbauer* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Sicherheitsrecht Bayern, Art. 61 PAG Rn. 1; ebenso *Graulich* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 16 BKAG Rn. 36.

1406 Zu dieser Dynamik etwa im Kontext von Gewalttäterdateien siehe etwa *Ruch/Feltes* NK 17 (2016), 62 (77 f.).

1407 *Ruch/Feltes* NK 17 (2016), 62 (76 f.).

1408 So auch *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 933; *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 25 Rn. 6; *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 3a.

Die Ausgestaltung des Datenabgleichs ist in der Regel dreigeteilt: Möglich sind Fahndungsabfragen, der Datenabgleich bei Störer:innen und der Datenabgleich bei anderen Personen. Zumindest der Fahndungsabgleich ist nicht auf die Datenbestände der jeweiligen Polizeiorganisation (also etwa: Polizei eines bestimmten Landes) beschränkt, sondern gleicht mindestens Personen- und Sachfahndungsdateien,[1409] also Verbunddateien, ab. Der Fahndungsbegriff ist dabei nicht legaldefiniert, sondern wird im Wesentlichen nach Polizeidienstvorschrift bestimmt, wonach es sich um die „planmäßige, allgemeine oder gezielte Suche nach Personen oder Sachen unter anderem auch im Rahmen der Strafverfolgung" handelt. Insofern kann ein Abgleich mit dem Fahndungsbestand auch dahingehend verstanden werden, dass zusätzlich zu den eigentlichen Fahndungsdateien Datenbestände zur Strafverfolgungszwecken einbezogen werden können. Demgegenüber ist der Datenabgleich bei Störer:innen und auch bei Nichtverantwortlichen prinzipiell nicht beschränkt. Hier können also grundsätzlich alle einem Abgleich technisch offenstehenden Datenbestände abgefragt werden. Während manche Normen so formuliert sind, dass eine Begrenzung auf die Bestände der jeweiligen Polizeiorganisation, also etwa einer bestimmten Landespolizei oder Polizeibehörde, denkbar ist,[1410] beziehen andere Vorschriften, etwa § 25 HSOG, explizit Datenbestände der Bundes- und Länderpolizeien mit ein. Auf Grundlage solcher Normen kann also mit allen in den Informationssystemen verfügbaren Datenbeständen abgeglichen werden.[1411] Man spricht beim Fahndungsabgleich, da nur ein begrenzter Teil der polizeilichen Datenbestände abgefragt wird, vom einfachen und bei dem Abgleich mit dem nicht beschränkten Datenbestand vom erweiterten Datenabgleich.[1412]

Die Eingriffsschwellen für die verschiedenen Datenabgleichformen sind teilweise etwas unterschiedlich formuliert. Grundsätzlich besteht aber das folgende Schema: Der erweiterte Datenabgleich ist in der ersten Alternative lediglich von der gefahrenabwehrrechtlichen Verantwortlichkeit abhängig, ansonsten bestehen keine weiteren Schwellen (vgl. etwa § 25 Abs. 1 S. 1

1409 Siehe dazu bereits oben S. 238 ff.

1410 So etwa *Arzt* zur nordrhein-westfälischen Rechtsgrundlage und mWn in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 25 Rn. 13 f.

1411 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 12; vgl. auch *Graf* in *Möstl/Weiner* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, § 45 Rn. 32.

1412 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 16.

HSOG: „[…] können […] abgleichen."). In der zweiten Alternative richtet sich die Maßnahme gegen Nichtverantwortliche und ist nur erlaubt, wenn dies zur Aufgabenerfüllung erforderlich ist. Da es sich bei Abgleich um einen Grundrechtseingriff handelt, muss die Erforderlichkeitsvoraussetzung allerdings immer mindestens erfüllt sein, sodass sie dort hineinzulesen ist, wo der Abgleich gegen Verantwortliche ansonsten voraussetzungslos gestattet wird. Auch der Fahndungsabgleich ist bei Erforderlichkeit für die Aufgabenerfüllung gestattet. Höhere Eingriffsschwellen sind regelmäßig nicht vorgesehen. Praktisch bedeutet dies, dass ein Datenabgleich immer durchgeführt werden kann, solange sich ein, wenn auch nur schwacher, Bezug zur polizeilichen Aufgabenerfüllung herstellen lässt. Damit sind nur evident willkürliche Abgleiche verboten. Als „Auffangtatbestand" kann zudem regelmäßig die Eigensicherung herangezogen werden.[1413] Im Einsatz wird sich – zumindest unter gegenwärtigen Bedingungen – die Rechtmäßigkeit kaum überprüfen lassen. Zwar ist im Falle von Störer:innen eine konkrete Gefahr erforderlich. Da aber auch von Nichtverantwortlichen Daten im Grunde unter denselben Voraussetzungen – Erforderlichkeit zur Aufgabenerfüllung – abgeglichen werden dürfen, erübrigt sich diese Einschränkung. Hinzukommt, dass in einigen Informationssystemen eine reine Fahndungsabfrage überhaupt nicht möglich ist, sodass regelmäßig ein kompletter Datenabgleich mit den verfügbaren Datenbeständen durchgeführt werden wird,[1414] was aufgrund von Unverhältnismäßigkeit rechtswidrig ist.

Eine stärkere Einhegung des Datenabgleichs erfolgt auch nicht unter Zweckgesichtspunkten. Die Vorschriften verweisen nur auf die sehr breiten Aufgabenbereiche der Polizeien und stellen keine Zweckvorgaben dar.[1415] Zudem ist zu beachten, dass es bei Datenabgleichen häufig zu Zweckänderungen kommt: Die Datenbestände der Polizeien sind häufig Mischdateien gem. § 483 Abs. 1 S. 2 StPO, sodass dort sowohl repressiv als auch präventiv erhobene Daten enthalten sein werden. Im Rahmen eines Abgleichs etwa zur Eigensicherung würden dann mitabgeglichene strafverfahrensrechtliche Daten zweckändernd zur Gefahrenabwehr genutzt werden. Dies wird

1413 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 13 f.

1414 *Bäuerle* in *Möstl/Bäuerle* (Hrsg.), Polizei- und Ordnungsrecht Hessen, § 25 Rn. 15.

1415 *Müller/Schwabenbauer in Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 934.

von den entsprechenden Vorschriften nicht kenntlich gemacht und insofern auch nicht mit eventuell erhöhten Voraussetzungen versehen.[1416]

Insgesamt weisen die Normen also mit Blick auf Anlass, Zweck und Umfang der einzubeziehenden Daten durchaus gravierende Bestimmtheitsdefizite auf.[1417] Es ist natürlich nicht von der Hand zu weisen, dass die Polizeien ihre Datenbestände auch nutzen können sollen und insbesondere in gefahrreichen Einsatzsituationen zu einer besseren Einschätzung und Reaktionsweise im Wege der informationellen Durchdringung ihres Gegenübers in der Lage sein sollen. Es scheint aber durchaus möglich insoweit zu einer befriedigenderen Regelungslage zu kommen. Denn die gegenwärtige Möglichkeit, in breitem Umfang und im Anlass wenig beschränkt personenbezogene Daten mit dem Datenbestand abzugleichen, wird mit einem zunehmenden Anwachsen des polizeilichen Informationswesens, wie es wohl bei der Zunahme der verfügbaren Daten zu erwarten ist, immer eingriffsintensiver. Durch ein Mehr an Daten zu einer Person oder mehr Personen, über die Daten in den Datenbeständen enthalten sind, nimmt die informationelle Durchschlagkraft des Datenabgleichs zu, da entweder detailliertere Datendoubles zur Verfügung stehen oder mehr Treffer, gleich welchen Inhalts, erzielt werden können.

Die Bedeutung des Datenabgleichs wird zudem durch neuere technologische Entwicklungen aufgewertet. So sieht etwa Art. 61 Abs. 2 BayPAG vor, dass ein Datenabgleich „auch unter Verwendung bildverarbeitender Systeme und durch Auswertung biometrischer Daten erfolgen" darf, „wenn andernfalls die Erfüllung polizeilicher Aufgaben gefährdet oder wesentlich erschwert würde". Damit ist insbesondere eine „Gesichtsfelderkennung[1418]", also eine automatisierte Erkennung biometrischer Merkmale gemeint. Die relativ erhöhte Erforderlichkeitsschwelle ist notwendig, da biometrische Daten zu den besonderen Kategorien personenbezogener Daten im Sinne von Art. 10 DRL-JI gehören. Zudem ist „stets" eine Datenschutzfolgenabschätzung gem. Art. 64 Abs. 2 S. 2 BayPAG vorzunehmen.[1419] Ob die Maßnahme nur stationär, in bestimmten Einsatzformen oder aber schon

1416 *Müller/Schwabenbauer in Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 941.

1417 So auch *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 25 passim.

1418 Gemeint ist wohl die biometrische Gesichtserkennung, das Gesichtsfeld ist ein augenärztlicher Fachbegriff.

1419 *Schmidbauer* in *W. Schmidbauer/Steiner,* Polizeiaufgabengesetz, Polizeiorganisationsgesetz, Art. 61 Rn. 8 ff.

im einfachen Streifendienst zum Tragen kommen soll, ist nicht bekannt. Jedenfalls erhöht insbesondere die Datenschutzfolgeabschätzung, die immer durchzuführen ist, die Wissensanforderungen an Polizeibeamt:innen merklich, da es sich um ein technisch komplexes und in der rechtlichen Bewertung anspruchsvolles Verfahren handelt. Vor dem Hintergrund neuer technischer Möglichkeiten zur Durchführung komplexerer Datenabgleiche, für die die bayerische Regelung nur ein Beispiel und den Anfang darstellen dürfte, ist zudem die Charakterisierung dieser Datenverarbeitungsform als wenig invasiv unhaltbar geworden.[1420]

e) Massendatenverarbeitungen: Rasterfahndung und Datenanalyse

Neben diesen Datenverarbeitungsformen, die einigermaßen begrenzt Daten für die Verarbeitung erfassen, treten zudem zunehmend Massendatenverarbeitungsverfahren.

Die klassische Form dieser Massendatenverarbeitung ist die Rasterfahndung, die polizeifremde Datenbestände untereinander oder auch mit polizeilichen Datensammlungen abgleicht, um nach einem bestimmten positiven oder negativen Muster wenige Daten aus dem ursprünglichen Massendatensatz auszusieben. Dafür müssten die Daten erhoben, abgeglichen und gespeichert werden. Das Verfahren wird auf nicht-öffentliche Daten angewendet, die bei öffentlichen oder privaten Stellen vorliegen.[1421] Vor allem da eine Vielzahl an Personen betroffen ist und deren Daten kombinatorisch ausgewertet werden, gilt die Rasterfahndung als besonders eingriffsintensiv. Einerseits wird durch die Maßnahme der Zweckbindungsgrundsatz stark angetastet und andererseits bewegt sie sich je nach Umfang der einbezogenen Datenbestände in Richtung einer anlasslosen Vorratsdatenspeicherung.[1422] Deshalb besteht ein Richter:innenvorbehalt und ein eng umgrenzter Anwendungsbereich für die Rasterfahndung.

Neben dieser nach außen gerichteten Form der polizeilichen Massendatenverarbeitung gibt es aber auch zunehmend Möglichkeiten der internen Massendatenverarbeitung. Die bereits erläuterte – defizitär geregelte –

1420 *Golla* Kriminologisches Journal 52 (2020), 149 (158).
1421 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 947.
1422 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 953.

automatisierte Datenanalyse hat strukturelle Ähnlichkeiten zur Rasterfahndung. So hebt das Verfahren die Zweckbindung der polizeiintern vorhandenen Daten auf. Zudem kann man mit dem Anwachsen der Datenbasis, also der polizeilicher Datensammlungen, ebenfalls von einer Intensitätssteigerung der Maßnahme ausgehen, auch wenn damit vielleicht noch keine Nähe zur anlasslosen Vorratsdatenspeicherung begründet würde. Aber je mehr Daten das Informationswesen in miteinander verknüpfbarer Form und Struktur enthält – etwa: ein umfassender, barrierefreier Datenspeicher, in dem Daten prinzipiell miteinander kombinierbar, abgleichbar et cetera sind, wie im Zuge von Polizei 2020 geplant – desto mehr kann die Polizei auch ihre eigenen Daten „rastern" und mit anderen erkenntnisgewinnbringenden Verarbeitungsverfahren auswerten, sodass sich tiefgehendere Erkenntnisse daraus ergeben. Aufgrund der strukturellen Ähnlichkeiten von Massendatenverarbeitungsverfahren ließe sich zumindest darüber nachdenken, ob eventuell ein verfassungsrechtlicher Richter:innenvorbehalt für diese invasiven Informationseingriffe besteht.[1423] Es ist zu erwarten, dass sich derartige Verfahren zukünftig noch stärker ausdifferenzieren und insgesamt weiterentwickeln werden, was bereits jetzt neue Herausforderungen für das Recht der polizeilichen Informationsverarbeitung mit sich bringt.[1424]

f) Verarbeitungen mit dem Zweck des Schutzes der informationellen Selbstbestimmung

Abgesehen von Datenverarbeitungsformen, die in das Recht auf informationelle Selbstbestimmung eingreifen, gibt es auch Verarbeitungspflichten der Polizei, die gerade der Gewährleistung, dem Schutz oder der Wiederherstellung der informationellen Selbstbestimmung dienen.[1425] Dabei handelt es sich um die Berichtigung, Löschung oder Einschränkung der Verarbeitung von Daten. Aus dem Datenschutzrecht folgt zunächst, dass nur valide Daten verarbeitet werden dürfen, sodass bei entsprechend festgestellter Un-

1423 Siehe dazu *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 962, im Kontext der Rasterfahndung.

1424 Siehe dazu bereits die Ausführungen zur Regelung der automatisierten Datenanalyse oben S. 281 ff.

1425 Siehe dazu etwa *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 77 BKAG Rn. 3 ff; *Ogorek* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 32.

richtigkeit eine Berichtigung erfolgen muss. Eine Löschung hat zu erfolgen, wenn dies eine gesetzliche Bestimmung vorschreibt, die Speicherung unzulässig (geworden) ist oder die Daten nicht mehr zur Aufgabenerfüllung erforderlich sind. Eine Einschränkung der Verarbeitung hingegen muss erfolgen, wenn eine Löschung – etwa, weil sie schutzwürdige Belange Betroffener beeinträchtigen würde oder noch für datenschutzrechtliche Überprüfungen erforderlich sind – nicht interessengerecht wäre. Der Umgang mit diesen Verpflichtungen ist von nicht zu unterschätzender Bedeutung für das Informationswesen in seiner Gänze, da etwa massenhaft falsche Daten oder entgegen entsprechenden Verpflichtungen nicht gelöschte Daten zu problematischen Zuständen führen können. Es ist also vor allem eine systematische Einhaltung der Verpflichtungen geboten.

IV. Fazit zu den rechtlichen Rahmenbedingungen des polizeilichen Informationswesens

Bis hierhin erfolgte die rechtliche Betrachtung der informationstechnologischen Infrastruktur und dem in ihr praktiziertem Informationshandeln fragmentarisch. Fügt man die einzelnen Detailbetrachtung zu einem mosaikhaften Ganzen zusammen, so zeichnet sich keine makellose normative Architektur zur Regulierung des polizeilichen Informationswesens ab. Vielmehr wird deutlich, dass die informationstechnologische Infrastruktur nur punktuell und zumeist unzureichend durch das Recht strukturiert wird und polizeiliche Informationspraktiken nur unzureichend normativ eingehegt werden. Vielfach sind Regelungen an entscheidenden Stellen vage und räumen der Polizei in der Bestimmung der zu speichernden Daten und Personen sowie im weiteren Umgang mit diesen Informationen einen erheblichen exekutiven Spielraum und eine große Definitionsmacht ein. Die Datenverarbeitung ist recht weitgehend zur Aufgabenerfüllung freigegeben, materiell-rechtliche Beschränkungen wirken hierbei kaum begrenzend. Limitationen sind eher prozeduraler Natur. Sie werden am meisten noch durch Rechte- und Rollenkonzepte – also: funktionsbezogene Zugriffsrechte auf bestimmte Daten oder eben nicht – als Ausgestaltung des Postulats der technisch-organisatorischen Datenschutzmaßnahmen errichtet. Ähnlich wie die technische Infrastruktur des polizeilichen Informationswesens befindet sich auch die rechtliche Architektur der polizeilichen Informationsordnung in keinem guten Zustand und bedarf der Sanierung.

Ohne weiteres wird sich diese allerdings nicht bewerkstelligen lassen. So führt etwa *Bäcker* angesichts der BKAG-Novellierung, die für den Informationsverbund als integralen Teil des polizeilichen Informationswesens essenziell ist, an: „Die Mängel dieser Regelungen lassen sich nicht mit punktuellen Änderungen des Entwurfs abstellen. Dieser Befund berührt […] die beabsichtigte Neugliederung der Informationsordnung des Bundeskriminalamts fundamental. Dieses Vorhaben sollte daher zurückgestellt werden, bis die derzeit offene Frage geklärt ist, ob sich hierfür grundrechtskonforme und praktikable Rechtsgrundlagen finden lassen."[1426] Gemeint sind hier die besprochenen Fehlkonstruktionen der §§ 16, 18, 19 BKAG,[1427] die aber zwischenzeitlich Gesetz geworden sind. Die Neugliederung wird aber auch sonst durch die Polizeigesetze bisher nicht hinreichend abgebildet. Erforderlich für eine adäquate Regulierung wäre gerade auch und zuallererst die Beantwortung der von *Bäcker* aufgeworfenen, bedeutsamen Frage, ob sich für das Konzept des neuen Informationsverbundes als gemeinsamem Datenhaus, in dem Daten nur noch einmal erfasst und dann anschließend im Rahmen der Rechtsgrundlagen beliebig verarbeitet werden sollen, überhaupt ein passendes Regelungskonzept wird finden lassen. Es geht also nicht nur im Bereich von neuen, informationstechnologisch fundierten Erhebungsmaßnahmen, sondern auch für die informationstechnologische Infrastruktur und ihre Weiterentwicklung um die Frage, ob die bestehenden Befugnisse und Regelungsformen auch zur effektiven Polizeiarbeit in der digitalisierten Gesellschaft herangezogen werden können oder ob es perspektivisch der Entwicklung und Konturierung neuer Regelungskonzepte bedarf.[1428]

Das gilt einmal für die Regelungen der Strukturen des polizeilichen Informationswesens, aber auch für die sich ändernde Qualität des polizeilichen Datenumgangs. Denn mit einer zunehmenden Datafizierung der Gesellschaft geht auch ein zunehmend datafiziertes Arbeiten der Polizei einher, was sich – nicht nur, aber auch – in einem spürbaren Anwachsen des polizeilichen Informationswesens bemerkbar macht, sowohl in Volumen als auch in Granularität der Daten. In der Folge werden die polizeilichen Datenbestände zunehmend zu einem Spiegel der sozialen Konflikte in der Gesellschaft. Zwar wird es sich immer um ein Zerrbild handeln, aber mit

1426 *Bäcker*, A-Drs. 18(4)806 D, S. 3.
1427 Siehe dazu bereits oben S. 334 ff.
1428 So *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 607 im Kontext neuer polizeilicher Ermittlungsmethoden.

sich stetig vergrößerndem Umfang und sich verbessernder Auflösung. Eine solche Abbildung von Ereignissen abweichenden Verhaltens und damit zusammenhängender Personen, Objekte, Institutionen und sonstiger Entitäten im polizeilichen Informationswesen ermöglicht es mit wachsender Akkuratheit, Devianz für die Polizei retrospektiv erfahrbar zu machen.

Dabei können sich – auch über die Multimedialität der Daten – Akkumulationen ergeben, die sonst eher auf eingriffsintensiven Maßnahmen wie längerfristigen Observationen beruhen, die eine Beobachtung durch die Polizei über einen längeren Zeitraum beschreibt und als Maßnahme aufgrund ihrer Intensität regelmäßig hohen Anforderungen inhaltlicher und verfahrensrechtlicher Art unterliegt. Solche Überwachungsmaßnahmen sind darauf ausgerichtet „unter Nutzung moderner Technik (…) möglichst alle Äußerungen und Bewegungen zu erfassen und bildlich wie akustisch festzuhalten",[1429] wobei neben der bloßen menschlichen Beobachtung („Verfolgung") als besagte „moderne Technik" etwa Fotoapparate, Kameras, Peilsender, GPS-Geräte, Richtmikrofone und ähnliche Geräte zum Einsatz kommen.[1430] Dabei ist gar nicht entscheidend, dass die Überwachung durchgängig durchgeführt wird, ausschlaggebend ist vielmehr die Wiederholung.[1431] In einer immer stärker digital vermittelten Welt ist es indessen nicht mehr ungewöhnlich, dass bei den Polizeien häufiger auch Daten in Form von (bewegten) Bildern, Standorten in Raum und Zeit oder sogar Äußerungen – man denke an Sprach- und Videonachrichten, die zunehmend zum digitalen Kommunikationsverhalten zählen – anfallen. Zugegebenermaßen erfolgen längerfristige Observationen in der Gegenwart und in Echtzeit, das heißt, die erhobenen Daten finden mit einer hohen Aktualität Eingang in das polizeiliche Informationswesen. Nichtsdestotrotz behalten die so zusammengetragenen Daten, auch über die Gegenwart ihrer Erhebung hinaus, ihre hohe Persönlichkeitsrelevanz. Ein Persönlichkeitsbild wird sich auch nach einigen Jahren damit noch zeichnen lassen. Ob es noch zutreffend ist, ist eine davon zu unterscheidende Frage. Für Daten, die über einen längeren Zeitraum durch verschiedene Polizeikontakte wegen (mutmaßlich) deviantem Verhalten zu einer Person akkumuliert worden sind, kann bezüglich der Persönlichkeitsrelevanz nur begrenzt eine andere

1429 BVerfGE 141, 220 (287) – Bundeskriminalamtgesetz.

1430 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 796.

1431 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 800.

Wertung hinsichtlich der Invasivität gelten. Hier wie da können sich durch wiederholte Datenerhebungen und Speicherungen im polizeilichen Informationswesen für Polizist:innen, die die Daten retrospektiv auswerten und für ihre Aufgabenerfüllung analysieren – alles Schritte, die prinzipiell von der Datenverarbeitungsgeneralklausel gedeckt werden – Persönlichkeitsbilder von (nicht unerheblich) grundrechtstangierender Auflösung ergeben. Ähnliches gilt für das Sozialprofil von Betroffenen, das durch die auf sie bezogenen Daten von und über Kontakt- und Begleitpersonen sichtbar wird. Hierdurch kann eine Analyse von Daten bezogen auf Erkenntnisse wie das Sozialprofil in die Nähe der Eingriffsintensität der Ausschreibung zur polizeilichen Beobachtung rücken.[1432] Der hierin liegende Eingriff wird zwar indirekt dadurch etwas abgefedert, dass nur Organisationseinheiten, die besonders gravierende Kriminalitätsformen bearbeiten, einen entsprechend breiten Zugriff auf die polizeilichen Datenbestände haben. Nichtsdestotrotz zeigt das Fehlen von materiell-rechtlichen Regelungskonzepten für diese Formen polizeiinterner Datenakkumulationen, dass eine wirkliche Auseinandersetzung mit diesen internen Datenverarbeitungsprozessen und ihren grundrechtlichen Implikationen bisher zu wenig stattgefunden hat.

V. Das interne Datenschutzkontrollregime

Die bisherigen Ausführungen haben auf die Aspekte des polizeilichen Informationswesens fokussiert, die den polizeilichen Kernaufgaben – Strafverfolgung und Gefahrenabwehr, jeweils auch mit den Vorfeldkompetenzen der Straftatenverhütung und Strafverfolgungsvorsorge – dienen und damit wesentlich für Umfang und Form der polizeiliche Sozialkontrolle sind. Neben diesem größten und aus polizeifunktionaler Sicht wichtigsten Teil des polizeilichen Informationswesens gibt eine weitere integrale Komponente, deren Bedeutung insbesondere mit der EU-Datenschutzreform von 2016 zugenommen hat und wohl auch weiter zunehmend wird. Begrifflich soll dieser Aspekt als internes Datenschutzkontrollregime gefasst werden. Ziel dieser Struktur ist es, über die Einhaltung der – wie dargestellt an etlichen Stellen problematischen – normativen Rahmenbedingungen des polizeilichen Informationswesens zu wachen. Seine Ausprägung findet das

1432 Siehe zu dieser Maßnahme und dem Faktor des Sozialrpofils *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 998.

interne Datenschutzkontrollregime im Wesentlichen in zwei Dimensionen: Einerseits in den behördlichen Datenschutzbeauftragten und andererseits in den technisch-organisatorischen Maßnahmen, die von den Datenschutzbeauftragten, aber auch anderen Teilen der Polizei zur Einhaltung der rechtlichen Vorgaben implementiert werden (müssen). Zudem sind beide Dimensionen Aufprägungen eines prozeduralen Grundrechtsschutzes. Schon im Volkszählungsurteil wurde die Bedeutung einer solchen internen verfahrensrechtlichen Kontrolle betont.[1433] Indem mit diesen Regulativen die polizeiliche Datenverarbeitungstechnologie und der Umgang mit dieser kontrolliert werden soll, haben die rechtlichen Vorgaben und die praktische Umsetzung des internen Datenschutzkontrollregimes direkten Einfluss darauf, wie die Polizei Informationen für ihre Aufgabenerfüllung verarbeiten kann und somit auch darauf, wie sich polizeiliche Sozialkontrolle materialisiert und entwickelt. Daneben treten offenkundig auch weitere Formen, denen sich der Datenschutz zur Kontrolle des polizeilichen Informationshandelns bedient. Zentral sind hier die Betroffenenrechte und die Datenschutzaufsicht durch die Landes- und den Bundesdatenschutzbeauftragten. Beide Instrumente sind aber kein integrierter Teil des polizeilichen Informationswesens und werden daher vorliegend weitestgehend ausgeklammert.

1. Personelle Ausprägung des internen Datenschutzkontrollregimes: Behördliche Datenschutzbeauftragte

Die Ausgestaltung der rechtlichen Rolle des Datenschutzbeauftragten erfolgt regelmäßig in den jeweiligen Datenschutzgesetzen und übernimmt im Wesentlichen die Regelungsinhalte, die die JI-Richtlinie vorgegeben hat. Geregelt werden die Aspekte der Benennung, der Stellung sowie der Aufgaben der behördlichen Datenschutzbeauftragten. Die gesetzlichen Vorgaben finden sich etwa in §§ 5, 6, 7 BDSG und den Entsprechungsvorschriften in den Landesdatenschutzgesetzen, die im Wesentlichen inhaltsgleich ausgestaltet sind. Zudem finden sich noch einige Sondervorschriften in den Bundes- und Landespolizeigesetzen (vgl. etwa §§ 70, 71, 72 BKAG).

Zunächst besteht eine Pflicht zur Benennung für alle Polizeibehörden, wobei aber unter Berücksichtigung ihrer Größe und Organisationsstruktur

1433 BVerfGE 65, 1 (44) – Volkszählung.

gemeinsame Datenschutzbeauftragte benannt werden können[1434] – etwa können mehrere untergeordnete Polizeibehörden eine Person als Datenschutzbeauftragte:n zugeordnet bekommen. Benannte müssen eine hinreichende berufliche Qualifikation sowie insbesondere Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis innehaben und auf der Grundlage ihrer Fähigkeit zur Erfüllung ihrer gesetzlichen Aufgaben in der Lage sein.[1435] Dabei ist es regelmäßig ausreichend, wenn die Datenschutzbeauftragten ihr spezifischen fachlichen Schwerpunkt haben – etwa im rechtlichen, technischen oder organisatorischen Gebiet – und ansonsten über Grundwissen in den anderen Bereichen verfügen, das sie mit organisationsintern zu gewährender Unterstützung in die Lage versetzt, ihre Aufgaben zu erfüllen.[1436]

Zentrale Stellschraube für die Effektivität der polizeilichen Datenschutzbeauftragten ist ihre Stellung innerhalb der Behördenstruktur. Sie müssen frühzeitig in datenschutzrechtliche Fragen eingebunden werden und sind bei ihrer Arbeit durch die datenschutzrechtlich verantwortliche Stelle zu unterstützen, etwa durch Ressourcen, aber auch durch Zugang zu den entsprechenden Verarbeitungsvorgängen. Auch wenn es die JI-Richtlinie selbst nicht vorschreibt, haben Bundes- und Landesgesetzgeber die Weisungsfreiheit der polizeilichen Datenschutzbeauftragten gesetzlich festgelegt.[1437] Diese Unabhängigkeit wird weiterhin durch ein Abberufungsverbot, den Schutz vor Sanktionierungen und – als spezielle polizeiorganisatorische Ausformung[1438] – die direkte Unterstellung unter die Leitungsebene verstärkt.[1439] Letzteres dient vor allem auch dem Einfluss der Datenschutzbeauftragten auf die polizeiinternen Regelungsprozesse. Jedoch ist die Unabhängigkeit im polizeilichen Bereich hier mitunter eingeschränkt. So kann sich etwa der oder die Datenschutzbeauftragte des Bundeskriminalamts in Zweifelsfällen nur im Benehmen mit der Behördenleitung an die Auf-

1434 *Körffer* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 5 Rn. 3.

1435 *Bergt/Schnebbe* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 5 Rn. 5.

1436 *Gola* in *Gola/Heckmann/Klug* ua, BDSG, § 5 Rn. 10.

1437 *Körffer* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 6 Rn. 2.

1438 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 72 BKAG Rn. 3.

1439 Die allgemeinen Vorschriften der Datenschutzgesetze schreiben nur eine Berichtslinie an die oberste Leitungsebene vor, nehemen aber insoweit keine organisatorische Einordnung vor, vgl. etwa *Bergt/Schnebbe* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 6 Rn. 6.

sicht, also den oder die Bundesdatenschutzbeauftragte:n wenden, im Konfliktfall soll das Bundesministerium des Innern entscheiden. Eine solche Limitierung ist weder verfassungs- noch unionsrechtlich zulässig, da so die verfahrensrechtlichen Sicherungen von Datenverarbeitungsprozessen unzulässig beschränkt werden.[1440] Während eine klärende Kommunikation mit der Behördenleitung in Zweifelsfragen unproblematisch ist, muss sich also der oder die Datenschutzbeauftragte auch im Konfliktfall ohne weitere Beschränkung an die Aufsicht wenden können.[1441] Ferner ist in der Position der Datenschutzbeauftragten auch der Kontaktpunkt für von polizeilicher Datenverarbeitung betroffene Personen und insoweit mit externen datenschutzrechtlichen Kontrollmechanismen verzahnt. Dieser Aspekt der Stellung wird durch eine Verschwiegenheitspflicht hinsichtlich betroffener Personen und der mit ihnen verbundenen Vorgänge flankiert. Zudem haben polizeiliche Datenschutzbeauftragte Verschwiegenheitspflichten und gegebenenfalls Zeugnisverweigerungsrechte, da sie regelmäßig mit sensiblen Informationen aus den und über die Polizeiorganisationen in Kontakt kommen.

Die größte Bedeutung kommt den eigenständigen Aufgaben der Datenschutzbeauftragten zu. Zusammengefasst haben sie die Aufgabe der Beratung, der Überwachung bzw. Kontrolle sowie der Kooperation. Die datenschutzrechtlich verantwortliche Stelle ist über datenschutzrechtliche Vorgaben zu unterrichten und im Rahmen der Gestaltung der Datenverarbeitung lösungsorientiert so zu beraten, dass gesetzliche Vorgaben eingehalten werden.[1442] Dabei handelt es sich um eine Pflicht, die proaktiv zu erfüllen ist.[1443] Vor dem Hintergrund der hohem Komplexität des polizeilichen Informationsrechts ist diese Aufgabe als anspruchsvoll anzusehen.

Gegenüber der alten Rechtslage hat insbesondere die Überwachungsaufgabe der Beauftragten eine Intensivierung erfahren. Umfassend zu überwachen ist nunmehr sowohl die Einhaltung des gesamten anwendbaren Datenschutzrechts als auch die Einhaltung der Datenschutz-Strategien, die vom Verantwortlichen zur Umsetzung des Datenschutzes entwickelt werden. Dazu gehören neben Aspekten des technischen Datenschutzes etwa

1440 *Smitis* in *Simitis* (Hrsg.), Bundesdatenschutzgesetz, § 4g Rn. 27.
1441 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 72 BKAG Rn. 4.
1442 *Paal* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Art. 39 DS-GVO Rn. 5.
1443 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 11.

auch Zuständigkeitsregelungen sowie Sensibilisierungen und Schulungen der Beamt:innen.[1444] Da ein Großteil der Regelungen, die es zur technischen Infrastruktur des polizeilichen Informationswesens gibt, und alle Formen des polizeilichen Umgangs mit personenbezogenen Daten entsprechende datenschutzrechtliche Implikationen aufweisen, müssen die Datenschutzbeauftragten einen weiten Teil der polizeilichen Informationsarbeit überwachen. Dabei können sie sich regelmäßig nicht auf eine Art papierne Überwachung, etwa anhand eines Verzeichnisses von Verarbeitungstätigkeiten, beschränken. Vielmehr muss die informationstechnologische Infrastruktur und der Umgang mit ihr etwa in Vor-Ort-Kontrollen überprüft werden.[1445] Eine Mischung aus Beratung und Kontrolle stellt die ebenfalls dem Aufgabenspektrum unterfallende Datenschutz-Folgenabschätzung dar. Diese ist – etwa gem. § 67 Abs. 1 BDSG – immer dann durchzuführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge" hat. Im Rahmen einer solchen Abschätzung sind die polizeilichen Datenschutzbeauftragten zu beteiligen, ihre Mitwirkung ist für sie verpflichtend und – da sie ihre Tätigkeiten risikobasiert priorisieren müssen (vgl. etwa § 7 Abs. 3 BDSG) – bevorzugt zu erledigen. Während die Beauftragten für die Durchführung selbst nicht zuständig sind, müssen sie im Rahmen ihrer Durchführung konsultieren und das Ergebnis kontrollieren.[1446] Hiermit sind insbesondere informationstechnologische Neuerungen ebenfalls der Kontrolle der Datenschutzbeauftragten überantwortet.

Schließlich sind die Datenschutzbeauftragten über ihre jeweilige Behörde hinaus auch kooperativ tätig. Einerseits gibt es gesetzlich vorgeschriebene innerpolizeiliche Kooperationspflichten. So gibt es in § 72 BKAG die Pflicht für den oder die Beauftragte:n des Bundeskriminalamts mit den Datenschutzbeauftragten der Landeskriminalämter, der Bundespolizei und des Zollkriminalamts zusammenzuarbeiten. Hier sollen insbesondere Synergieeffekte im Rahmen des Umgangs mit den normativen Rahmenbe-

1444 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 13.

1445 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 15.

1446 *Gola* in *Gola/Heckmann/Klug* ua, BDSG, § 7 BDSG Rn. 8.

dingungen des polizeilichen Informationswesens genutzt werden.[1447] Daneben ist aber auch eine Vereinheitlichungswirkung im Umgang mit Daten, insbesondere im polizeilichen Informationsverbund, theoretisch aber auch darüber hinaus, denkbar. Zudem sind aber die polizeilichen Datenschutzbeauftragten jeweils Kontaktpunkt für die Aufsichtsbehörden in Bund und Ländern. Vor allem aber besteht eine Kooperationspflicht mit der Aufsichtsbehörde des Bundes bzw. des jeweiligen Landes. Die polizeilichen Datenschutzbeauftragten sind die ersten Ansprechpersonen in datenschutzrechtlichen Angelegenheiten. Damit ist nochmal die besondere Relevanz der Position der polizeiinternen Datenschutzbeauftragten hervorgehoben. Mit der Kooperationspflicht, wenn der Kontakt von der Aufsichtsbehörde ausgeht, ist auch das Recht zur Hinzuziehung der Aufsichtsbehörde zur Beratung verbunden. Insoweit besteht das Potenzial, dass sich zwischen internen Datenschutzbeauftragten und der Aufsicht eine datenverarbeitungshemmende Achse bildet, die mit den Anliegen der polizeilichen (Informations-)Arbeit zum Zwecke von Gefahrenabwehr und Strafverfolgung in Konflikt tritt.[1448]

Insgesamt haben die polizeilichen Datenschutzbeauftragten damit aus rechtlicher Sicht eine zentrale Position im polizeilichen Informationswesen, da sie über ihre Stellung und Aufgaben umfassend mit Datenverarbeitungsvorgängen und der diesen zugrundeliegenden Technologien befasst sind und beides unter Rechtmäßigkeitsgesichtspunkten überwachen und kontrollieren. Sie sind zudem vor allem im Rahmen ihrer Beratungsaufgaben durch ihre Einbindung in die technisch-organisatorischen Maßnahmen auch mit der zweiten Ausprägung des internen Datenschutzkontrollregimes des polizeilichen Informationswesens eng verwoben.

2. Technisch-organisatorische Ausprägungen des internen Datenschutzkontrollregimes

Die Datenschutzbeauftragten – selbst, wenn sie noch Mitarbeiter:innen haben – können das polizeiliche Informationswesen jedoch nicht allein mit den ihnen zur Verfügung stehenden (menschlichen) Fähigkeiten überwachen und kontrollieren. Vielmehr haben sich im internen Datenschutzkontrollregime, zunächst anlässlich verfassungsrechtlicher Vorgaben, seit 2016

1447 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 72 BKAG Rn. 4.
1448 *Bergt* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 39 DS-GVO Rn. 17 ff.

vor allem aufgrund unionsrechtlicher Vorschriften, Instrumente zur Unterstützung der Datenschutzbeauftragten bei ihren Aufgaben und generell zur Einhaltung datenschutzrechtlicher Bestimmungen herausgebildet. So schreibt Art. 19 JI-Richtlinie nunmehr vor, dass „geeignete technische und organisatorische Maßnahmen" implementiert werden, „um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung in Übereinstimmung mit dieser Richtlinie erfolgt." Diese Grundnorm wird durch die JI-Richtlinie und die jeweiligen Umsetzungsgesetz in konkretere Bahnen gelenkt, wobei der Konkretisierungsgrad sich unterscheidet.

Nochmals aufgegriffen wird der Begriff der technisch-organisatorischen Maßnahmen in Art. 29 JI-Richtlinie, der zu diesen verpflichtet, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten."[1449] Beabsichtigt ist damit die Etablierung eines Sicherheitsstandards für die personenbezogenen Daten der Betroffenen, nicht für das polizeiliche Informationswesen als vulnerable Infrastruktur.[1450] Dazu sollen etwa Pseudonymisierung und Verschlüsselung beitragen (vgl. § 64 Abs. 2 S. 1 BDSG). Vor allem sind aber die Maßnahmen bei automatisierten Verarbeitungen, wie sie meistens im polizeilichen Informationswesen auftreten, umzusetzen, wozu etwa gemäß § 64 Abs. 3 S. 1 BDSG Zugriffskontrollen, Speicherkontrollen, Benutzerkontrollen, Übertragungskontrollen, Eingabekontrollen und weitere Maßnahmen gehören. Vor allem für die Vorgangsbearbeitungs- und Fallbearbeitungssysteme, in denen ein Großteil des polizeilichen Datenumgangs stattfindet, sind verhältnismäßig austarierte Zugriffs- und Berechtigungskonzepte notwendig, mit denen einerseits gewährleistet wird, dass die jeweilige Organisationseinheit oder Beamt:in alle Daten hat, die zur jeweilig aktuellen Aufgabenerfüllung benötigt werden. Andererseits müssen solche Verarbeitungsvorgänge unterbunden werden, die sich gegen gesetzliche Bestimmungen richten, wie beispielsweise die Nutzung von Daten aus abgeschlossenen Vorgängen, die grundsätzlich nur noch zur Vorgangsverwaltung und Dokumentation genutzt werden.[1451]

Besondere Bedeutung erlangen Zugriffsberechtigungen zudem im polizeilichen Informationsverbund, in dem gemäß § 29 Abs. 4 BKAG auch § 15 BKAG zu beachten ist, der die Zugriffsberechtigungen regelt. Die

1449 Siehe dazu bereits oben S. 192 f.

1450 *Bock* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, § 64 Rn. 1.

1451 Arzt in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1196. Zu diesem Problem siehe bereits oben S. 254 ff.

Vorschrift dient – wie aber letztlich alle Zugriffsberechtigungen im polizeilichen Bereich – zumindest auch der Einhaltung des Grundsatzes der hypothetischen Datenneuerhebung. Durch das Berechtigungskonzept soll festgelegt werden, wer auf die gemäß § 14 BKAG gekennzeichneten Daten zugreifen kann. Die Zugriffsberechtigungen sind dabei inhaltlich so zu gestalten, dass nur Daten zur Verfügung stehen, deren Kenntnis zur Erfüllung der jeweiligen Dienstpflichten erforderlich ist, sodass etwa anhand des „jeweiligen Dienstposten[s] eines Mitarbeiters ergebenden Dienstpflichten (zum Beispiel Durchführung von Ermittlungen im Bereich des islamistischen Terrorismus, §§ 129a, 129b StGB) [zu] bestimmen [ist], wie die Zugriffsberechtigung auszugestalten ist."[1452] Dasselbe gilt für die Befugnis zur Änderung, Berichtigung oder Löschung von personenbezogenen Daten.[1453] Die Vergabe orientiert sich an einem zugrundeliegenden Rechte- und Rollenkonzept, in dem festgelegt ist, „für welche Funktionen und Dienstposten welche Berechtigungen – sowohl hinsichtlich des Zutritts zu Arbeitsbereichen als auch hinsichtlich des Zugriffs auf Daten – erforderlich sind."[1454] Zudem soll eine formale Gestaltung der Systeme in einer Weise erfolgen, dass die Abfragegründe, die Polizist:innen angeben, standardisiert sind, um eine effektivere Dokumentation zu ermöglichen und den Datenumgang besser steuern zu können, gleichzeitig aber auch eine höhere Nutzer:innenfreundlichkeit zu gewährleisten.[1455] Auch hier ist die Verpflichtung zur technisch-organisatorischen Ausgestaltung an den Stand der Technik gekoppelt. Diese offene Formulierung der Vorgaben zu den technisch-organisatorischen Maßnahmen ist allerdings nicht unbedenklich. Zwar ist sie mit Blick auf die Differenzen zwischen einzelnen Polizeien, etwa was Stand der Technik oder auch Ressourcen angeht, grundsätzlich nachvollziehbar. Rekapituliert man jedoch, dass der Datenschutz zur Einhegung polizeilichen Informationshandelns beitragen soll, ist die graduelle Beliebigkeit der Implementierung technisch-organisatorischer Maßnahmen problematisch, weil ihre inhaltliche Ausgestaltung der verantwortlichen Stelle überlassen wird.[1456]

1452 BT-Drs. 18/11163, S. 96.
1453 BT-Drs. 18/11163, S. 96.
1454 BT-Drs. 18/11163, S. 97.
1455 BT-Drs. 18/11163, S. 97.
1456 In ähnlichem Kontext *Arzt* in *Möstl/Kugelmann* (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Nordrhein-Westfalen, § 22 Rn. 55.

In eine ähnliche Richtung zielen auch die Vorgaben des Art. 20 JI-Richtlinie, der den Verantwortlichen zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (auch privacy by design und privacy by default genannt) verpflichtet. Unter die erstgenannte Ausgestaltungsmaxime fällt etwa die Datenminimierung oder ebenfalls die Pseudonymisierung.[1457] So wäre etwa eine Ausgestaltung des Datenabgleichs in einer Weise, die abfragenden Polizist:innen nur eine sehr begrenzte Datenauswahl an die Hand gibt, eine solche Technikgestaltung.[1458] Datenschutzrechtliche Voreinstellungen haben für von der Polizei eingesetzte Datenverarbeitungssysteme Bedeutung.[1459] So kann es schon einen Unterschied machen, welche Daten wie in einem Informationssystem auf einen Suchbefehl angezeigt werden. Hier wäre etwa darauf zu achten, dass nur zweckerforderliche Daten angezeigt werden. Im Zusammenhang mit Datenschutz durch Technikgestaltung ist auch vorgeschlagen worden, eine regelmäßige automatisierte Erkundigung der Polizeibehörden bei den Staatsanwaltschaften über den Stand von relevanten Strafverfahren einzurichten. Damit könnte rechtswidrigen Datenverarbeitungen vorgebeugt werden, die sich daraus ergeben, dass die Polizeien weiter Daten verarbeiten, obwohl das zugehörige Verfahren längst in einer den Rechtsgrund für die Verarbeitung entziehenden Weise beendet worden ist.[1460] Auch beim Datenschutz durch Technikgestaltung ist allerdings eine recht flexible Ausgestaltung der Maßnahmen durch eine offene gesetzliche Formulierung möglich, was jedoch insbesondere im Bereich von Technikregulierung nachvollziehbar ist. Recht breit sind auch die Vorgaben zu technisch-organisatorischen Maßnahmen anlässlich der Verarbeitung besonderer Kategorien personenbezogener Daten, wie sie etwa in § 48 Abs. 2 BDSG vorgeschrieben werden.

1457 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 71 Rn. 1 f.

1458 Zur Gebotenheit einer solchen Gestaltung siehe etwa *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 940: "Es ist nicht zulässig, dass die Polizei beispielsweise im Rahmen einer allgemeinen Verkehrskontrolle den Zugriff auf sämtliche gespeicherten Daten über einen Betroffenen erhält, obwohl dies weder für die konkrete Aufgabe noch zu Fahndungszwecken erforderlich ist. Wenn man es überhaupt für zulässig hält, dass solche Daten in allgemein zugänglichen Fahndungsbeständen erfasst werden, muss zumindest die Einhaltung des Erforderlichkeitsprinzips technisch durch Zugriffsbeschränkungen gewährleistet werden".

1459 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 71 Rn. 4.

1460 BayLfD, 27. Tätigkeitsbericht 2015/2016, S. 60; *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 845.

Eine konkrete technische Maßnahme, die der Kontrolle der Rechtmäßigkeit polizeilichen Informationshandelns dienlich ist, sind die Protokollierungspflichten im Datenumgang, wie sie Art. 25 JI-Richtlinie für automatisierte Verarbeitungssysteme aufstellt, also für einen Großteil der Datenverarbeitung im polizeilichen Informationswesen. So schreibt die auf Bundesebene umsetzende Regelung des § 76 BDSG vor, dass die Verarbeitungsvorgänge der Erhebung, Veränderung, Abfrage, Offenlegung einschließlich Übermittlung, Kombination und Löschung protokolliert werden müssen. Protokolle zu Übermittlungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit und so weit wie möglich – idealerweise lückenlos – die Identität der abfragenden und empfangenden Person festzustellen. Nur so kann – was Zweck der generierten personenbezogenen Protokolldaten ist – die Rechtmäßigkeit der Datenverarbeitung vom Verantwortlichen selbst, zumeist durch den oder die polizeiliche:n Datenschutzbeauftragte:n oder durch die Aufsichtsbehörde, überprüft werden. Die Protokolle können sodann auch zweckändernd in Strafverfahren wegen unrechtmäßiger Datenverarbeitung genutzt werden.[1461] Die Löschungsfrist solcher Protokolldaten – am Ende des auf deren Generierung folgenden Jahres, § 76 Abs. 4 BDSG – ist jedoch problematisch kurz, da vor allem die anlassunabhängigen Kontrollen der Aufsichtsbehörden diesem Turnus nicht unbedingt folgen können.[1462] Im Bereich der polizeilichen Informationsverbundes gelten zudem noch besondere Protokollierungsvorschriften aus § 81 BKAG, wobei die Löschungsfrist noch kürzer bemessen ist, was ebenfalls verfassungs- und unionsrechtswidrig sein dürfte, weil es eine ausreichende prozedurale Sicherung der Datenverarbeitung verhindert. Positiv ist hingegen, dass den polizeilichen Datenschutzbeauftragten die Protokolldaten in elektronisch auswertbarer Form zur Verfügung gestellt werden, was eine effektive Kontrolle fördern dürfte.

Auch der technisch-organisatorischen Dimension des internen Datenschutzkontrollregimes zuzuordnen sind Aussonderungsprüffristen, die der Einhaltung der Löschungsverpflichtung aus § 75 BDSG dienen. Dieses Pflichtenregime ist eine der zentralen Stellschrauben für den Umfang des polizeilichen Informationssystems. Es bestimmt entscheidend darüber mit, wie weit zurück und wie detailliert das polizeiliche Gedächtnis abwei-

1461 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 76 Rn. 5.

1462 Müller/Schwabenbauer in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1044.

chendes Verhalten und damit zusammenhängende Informationen erinnern kann. Damit sind die Aussonderungsprüffristen auch eine Einflussgröße für die Intensität der von der Polizei ausübbaren Sozialkontrolle. Grundsätzlich ist dabei keine laufende Überprüfung des Datenbestandes vorgesehen, weil es die Arbeitskraft der Polizeien übersteigen würde. Stößt jedoch jemand im Rahmen der Sachbearbeitung oder – was wohl praktisch eher der Fall sein wird – im Rahmen eines konkreten Löschungsantrags eines Betroffenen auf die Unrechtmäßigkeit einer Datenverarbeitung, so kann auch abseits der sonst festgelegten Fristen gelöscht werden. Regelmäßig wird jedoch nach einer Fristenregelung verfahren. In der Regel – § 77 BKAG kann hier gut als Maßstab stehen, da die Norm auch für den polizeilichen Informationsverbund gilt – sind dabei die Daten bei Erwachsenen nach zehn, bei Jugendlichen nach fünf und bei Kindern nach zwei Jahren auf ihre mögliche Aussonderung hin zu prüfen. Bei sonstigen Personen im Sinne des § 19 BKAG sind diese Fristen nochmals herabgesetzt (Erwachsene: fünf Jahre, Jugendliche: drei Jahre). Ohne Zustimmung ist die Speicherung dieser Personendaten grundsätzlich auf ein Jahr beschränkt, wobei eine Verlängerung bei weiterem Vorliegen der Voraussetzungen des § 19 Abs. 1 BKAG vorgenommen werden kann. Hier gibt es eine abgestufte Limitierung auf drei, fünf oder zehn Jahre. Danach ist die Speicherung dann zu beenden. Es ist zu betonen, dass es sich bei den übrigen Fristen nicht um Höchstspeicherfristen handelt, nach denen unbedingt zu löschen wäre. Vielmehr ist zu prüfen, ob weiter gespeichert und damit auch verarbeitet werden kann. Mit Ablauf der Fristen ist jedoch regelmäßig von einem Wegfall der Erforderlichkeit auszugehen, wobei eine Prognose ergeben kann, dass es je nach Person und Lebensumfeld nicht ausgeschlossen erscheint, dass es erneut zu einer Straffälligkeit kommen wird.[1463] Insgesamt dürfte damit nicht gerade eine großzügige Löschungspraxis befördert werden, was das polizeiliche Informationswesen eher erinnerungsfähig macht. Dass gilt umso mehr, wenn eine weitergehende Speicherung zur Vorgangsverwaltung möglich ist, diese aber nur unzureichend vor zweckentfremdendem Datenumgang abgeschirmt wird.[1464]

Ein mit der europäischen Datenschutzreform eingeführtes Instrument, das die bisherige Vorabkontrolle ersetzt, ist die Datenschutz-Folgenabschätzung.[1465] Mit ihr sollen bei Verarbeitungsvorgängen mit besonders hohem

1463 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, § 77 BKAG Rn. 16, 18.
1464 Siehe dazu bereits oben S. 254 ff.
1465 *Hansen* in *Brink/H. Wolff*, BeckOK Datenschutzrecht, § 67 Rn. 5.

Risikopotenzial für Betroffene diese Risiken möglichst frühzeitig analysiert und durch entsprechende Datenschutz-Maßnahmen nach Möglichkeit kompensiert werden.[1466] Sie ist immer dann durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge hat (vgl. etwa § 67 Abs. 1 BDSG). So soll eine strukturelle Stärkung des Datenschutzes bewirkt werden.[1467] Grundsätzlich sollen nicht einzelne Verarbeitungsvorgänge, sondern die übergeordneten Systeme und Verfahren zu überprüfen sein und zwar bei der Einführung neuer Verarbeitungssysteme bzw. -verfahren oder wesentlichen Veränderungen an bestehenden.[1468] Insgesamt bleiben die Umstände, die eine Datenschutz-Folgenabschätzung notwendig machen allerdings eher vage.[1469] Allerdings droht im Bereich der Datenverarbeitungstätigkeiten der Polizei- und Strafverfolgungsbehörden regelmäßig ein Eingriff in die Rechtsgüter natürlicher Personen. Insbesondere im Rahmen der repressiven Kriminalitätsbekämpfung, wo die Daten als belastendes Beweismaterial im Strafverfahren verwendet werden sollen, drohen häufig empfindliche Freiheitseinbußen für Betroffene.[1470] Insofern ist im polizeilichen Bereich regelmäßig von einer Gefahr für Betroffene auszugehen.

Im Rahmen einer Datenschutz-Folgenabschätzung sind die jeweiligen Datenschutzbeauftragten zu beteiligen, was diesen wiederum einen maßgeblichen Einfluss auf die Verwirklichung des Datenschutzes in sensiblen und risikoreichen Verarbeitungsbereichen geben kann. Auch inhaltlich sind die Folgenabschätzungen nicht komplett determiniert, müssen aber gewisse Mindestinhalte aufweisen. Dazu gehören eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck, eine Bewertung der Gefahren

1466 *Nolden* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 67 Rn. 2.

1467 *Johannes/Weinhold* in *Sydow* (Hrsg.), Bundesdatenschutzgesetz, § 67 Rn. 14.

1468 *Johannes/Weinhold* in *Sydow* (Hrsg.), Bundesdatenschutzgesetz, § 67 Rn. 14.

1469 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 67 Rn. 2 Das hat auch zur Folge, dass der Einsatz dieses wichtigen Datenschutzinstruments nicht ohne Probleme abläuft, siehe dazu unten S. 398.

1470 *Schwichtenberg* in *Kühling/Buchner,* Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, § 67 Rn. 21 f.

für die Rechtsgüter der betroffenen Personen und schließlich die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll. Nur wenn diese Mindestanforderungen beachtet werden, kann das bewertete System oder Verfahren auf seine Gefahrenträchtigkeit hin eingeschätzt werden. Die getroffenen Maßnahmen zur Risikominimierung müssen, soweit erforderlich, durch den Verantwortlichen überprüft werden, was die Datenschutz-Folgenabschätzung zu einem iterativen Prozess macht.[1471] Da das Risikopotenzial von Verarbeitungsvorgängen von vielen verschiedenen Faktoren bestimmt werden kann, die sich in einem ständigen insbesondere technischen Anpassungsprozess befinden und dann Auswirkungen auf die mit ihnen in Verbindung stehenden Verarbeitungsvorgängen haben können, trägt diese mitlaufende Überprüfungspflicht der Dynamik des polizeilichen Informationswesens in sinnvoller Weise Rechnung.

Neben die Datenschutz-Folgenabschätzung, die bereits teilweise auch der Dokumentation von risikoreichen Verarbeitungsvorgängen dient, tritt nunmehr noch das Verzeichnis von Verarbeitungstätigkeiten, das eine umfassende Dokumentation der im Zuständigkeitsbereich eines Verantwortlichen durchgeführten Datenverarbeitungen leisten soll. Neben der Effektivierung der Datenschutzaufsicht, der dieses Verzeichnis die Kontrolle erleichtern soll, hilft es auch der verantwortlichen Stelle, den Überblick zu behalten.[1472] Ein solches Verzeichnis hat etwa die Kategorien der im polizeilichen Informationsverbund durchgeführten Datenverarbeitungen zu enthalten, aber auch die Datenverarbeitungen in den polizeieigenen Informationssystemen.[1473] Enthalten sein müssen zudem etwa Informationen zum Verarbeitungszweck, zur Verwendung von Profiling (Art. 4 Nr. 4 DS-GVO), zum Verfahren bei Übermittlungen oder auch zur Protokollierung.[1474] Mit dem Wegfall der Dateienstruktur in Teilen des polizeilichen Informationswesens ersetzt das Verzeichnis von Verarbeitungstätigkeiten die bisherigen Errichtungsanordnungen an einigen Stellen,[1475] wodurch der Grad der

1471 *Nolte/Werkmeister* in *Gola/Heckmann/Klug* ua, BDSG, § 67 Rn. 34.

1472 *Paal* in *Paal/Pauly/Ernst* (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, § 70 Rn. 3.

1473 *Ruthig* in *Schenke/Graulich/Ruthig*, Sicherheitsrecht, § 80 BKAG Rn. 4.

1474 *Müller/Schwabenbauer* in *Bäcker/Denninger/Graulich* (Hrsg.), Handbuch des Polizeirechts, G. Rn. 1038.

1475 Etwa im Informationsverbund, nicht hingegen im Regelungsbereich der StPO, vgl. BT-Drs. 19/4671, 46. Allerdings ist dieser Bereich im Vergleich eher von geringerer Bedeutung für das polizeiliche Informationssystem in seiner Gesamtheit.

inhaltlichen Konkretisierung von Datenverarbeitungen absinkt.[1476] Zum Zweck der Selbstkontrolle kann das Instrument aber dennoch nützlich sein, etwa indem durch das Vergegenwärtigen von Zweckbindungen „Überwachungsauswüchse" eingehegt werden.[1477]

3. Abschließende Bemerkungen

Das interne Datenschutzkontrollregime ist in seinem Kern – auch wenn es für seine verschiedenen Instrumente Vorläufer gab – ein Ergebnis der europäischen Datenschutzreform. Dieses unionrechtliche Gesetzgebungspaket hat vor allem eine Prozeduralisierung des Datenschutzes mit sich gebracht.[1478] Das interne Datenschutzkontrollregime ist ein direkter Ausdruck davon, denn es handelt sich dabei ganz überwiegend um eine verfahrensrechtliche Sicherung von Datenverarbeitungsprozessen, die dem Schutz der Betroffenen dient. Wie einleitend erläutert, sind die Regelungen dieses Kontrollsystems und ihre praktische Ausgestaltung überaus relevant für die originäre Polizeiarbeit. Besondere Bedeutung kommt insofern den internen Datenschutzbeauftragten zu, die neben ihren Aufgaben auch in viele der technisch-organisatorischen Maßnahmen des Datenschutzkontrollregimes involviert sind. Sie sind neben den anderen (auch polizeiexternen) Akteuren des Datenschutzes gleichfalls ein wichtiges Element, das dazu beiträgt, „dass Vertrauen und Rechtssicherheit entstehen können und der Umgang mit Daten in einen demokratischen Diskurs eingebunden bleibt."[1479] Auch wenn sie nicht dieselben Möglichkeiten zur Beseitigung von Missständen wie die jeweiligen Aufsichtsbehörden haben, sind die internen Datenschutzbeauftragten aufgrund ihrer Nähe zu den Technologien, Prozessen und Beamt:innen eine zentrale Ressource für die Aufsichtsbehörden. Gleichzeitig sind sie aufgrund ihrer vorgeschriebenen Involvierung in alle wichtigen Datenverarbeitungsprozesse in der Lage, wichtige Steuerungsimpulse für die polizeiliche Informationsverarbeitung zu geben. Ihre Stellung und Einbindung in die Dynamiken des polizeilichen Informationswesens – zumindest wie es sich im jeweiligen Zuständigkeitsbereich darstellt – machen sie außerdem zu einer relevanten Informationsquelle für die tat-

1476 Siehe dazu bereits oben S. 233 sowie unten S. 401.
1477 *Johannes/Weinhold* in *Sydow* (Hrsg.), Bundesdatenschutzgesetz, § 70 Rn. 38.
1478 *Ruthig* in *Schenke/Graulich/Ruthig,* Sicherheitsrecht, Vorb. § 69 BKAG Rn. 1.
1479 So BVerfGE 133, 277 (365) – Antiterrordateigesetz-Urteil in dem etwas engeren, aber angrenzenden Kontext der Transparenz der Datenverarbeitung.

sächlichen Wirkweisen polizeilicher Informationsverarbeitung, worum es im Folgenden gehen soll.