digital | recht

Staat und digitale Gesellschaft

Sebastian Golla

Die kriminalbehördliche Informationsordnung

Band 5

Sebastian Golla

Die kriminalbehördliche Informationsordnung

digital | recht
Staat und digitale Gesellschaft

Herausgegeben von
Prof. Dr. Matthias Bäcker, LL.M.
Prof. Dr. Roland Broemel
Prof. Dr. Thomas Burri, LL.M.
Prof. Dr. Albert Ingold
Prof. Dr. Antje von Ungern-Sternberg
Prof. Dr. Silja Vöneky

Trier, 2024

Band 5

Sebastian Golla, geboren 1988; seit 2020 Juniorprofessur für Kriminologie, Strafrecht und Sicherheitsforschung im digitalen Zeitalter an der Ruhr-Universität Bochum.

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

Dieses Buch steht gleichzeitig als elektronische Version über den Publikations- und Archivierungsserver OPUS der Universität Trier https://ubt.opus.hbz-nrw.de/home und über die Webseite der Schriftenreihe https://digitalrecht-oe.uni-trier.de zur Verfügung.

ISBN: 978-3-75984-835-2
URN: urn:nbn:de:hbz:385-2024080510
DOI: https://doi.org/10.25353/ubtr-4bc8-4b57-9bad

Die Schriftenreihe wird gefördert von der Universität Trier und dem Institut für Recht und Digitalisierung Trier (IRDT).
Anschrift der Herausgeber: Universitätsring 15, 54296 Trier.

UNIVERSITÄT TRIER

IRDT Institut für Recht und Digitalisierung Trier

Vorwort

Mein erster Ansprechpartner für dieses Projekt war *Prof. Dr. Matthias Bäcker* in Mainz. Er hat meinen Blick auf das Sicherheitsrecht geprägt und mich ermutigt, fachsäulenübergreifend zu forschen. Dafür danke ich ihm herzlich.

Der strafrechtlichen Fachgruppe in Bochum bin ich für Unterstützung und regen Austausch verbunden. Besonderer Dank gilt *Prof. Dr. Ingke Goeckenjan,* die die Betreuung der Arbeit übernommen und das Erstgutachten erstellt hat.

Für die Diskussionen über die kriminologischen Fragen der Untersuchung danke ich *Prof. Dr. Tobias Singelnstein.*

Prof. Dr. Julian Krüper danke ich dafür, dass er in sensationeller Geschwindigkeit ein ausführliches Zweitgutachten aus öffentlich-rechtlicher Sicht angefertigt hat.

Im Sommersemester 2024 wurde die vorliegende Arbeit von der juristischen Fakultät der Ruhr-Universität Bochum als Habilitationsschrift angenommen. Literatur und Rechtsprechung wurden bis einschließlich März 2024 berücksichtigt.

Bochum, im Juli 2024 Sebastian Golla

Inhaltsverzeichnis

Einleitung
in die kriminalbehördliche Informationsordnung

Die Polizeien und Staatsanwaltschaften betreiben eine Vielzahl von elektronischen Systemen, in denen sie Informationen speichern und ordnen. Es handelt sich um Informationen über Personen, Gegenstände und Ereignisse. Sie sollen unter anderem dazu verwendet werden, um Straftaten zu verhindern und zu verfolgen. Zu welchem Zweck die Informationen am Ende genau verwendet werden, steht bei ihrer Speicherung noch nicht notwendigerweise fest.

Auch wie viele polizeiliche und staatsanwaltschaftliche Dateien und Informationssysteme es gibt und wie viele Menschen in Deutschland darin erfasst sind, ist kaum abzuschätzen. Nähere Informationen und konkrete Zahlen liegen lediglich zu einzelnen Dateien vor, die auf ein besonderes Interesse der Öffentlichkeit stoßen. Das gilt etwa für die vom Bundeskriminalamt betriebene Datei „Gewalttäter Sport", die regelmäßig in der Berichterstattung reichweitenstarker Medien vorkommt.[1] Aufgrund zahlreicher parlamentarischer Anfragen[2] lässt sich für diese Datei feststellen, dass sich die Zahl der darin erfassten Personen über die letzten Jahre im hohen vierstelligen bis niedrigen fünfstelligen Bereich bewegt.

Die Datei „Gewalttäter Sport" soll vor allem dazu genutzt werden, um gewalttätige Auseinandersetzungen im Zusammenhang mit Fußballspielen zu verhindern. Sie kann aber auch für Zwecke der Strafverfolgung eingesetzt werden.[3] Fußballfans verbinden mit einer Eintragung als Gewalttäter das Risiko, in das Visier der Polizei zu geraten und dadurch verschärften Kontrollen ausgesetzt zu sein sowie gezielt als Gefährder angesprochen zu werden. Dabei ist die Befürchtung verbreitet, nur deshalb eingetragen zu werden, weil man „zur falschen Zeit am falschen Ort" war, ohne tatsächlich gewalttätiges Verhalten an den Tag gelegt zu haben.[4] Eintragungen in die Gewalttäter-Datei und

---

[1] Vgl. etwa kicker.de vom 19. Februar 2021, Woher kommen über 1000 neue „Gewalttäter Sport"?, abrufbar unter https://www.kicker.de/woher-kommen-ueber-1000-neue-gewalttaeter-sport-797805/artikel (alle zitierten Online-Quellen wurden zuletzt am 1. Juli 2024 abgerufen).

[2] Siehe nur LT Nds-Drs. 14/374, S. 4; LT NRW-Drs. 16/5205, S. 2; BT-Drs. 14/721, S. 2; BT-Drs. 16/11934, S. 3; BT-Drs. 19/5195, S. 2; BT-Drs. 19/11842, S. 8; BT-Drs. 19/28886, S. 3.

[3] *Arzt*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 1255.

[4] Arbeitsgemeinschaft Fananwälte, Datei Gewalttäter Sport, abrufbar unter https://www.fananwaelte.de/?page_id=42.

ihre rechtlichen Grundlagen waren bereits Gegenstand mehrerer verwaltungsgerichtlicher Entscheidungen.[5]

Hinsichtlich der Zahl der darin erfassten Personen ist die Datei „Gewalttäter Sport" vergleichsweise groß. Betrachtet man den gesamten Komplex kriminalbehördlicher Dateien und Informationssysteme, ist sie aber nur ein kleiner Mosaikstein. Die vorliegende Untersuchung bezeichnet diesen großen Komplex als kriminalbehördliche Informationsordnung. Als Gegenstand umfasst die kriminalbehördliche Informationsordnung die Gesamtheit der Informationsressourcen jener Behörden, die Straftaten verhindern oder diese verfolgen sollen.[6] Diese Informationsressourcen sind ihrer Art nach vielfältig. Sie können den Zweck haben, Informationen zu speziellen Phänomenen zu sammeln oder als allgemeine Systeme zur Fallbearbeitung und Vorgangsverwaltung dienen. Sie können durch einzelne Behörden oder durch mehrere Behörden gleichzeitig genutzt werden. Insgesamt ist dieses System von Informationsressourcen von großer Bedeutung für die Verfolgung und Verhinderung von Straftaten. Einzelne Systeme und Dateien werden von den Kriminalbehörden routinemäßig abgerufen und prägen so den Verlauf von Verfahren zu Strafverfolgung und Gefahrenabwehr.

Die Bedeutung der Informationsordnung ergibt sich aber nicht nur aus der Summe der einzelnen Dateien und Systeme, die im Einsatz sind. Sie ergibt sich zunehmend auch aus der Vernetzung dieser Ressourcen. Das Bedürfnis, die Inhalte aus verschiedenen Informationsquellen miteinander zu verknüpfen, hat in den letzten Jahren zugenommen. Derzeit sind verstärkte Bemühungen von Kriminalbehörden und technischen Dienstleistern nachzuvollziehen, um Inhalte aus polizeilichen Datenbanken und externen Datenquellen zusammenzuführen und kombiniert auszuwerten. Aus der Sicht der Kriminalbehörden ist dies nachvollziehbar. Die vorhandenen Informationsquellen sollen effektiver zur Abwehr von Gefahren und Verfolgung von Straftaten genutzt werden. Die Bemühungen zur Verknüpfung von Daten und Informationssystemen sind auch eine Reaktion auf Kritik, man habe das vorhandene Wissen in konkreten Fällen nicht gut genug ausgeschöpft.[7]

Den operativen Bedürfnissen der Behörden stehen die Interessen von Bürger*innen entgegen, die durch die Informationsordnung und ihre zunehmende Vernetzung neuen Risiken ausgesetzt sind. Diese Risiken sind noch nicht vollständig ausgeleuchtet. Mit dem Schlagwort Datenschutz sind sie nur unzureichend beschrieben. Die Rechts-

[5] BVerwG NJW 2011, 405 ff.; OVG Lüneburg BeckRS 2009, 31332; OVG Magdeburg BeckRS 2012, 57512; OVG Münster DVBl. 2013, 1460 ff.

[6] Definition der Kriminalbehörden angelehnt an *Bäcker*, in: FS Schenke, S. 331.

[7] Siehe etwa im Zusammenhang mit den Terroranschlägen des NSU und auf den Berliner Weihnachtsmarkt auf dem Breitscheidplatz unten Teil 1 B. V.

streitigkeiten und Diskussionen, die anhand einzelner Systeme wie INPOL und Ressourcen wie der Datei „Gewalttäter Sport" geführt wurden, deuten einige Probleme an: Personen können durch ihre Eintragung in die Systeme unter Umständen stigmatisiert und kriminalisiert werden. Welche Daten erfasst werden und was mit ihnen geschieht, ist für die Öffentlichkeit nur schwer durchschaubar. Auch die Anlässe für eine Erfassung sind nicht ohne Weiteres nachvollziehbar.

Die Intransparenz der Systeme und der Handlungen, die hierin stattfinden, dürfte auch ein Grund dafür sein, warum die kriminalbehördliche Informationsordnung bislang sowohl in tatsächlicher als auch in rechtlicher Hinsicht kaum näher erforscht wurde. Vereinzelt haben sich zwar bereits juristische und kriminologische Untersuchungen mit kriminalbehördlichen Informationsressourcen wie elektronischen Informationssystemen und Kriminalakten befasst.[8] An einer umfassenden Untersuchung der kriminalbehördlichen Informationsordnung fehlt es aber noch. Das mag unter anderem daran liegen, dass die Materie zunächst abstrakt und technisch anmutet. Es leuchtet nicht jedem unmittelbar ein, warum die Strukturierung von Informationssystemen sowie die Ablagerung und Ordnung von Informationen darin einer vertieften eigenständigen Untersuchung bedarf. Um zu zeigen, dass dies der Fall ist und um einige mögliche Probleme der Informationsordnung zu illustrieren, werden im Folgenden zunächst fünf Beispielfälle geschildert (A.). Auf dieser Grundlage werden die Erkenntnisziele der Untersuchung formuliert (B.), bevor ihr Gegenstand eingegrenzt (C.), ihr methodischer Ansatz erörtert (D.) und schließlich ihr Gang beschrieben wird (E.).

A. Beispielfälle

Die folgenden Fälle sind an reale Begebenheiten angelehnt. Sie wurden für die Zwecke dieser Untersuchung vereinfacht und teilweise abgewandelt. Sie sollen einige Probleme veranschaulichen, die in dieser Arbeit eine Rolle spielen. Im Laufe der Untersuchung werden die Beispielfälle immer wieder aufgegriffen.

Fall 1: Erfassung in einer Rauschgiftdatei

A wurde im Jahr 2014 als 18jähriger wegen des Besitzes einer geringen Menge Marihuana polizeilich erfasst. Seitdem ist er in einer bundesweiten polizeilichen Datei eingetragen, die der Bekämpfung der Rauschgiftkriminalität dient. Im Jahr 2022 wird er

[8] Aus juristischer Sicht *Ahlf*, Polizeiliche Kriminalakten, passim; *Rachor*, S. 52 ff.; *Ringwald*, passim; *Zöller*, passim; aus kriminologischer Sicht *Creemers/Guagnin*, KrimJ 2014, 134 ff.; *Jacobs*, passim; *Lageson*, passim.

im Rahmen einem zufälligen Verkehrskontrolle mit seinem Kraftfahrzeug angehalten und überprüft. Bei einer Abfrage seiner Daten erscheint die Information, dass er in der Rauschgiftdatei eingetragen ist. Die kontrollierenden Polizeibeamt*innen befragen A darauf hin, ob er Drogen bei sich führe.

Dieser Fall zeigt, dass auch Straftaten von geringer Bedeutung zu Datenspeicherungen führen können, die für die betroffenen Personen über längere Zeit eine stigmatisierende Wirkung entfalten. Dass A in dem geschilderten Beispiel acht Jahre nach seiner „Jugendsünde" als potentieller Besitzer von Drogen angesprochen wird, dürfte für ihn zumindest nicht angenehm sein. Der Fall ist angelehnt an eine Praxis, die im Zusammenhang mit der bundesweiten Falldatei Rauschgift bekannt wurde. In dieser Datei werden unter anderem Daten über Verstöße gegen das Betäubungsmittelgesetz gespeichert. Die Falldatei Rauschgift geriet Mitte der 2010er-Jahre nach Kontrollen durch die Datenschutzbeauftragten von Bund und Ländern in die Kritik, weil in ihr unverhältnismäßig viele Daten über Bagatellfälle aufgefunden worden waren.[9] Beispielsweise fanden sich bei den Kontrollen durch die Datenschutzaufsicht Einträge zu Personen, die einen einzelnen Joint geraucht hatten oder eine private Feier ausgerichtet hatten, auf der von anderen Personen Drogen konsumiert wurden.[10] Rechtlich stellen sich unter anderem Fragen nach dem notwendigen Anlass für eine Speicherung in einer derartigen Datei und der angemessenen Länge der Speicherdauer.

Fall 2: Freispruch mit Restverdacht

B wurde wegen des sexuellen Missbrauchs eines Jugendlichen angeklagt. Im Hauptverfahren ergeben sich erhebliche Zweifel daran, dass B die ihr vorgeworfene Tat begangen hat. Sie wird freigesprochen; das Urteil wird rechtskräftig. Nach Einschätzung der Staatsanwaltschaft ist der Verdacht, dass B die Tat begangen haben könnte, aber noch nicht ausgeräumt. Die Behörde möchte daher die Information über den Vorwurf gegen B und den aus ihrer Sicht fortbestehenden Restverdacht in einer Datei speichern, die der Strafverfolgung von Sexualstraftäter*innen und ihrer Vorbereitung dient.

In diesem Fall steht der Vorwurf einer potentiell schweren Straftat im Raum, bei dem ein Interesse an einer längerfristigen Datenspeicherung grundsätzlich eher nachvollziehbar ist als bei einem geringfügigen Verstoß gegen das Betäubungsmittelgesetz. Allerdings stellt sich die Frage, wie sich der Umstand, dass B freigesprochen wurde, und die rechtlich gewährleistete Unschuldsvermutung auf die Zulässigkeit einer weiteren

[9] BfDI, Pressemitteilung 18/2016 vom 10. November 2016, Erste gemeinsame Kontrolle der bundesweiten Rauschgiftdatei: Datenschutzbeauftragte beanstanden rechtswidrige Speicherung; vgl. auch *Arzt*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 1259.

[10] BfDI, Pressemitteilung 18/2016 vom 10. November 2016, Erste gemeinsame Kontrolle der bundesweiten Rauschgiftdatei: Datenschutzbeauftragte beanstanden rechtswidrige Speicherung.

Speicherung der Daten auswirken. Wird die Annahme eines „Restverdachts" aufgrund des rechtskräftigen Freispruchs unzulässig? Für B ist die Kategorisierung als mögliche Sexualstraftäterin in einer staatsanwaltschaftlichen Datei jedenfalls potentiell stark beeinträchtigend. In der Praxis haben Datenspeicherungen trotz Freisprüchen und der Einstellung von Verfahren bereits zu gerichtlichen Streitigkeiten geführt.[11] Wie mit derartigen Fällen umzugehen ist, wird näher zu untersuchen sein.

Fall 3: Die Verwechslung

C ist syrischer Staatsangehöriger. Da sein genaues Geburtsdatum unbekannt ist, ist in seiner Aufenthaltserlaubnis als Geburtsdatum der 1. Januar 1990 eingetragen. Der vollständige Name von C besteht, der traditionellen Struktur arabischer Personennamen gemäß, aus vier Teilen. Von diesen vier Teilen sind in der Aufenthaltserlaubnis einer als Vorname und die übrigen als Nachnamen eingetragen. Als C bei einem Ladendiebstahl erwischt wird, erfasst die örtliche Polizeidirektion ihn mit den in der Aufenthaltserlaubnis enthaltenen Angaben zu Name und Geburtsdatum in einer Falldatei. Weil sich Bestandteile des Namens von C in verschiedenen Schreibweisen in das deutsche Alphabet transkribieren lassen, speichert eine Mitarbeiterin der Polizeidirektion einige ihr bekannte alternative Schreibweisen der genannten Namensbestandteile als Aliasnamen in dem System. Dann gleicht sie die zu C erfassten Daten mit den Beständen eines Fahndungssystems ab. Dabei findet sie den Datensatz des D, für den ein Haftbefehl vorliegt. Für D ist ebenfalls der 1. Januar 1990 als Geburtsdatum angeben. Zwei der hinterlegten Familien- und Aliasnamen von D sind mit jenen des C identisch. Die Mitarbeiterin glaubt daher, dass es sich bei C um D handele und der Haftbefehl ihm gelte. Darauf wird C inhaftiert.

Dieser Fall zeigt einige spezielle Probleme bei der Erfassung von Personen in Informationssystemen und der Auswertung von Daten auf. Er ist angelehnt an den Fall des Syrers Amad A., der am 6. Juli 2018 von der Polizei im niederrheinischen Geldern festgenommen und dann aufgrund eines Haftbefehls inhaftiert wurde, welcher nicht ihm galt, sondern einem gewissen Amedy G.[12] Amad A. blieb in Haft, bis es am 17. September 2018 in seiner Zelle in der Justizvollzugsanstalt Kleve brannte. Er erlag wenige Tage später seinen Verbrennungen und Vergiftungen. Die fälschliche Verhaftung und die

[11] Vgl. nur BVerfG NJW 2002, 3231 (3232); BVerwG NJW 2011, 405 (406); OVG Saarlouis ZD 2018, 233 (234).

[12] Vgl. ausführlich zum Sachverhalt LT NRW-Drs. 17/16940, S. 29 f.; Monitor vom 11. Juli 2019, Amad A. – Unschuldig hinter Gittern verbrannt, abrufbar unter https://www1.wdr.de/daserste/monitor/videos/video-amad-a---unschuldig-hinter-gittern-verbrannt-100.html.

Ursachen des Brandes wurden durch einen Parlamentarischen Untersuchungsausschuss in NRW teilweise aufgeklärt.[13] In einer frühen offiziellen Darstellung zu dem Fall war als Grund für die Inhaftierung von Amad A. eine Verwechslung genannt worden. Die Polizei habe bei einer Datenabfrage zu Amad A. den Datensatz von Amedy G. gefunden und Amad A. für jenen gehalten. Nordrhein-Westfalens Innenminister *Herbert Reul* erklärte in einer Fragestunde im Landtag, dass dies auf einem so genannten Kreuztreffer im polizeilichen Informationssystem ViVA (Verfahren zur integrierten Vorgangsbearbeitung und Auskunft) beruht haben könnte. Ein Kreuztreffer wird angezeigt, wenn Personen gemeinsame persönliche Merkmale – wie Familien- und Aliasnamen – aufweisen. Sowohl Amad A. als auch Amedy G. war der Alias „Amed" zugeordnet. Daher könnte das System bei der Suche nach Amad A. den Datensatz von Amedy G. angezeigt haben.

An dieser Darstellung des Sachverhalts entstanden später aus zwei Gründen Zweifel: Erstens hätte die Polizei bei einem Kreuztreffer manuell überprüfen müssen, ob der gefundene Datensatz zu Amad A. passte. Die im Informationssystem hinterlegten Fotos und Beschreibungen von Amad A. und Amedy G. zeigten aber keine Ähnlichkeiten. Zweitens stützen Protokolle der Abfragen der Informationssysteme diese Darstellung nicht. Auf dieser Grundlage entstand der Verdacht, dass die Polizei die betreffenden Datensätze vorsätzlich verändert haben könnte. Anfang Mai 2019 wurde bekannt, dass eine Sachbearbeiterin der Kreispolizei Siegen die Datensätze von Amad A. und Amedy G. bereits zwei Tage vor der Inhaftierung von Amad A. in dem Informationssystem zusammengeführt haben soll.[14] Demnach wäre aus den beiden „Datenbankidentitäten" eine dritte entstanden, der auch der Haftbefehl von Amedy G. zugeordnet wurde. Von diesem Geschehensablauf gingen auch die zuständige Staatsanwaltschaft und der Parlamentarische Untersuchungsausschuss aus.[15]

Der hier vereinfacht dargestellte Sachverhalt veranschaulicht mögliche Risiken durch die ungenaue Speicherung und Auswertung von Daten in polizeilichen Informationssystemen. Die Übereinstimmung von mehreren persönlichen Merkmalen wie Geburtsdatum und Aliasnamen in verschiedenen Datensätzen lässt nicht unbedingt darauf schließen, dass die Personen, auf die sie sich beziehen, identisch sind. Die hinterlegten Daten können je nach Kontext eine völlig unterschiedliche Bedeutung und Aussagekraft haben. So zum Beispiel ein übereinstimmendes Geburtsdatum: Es erscheint in dem vorliegenden Fall nicht als hilfreiches Merkmal zur eindeutigen Identifikation von Personen, da die Angabe des 1. Januar bei ungesicherten Angaben einer üblichen

[13] LT NRW-Drs. 17/16940, S. 1110 ff.

[14] WDR vom 6. Mai 2019, Fall Amad A.: Lag der Polizeifehler in Siegen?, abrufbar unter https://www1.wdr.de/nachrichten/landespolitik/kleve-amada-polizei-100.html.

[15] LT NRW-Drs. 17/16940, S. 1110 f.

Praxis von Ausländerbehörden entspricht. Solche ungesicherten Angaben kommen häufig vor, da es nicht in allen Staaten der Welt üblich ist, den Zeitpunkt der Geburt einer Person tagesgenau zu erfassen. Auch die Praxis zur Erfassung arabischer Namen in Informationssystemen kann Ungenauigkeiten und Verwechslungen begünstigen. Informationssysteme, die Personennamen nach dem europäischen Schema von Vor- und Nachnamen erfassen, sind nicht dafür geeignet, Namen aus allen anderen Kulturkreisen ihrer Struktur nach richtig zu erfassen. Hinzu kommt, dass für die Transkription von Namen aus Sprachen, die nicht das lateinische Alphabet verwenden, in einigen Fällen keine einheitliche Praxis existiert. Kommen mehrere Varianten einer Transkription in Frage und werden – wie in dem vorliegenden Beispielfall – alternative Schreibweisen als Aliasnamen ergänzt, kann das zu Verwechslungen führen.

Die mit diesem Fall aufgezeigten komplexen Herausforderungen und Risiken bei der Erfassung von Personen legen rechtliche Überlegungen zu den genauen Anforderungen nahe, die an die Datenqualität zu stellen sind. Wie kann sichergestellt werden, dass Informationen auch unter Berücksichtigung des Kontextes ihrer Erhebung erfasst werden? Es stellt sich auch die Frage, wie diskriminierende Auswirkungen bei der Speicherung von Personendaten verhindert werden können. Vor allem, wenn bestimmte Risiken bei der Datenspeicherung gerade Personen aus anderen Kulturkreisen betreffen, könnte es notwendig sein, dies schon bei der Gestaltung der Systeme zu berücksichtigen.

Fall 4: Die gescheiterte Sicherheitsüberprüfung

E möchte eine Stelle bei einem Sicherheitsdienst antreten, der unter anderem im Auftrag von Behörden tätig wird. Hierfür erfolgt eine Prüfung der Voraussetzungen für die Aufnahme einer sicherheitsrelevanten Tätigkeit, bei der auch Daten aus dem polizeilichen System INPOL herangezogen werden. E besteht diese Prüfung nicht. Er kann die Stelle daraufhin nicht antreten. Er möchte wissen, ob in INPOL gespeicherte Informationen für das Ergebnis der Prüfung ausschlaggebend waren und welcher Art diese Informationen sind. Daher stellt er einen Antrag auf Auskunft zu den über ihn gespeicherten Daten an das Bundeskriminalamt, das INPOL unterhält. Die Behörde lehnt eine Auskunft ab. Zu E lägen Daten vor, die aber nicht durch das Bundeskriminalamt gespeichert worden seien. Verantwortlich für diese Daten sei allein die „Datenbesitzerin“, die die Informationen abgespeichert habe, aber nicht benannt werden dürfe.

Diesem kafkaesk anmutenden Fall liegt eine Entscheidung des Verwaltungsgerichts Wiesbaden zugrunde, das die Frage nach der Reichweite des Auskunftsrechts des Klägers zunächst dem Europäischen Gerichtshof vorlegte,[16] sein Vorabentscheidungsersuchen aber später zurücknahm.[17] Im Vordergrund standen hierbei konkrete Fragen nach der Reichweite des Auskunftsrechts im Lichte von Art. 8 Abs. 2 Satz 2 GRCh und Art. 15 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (JI-Richtlinie). Allgemeiner betrachtet wirft der Fall ein Schlaglicht auf die Intransparenz der polizeilichen Informationsordnung aus Sicht der Betroffenen. Selbst bei einem förmlich vorgebrachten Auskunftsbegehren wird es E hier schwer gemacht, die Verarbeitung ihn betreffender Daten in einer vernetzten Struktur nachzuvollziehen. Der Fall zeigt auch die schwerwiegenden Auswirkungen auf, die die Speicherung von Informationen in einem kriminalbehördlichen System für den Einzelnen haben kann. Hier hängt von den gespeicherten Daten die Möglichkeit zur Ausübung einer beruflichen Tätigkeit ab. Für die Untersuchung stellt sich die Frage, wie der Problematik der fehlenden Transparenz durch rechtliche und organisatorische Maßnahmen begegnet werden kann.

Fall 5: Die Hass-Datenbank

Zum 1. Februar 2022 wurden die Betreiber*innen sozialer Medien, die in den Anwendungsbereich des Netzwerkdurchsetzungsgesetzes (NetzDG) fallen, gesetzlich dazu verpflichtet, dem Bundeskriminalamt bestimmte Inhalte zu melden, die ihnen von Nutzer*innen als rechtswidrig angezeigt wurden und bei denen Anhaltspunkte für das Vorliegen einer Straftat bestehen. Es sei angenommen, dass das Bundeskriminalamt auf dieser Grundlage eine sechsstellige Anzahl von Meldungen im Jahr erhält. Der größte Teil der gemeldeten Inhalte ist dabei öffentlich im Internet zugänglich. Solche Meldungen, die unter anderem wegen möglicher Fälle von Volksverhetzung und Bedrohungen eingehen, speichert das Amt in einer Falldatei mit dem Titel „Hass und Hetze im Internet".

Die Einträge in der Datei sollen einerseits dazu dienen, um die Verfolgung von Straftaten in den gemeldeten Sachverhalten zu ermöglichen. Sie sollen aber auch in Angelegenheiten des Staatsschutzes zur Abwehr von Gefahren eingesetzt werden, wenn beispielsweise Drohungen gegen Politiker*innen ausgesprochen werden. Die Einträge enthalten neben den Beiträgen aus sozialen Medien die von den Betreiber*in-

[16] VG Wiesbaden, Beschluss vom 30. Juli 2021, 6 K 421/21.WI.

[17] EuGH, Beschluss vom 9. August 2022, Rs. C-481/22, vgl. näher zu dem Fall *Golla/Michel*, in: Thüne/Klass/Feltes, S. 330 ff.

nen dazu gemeldeten IP-Adressen und Namen der Nutzer*innen. Sofern sich aus diesen Angaben keine unmittelbaren Rückschlüsse auf die Identität der Nutzer*innen ergeben, hofft das Bundeskriminalamt, die Identität der Personen aufgrund der verwendeten Pseudonyme, Profilbilder und Sprachmuster feststellen zu können. Dies soll durch einen Abgleich der Inhalte mit weiteren polizeilichen Datenbeständen sowie öffentlich zugänglichen Informationen im Internet erfolgen. Konkret will das Bundeskriminalamt Methoden des maschinellen Lernens einsetzen, um die Verfasser*innen von Texten, die etwa den Tatbestand der Volksverhetzung (§ 130 StGB) erfüllen, anhand ihres „sprachlichen Fingerabdrucks" zu identifizieren.

Dieser weitgehend fiktive Fall orientiert sich an der in § 3a NetzDG geregelten Meldepflicht, auf deren Grundlage es zu einer konsequenteren Strafverfolgung von Hass und Hetze im Internet kommen sollte. Das Bundeskriminalamt rechnete vor der Geltung dieser Pflicht mit etwa 250.000 Meldungen im Jahr.[18] Nachdem das Verwaltungsgericht Köln die Meldepflicht im März 2022 für unionsrechtswidrig erklärte,[19] erscheint es unwahrscheinlich, dass sie in dieser Form jemals Anwendung finden wird.[20] Unabhängig vom Schicksal der konkreten Regelung veranschaulicht der Fall neue Begehrlichkeiten von Kriminalbehörden, die in einer Zeit entstehen, in der sich Freizeitaktivitäten und die Entfaltung der Persönlichkeit zunehmend in den virtuellen Raum verlagern. Hierdurch entsteht eine Masse von neuen Daten, die potentiell für die Behörden relevant und zu großen Teilen sogar ohne besondere Zugriffshürden zugänglich sind. Tatsächlich und rechtlich stellt sich die Frage, wie ein potentiell massenhafter Zufluss von Daten, wie er durch die Meldepflicht entsteht, zu bewältigen und regulieren ist. Auf Seite der Betroffenen sind die Interessen zu beachten, die der Speicherung und Verknüpfung ihrer Daten entgegenstehen können – selbst, wenn diese öffentlich im Internet abrufbar sind. Auch der in dem Fall geplante Einsatz komplexer Methoden zur Verknüpfung von Daten wirft rechtliche Fragen auf. Diese betreffen zwar nicht unmittelbar die Speicherung der Daten, allerdings kann diese auch nicht ganz unabhängig von ihrer späteren Verwendung beurteilt werden.

[18] Tagesschau.de vom 11. Januar 2022, BKA rechnet mit 150.000 Strafverfahren jährlich, abrufbar unter https://www.tagesschau.de/inland/bka-internet-hass-101.html.

[19] VG Köln MMR 2022, 330.

[20] Ab dem 17. Februar 2024 wird allerdings Art. 18 des neuen europäischen Gesetzes über digitale Dienste (Digital Services Act) die Anbieter von Hostingdiensten dazu verpflichten, Informationen über den Verdacht von Straftaten an die zuständigen Behörden zu melden.

B. Erkenntnisziele

Die vorliegende Untersuchung verfolgt drei zentrale Erkenntnisziele. Sie will

I. herausarbeiten, welche eigenständige tatsächliche und rechtliche Relevanz informationsordnende Tätigkeiten der Kriminalbehörden haben,

II. klären, welche konkreten Anforderungen an die kriminalbehördliche Informationsordnung aus Sicht ihrer Anwender*innen bestehen und wie diese durch die Interessen der Informationssubjekte begrenzt werden sowie

III. untersuchen, wie die rechtlichen Grundlagen der kriminalbehördlichen Informationsordnung angepasst werden könnten, um die im zweiten Schritt festgestellten Anforderungen besser als bisher zu erfüllen.

I. Die Relevanz informationsordnender Tätigkeiten

Kriminalbehörden errichten Informationssysteme und speichern Daten hierin. Das ist es, was diese Untersuchung im Kern unter informationsordnenden Tätigkeiten versteht.[21] Sie geht von der These aus, dass diesen Tätigkeiten eine hohe eigenständige tatsächliche und rechtliche Relevanz zukommt. Dies beruht auf der Annahme, dass die Strukturierung von Informationssystemen sowie die Speicherung von Daten hierin spätere Aktivitäten zur Strafverfolgung stark prägen können.

Wie die Gestaltung eines Informationssystems sich auf die spätere Verwendung der darin gespeicherten Daten auswirken kann, zeigt beispielsweise *Fall 3*. Das in diesem Fall verwendete System ist nicht in der Lage, die verschiedenen Schreibweisen und die Struktur arabischer Namen korrekt zu erfassen. Dies führt zu einer Verwechslung mit schweren Folgen für einen Betroffenen. Wie die Speicherung von Daten Personen beeinträchtigen kann, zeigt sich in *Fall 1* und *Fall 4*. In *Fall 1* führt eine lange zurückliegende Datenspeicherung zu einer Ansprache als potentieller Drogenkonsument. In *Fall 4* verhindert das Vorhandensein bestimmter Angaben in einer polizeilichen Datenbank das Bestehen einer Sicherheitsüberprüfung.

Um die Bedeutung informationsordnender Tätigkeiten näher herauszuarbeiten, grenzt die Untersuchung diese von Tätigkeiten der Informationsgewinnung ab, beleuchtet die Stellung kriminalbehördlicher Informationsressourcen in der Sicherheitsarchitektur der Bundesrepublik insgesamt und setzt sich schließlich mit der tatsächlichen Entwicklung der kriminalbehördlichen Informationsordnung auseinander. Auch die rechtliche Relevanz informationsordnender Tätigkeiten wird näher untersucht.

[21] Siehe im Einzelnen unten Teil 1 A. I.

Hierfür wird dargestellt, welche rechtlichen Grundlagen für die Einrichtung von kriminalbehördlichen Informationsressourcen und die Speicherung von Daten hierin auf verfassungsrechtlicher, unionsrechtlicher und einfachgesetzlicher Ebene bestehen. Dabei werden neben Regelungen des Strafprozessrechts auch solche des Polizeirechts und des Datenschutzrechts mit einbezogen.

II. Anforderungen an die kriminalbehördlichen Informationsordnung

Kriminalbehördliche Informationsressourcen werden für die Bedürfnisse ihrer Anwender*innen geschaffen. Sie sollen Polizei und Staatsanwaltschaften dabei unterstützen, die ihnen gesetzlich zugewiesenen Aufgaben zu erfüllen. Die Bedürfnisse der Kriminalbehörden sind komplex. Sie verändern sich mit der Zeit unter anderem aufgrund des technologischen Wandels. So zeigt etwa *Fall 5* exemplarisch die aktuelle Bemühung auf, Daten aus verschiedenen Quellen miteinander zu verknüpfen, um Erkenntnisse für die Strafverfolgung zu gewinnen.

Die vorliegende Arbeit untersucht, welche konkreten Anforderungen kriminalbehördliche Anwender*innen an die Informationsordnung stellen und wie sich diese gewandelt haben. Es soll aber nicht nur die Perspektive der Anwender*innen berücksichtigt werden. Auch die Interessen der Personen, über die Informationen in den Systemen gespeichert werden, sind zu beachten. Die Interessen der Betroffenen können den Interessen der Anwender*innen entgegenlaufen. Dies ist vor allem der Fall, wenn durch die Umsetzung der Anforderungen neue Risiken für sie entstehen. Die oben geschilderten Fälle veranschaulichen als mögliche Risiken beispielhaft die Kriminalisierung (*Fall 1*), die Stigmatisierung (*Fall 4*) und die Verwechslung (*Fall 3*) von Personen.

III. Fortbildung des Informationsordnungsrechts

Der Umgang mit kriminalbehördlichen Informationsressourcen ist bereits rechtlichen Regelungen unterworfen, allerdings ist ihre Dichte nicht besonders hoch. Rechtliche Vorgaben können dazu beitragen, dass kriminalbehördliche Informationssysteme die Anforderungen aus Sicht ihrer Anwender*innen erfüllen. Sie können ihre Funktionen rechtlich absichern. Sie können diese aber auch begrenzen, indem sie die Strukturen und die erlaubte Nutzung von Informationsressourcen einhegen. Dadurch kann das Recht dazu beitragen, dass die Risiken für die betroffenen Informationssubjekte abgemildert werden.

Die Arbeit untersucht rechtsetzungsorientiert, wie eine Änderung bzw. Ergänzung der rechtlichen Regelungen dazu beitragen könnte, den Anforderungen der Anwender*innen sowie den Interessen der in den Systemen gespeicherten Personen besser ge-

recht zu werden als bisher. Sie will auf Grundlage der im Zusammenhang mit dem ersten und zweiten Ziel gewonnenen Erkenntnisse Leitlinien für eine Fortbildung des Informationsordnungsrechts entwickeln.

C. Gegenstand der Untersuchung

Gegenstand der Untersuchung sind die Informationsordnung der deutschen Kriminalbehörden sowie ihre rechtlichen Grundlagen. Der Begriff der Informationsordnung wird dabei in einem handlungsbezogenen und in einem gegenstandsbezogenen Sinne verwendet. Handlungsbezogen bezeichnet die Informationsordnung die Speicherung und Strukturierung von Informationen in dafür vorgesehenen Ressourcen sowie die Errichtung und Einrichtung der Ressourcen selbst.[22] Gegenstandsbezogen umfasst die staatliche Informationsordnung[23] ein System von Datensammlungen, das neben der Strafverfolgung und Gefahrenabwehr so vielfältigen Zwecken wie der Daseinsvorsorge, der Planung und Fiskalverwaltung dient.[24] Die Gesamtheit der Ziele dieses Systems lässt sich mit dem Begriff der Informationsvorsorge[25] umschreiben.

---

[22] Siehe näher zum Begriff der informationsordnenden Tätigkeiten unten Teil 1 A. I.

[23] Das Bundesverfassungsgericht bezeichnet in seiner Rechtsprechung mit dem Begriff der Informationsordnung staatliche Datensammlungen. Dies schließt Sammlungen der Strafverfolgungs-, Polizei- und Sicherheitsbehörden mit ein; vgl. BVerfGE 120, 351 (359). In einem ähnlichen Sinne werden teilweise die Begriffe „Informationsmanagement" und „Datenmanagement" verwendet; vgl. etwa BMI, Polizei 2020, S. 2; *Bull*, iur 1986, 287 (293); *Gärditz*, GSZ 2017, 1 (4); *Rudolph*, S. 9; vgl. zu dem Konzept des Informations- und Wissensmanagements als „Gesamtheit der Maßnahmen zur Schaffung einer ‚intelligenten' Organisation" *Collin/Spiecker gen. Döhmann*, in: Spiecker gen. Döhmann/Collin, S. 3 (6); *Willke*, S. 39 f. Die Begriffe Informationsordnung und Informationsmanagement werden regelmäßig mit dem Ideal einer optimalen Allokation bzw. Verfügbarkeit von Informationen verbunden; vgl. *Beyer*, S. 2, 21; *E. Fuchs*, in: Reinermann, S. 125 (126); siehe dazu näher unten Teil 2 A. Abzugrenzen ist das hier zugrunde gelegte Verständnis des Begriffes der Informationsordnung von einem weiten Verständnis, das die Informationsordnung als Oberbegriff für die rechtliche Regulierung des Informationswesens begreift; so etwa bei *Bull*, S. 30 f.; *Kloepfer*, S. 23 f.; *von Lewinski*, S. 63; *Rogall*, S. 55 f.; *Vesting*, in: FS BVerfG, S. 219 (222 ff.); *Zöllner*, S. 7; vgl. im Überblick zu der uneinheitlichen Verwendung des Begriffes *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts II, § 20 Rn. 4.

[24] Das Erfassen und Ordnen von Daten lässt sich als Charakteristikum des modernen Staats ansehen, das in allen Bereichen zur Verwaltung Ausdruck findet; vgl. *von Lewinski*, in: Seckelmann, S. 107.

[25] Die Informationsvorsorge ist hier anders als bei *Scholz/Pitschas*, S. 103 f. nicht als genuine Staatsaufgabe, sondern als Sammelbegriff für eine Vielzahl von Tätigkeiten zu verstehen. Vgl. kritisch zur „Überhöhung" der Informationsvorsorge zu einer eigenständigen staatlichen Aufgabe *Kowalczyk*, S. 18. Enger, auf den polizeilichen Tätigkeitsbereich bezogen, definiert *Pitschas*, in: Schriftenreihe der Polizei-Führungsakademie 4/91, S. 7 (9) die Informationsvorsorge als „Gesamtheit derjenigen Tätigkeiten, die in Sicherung der

Vorliegend wird nur die Informationsordnung der Kriminalbehörden untersucht. Als Kriminalbehörden sind vor allem Polizeien und Staatsanwaltschaften von Interesse, wobei der größere und wichtigere Teil der vorhandenen Informationssysteme sich bei den Polizeien befindet. Nicht Gegenstand dieser Untersuchung sind das Bundesamt für Justiz und das von ihm nach dem Bundeszentralregistergesetz geführte Zentralregister[26] sowie Informationssysteme anderer Sicherheitsbehörden. Kriminalbehördliche Informationssysteme auf europäischer Ebene wie das Schengener Informationssystem bezieht die Untersuchung am Rande mit ein.[27]

für die Gefahrenabwehr, -erforschung und -vorsorge sowie für die vorbeugende Bekämpfung von Straftaten erforderlichen Informationen von den Polizeibehörden mittels Einsatz entsprechender Informationsquellen, unter Knüpfung polizeiübergreifender ‚Informationsnetze' sowie mittels Einsatz der modernen IuK-Technik verrichtet werden." *Aulehner*, S. 96; *Middel*, S. 332 sowie *Möstl*, S. 212 verstehen unter Informationsvorsorge wiederum schlicht die Datenerhebung und -verarbeitung im Vorfeld von Gefahr und Straftatverdacht.

[26] Vgl. hierzu *Siebrasse*, S. 4 ff.

[27] Siehe unten Teil 1 B. VI.

Die kriminalbehördliche Informationsordnung	*Gegenstandsbezogen*: Gesamtheit der Informationsressourcen jener Behörden, die Straftaten verhindern oder diese verfolgen sollen.
	Handlungsbezogen: Die Speicherung und Strukturierung von Informationen in kriminalbehördlichen Ressourcen sowie die Einrichtung und Ausgestaltung der Ressourcen selbst.
	Informationsordnungsrecht: Gesamtheit der rechtlichen Regelungen, die sich auf die Informationsordnung beziehen.

Von einem besonderen Interesse für die vorliegende Untersuchung sind jene Informationsressourcen bei Polizeien und Staatsanwaltschaften, die auf der elektronischen Datenverarbeitung (EDV) beruhen. Der Umgang mit Informationen einschließlich ihrer Sammlung und Ordnung war schon vor dem Einsatz der EDV ein zentraler Aspekt kriminalbehördlicher Tätigkeiten.[28] Auch heute halten Polizei und Staatsanwaltschaften noch eine Vielzahl von Informationen in Ressourcen fest, die nicht in elektronischer Form vorliegen, etwa in Aktenarchiven oder Handbüchern.[29] Mit dem Einsatz der Computertechnik hat sich das Handlungsfeld der Informationsordnung allerdings grundlegend verändert und seine Bedeutung ist gestiegen.[30] Dies zeigte sich schon in den Anfangszeiten der EDV in den 1960er- und 1970er-Jahren.[31] Gerade die vergleichsweise früh entwickelten polizeilichen Informationssysteme und Datenbanken lassen sich mit *Tobias Singelnstein* als „[erster] Bereich staatlicher Sozialkontrolle, in dem Digitalisierung eine nachhaltige Wirkung gezeigt hat“[32], begreifen.

[28] Vgl. *Baldus*, Die Verwaltung 2014, 1 (9); *Gärditz*, GSZ 2017, 1 (4); *Hornung/Schindler*, in: Gusy/Kugelmann/Würtenberger, S. 247 (252 f.); *Möstl*, DVBl. 2007, 581; *Rusteberg*, in: Brings-Wiesen/Ferreau, S. 191 (197 f.); *Stephan*, VBlBW 2005, 410; *Weßlau*, S. 54; speziell zu Registrierungs- und Identifikationstechniken *Derin/C. Meyer/Wegner*, Bürgerrechte & Polizei/CILIP 121 (4/2020), 3 ff.

[29] Vgl. im polizeilichen Zusammenhang *Grutzpalk*, in: Grutzpalk, S. 15 (24).

[30] Vgl. aus rechtlicher Sicht *Poscher*, Die Verwaltung 2008, 345 (347); *Schulze-Fielitz*, in: FS Schmitt Glaeser, S. 407 (418); aus tatsächlicher Sicht *Busch/Funk/Kauß/Narr/Werkentin*, S. 115 ff.; *Grutzpalk*, in: Grutzpalk, S. 15 (18); *Weßlau*, S. 55.

[31] *Bergien*, Zeithistorische Forschungen, 2017, 258 ff. m.w.N.

[32] *Singelnstein*, in: FS Rogall, S. 725 (729); vgl. zur sozialen Kontrolle durch den Einsatz avancierter Technologien bei der Polizei *Nogala*, S. 145 ff.

D. Methodischer Ansatz

Die kriminalbehördliche Informationsordnung ist nicht nur in tatsächlicher Hinsicht komplex. Sie wirft auch eine Vielzahl juristischer Fragen auf, die unterschiedlichen Rechtsgebieten zuzuordnen sind. Die Speicherung von Daten zu Zwecken der Strafverfolgung ist im Strafprozessrecht geregelt (§§ 481 ff. StPO), allerdings sind hierfür auch das Polizeirecht und das Datenschutzrecht zu berücksichtigen. Regelungen über Datenstrukturen und die behördliche Organisation der Informationsordnung sind in einem verwaltungsrechtlichen Zusammenhang zu betrachten. Dazu spielen jeweils verfassungsrechtliche Grundlagen eine wichtige Rolle.

Um der Vielfalt der berührten Fragen gerecht zu werden und die oben geschilderten Erkenntnisziele zu erreichen, wählt die vorliegende Untersuchung einen methodischen Ansatz, der seine Wurzeln in der Materie des Informationsrechts hat. Dieser Ansatz zielt darauf, die tatsächlichen Zustände (Ist-Zustände) und die erwünschten Zustände (Soll-Zustände) der kriminalbehördlichen Informationsordnung zu identifizieren. Diese Zustände werden miteinander abgeglichen, um Abweichungen von Ist und Soll festzustellen. Auf dieser Grundlage werden Möglichkeiten untersucht, den tatsächlichen Zustand der Informationsordnung ihrem erwünschten Zustand durch rechtliche Regelungen anzunähern.

Im Folgenden werden zunächst die Möglichkeiten eines informationsrechtlichen Ansatzes untersucht, um die formulierten Erkenntnisziele zu erreichen (I.). Im Anschluss wird die konkret ausgewählte und für die Untersuchung angepasste Methode näher beschrieben (II.).

I. Möglichkeiten eines informationsrechtlichen Ansatzes

Das Informationsrecht ist bisher ebenso wie die mit ihm verwandte Rechtsinformatik[33] nicht gerade als ein Gebiet bekannt geworden, aus dem sich wissenschaftlich tragfähige Methoden entwickelt haben. Meist wird der Begriff des Informationsrechts verwendet,

[33] Gegenstand und Selbstverständnis der Rechtsinformatik überschneiden sich teilweise mit dem Informationsrecht. Eine trennscharfe Abgrenzung hat sich nicht durchgesetzt; vgl. *Hilgendorf*, in: Taeger/Vassilaki, S. 1 (3). Klar vom Informationsrecht trennen lässt sich die Rechtsinformatik nur, wenn man sie in einem engen Sinne vor allem als ein Teilbereich der Informatik („Bindestrich-Informatik") versteht, der sich mit dem Einsatz automatisierter Datenverarbeitung zur rechtlichen Zwecken befasst; vgl. *Bull*, iur 1986, 287 (290); *Spiecker gen. Döhmann*, in: Funke/Lachmayer, S. 181 (197). Aufgrund der traditionellen methodischen Verknüpfung mit der Informatik erscheint es konsequent, die Rechtinformatik vorrangig als technische Disziplin einzuordnen.

um eine Querschnittsmaterie[34] zu beschreiben, die die Summe aller Rechtsnormen umfasst, die sich auf Informationen[35] bzw. den Umgang[36] mit ihnen beziehen.[37] Ein wenig eingrenzen lässt sich das Gebiet, wenn man es auf den Umgang mit Informationen mittels moderner technischer Hilfsmittel beschränkt.[38] Insofern ließe sich auch von einem Informationstechnikrecht[39] sprechen, das nicht nur der Natur von Informationen, sondern auch technologischen Dynamiken auf besondere Weise Rechnung trägt.

[34] Vgl. *Bull*, iur 1986, 287 (288); *Hoeren*, Internetrecht, 3. Aufl. 2018, Rn. 3; *Kloepfer*, S. 29; *Sieber*, NJW 1989, 2569 (2579); *Spiecker gen. Döhmann*, in: Vesting/Korioth, S. 263 (281); *G. Sydow*, NVwZ 2008, 481 ff.

[35] Vgl. zur Notwendigkeit der Klärung des Informationsbegriffs in diesem Zusammenhang *Hilgendorf*, in: Taeger/Vassilaki, S. 1 (7); *Sieber*, NJW 1989, 2569 (2572).

[36] Teilweise wird ausdrücklich der menschliche Umgang mit Informationen in das Zentrum der Betrachtung gerückt; vgl. etwa *Werckmeister*, DVR 1978, 97 (98). Dies ergibt Sinn, weil der Adressat informationsrechtlicher Regelungen stets derjenige sein wird, der mit Informationen umgeht und das menschliche Verhalten den Fixpunkt der Rechtsordnung insgesamt darstellt; vgl. ähnlich zu der Regelung des Umgangs mit Technik *Lepsius*, VVDStRL 2004, S. 264 (278); *Heymann/Wengeroth*, in: Beck/Bonß, S. 106, 116 ff.; *Popitz*, S. 160; zum Recht als normative Ordnung menschlichen Verhaltens *Kelsen*, S. 4 ff.

[37] Vgl. *Bull*, iur 1986, 287; *Hilgendorf*, in: Taeger/Vassilaki, S. 1 (6); *Werckmeister*, DVR 1978, 97 (98 f.); spezifischer *Sieber*, NJW 1989, 2569 (2574). Es lässt sich dabei zwischen explizitem und implizitem Informationsrecht unterscheiden. Explizit informationsrechtliche Regelungen sind solche, die Vorgaben an Informationsverarbeitungsvorgänge oder Informationsstrukturen enthalten. Implizit informationsrechtliche Vorgaben sind solche, „die nicht unmittelbar ihren Informationsbezug auf die Stirn geschrieben haben, die aber Steuerungsauswirkungen auf Informationsflüsse haben"; *Burkert*, in: GS Steinmüller 2014, S. 177 (185); vgl. ähnlich *Albers*, Rechtstheorie 2002, 61 (78). Zu den explizit informationsrechtlichen Regelungen gehören etwa Gesetze über Datenschutz und IT-Sicherheit, zu den implizit informationsrechtlichen Vorgaben etwa die Kompetenzregelungen des Grundgesetzes.

[38] In diese Richtung *Sieber*, NJW 1989, 2569 (2573).

[39] Vgl. zu dem Begriff des Informationstechnikrechts *Spiecker gen. Döhmann*, in: Funke/Lachmayer, S. 181 (187). Der weite Begriff des Informationsrechts vernachlässigt, dass das rechtliche Interesse an einer spezifischen Betrachtung von Informationen besonders von technischen Entwicklungen getrieben ist. Auf der anderen Seite vermeidet der weite Ansatz eine Einengung der Betrachtung auf bestimmte Technologien.

Aber auch das so eingegrenzte Informationstechnikrecht bleibt ein weites Feld.[40] Als eigenständiges Rechtsgebiet steckt das Informationsrecht auch nach mehr als fünfzig Jahren[41] noch in einer Findungsphase.

Ursprünglich wurde es unter anderem als Aufgabe des Informationsrechts angesehen, rechtsdogmatische Grundlagen zu etablieren, um Informationsordnungen und Informationsflüsse in einzelnen Bereichen zu betrachten.[42] Aus ihm heraus sollten Methoden entwickelt werden, um rechtlich mit dem informationstechnischen Fortschritt umzugehen.[43] Auch wenn dies bisher kaum gelungen ist,[44] will die vorliegende Untersuchung diesen Faden aufgreifen. Das Informationsrecht bietet Ansätze, um die Auswirkungen technischer Entwicklungen auf das Recht zu erfassen und für seine Fortbildung zu berücksichtigen.

Die kriminalbehördliche Informationsordnung als Gegenstand dieser Untersuchung ist von einer besonderen informationstechnischen Dynamik geprägt. An dem Gegenstand lassen sich komplexe Wechselwirkungen gesellschaftlicher, technologischer und rechtlicher Entwicklungen nachvollziehen, die in dieser Arbeit näher untersucht werden sollen.[45] Die Untersuchung erfolgt auf Grundlage der These, dass die informationstechnische Dynamik dazu führt, dass die tatsächliche und rechtliche Rele-

---

[40] Bisher hat sich keine klare Eingrenzung des Informationsrechts durchgesetzt. Durch die Allgegenwärtigkeit von Informationen und die Notwendigkeit ihrer differenzierten Behandlung als Regelungsgegenstand stellt sich auch die Frage, inwiefern es überhaupt möglich ist, allgemeine Grundsätze bzw. eine umfassende Dogmatik zu der rechtlichen Behandlung von Informationen jenseits spezifischer Regelungsgebiete zu entwickeln. Ein sich vollständig „aus den bestehenden Rechtsdisziplinen herauslösendes" Informationsrecht (*Werckmeister*, DVR 1978, 97 (99)) erscheint nur als theoretisches Konstrukt möglich bzw. ist jedenfalls mit der „Gefahr eines Verlusts an dogmatischer Differenziertheit" verbunden (*Hilgendorf*, in: Taeger/Vassilaki, S. 1 (9).). Vor diesem Hintergrund erscheint auch das – rechtspolitisch derzeit nicht mehr aktuelle – Projekt eines Informationsgesetzbuches als problematisch und dessen Scheitern wenig verwunderlich; vgl. *Augsberg*, S. 1 f.; *Schoch*, VVDStRL 1997, S. 160 (163 f.).

[41] Die ersten Versuche, das Informationsrecht als eigene Disziplin zu etablieren, stammen aus den späten 1960er und frühen 1970er-Jahren, als die Computertechnik in erstmals Einsatz in der Verwaltung fand. In der gleichen Zeit liegen die Wurzeln der deutschen Rechtsinformatik; vgl. *Dumortier*, in: FS Kilian, S. 59; *Hoeren*, Internetrecht, 3. Aufl. 2018, Rn. 12; *Fiedler*, JuS 1970, 432; *Kilian*, CR 2017, 202 ff.; vgl. zu den früheren Entwicklungen der Rechtskybernetik und der US-amerikanischen Rechtsinformatik *Hoeren*, JuS 2002, 948 (948 f.).

[42] Vgl. *Burkert*, in: GS Steinmüller, S. 177 (182); *Fiedler*, JZ 1966, 689 (693).

[43] Vgl. *Hoeren*, JuS 2002, 947 (949 f.); *Hoeren*, in: Duve/Ruppert, S. 212 (226); *Knackstedt/Eggert/Gräwe/Spittka*, MMR 2010, 528 (530); *Möstl*, DVBl. 2007, 581 (586).

[44] Auch die Rechtstheorie hat Ansätze zum Umgang mit informationstechnischen Entwicklungen bisher nicht überzeugend integrieren können; vgl. *Hilgendorf*, in: Taeger/Vassilaki, S. 1 (9).

[45] Vgl. zu der Untersuchung der Wechselwirkungen zwischen Recht und Technik anhand von vielfältigen Gegenständen wie Dampfkesselanlagen, der Kernenergie und Weltraumwaffen *Berg*, JZ 1985, 401; *Bull*, Der Staat 2019, 57 f.; *Nicklisch*, NJW 1986, 2287 (2288) sowie grundlegend *Boehme-Neßler*, in: Hill/Schliesky, S. 237 (238 ff.); *Spiecker gen. Döhmann*, in: Funke/Lachmayer, S. 181 (183 ff.).

vanz der Einrichtung und Verwendung von Informationssystemen in Kriminalbehörden steigt. Es wird auch angenommen, dass diese Dynamik bedingt, dass sich die Anforderungen an die Informationssysteme sowie die aus ihrer Nutzung folgenden Risiken für die Betroffenen verändern. Der sogleich näher beschriebene informationsrechtliche Ansatz dieser Arbeit soll einen Rahmen dafür bieten, die konkrete informationstechnische Dynamik genauer zu erfassen und hieraus Folgerungen für die Fortbildung des Rechts zu ziehen.

Zur grundlegenden Erfassung dieser Dynamik werden Erkenntnisse aus der Techniksoziologie sowie den Science & Technology Studies herangezogen. Die Forschung in diesen Feldern geht weitgehend von einer untrennbaren Verbindung bzw. Ko-Evolution gesellschaftlicher und technischer Entwicklungen aus.[46] Technik ist in diesem Zusammenhang als sozialer Konstruktionsprozess zu begreifen.[47] Demnach lösen technologische Entwicklungen allein zwar keinen sozialen Wandel aus, ermöglichen diesen aber zumindest.[48] Die Betrachtung technischer Entwicklungen als soziale Konstruktionsprozesse lässt sich für juristische Untersuchungen fruchtbar machen.[49] Sozio-technische Entwicklungen treiben die Entwicklung des Rechts auf der einen Seite an und

[46] Vertreter der Techniksoziologie führten in den 1980er- und 1990er-Jahren zunächst Grundsatzdiskussionen darüber, ob die Prägung der Gesellschaft durch technische Entwicklungen (Technikdeterminismus) oder die Prägung der Technik durch gesellschaftliche Faktoren (Sozialdeterminismus) die dominante Logik im Verhältnis von Technik und Gesellschaft sei. Die einseitig deterministischen Ansätze konnten sich nicht allerdings nicht durchsetzen; vgl. *Dolata/Werle*, in: Dolata/Werle, S. 15 ff.; *Weyer*, S. 31 ff. jeweils m.w.N.

[47] *Pinch/Bijker*, in: Bijker/Hughes/Pinch, S. 17 (24 ff.); *Rammert*, S. 4 ff.; *Weyer*, S. 32; vgl. auch *Lepsius*, VVDStRL 2004, S. 264 (279).

[48] *Weyer*, S. 34; vgl. auch *Dolata/Werle*, in: Dolata/Werle, S. 15 (37); *Disco/van der Meulen*, in: Disco/van der Meulen, S. 1 (2 ff.).

[49] Dass „[t]echnisches Handeln und technische Sachverhalte [...] im Recht immer erst als soziales Handeln und als soziale Sachverhalte von Belang" werden, stellte *Huber*, S. 8 bereits 1959 fest. Andere frühe Untersuchungen des Verhältnisses von Technik und Recht legen hingegen eher eine dominante Rolle der Technik zugrunde; vgl. etwa *Forsthoff*, S. 33 ff., der die technische Realisation „vermöge der ungeheuren Akzeleration und Intensitätssteigerung, die sie in den letzten Jahrzehnten erfahren hat" als gegenüber der sozialen Realisation prädominant beschreibt; vgl. zu der These vom Machtzerfall des Staates im Angesicht der Entfaltung der modernen Technik *R. Wolf*, Leviathan 15 (1987), 357. Aus jüngerer Zeit beziehen sich etwa die Untersuchungen der Kasseler Schule zur sozial- und verfassungsrechtlichen Technikgestaltung ausführlich auf den sozialen Handlungskontext technischer Entwicklungen; vgl. *Roßnagel/Wedde/Hammer/Pordesch*, S. 34. Ein ähnliches Verständnis legt *Hoffmann-Riem*, S. 238 zugrunde, nach dem das Recht mit Blick auf verschiedene Innovationen – ob technischer, gesellschaftlicher oder sonstiger Art – nicht „nur als eine Art Black Box", sondern auch als ein Spiegel dieser Entwicklungen zu betrachten ist. Dies ermögliche es, passende rechtliche Reaktionen auf technische Entwicklungen zu entwickeln und „Differenzierungspotentiale des Rechts zu nutzen."

setzen dieses bisweilen unter Druck. Das Recht reagiert dabei auf technische Entwicklungen und wird von diesen in Form[50] und Inhalt mitgestaltet. Letzteres geschieht entweder durch gesetzgeberische Intervention[51] oder weil sich der Bedeutungsgehalt von Normen unmittelbar durch technische Entwicklungen verändert.[52] Auf der anderen Seite können rechtliche Vorgaben den Einsatz und die Entwicklung von Technologien in gewissen Grenzen[53] formen bzw. sogar gezielt steuern.[54] Das Recht steht dabei vor der komplexen Aufgabe, technologische Entwicklungen je nach ihren möglichen Auswirkungen sowohl einzuhegen als auch zu fördern.[55] Selten können die Auswirkungen technologischer Entwicklungen einseitig als positiv oder negativ bewertet werden. Dies zeigt sich auch an der kriminalbehördlichen Informationsordnung, deren technische Weiterentwicklung zur Gewährleistung der öffentlichen Sicherheit und effektiven Strafverfolgung beitragen, aber auch neue Risiken für Bürger*innen schaffen kann.

Die vorliegende Untersuchung will durch die Anwendung eines informationsrechtlichen Ansatzes in erster Linie die oben beschriebenen Erkenntnisziele erreichen. Daneben will sie aber auch einen Beitrag zu der rechtswissenschaftlichen Methodik leisten,

---

[50] Die Veränderung rechtlicher Formate kann sich wiederum in der inhaltlichen Entwicklung des Rechts niederschlagen. Dies zeigt sich an den Trägermedien des Rechts. Die Verkörperung von Gesetzen und juristischen Texten auf Papyrus ermöglichte im Vergleich zu der Verkörperung auf Tontafeln mehr Ausführlichkeit und rechtliche Komplexität; *Boehme-Neßler*, in: Hill/Schliesky, S. 237 (239). Die Erfindung des modernen Buchdrucks durch *Johannes Gutenberg* Mitte des 15. Jahrhunderts wirkte sich ebenfalls grundlegend auf die Verbreitung und Wirkung des (kodifizierten) Rechts aus; vgl. *Berg*, JZ 1985, 401 (403). Ob jüngere oder noch ausstehende technische Entwicklungen wie die elektronische Datenverarbeitung oder die Entwicklung leistungsfähiger künstlicher Intelligenzen in ihren Auswirkungen auf das Recht mit der Erfindung des Buchdrucks vergleichbar sind, wird sich zeigen. Dass diese Entwicklungen aber neue Ausdrucksformen des Rechts befördern und ermöglichen, lässt sich aber nicht abstreiten; vgl. etwa zu eines automatisierten „Vollvollzugs" des Rechts mittels moderner Technologien *Rademacher*, JZ 2019, 702 ff.

[51] Im sicherheitsrechtlichen Kontext beispielsweise werden technische Entwicklungen immer wieder als Grund für die Notwendigkeit der Ausweitung behördlicher Aufgaben und Befugnisse angegeben; vgl. *Riegel*, DVBl. 1987, 325 (328).

[52] Dies ist am Anwendungsbereich strafprozessualer und polizeirechtlicher Ermittlungsbefugnisse nachvollziehen; vgl. EGMR (Große Kammer), Urteil vom 4. Dezember 2008, S. u. Marper gegen Vereinigtes Königreich, No. 30562/04 und 30566/04 § 71 = NJOZ 2010, 696 (698); *Aden/Fährmann/Bosch,* KrimJ 2020, 135 (143 f.); *Hoffmann-Riem*, S. 559; *Molnar*, Surveillance & Society 2017, 381 (383); *Poscher*, Die Verwaltung 2008, 345 (347).

[53] Die Wirkungsmacht rechtlicher Vorgaben gegenüber technischen Entwicklungen ist naturgemäß unvollkommen; vgl. *Boehme-Neßler*, in: Hill/Schliesky; S. 237 (257); *Murswiek*, VVDStRL 1990, S. 207 (228).

[54] Vgl. *Schuhr*, Rechtstheorie 2015, 225 (240); *Spiecker gen. Döhmann*, in: Hill/Schliesky, S. 137 (140); *Spiecker gen. Döhmann*, in: Funke/Lachmayer, S. 181 (182).

[55] *Bull*, Der Staat 58 (2019), 57 (63); *Gärditz*, Der Staat 54 (2015), 113 (126 f.); *Murswiek*, VVDStRL 1990, S. 207 (209); *Ronellenfitsch*, DVBl. 1989, 851 (852); vgl. speziell zu dem Aspekt der Förderung *Boehme-Neßler*, in: Hill/Schliesky, S. 237 (240); *Kitschelt*, in: Grimm, Staatsaufgaben, S. 391 (392), *Trute*, in: Isensee/Kirchhof, Handbuch des Staatsrechts IV, 3. Aufl. 2006, § 88 Rn. 18 ff.

um stark informationstechnisch geprägte Bereiche des Rechts zu untersuchen. Die bereichsspezifische Erprobung eines informationsrechtlichen Ansatzes kann zwar keine grundlegenden methodischen Lücken schließen, aber zumindest ein Anwendungsbeispiel liefern. Die Weiterentwicklung des Informationsrechts ist schon aufgrund der schieren Weite der Materie neben einer Betrachtung seiner zentralen Bestandteile[56] und allgemeiner Teilfragen auf bereichsspezifische Untersuchungen angewiesen.[57] Auch für das Strafprozess- und Polizeirecht bedarf es spezifischer informationsrechtlicher Ansätze, um die Besonderheiten der Regelungen zur Informationsverarbeitung betrachten und den Wandel der Regelungsstrukturen erfassen zu können.[58]

Mit ihrem konkreten Ansatz sucht die Arbeit Anschluss an Ansätze zur Abgrenzung eines Sicherheitsinformationsrechts und eines polizeilichen Informationsrechts[59] unter Berücksichtigung des besonderen Verwaltungsrechts.[60] Überlegungen zur Abgrenzung eines polizeilichen Informationsrechts kamen zunächst auf, als die informationellen Befugnisse der Polizei nach dem Volkszählungsurteil des Bundesverfassungsgerichts gesetzlich geregelt wurden.[61] Aktuell geben unter anderem die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (JI-Richtlinie) und ihre Umsetzung Anlass zu einer näheren Betrachtung des polizeilichen Informationsrechts auf nationaler und europäischer Ebene.

---

[56] Als zentrale Bestandteile lassen sich vor allem die Regelungen zu Datenschutzrecht und Informationsfreiheitsrecht begreifen, die sich praktisch zu Fixpunkten des Informationsrechts entwickelt haben.

[57] *Albers*, Rechtstheorie 2002, 61 (89); *Hilgendorf*, in: Taeger/Vassilaki, S. 1 (9); kritisch zu dieser „Referenzgebietsmethodik" hingegen *Augsberg*, S. 4, der auf die Gefahr eines hermeneutischen Zirkels verweist.

[58] Ähnlich *Möstl*, DVBl. 2007, 581 (582); vgl. auch *Gärditz*, GSZ 2017, 1 (4), nach dem „eine kohärente sicherheitsverfassungsrechtliche Dogmatik für Informationseingriffe bislang Desiderat geblieben" ist.

[59] *Möstl*, DVBl. 2010, 808; *Peitsch*, Die Polizei 1991, 305 ff.; *Würtenberger*, in: FS Steiner, S. 948 ff.; vgl. auch *Riegel*, Die Polizei 1991, 1 (2 ff.).

[60] Zwar lassen sich Verwaltungen schon seit jeher als „informationsverarbeitende Systeme" (*Albers* in: Spiecker gen. Döhmann/Collin, S. 50 (52) und ihrer Verfahren als „Prozesse der Informationsgewinnung und -verarbeitung" (*Collin/Spiecker gen. Döhmann*, in: Spiecker gen. Döhmann/Collin, S. 3 (8)) begreifen. In der verwaltungsrechtlichen Dogmatik spielte der Umgang mit Informationen und Wissen jedoch lange eine eher untergeordnete Rolle. Ansätze zur Herausbildung eines Informationsverwaltungsrechts lassen sich verstärkt seit den 1990er-Jahre nachzuvollziehen; vgl. dazu nur *Augsberg*, passim; *Gurlit*, DVBl. 2003, 1119 (1131 ff.); *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts II, § 20 Rn. 1 ff. Die Betrachtungen konzentrierten sich zunächst vor allem auf Aspekte des Datenschutz- und Informationsfreiheits- bzw. Informationszugangsrechts. Es kamen dann Themen wie das staatliche Informationshandeln (etwa in Form von Warnungen oder Empfehlungen) und der Umgang mit Wissen hinzu.

[61] Vgl. *Neumann*, S. 14 ff.; *Peitsch*, ZRP 1992, 127; *Pitschas*, ZRP 1993, 174.

II. Konkreter Ansatz

Die in dieser Untersuchung konkret angewandte Methode lehnt sich an den St. Galler Ansatz zum Informationsrecht an. Der St. Galler Ansatz verbindet eine juristische Methodik mit einer Methodik der Anwendungsinformatik, um informationsrechtliche Regelungen weiterzuentwickeln.[62] Er vergleicht den tatsächlichen Zustand von Vorgängen der Informationsverarbeitung mit ihrem erwünschten Zustand im Sinne einer möglichst effizienten Verarbeitung. Auf Grundlage des Ergebnisses dieses Abgleichs betrachtet er bei Abweichungen Möglichkeiten, um den Ist-Zustand durch rechtliche Regelungen an den Soll-Zustand heranzuführen.[63]

Nach einer Vorbemerkung über die Gewinnung von Informationen über die Ist- und Soll-Zustände (1.) wird die modifizierte Variante des St. Galler Ansatzes, die in dieser Untersuchung zum Einsatz kommt, in ihren drei Arbeitsschritten vorgestellt (2. bis 4.).

1. Gewinnung von Informationen über Ist- und Soll-Zustände

Der St. Gallener Ansatz zum Informationsrecht basiert auf der Feststellung von Ist- und Soll-Zuständen von Vorgängen der Informationsverarbeitung. Um diese Zustände für die kriminalbehördliche Informationsordnung zu beschreiben, können zunächst vorhandene wissenschaftliche Untersuchungen und behördliche Informationen herangezogen werden. Aufgrund der Komplexität der kriminalbehördlichen Informationsordnung und der vergleichsweise dünnen Quellenlage zu diesem Themenbereich erscheint dies aber nicht ausreichend. Daher sollen zusätzlich Informationen aus einer eigenen qualitativen Forschung genutzt werden.

Für diese Untersuchung wurden fünf leitfadenorientierte Interviews mit Mitarbeiter*innen unterschiedlicher Datenschutzaufsichtsbehörden geführt, die für die Kontrolle der Datenverarbeitung im kriminalbehördlichen Bereich zuständig sind.[64] In drei weiteren leitfadenorientierten Interviews kamen Mitarbeiter*innen unterschiedlicher Polizeibehörden zu Wort, welche in ihrer Tätigkeit schwerpunktmäßig mit der Einrichtung und Auswertung polizeilicher Informationsressourcen befasst sind.[65] Dies reichte von Tätigkeiten, die stark mit der Nutzung derartiger Systeme verknüpft sind (POL2, POL3) – wie etwa als Datenanalyst – bis zu der fachlichen Verantwortlichkeit für die

[62] *Burkert*, in: GS Steinmüller, S. 177 (182).

[63] *Burkert*, in: GS Steinmüller, S. 177 (182 ff.); vgl. auch *Gasser/Burkert/Thouvenin/Nolan*, in: FS Weber, S. 469 (478 ff.).

[64] Im Verlauf der Arbeit werden die Interviews mit den Codes DSA1-DSA5 referenziert. Der Leitfaden für die Interviews findet sich im Anhang der Arbeit.

[65] Im Verlauf der Arbeit werden die Interviews mit den Codes POL1-POL3 referenziert. Der Leitfaden für die Interviews findet sich im Anhang der Arbeit.

Informationssysteme in der jeweiligen Polizeibehörde (POL1). Die Auswahl der Interviewten und einbezogenen Behörden erfolgte unter Beachtung einer möglichst großen Diversität, besonders hinsichtlich ihrer Struktur und ihrer geographischen Lage.

Die Interviews mit den Mitarbeiter*innen von Aufsichtsbehörden konzentrierten sich inhaltlich vor allem auf die polizeiliche Datenverarbeitung. Die Interviewpartner*innen wurden zunächst zu ihrer Kontrolltätigkeit im Zusammenhang mit polizeilichen Informationsressourcen befragt. Darauf folgten zunächst offene und dann konkretere Fragen zu Problemen bei der Nutzung und Kontrolle von Informationsressourcen, die den Interviewten bei ihrer praktischen Tätigkeit bekannt geworden waren. Die Interviewten bekamen unter anderem Gelegenheit, Risiken für die von der Datenverarbeitung betroffenen Personen und die aus ihrer Sicht bestehenden Möglichkeiten, um diese Risiken abzumildern, zu schildern. Die Interviewten berichteten sowohl von Fällen, in denen sie Beschwerden von Betroffenen nachgegangen waren als auch von Fällen, in denen sie proaktiv Informationsressourcen der Polizei kontrolliert hatten.

Die Interviews mit Mitarbeiter*innen der Polizei dienten primär dazu, deren Anforderungen an die Informationsordnung, aber auch aktuelle Probleme und Risiken beim Umgang mit Informationssystemen zu identifizieren. Die Interviewten wurden zunächst zu ihren konkreten Tätigkeiten im Zusammenhang mit polizeilichen Datenbanken befragt. Im Anschluss bekamen sie durch offene und dann konkretere Fragen die Gelegenheit, ihre Anforderungen an die Informationsressourcen zu beschreiben und dabei auch Herausforderungen und Probleme zu schildern. Die Gewinnung von Mitarbeiter*innen der Polizei für die Interviews war deutlich mühsamer als jene von Mitarbeiter*innen der Datenschutzaufsicht. Daraus erklärt sich die geringere Anzahl der durchgeführten Interviews im polizeilichen Bereich. Während fünf von sechs angefragten Datenschutzaufsichtsbehörden Interviews mit den zuständigen Mitarbeiter*innen ermöglichten, führten zehn Anfragen bei verschiedenen Polizeibehörden zu nur drei Interviews. Dabei wurden die Anfragen größtenteils ohne Begründung abgelehnt oder blieben unbeantwortet. Zwei Anfragen wurden nach ursprünglicher Interessensbekundung an der Materie abgelehnt, nachdem innerbehördliche Rücksprache erfolgt war. Eine dieser Anfragen wurde mit der mündlich erteilten Begründung abgelehnt, dass sich innerhalb der Behörde – einem Landeskriminalamt – niemand fände, der sich in der Lage sehe, zu der komplexen Materie Auskunft zu geben.

Die Auswertung sämtlicher Interviews wurde nach der Methode der qualitativen Inhaltsanalyse nach *Philipp Mayring* durchgeführt.[66] Sie erfolgte mit dem primären Ziel, die von den Interviewten geschilderten Ist- und Soll-Zustände zusammenzufassen.

[66] *Mayring*, S. 11 ff.

2. Der Ist-Zustand der kriminalbehördlichen Informationsordnung

Der Ist-Zustand wird durch die Beschreibung des Vorgangs oder der Vorgänge der Informationsverarbeitung festgestellt, auf die der St. Gallener Ansatz angewendet werden soll. Vorliegend geht es um die Speicherung von Daten in kriminalbehördlichen Systemen sowie die Einrichtung dieser Systeme. Die Untersuchung betrachtet den Gesamtkomplex der kriminalbehördlichen Informationsordnung, seine historische Entwicklung und seine Stellung in der Sicherheitsarchitektur der Bundesrepublik. Ein wichtiger Aspekt der Untersuchung ist auch, wie tatsächlich mit den einschlägigen Systemen gearbeitet wird. Hierfür dienen besonders die für diese Untersuchung geführten Interviews mit Mitarbeiter*innen unterschiedlicher Polizeibehörden als Informationsquellen.

Die kriminalbehördliche Informationsordnung befindet sich derzeit im Wandel. Durch die Umsetzung des Programmes Polizei 20/20 soll der polizeiliche Informationsverbund grundlegend verändert und modernisiert werden.[67] Soweit die Perspektiven hierzu konkret absehbar sind, werden sie bereits bei der Feststellung des Ist-Zustandes mit berücksichtigt.

3. Der Soll-Zustand der kriminalbehördlichen Informationsordnung

Der Soll-Zustand ergibt sich nach dem St. Gallener Ansatz aus zwei Komponenten: Einem Soll-Zustand nach dem Modell eines möglichst effektiven Informationsflusses und einem Soll-Zustand aus rechtlich-normativer Sicht. Aus diesen beiden Komponenten wird ein „integrierter Soll-Zustand" – also ein Wunschzustand im Ausgleich der rechtlichen und tatsächlichen Anforderungen – ermittelt.

a. Soll-Zustand nach Modell eines effektiven Informationsflusses

Der Soll-Zustand der kriminalbehördlichen Informationsordnung nach dem Modell eines möglichst effektiven Informationsflusses ist vor allem aus Sicht ihrer Anwender*innen zu bestimmen. Die konkreten Anforderungen an die Informationsverarbeitung aus kriminalbehördlich-operativer Perspektive sind näher zu untersuchen. Zum Teil ergeben sich die Anforderungen an die kriminalbehördliche Informationsordnung aus behördlichen Dokumenten, Leitfäden und politischen Papieren.[68] Um die konkreten Bedürfnisse aus operativer Sicht zu erfassen, dienen zusätzlich die drei für diese Untersuchung geführten Interviews mit Mitarbeiter*innen von Polizeibehörden als Quellen.

---

[67] Siehe unten Teil 1 B. III. 3.
[68] Vgl. *Grutzpalk*, in: Grutzpalk, S. 8 (9).

Bei der Untersuchung der Anforderungen an Informationsressourcen aus kriminalbehördlich-operativer Sicht ist zu berücksichtigen, dass diese unter anderem aufgrund von technologischen Entwicklungen einem stetigen Wandel unterliegen. Die Vorstellungen davon, was Informationssysteme leisten können sollen, verändern sich mit den zur Verfügung stehenden technischen Möglichkeiten. Der Wandel der Anforderungen ist im Zusammenhang mit der Veränderung kriminalbehördlicher Tätigkeiten aufgrund technologischer Entwicklungen insgesamt zu betrachten. Diese Veränderung war bereits Gegenstand techniksoziologischer, polizeiwissenschaftlicher und kriminologischer Untersuchungen. Derartige Untersuchungen bezogen sich etwa auf den Umgang der Polizei mit neuen Informationstechnologien im Allgemeinen,[69] speziell auf den Umgang mit Informationssystemen[70] und das polizeiliche Wissensmanagement[71].

Einige der soziologischen Betrachtungen zu dem Themenfeld Polizei und Informationstechnologien gingen zunächst davon aus, dass neue Technologien die Polizeiarbeit als Werkzeuge zwar erleichterten, sich aber nicht grundsätzlich auf deren Praktiken und Handlungsmodelle auswirken würden.[72] Hierzu existierten allerdings bereits früh abweichende Auffassungen.[73] Prominent betonte auch der ehemalige BKA-Präsident *Horst Herold* die Prägung der polizeilichen Arbeit durch die technische Entwicklung.[74] *Herold* ging tendenziell von einer dominanten technologischen Logik aus, als er 1968 formulierte, dass „das maschinelle Sein das polizeiliche Bewusstsein" bestimme.[75] Jüngere Untersuchungen nehmen ebenfalls einen großen Einfluss informationstechnischer Entwicklungen auf die polizeiliche Arbeit an.[76] Setzt die Polizei neue technische

[69] Vgl. nur *Ariel*, in: Weisburd/Braga, S. 485; *Byrne/Marx*, Cahiers Politiestudies 3/2011, 17 ff.; *Koper/Lum*, in: Weisburd/Braga, S. 517 ff.; *Lum/Koper/Willis*, Police Quarterly 20 (2017), 135 ff.; *Manning*, Crime and Justice 15 (1992), 349 ff.; *Manning*, passim sowie aus politikwissenschaftlicher Perspektive *Heinrich*, passim.

[70] *Creemers*, in: Grutzpalk, S. 101 ff.; *Creemers/Guagnin*, KrimJ 2014, 134 ff.; vgl. auch *Byrne/Marx*, Cahiers Politiestudies 3/2011, 17 (27).

[71] *Grutzpalk*, in: Grutzpalk, S. 15 ff.; *Hoppe/Grutzpalk*, Polizei & Wissenschaft 4/2018, 13 ff.

[72] *Manning*, Crime and Justice 15 (1992), 349 (381 ff., 388 f.); *Ponsaers*, Policing 2001, 470 (485 ff.); vgl. auch *Ericson/Haggerty*, S. 33 m.w.N.; dazu kritisch *Van Brakel/De Hert*, Cahiers Politiestudies 3/2011, 163 (171).

[73] Vgl. *Nogala*, vorgänge 2019, 21 f.

[74] *Herold*, in: Taschenbuch für Kriminalisten, S. 240 (242 f.); *Herold* im Interview mit *Cobler*, Transatlantik 11/1980, 29 (40); siehe zu der Rolle *Herolds* bei der Entwicklung der polizeilichen Informationsordnung unten Teil 1 B. III. 1.

[75] *Herold*, in: Taschenbuch für Kriminalisten, 1968, S. 240; vgl. hierzu *Schwinghammer*, KrimJ 1980, 421 (422 f.).

[76] Vgl. nur *Ariel*, in: Weisburd/Braga, S. 485 (487); *Byrne/Marx*, Cahiers Politiestudies 3/2011, 17 ff.; *Koper/Lum*, in: Weisburd/Braga, S. 517 ff.; *Lum/Koper/Willis*, Police Quarterly 20 (2017), 135 ff.; *Narr*, Bürgerrechte & Polizei/CILIP 76 (3/2003), 6.

Hilfsmittel ein, sind diese demnach nicht nur als Werkzeuge in einem konkreten Einsatzszenario zu betrachten. Es ist auch zu berücksichtigen, welche Auswirkungen die neuen Möglichkeiten auf das Denken und Handeln der Polizei insgesamt haben.[77]

Der Einfluss des technologischen Wandels auf die kriminalbehördliche Tätigkeit im Allgemeinen sowie auf das Feld der Informationsordnung im Besonderen ist also komplex. Seine konkreten Auswirkungen betrachtet die Untersuchung anhand der einzelnen Anforderungen, die die Anwender*innen stellen.

b. Soll-Zustand aus rechtlich-normativer Sicht und Risiken für die Betroffenen

Der Soll-Zustand aus rechtlich-normativer Sicht bestimmt sich nach dem St. Gallener Ansatz aus den für den jeweiligen Bereich der Informationsverarbeitung geltenden rechtlichen Regeln. Da der Ansatz zur Weiterentwicklung einfachrechtlicher Regelungen dienen soll, bietet es sich an, hierbei auch verfassungsrechtliche und unionsrechtliche Vorgaben heranzuziehen.[78] Die verfassungsrechtlichen Vorgaben eignen sich aufgrund ihrer Flexibilität und Offenheit als „Grundprogramme“[79], um dynamischen sozio-technischen Entwicklungen zu begegnen.[80] Für die kriminalbehördliche Informationsordnung sind hierbei die Grundrechte der von der Datenverarbeitung betroffenen Personen, aber auch die Kompetenzordnung des Grundgesetzes zu beachten.

In Modifikation des ursprünglichen St. Gallener Ansatzes werden in dieser Untersuchung neben den konkreten rechtlichen Vorgaben, die für informationsordnende

---

[77] Nachzuvollziehen ist auch, dass Polizist*innen immer mehr Zeit auf den Umgang mit modernen Informationstechnologien einschließlich Ressourcen zur Informationsordnung verwenden. Es ist seit den 1970er-Jahren empirisch belegt, dass der Anteil des Umgangs mit Informationen und Wissen „am Schreibtisch“ an der Polizeiarbeit im Vergleich zu anderen Tätigkeiten gestiegen ist.; vgl. *Ericson/Haggerty*, S. 20 f. m.w.N.; zum aktuellen Anteil informationsordnender Tätigkeiten am polizeilichen Alltag *Hoppe/Grutzpalk*, Polizei & Wissenschaft 4/2018, 13 (20). Die Pflichten zur Dokumentation polizeilichen Handelns in Formularen hatten bereits zugenommen, bevor die elektronische Datenverarbeitung bei der Polizei eingeführt wurde. Mit der Computerisierung der Polizei ist der Anteil, den die Ordnung von Informationen an der polizeilichen Arbeit hat, noch weiter angestiegen. Vor diesem Hintergrund stellt sich auch die Frage, inwiefern sich der Einsatz von Informationstechnologien „produktivitätssteigernd“ auf die Tätigkeit von Kriminalbehörden in dem Sinne auswirkt, dass sie ihre Aufgaben schneller und besser erfüllen können als ohne diesen Einsatz.

[78] In der bisherigen Auseinandersetzung mit dem St. Gallener Ansatz ist die Frage, welche rechtlichen Vorgaben bis zu welcher Tiefe berücksichtigt werden sollen, weitgehend offen geblieben; vgl. *Burkert*, in: GS Steinmüller 2014, S. 177 (190).

[79] Vgl. mit einem anderen Verständnis von rechtlichen Programmen als Regeln darüber, wie die „Werte Recht und Unrecht zugeteilt werden“ in Abgrenzung zu rechtlichen Codes *Luhmann*, Das Recht der Gesellschaft, S. 93, 176 ff.

[80] Vgl. *Halfmann*, in: Schulte/Schröder, Handbuch des Technikrechts, 2. Aufl. 2011, S. 93 (95 f.); *Roßnagel/Wedde/Hammer/Pordesch*, S. 3 m.w.N.

Tätigkeiten bestehen, auch die Implikationen, die die Anforderungen aus kriminalbehördlich-operativer Sicht für die Informationssubjekte haben, mit einbezogen. Diese Implikationen sind bei der Betrachtung der rechtlichen Grenzen der Informationsverarbeitung zu berücksichtigen. Um die Risiken für die Betroffenen näher zu ergründen, werden sie kriminologisch untersucht. Dabei liegt ein besonderes Augenmerk darauf, inwiefern Personen, über die Daten in Informationsressourcen gespeichert werden, hierdurch kriminalisiert werden können. Ein solches Risiko durch Eintragungen in Informationssysteme wird in der Literatur teilweise angenommen,[81] wurde aber bislang noch nicht näher untersucht. Beispielhaft veranschaulicht *Fall 1* die Risiken einer Stigmatisierung und Kriminalisierung durch Eintragungen in polizeiliche Informationssysteme. In diesem Fall führte eine Eintragung aufgrund einer eher geringfügigen Straftat dazu, dass eine Person auch nach langer Zeit als potentieller Drogenkonsument angesprochen wird.

Zur Feststellung der Risiken für die Betroffenen dienen die im Rahmen dieser Untersuchung geführten Interviews mit Mitarbeiter*innen der Datenschutzaufsicht als wichtige Quellen. Die mit einer Vielzahl von Bürgereingaben befassten Datenschutzaufsichtsbehörden sind eine wichtige Institution zum Schutz der Persönlichkeitsrechte der Betroffenen. Für die Personen, über die Informationen in kriminalbehördlichen Systemen gespeichert sind, sind diese regelmäßig kaum durchschaubar. Es gestaltet sich für Bürger*innen schwierig, Informationen darüber zu erlangen, wie und wofür die Systeme sowie die darin gespeicherten Daten genutzt werden. Dies veranschaulicht etwa *Fall 4*, in dem die betroffene Person mit einem Auskunftsbegehren gegenüber dem Bundeskriminalamt scheiterte.

c. Integrierter Soll-Zustand

Aus dem Soll-Zustand aus kriminalbehördlich-operativer Sicht und dem Soll-Zustand aus rechtlich-normativer Sicht einschließlich der Implikationen für die Betroffenen ist ein integrierter Soll-Zustand zu bilden. Soweit sich zwischen den Anforderungen an eine effiziente Informationsverarbeitung und dem rechtlichen Soll-Zustand Diskrepanzen ergeben, sind diese zugunsten der rechtlich bindenden Vorgaben zu lösen. In dieser Arbeit wird der integrierte Soll-Zustand dadurch gebildet, dass die Anforderungen aus kriminalbehördlich-operativer Sicht im Zusammenhang mit ihren rechtlichen Rahmenbedingungen und den Implikationen für die Betroffenen untersucht werden.

[81] Vgl. *Lageson*, S. 65; *Singelnstein*, in: MüKo-StPO, 2019, Vorbemerkung zu § 483 Rn. 5 („Kriminalisierung durch Dateien“).

4. Abgleich

Im dritten und letzten Schritt werden der festgestellte Ist-Zustand und der integrierte Soll-Zustand miteinander abgeglichen. Zeigen sich zwischen Ist und Soll Diskrepanzen, was regelmäßig der Fall sein dürfte, werden Möglichkeiten untersucht und Leitlinien entwickelt, um den Ist-Zustand durch rechtliche Regelungen an den Soll-Zustand heranzuführen.[82] Dabei ist nicht zu erwarten, dass sich sämtliche Differenzen zwischen Ist und Soll durch rechtliche Regelungen beseitigen lassen. Dies wird die technische und organisatorische Realität nicht zulassen. Im Rahmen der vorliegenden Untersuchung sollen einige ausgewählte Regelungsansätze untersucht werden, um Ist und Soll einander anzunähern. Dabei geht es darum, sowohl den Anforderungen der Anwender*innen kriminalbehördlicher Informationsressourcen als auch den Interessen der Betroffenen besser als bisher gerecht zu werden.

E. Gang der Untersuchung

Der Gang der Untersuchung folgt den zuvor formulierten Erkenntniszielen. Der erste Teil untersucht die kriminalbehördliche Informationsordnung als Instrument zur Strafverfolgung. Er betrachtet die tatsächliche Relevanz von kriminalbehördlichen Informationssystemen sowie den sich darin abspielenden Handlungen. Er analysiert die Stellung kriminalbehördlicher Informationsressourcen in der Sicherheitsarchitektur der Bundesrepublik Deutschland sowie der Europäischen Union und beleuchtet ihre tatsächliche Entwicklung seit Beginn der Einführung der EDV in der Verwaltung bis heute. Dieser Teil dient vor allem zur Feststellung der Ist-Zustände der kriminalbehördlichen Informationsordnung.

Der zweite Teil befasst sich mit den Anforderungen, die Kriminalbehörden an ihre Informationssysteme stellen. Im Lichte dieser Anforderungen werden auch ihre rechtlichen Rahmenbedingungen und die Implikationen ihrer Umsetzung für die von der Datenverarbeitung Betroffenen untersucht. Schließlich werden Konflikte der Anforderungen an die Informationsordnung untereinander und gemeinsame Herausforderungen bei ihrer Umsetzung in den Blick genommen. Dieser Teil dient sowohl zur Identifikation von Ist-Zuständen – in Form bestehender Herausforderungen und Probleme – als auch zur Identifikation von Soll-Zuständen – in Form von Anforderungen und Zielen – der kriminalbehördlichen Informationsordnung.

Der dritte und abschließende Teil der Arbeit untersucht Ansätze zur Fortbildung der rechtlichen Grundlagen der kriminalbehördlichen Informationsordnung. Dabei

[82] *Burkert*, in: GS Steinmüller, S. 177 (185).

werden konkrete Möglichkeiten unter die Lupe genommen, um die Ist-Zustände den Soll-Zuständen anzunähern. Als konkrete Regelungsaspekte werden die behördliche Zentralisierung der Informationsordnung, eine stärkere Vereinheitlichung des Informationsordnungsrechts, die genauere Festlegung der für informationsordnende Tätigkeiten notwendigen Anlässe sowie die Schaffung neuer struktureller Regelungen für kriminalbehördliche Informationsressourcen betrachtet.

Teil 1

Die kriminalbehördliche Informationsordnung als Instrument zur Strafverfolgung

Dieser Teil der Untersuchung befasst sich mit der tatsächlichen Relevanz der kriminalbehördlichen Informationsordnung und ihren aktuellen rechtlichen Rahmenbedingungen. Er dient dazu, den Ist-Zustand der kriminalbehördlichen Informationsordnung herauszuarbeiten und einen Überblick über ihren Soll-Zustand aus rechtlicher Sicht zu geben. Dadurch werden die Grundlagen geschaffen, um später einen Abgleich von Ist und Soll durchzuführen und zu untersuchen, wie diese Zustände einander durch eine Fortbildung der rechtlichen Grundlagen angenähert werden könnten.

Die kriminalbehördliche Informationsordnung wird hier einerseits im handlungsbezogenen Sinne und andererseits im gegenstandsbezogenen Sinne untersucht. Zunächst wird im handlungsbezogenen Sinne beleuchtet, inwiefern das Speichern und Strukturieren von Informationen in kriminalbehördlichen Systemen sowie deren Errichtung und Einrichtung Tätigkeiten sind, die einer eigenständigen Würdigung und einer Abgrenzung zu anderen Schritten der Informationsverarbeitung bedürfen (A.). Darauf werden im gegenstandsbezogenen Sinne die Stellung kriminalbehördlicher Informationsressourcen in der Sicherheitsarchitektur sowie ihre tatsächliche Entwicklung betrachtet (B.). Schließlich erfolgt ein Überblick über die rechtlichen Grundlagen der kriminalbehördlichen Informationsordnung im handlungs- und gegenstandsbezogenen Sinne (C.).

A. Die Eigenheiten informationsordnender Tätigkeiten

Dieser Abschnitt setzt sich mit den informationsordnenden Tätigkeiten der Kriminalbehörden und ihren Eigenheiten auseinander. Er dient dazu, die für diese Untersuchung relevanten Tätigkeiten einzugrenzen und ihre eigenständige Bedeutung herauszuarbeiten.

Zunächst wird klargestellt, was im Rahmen dieser Untersuchung unter informationsordnenden Tätigkeiten zu verstehen ist (I.). Sodann werden informationsordnende Tätigkeiten von Tätigkeiten der Informationsgewinnung abgegrenzt (II.).

Schließlich wird untersucht, inwiefern bei informationsordnenden Tätigkeiten die Grenzen zwischen Prävention und Repression verwischen (III.).

I. Informationsordnende Tätigkeiten

Für die vorliegende Untersuchung sind als informationsordnende Tätigkeiten vor allem die Speicherung und Strukturierung von Informationen (1.) sowie die Errichtung und Einrichtung von Informationsressourcen (2.) von Interesse.

1. Die Speicherung und Strukturierung von Informationen

Mit der gebräuchlichen datenschutzrechtlichen Terminologie lässt sich das Speichern als „Erfassen, Aufnehmen oder Aufbewahren" von Informationen „auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung"[1] verstehen. Damit umfasst die Speicherung als Sammelbegriff einerseits den Akt der Erfassung von Informationen nach ihrer Erhebung, die ein eigener Verarbeitungsschritt ist. Informationen werden durch die Speicherung in verkörperter Form als Daten festgehalten.[2] Andererseits umfasst der Begriff der Speicherung die Aufbewahrung bzw. Bevorratung von Informationen als dauerhaften Vorgang, der ihrer Erfassung folgt.

Als Strukturierung, Ordnung oder Organisation von Informationen lassen sich – ebenfalls angelehnt an die Terminologie des Datenschutzrechts[3] – Vorgänge verstehen, die dazu beitragen, die Möglichkeit zum Auffinden, Abrufen und Auswerten von Daten zu verbessern.[4] Das Strukturieren und Ordnen ist eng mit dem Speichern verwandt, da es nicht dazu dient, neue Informationen zu generieren oder vorhandene Daten in konkreten Verfahren zu nutzen, sondern schlicht dazu, Daten für spätere Nutzungen bereitzuhalten.

Die Speicherung und Strukturierung als Schritte der Informationsverarbeitung finden also in einer Zwischenphase nach der erstmaligen Erhebung und vor einer künftigen Verwendung statt. Die Information lässt sich in diesem Stadium nach einem von

[1] So – beschränkt auf personenbezogene Daten – die Legaldefinition in § 3 Abs. 4 Satz 2 Nr. 1 BDSG aF.

[2] *Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, Art. 4 Nr. 2 DS-GVO Rn. 24.

[3] Vgl. Art. 4 Nr. 2 DSGVO, § 46 Nr. 2 BDSG.

[4] *Herbst*, in: Kühling/Buchner, 3. Aufl. 2020, Art. 4 Nr. 2 DS-GVO Rn. 23; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, 2019, Art. 4 Nr. 2 DS-GVO Rn. 18.

Gregory Bateson[5] entwickelten und von *Marion Albers*[6] in die Rechtstheorie eingeführten Modell der Information als Differenz zweier verknüpfter Differenzen als „unvollendet" verstehen.[7] Nach einer Kurzdefinition von *Albers* sind Informationen „das, was als Aussage eines Datums mit Hilfe einer Interpretationsleistung ermittelt wird."[8] Information ist demnach „durch Selektivität gekennzeichnet [...] und [wird] durch Selektionsleistungen erzeugt"[9]. Erst nach einer selektiven Interpretationsleistung können Informationen danach als vollendet gelten.[10] Eine Interpretation erfahren gespeicherte Informationen nach ihrer erstmaligen Erfassung erst wieder, wenn sie einer neuen Verwendung zugeführt werden. Das geschieht etwa durch ihren Abruf und ihre Auswertung.[11] So wird beispielsweise in *Fall 1* die Information in einer Datenbank erfasst, dass A durch den Besitz einer geringen Menge Marihuana gegen das Betäubungsmittelgesetz verstoßen hat. Durch diese Erfassung findet eine Selektionsleistung statt. Eine weitere Interpretation erfährt die Information aber erst nach acht Jahren wieder, als A bei einer Verkehrskontrolle angehalten und der Datensatz bei dieser Gelegenheit von der Polizei abgerufen wird.

---

[5] *Bateson*, S. 407 ff.; vgl. auch *Luhmann*, Soziale Systeme, S. 68 f.; 112.

[6] *Albers*, Rechtstheorie 2002, 61, (67 ff.); *Albers*, Informationelle Selbstbestimmung, S. 88 ff., vgl. kritisch hierzu *Pohle*, S. 213, der unter anderem darauf hinweist, dass dem Datenschutz der Informationsbegriff der Semiotik zugrunde liegt; im Kontext des Informationsverwaltungsrechts ebenfalls einen differenztheoretischen Informationsbegriff zugrunde legend *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts II, 2. Aufl. 2012, § 20 Rn. 18.

[7] Vgl. ähnlich im Zusammenhang mit erkennungsdienstlichen Unterlagen *Dreier*, JZ 1987, 1009 (1016).

[8] *Albers*, Rechtstheorie 2002, 61 (71). Über den Begriff der Information herrscht im rechtlichen Diskurs ebenso wenig Einigkeit wie in anderen wissenschaftlichen Zusammenhängen; vgl. nur *Aulehner*, S. 224 ff.; *Hilgendorf*, in: Taeger/Vassilaki, S. 1 (3); *Hoeren*, JuS 2002, 947; *Schoch*, VVDStRL 1997, S. 160 (166); *Vesting*, in: FS BVerfG, S. 219 ff. Es ist nicht Ziel dieser Untersuchung, eine neue oder einheitliche Definition des Begriffs zu prägen. Sie greift hier einen Interpretationsansatz auf, der eine systematische Betrachtung des Informationsordnungsrechts ermöglicht.

[9] *Albers*, Rechtstheorie 2002, 61 (68); vgl. auch *Haefner*, S. 15. Eine Selektivität besteht sowohl in dem Akt des Mitteilens als auch im Akt des Verstehens – mitgeteilter und verstandener Informationsgehalt müssen nicht zwangsläufig übereinstimmen.

[10] *Albers*, Rechtstheorie 2002, 61 (71).

[11] Zwar lässt sich hier speziell im polizeilichen Kontext kritisch einwenden, dass die Interpretationsleistung bei der Verwendung von Informationen aus Datenbanken teilweise gering ist: Ressourcen der polizeilichen Informationsordnung sind regelmäßig nicht auf die kritische Reflektion der darin gespeicherten Informationen ausgelegt. Vielmehr sind sie gestaltet, um zur unmittelbaren Grundlage operativen Handelns gemacht zu werden; vgl. *Franko Aas*, Punishment & Society 2004, 379 (385); *Petri,* in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 409. Allerdings muss zumindest nach den eingriffsrechtlichen Vorgaben eine Bewertung von Informationen aus einer Informationsressource wie einer Datenbank erfolgen, bevor eine weitere Maßnahme daran geknüpft wird. Eine in einer polizeilichen Datenbank hinterlegte Information vervollkommnet sich also erst mit dem Moment ihres Abrufs oder ihrer Auswertung.

In dem Stadium zwischen der erstmaligen Gewinnung von Informationen und ihrer späteren Verwendung, in dem sich Speicherung und Strukturierung bewegen, stellen sich besondere tatsächliche und rechtliche Fragen. Es ist näher zu untersuchen, welche Risiken das bloße Vorhandensein von Informationen in den einschlägigen Systemen langfristig mit sich bringt. Es fragt sich auch, wie der Schritt der Speicherung in seinen notwendigen Zusammenhängen mit der vorhergehenden Erhebung und der nachgelagerten Verwendung von Informationen rechtlich sinnvoll behandelt werden kann.

2. Die Errichtung und Einrichtung von Informationsressourcen

Neben dem Speichern von Informationen sind die Errichtung und Einrichtung von Informationsressourcen relevante informationsordnende Tätigkeiten, die tatsächlich wie rechtlich einer genaueren Betrachtung bedürfen. Während die Errichtung die Schaffung einer Informationsressource wie z.B. einer polizeilichen Datei meint, ist unter ihrer Einrichtung die nähere Ausgestaltung bzw. Strukturierung zu verstehen.[12] Die Einrichtung umfasst etwa die Wahl der Möglichkeiten, welche Arten von Daten in welcher Ausführlichkeit in einer Datei gespeichert werden können.

Bei der Errichtung und Einrichtung werden Weichenstellungen vorgenommen, die für die weitere Informationsverarbeitung folgenreich sein können. Schon die Entscheidung, eine bestimmte Informationsressource zu erschaffen, hat Auswirkungen. Der Betrieb von Dateien wie „Gewalttäter Sport" oder der in *Fall 5* beschriebenen fiktiven Falldatei „Hass und Hetze im Internet" ist mit Schwerpunktsetzungen bei der Kriminalitätsbekämpfung verbunden. Die Gewalttäter-Dateien sind ein Beispiel dafür, dass bereits der Titel einer Informationsressource Implikationen für die Betroffenen haben kann. Eine Eintragung gleich welcher Art kann hier dem äußeren Anschein nach einer Einstufung als Gewalttäter gleichkommen. Das Problem einer Stigmatisierung der Betroffenen durch Einträge in Datenbanken soll im späteren Verlauf der Untersuchung näher thematisiert werden.[13]

Auch Entscheidungen über die Strukturierung und Ausgestaltung von Informationsressourcen können Folgen für die Betroffenen haben. So hat beispielsweise die Stan-

[12] Vgl. *von Lewinski*, in: Seckelmann, S. 107 (112), der zwischen fünf rechtlichen Problemfeldern der Informationsordnung unterscheidet: 1. dem Errichten bzw. Schaffen eines logischen Raums, 2. seiner Einrichtung, 3. der Verortung (eines Individuums) in diesem Raum, 4. dem Einsatz und der Nutzung sowie 5. der Öffnung des Raums.

[13] Siehe unten Teil 2 A. II.

dardisierung von Auswahlmöglichkeiten in einer Datei einen erheblichen Einfluss darauf, welche Informationen in welcher Form gespeichert werden.[14] Der Ausschluss bzw. die Einschränkung von Auswahlmöglichkeiten kann unter Umstände zu nachteiligen Effekten führen. Dies kann beispielsweise der Fall sein, wenn Formulare Namen aus bestimmten Kulturkreisen nicht darstellen können oder eine streng binäre Geschlechterordnung zugrunde legen. *Fall 3* stellt in dieser Hinsicht mehrere Probleme heraus: Namen, die nicht der in Deutschland üblichen Form von Vor- und Nachname folgen sowie zusätzlich einer Transkription bedürfen, sind in Informationssystemen regelmäßig nur schwer zu erfassen. Wenn außerdem die Angabe eines konkreten Geburtsdatums verpflichtend ist, kann dies dazu führen, dass bei mehreren Personen mit unbekannten Geburtsdaten im gleichen Jahr schlicht der 1. Januar eingetragen wird. Wenn das bei vielen Personen geschieht, entstehen erhebliche Verwechslungsrisiken. Für den weiteren Verlauf der Untersuchung stellt sich die Frage, wie den Risiken zu begegnen ist, die bereits in der Errichtung und Einrichtung von Informationsressourcen und nicht erst in ihrer späteren Nutzung veranlagt sind.

II. Abgrenzung von Informationsordnung und Informationsgewinnung

Die informationsordnenden Tätigkeiten sind von jenen der Informationsgewinnung abzugrenzen. Letztere sind die Tätigkeiten der Kriminalbehörden, durch die diese im Rahmen konkreter Verfahren Sachverhalte ermitteln. Auch die Gewinnung von Erkenntnissen durch die Auswertung bereits vorhandener Informationen ist ein Aspekt der Informationsgewinnung. Die Informationsgewinnung und ihre rechtlichen Rahmenbedingungen standen schon oft im Mittelpunkt vertiefter rechtswissenschaftlicher Untersuchungen. Zuletzt erhielt besonders die verdeckte Erhebung von Informationen durch technisch gestützte Eingriffe viel Aufmerksamkeit in der juristischen Literatur.[15] Die technischen Möglichkeiten in diesem Bereich haben sich in den letzten Jahrzehnten deutlich weiterentwickelt. Darauf aufbauend haben die Gesetzgeber von Bund und Ländern zahlreiche neue Befugnisse für Überwachungsmaßnahmen geschaffen. Prominent diskutierte Maßnahmen zur Informationsgewinnung wie beispielsweise die Quellen-Telekommunikationsüberwachung oder die „Online-Durchsuchung" bedeuten gravierende Grundrechtseingriffe und sind nur unter strengen Voraussetzungen zulässig.

[14] Bei Dateien wird insofern zwischen „geschlossenen" Katalogen, in denen die Auswahlmöglichkeiten abschließend festgelegt sind, und „lernenden" Katalogen, in denen Nutzer der Dateien bisher unbekannte Kategorien hinzufügen können, unterschieden; BVerfGE 133, 277 (296).

[15] Vgl. etwa *Brodowski*, passim; *Hauck*, passim; *Neumann*, S. 35 ff.; *Puschke*, S. 28 ff.; *Schwabenbauer*, passim*; Son*, S. 102 ff., 295 ff.

Im Vergleich zu derart eingriffsintensiven Maßnahmen der Informationsgewinnung wirken die Tätigkeiten der Informationsordnung eher buchhalterisch und beinahe unscheinbar. Dementsprechend wurden Aspekte der Informationsordnung wie kriminalbehördliche Informationssysteme[16] oder Kriminalakten[17] und der Umgang mit ihnen bisher nur vereinzelt genauer untersucht. Aktuelle Entwicklungen auf diesem Bereich finden wissenschaftlich vergleichsweise wenig Beachtung. Auch eine Abgrenzung der Komplexe von Informationsgewinnung und Informationsordnung nimmt die rechtswissenschaftliche und kriminologische Forschung bisher noch nicht ausdrücklich vor.[18] In diese Richtung gehen allerdings Ansätze zur Unterscheidung verschiedener Phasen der Nutzung von Informationstechnik durch Sicherheitsbehörden[19] und die – gesetzlich etablierte – Unterscheidung verschiedener Phasen des Umgangs mit personenbezogenen Daten im Datenschutzrecht.[20]

Eine differenziertere Betrachtung von Tätigkeiten der Informationsordnung als bisher wäre deshalb wünschenswert, weil diese einer eigenen Rationalität folgen und andere Implikationen für die Rechte der betroffenen Personen haben als jene der Informationsgewinnung. Die Bevorratung von Informationen in Datenbanken lässt sich als eine moderne Form des kulturellen Ausdrucks beschreiben, die nicht der Logik von

---

[16] *Ringwald*, passim; *Zöller*, passim.

[17] *Ahlf*, Polizeiliche Kriminalakten, passim; *Rachor*, S. 52 ff.; aus US-amerikanischer Perspektive *Jacobs*, passim.

[18] Mit entsprechenden Ansätzen aber *Bäcker*, Kriminalpräventionsrecht, S. 473 f.; *Weßlau*, S. 23 f.; vgl. im Zusammenhang mit dem administrativen Wissensmanagement auch *Augsberg*, S. 159.

[19] So unterscheiden *Hornung/Schindler*, in: Gusy/Kugelmann/Würtenberger, S. 247 (253 f.) beispielsweise zwischen der Beschaffung von Informationsgrundlagen, der Aufbereitung von Informationen und ihrer Nutzung für Folgemaßnahmen und die Kommunikation an Dritte. Im Rahmen dieser Dreiteilung wird sich der Aspekt der Informationsordnung am ehesten der Phase der Aufbereitung zuordnen lassen. Allerdings sehen *Hornung* und *Schindler* diese Phase des Informationsumgangs vor allem unter dem Gesichtspunkt der Analyse von Daten als relevant an. Die eigenständige Bedeutung der Bevorratung von Informationen würdigen sie dabei nicht.

[20] Die Differenzierung zwischen verschiedenen Phasen der Datenverarbeitung ist dabei im deutschen Datenschutzrecht deutlicher ausgeprägter als im europäischen Datenschutzrecht. Grundkategorien des Umgangs mit personenbezogenen Daten waren im BDSG vor Geltung der DSGVO die Erhebung, Verarbeitung und Nutzung. Dabei bildete die Speicherung personenbezogener Daten einen Aspekt der Verarbeitung personenbezogener Daten. § 3 Abs. 4 Nr. 1 BDSG 2009 definierte die Speicherung als „Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung“ wohingegen das Erheben „das Beschaffen von Daten über den Betroffenen“ bedeutete (§ 3 Abs. 3 BDSG 2009). Hieraus wird deutlich, dass das Erfassen und Bevorraten von Daten als Eingriff von anderer Qualität als die erstmalige Beschaffen zu verstehen war. Im Unionsrecht fand sich eine solch klare Differenzierung weder in der Datenschutzrichtlinie, noch findet sie sich in der DSGVO und der JI-Richtlinie.

Zwecken und Narrativen unterliegt.[21] So unterscheiden sich auch Vorgänge der Datenspeicherung von Vorgängen ihrer Erhebung und Auswertung. Die erstmalige Gewinnung von Daten und ihre Analyse geschehen regelmäßig im Rahmen konkreter Verfahren zu festgelegten Zwecken. Bei der Speicherung und Strukturierung von Daten ist dies seltener der Fall. Damit sind diese Vorgänge durch das datenschutzrechtliche Prinzip der Zweckbindung nur eingeschränkt in den Griff zu bekommen. Auch die hergebrachten Eingriffsschwellen für Ermittlungshandlungen aus Polizei- und Strafprozessrecht – Gefahr und Tatverdacht – lassen sich für informationsordnende Tätigkeiten nicht ohne Weiteres anwenden. Welche Anlässe derartigen Tätigkeiten besser gerecht werden, wird näher zu untersuchen sein.[22]

Obwohl der Komplex der Informationsordnung einer eigenständigen Betrachtung bedarf, können Tätigkeiten der Informationsgewinnung und solche der Informationsordnung nicht völlig voneinander getrennt werden. Sie hängen sowohl in tatsächlicher Hinsicht als auch in ihrer rechtlichen Bewertung miteinander zusammen. Die Speicherung und Strukturierung von Informationen sind Tätigkeiten der Informationsgewinnung sowohl vor- als auch nachgelagert. Nachgelagert sind sie ihnen deswegen, weil die Speicherung notwendigerweise an Maßnahmen zur Informationsgewinnung anknüpft. Daten müssen erhoben worden sein, um gespeichert werden zu können. Vorgelagert sind Speicherung und Strukturierung der Informationsgewinnung deswegen, weil die Daten bereitgehalten werden, um in konkreten Verfahren verwendet und ausgewertet zu werden. Dabei erfahren sie eine neue Interpretation. Das Informationsordnungsrecht ist damit im Verhältnis zur Informationsgewinnung gleichermaßen ein „Vorfeldrecht" wie ein „Nachfeldrecht".

Dass die rechtlichen Grundlagen für die Informationsordnung und Informationsgewinnung nicht ganz getrennt voneinander betrachtet werden können, haben das Bundesverfassungsgericht und der Europäische Gerichtshof deutlich gemacht. Zwischen den Anforderungen an die Speicherung und die weitere Verwendung von Daten besteht ein Kompensationsverhältnis. Nach dem Bundesverfassungsgericht entscheidet die verhältnismäßige Ausgestaltung der rechtlichen Regeln über die Verwendung von Daten „nicht nur über die Verfassungsmäßigkeit dieser einen eigenen Eingriff begründenden Bestimmungen selbst, sondern wirkt auf die Verfassungsmäßigkeit schon der Speicherung als solcher zurück."[23] Ähnlich setzt der Europäische Gerichtshof die

[21] Vgl. *Manovich*, S. 218 ff.; ähnlich *Poster*, S. 91.
[22] Siehe unten Teil 3 C.
[23] BVerfGE 125, 260 (327 f.).

Voraussetzungen für eine Speicherung der Daten in ein Verhältnis zu dem Voraussetzungen für den Zugang zu ihnen.[24] Insgesamt können also hohe Schwellen für den Zugang zu Daten und deren Auswertung in einem gewissen Maße fehlende Einschränkungen bei der Speicherung kompensieren und umgekehrt. Dies erscheint aufgrund des tatsächlichen Zusammenhangs zwischen diesen Phasen der Informationsverarbeitung sachgerecht.

Bei der rechtlichen Bewertung der Speicherung und Strukturierung von Informationen sind auch neue technische Möglichkeiten zu ihrer Auswertung zu berücksichtigen. Dass technologische Entwicklungen komplexe Verknüpfungen und Auswertungen von Daten erlauben, erhöht bereits die Bedeutung ihrer Speicherung[25] und Strukturierung. Heute stehen im Zusammenhang mit der Auswertung von Informationen besonders Methoden der künstlichen Intelligenz[26] im Fokus. Praktisch geht es unter anderem darum, mit Hilfe selbstlernender Systeme neue Informationen aus großen Datenbeständen („Big Data")[27] zu gewinnen.[28] Dies illustriert beispielsweise *Fall 5*, in dem durch maschinelles Lernen die Sprachmuster von Personen erkannt werden sollen, um diese zu Zwecken der Strafverfolgung zu identifizieren.

Im Ergebnis ist eine differenzierte, aber nicht isolierte Betrachtung der unterschiedlichen Tätigkeitskomplexe von Informationsgewinnung und Informationsordnung geboten. Die Systeme zur Erhebung, Speicherung und Auswertung von Informationen sind notwendigerweise miteinander verbunden. Sie können in ihrer Gesamtheit als rhizomatisch wachsendes Gefüge betrachtet werden.[29] Datenbanken und Informations-

[24] EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights, Rn. 60.

[25] Dies stellte das Bundesverfassungsgericht bereits in seinem Volkszählungsurteil fest; BVerfGE 65, 1 (43).

[26] Vgl. zu ihrem Einsatz im polizeilichen und sicherheitsbehördlichen Bereich aktuell *Golla*, KrimJ 2020, 149 ff.; *Wischmeyer*, in: Kulick/Goldhammer, S. 193 ff.; aus früherer Sicht *Manning*, Crime and Justice 15 (1992), 349 (381) m.w.N. Während das Interesse an Technologien der künstlichen Intelligenz im juristischen Bereich nach einer ersten Welle der Aufmerksamkeit in den 1970er-Jahren zunächst wieder abflaute (vgl. *Hoeren*, JuS 2002, 947 (949)), ist es heute größer denn je. Dies ist auf erhebliche technologische Fortschritte unter anderem bei der Entwicklung und Beherrschung lernfähiger Algorithmen in den 2010er-Jahren zurückzuführen.

[27] Vgl. zu „Big Data" in der polizeilichen Arbeit *Ferguson*, University of Pennsylvania Law Review 163 (2015), 327 (350 ff.); *Momsen/Rennert*, KriPoZ 2020, 160 ff.; zu den Herausforderungen für die Kriminologie *Chan/Moses*, Theoretical Criminology 20 (2016), 21 ff.

[28] Vgl. zu der rechtlichen Bewertung von „Data Mining"-Verfahren *Brinkhoff*, Eur J Secur Res 2017 (2), 57 ff.; *Gless*, in: GS Weßlau, S. 164 (167 f.); *Körffer*, DANA 2014, 146 ff.

[29] Vgl. zu der Notwendigkeit der gemeinsamen Betrachtung von Überwachungstechnologien aus sozialwissenschaftlicher Sicht *Haggerty/Ericson*, British Journal of Sociology 51 (2000), 605 (610) („surveillance as an assemblage"); dem folgend *Creemers*, in: Grutzpalk, S. 101 (107); *S. Kaufmann*, in: Gusy/Kugelmann/Würtenberger, S. 3 (18).

systeme bilden in diesem Geflecht Knotenpunkte, an denen Informationen zusammenlaufen und neue Informationen erzeugt werden.[30] Gerade aufgrund des Wachstums staatlicher Datensammlungen verlangt das Bundesverfassungsgericht vom Gesetzgeber, vor der Einführung neuer Pflichten und Rechte zur Speicherung von Daten, eine „Überwachungsgesamtrechnung"[31] vorzunehmen und die „Gesamtheit der verschiedenen schon vorhandenen Datensammlungen" zu betrachten.[32] Dieses Erfordernis erscheint aufgrund der schwer abschätzbaren möglichen Auswirkungen dieser Sammlungen und der komplexen Verzahnung informationsverarbeitender Maßnahmen sinnvoll. Die Prüfung der Verhältnismäßigkeit einer einzelnen Maßnahme zur Datenspeicherung oder Datenauswertung eignet sich nur eingeschränkt, um diese einzuhegen, wenn sie dabei ihren Kontext in einem Gesamtsystem von Informationsgewinnung und Informationsordnung nicht berücksichtigt.[33]

III. Informationsordnung zwischen Prävention und Repression

Wenn die Polizei informationsordnende Tätigkeiten vornimmt, ist es oftmals nicht leicht, diese eindeutig ihrem präventiven oder repressiven Tätigkeitsbereich zuzuordnen. Dies entspricht einer allgemeinen Gemengelage bei der Zuordnung von Handlungen nach dieser Dichotomie, die im Folgenden zunächst kurz dargestellt wird (1.). Im Anschluss wird auf die spezifischen Schwierigkeiten der Zuordnung bei informationsordnenden Tätigkeiten eingegangen (2.).

---

[30] *Creemers*, in: Grutzpalk, S. 101 (107); vgl. auch *Lyon*, in: Lyon, S. 13 (14).

[31] Vgl. dazu *F. Braun/F. Albrecht,* VR 2017, 151 ff.; *Knierim*, ZD 2011, 17 (19); *Moser-Knierim*, S. 236 ff.; *Roßnagel*, NJW 2010, 1238 (1240 f.); kritisch mit Blick auf die Operationalisierbarkeit *Hornung/Schnabel*, DVBl. 2010, 824 (827 f.); mit einem Vorschlag zur gesetzlichen Verankerung BT-Drs. 19/23695, S. 5 f.; mit dem konkreten Konzept eines Überwachungsbarometers *Poscher/Kilchling/Landerer*, GSZ 2021, 225 ff.

[32] Konkret betonte das Bundesverfassungsgericht die Auswirkungen einer Vorratsdatenspeicherung von Telekommunikationsdaten auf weitere staatliche Datensammlungen: Diese zwinge „den Gesetzgeber bei der Erwägung neuer Speicherungspflichten oder -berechtigungen in Blick auf die Gesamtheit der verschiedenen schon vorhandenen Datensammlungen zu größerer Zurückhaltung" (BVerfGE 125, 260 (324)). Da eine totale Erfassung und Registrierung der Freiheitswahrnehmung der Bürger*innen mit der verfassungsrechtlichen Identität der Bundesrepublik Deutschland nicht vereinbar wäre, werde der Spielraum für weitere anlasslose Datenspeicherungen durch die Existenz der Vorratsdatenspeicherung geringer; vgl. zur Grundrechtsrelevanz kumulativer Nutzung von Maßnahmen zur Informationsbeschaffung schon BVerfGE 112, 304 (319 f.); *Puschke*, S. 61 ff.

[33] Vgl. *Knierim*, ZD 2011, 17 (19).

1. Die Gemengelage zwischen Prävention und Repression

Die eindeutige Verortung polizeilicher Tätigkeiten im präventiven oder repressiven Bereich ist in vielen Fällen schwierig.[34] Oftmals ist die Zuordnung einer einzelnen Handlung nach dem Modell doppelfunktionaler Maßnahmen[35] nur theoretisch möglich; es entsteht eine undurchsichtige Gemengelage zwischen Prävention und Repression.[36] Daher wird auch die Sinnhaftigkeit der Unterscheidung polizeilicher Handlungen nach präventiver und repressiver Zielrichtung seit geraumer Zeit immer wieder in Frage gestellt.[37]

Mögliche Gründe dafür, dass die Gemengelage zwischen Prävention und Repression sich verschärft oder jedenfalls zunehmend Aufmerksamkeit erhält, sind sowohl in rechtlichen als auch in technischen Entwicklungen zu suchen. Auf der rechtlichen Seite trägt die Tendenz hin zu einem präventiven Strafrecht zu einem Verschleifen des präventiven und repressiven Tätigkeitsbereichs bei. So wurden das Straf- und Strafverfahrensrecht zuletzt „immer mehr in den Dienst einer unmittelbaren Kriminalprävention gestellt“[38]. Dies geschah insbesondere durch die Vorverlagerung von Strafbarkeiten in Form der Schaffung abstrakter Gefährdungsdelikte.[39] Diese Entwicklung im materiellen Strafrecht wirkt sich auch auf das Strafprozessrecht aus. Durch die Vorverlagerung der Strafbarkeit ist es auch eher möglich, den Anfangsverdacht einer Straftat anzunehmen. Hierdurch eröffnen sich in einem früheren Stadium als zuvor Ermittlungsinstrumente sowie die Möglichkeit, Beschuldigte in Untersuchungshaft zu nehmen.[40]

In einer ähnlichen Weise wirkt das präventive materielle Strafrecht mit dem Polizeirecht zusammen. Die vorverlagerte Strafbarkeit ist über das Schutzgut der öffentlichen

---

[34] Dazu nur *Möstl*, S. 216; *Ringwald*, ZRP 1988, 178 (182); *Schoreit*, NJW 1985, 169 (170); *Stephan*, VBlBW 2005, 410 (411); *Wolter*, in: FS Rolinski, S. 273 (276); vgl. insgesamt für den Bereich der polizeilichen „Wissensproduktion“ *Denninger*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. D Rn. 4; im Zusammenhang mit der Vorratsspeicherung von Telekommunikationsdaten *Puschke*, in: FS Eisenberg, S. 695 (703).

[35] Dieses geht zurück auf *Emmerig*, DVBl. 1958, 338 ff.

[36] Vgl. nur *Gärditz*, S. 7 f.; *Schünemann*, Kriminalistik 1999, 74 (76); Arbeitskreis AE, S. 28 f.

[37] *Albers*, Determination, S. 21 ff.; *Gusy*, StV 1993, 269 (275); *Häring*, Kriminalistik 1979, 269 (271); *Stümper*, Kriminalistik 1975, 49 (53); *Stümper*, Kriminalistik 1980, 242 ff. Forderungen, die strenge Unterscheidung zwischen präventivem und repressivem Bereich aufzulösen, entstand zunächst aus dem Wunsch, Bedrohungen wie die organisierte Kriminalität und Terrorismus effektiver bekämpfen zu können; vgl. *Kniesel*, Die Polizei 2018, 265 (268). Auf diesem Gedanken beruht die Idee der Einführung einer einheitlichen Kategorie operativen polizeilichen Handelns; vgl. hierzu *Rudolph*, S. 6 f.; *Weßlau*, S. 25 ff.

[38] *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 14.

[39] *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 14.

[40] *Rusteberg*, Föderale Sicherheitsarchitektur, S. 9.

Sicherheit auch für die polizeirechtliche Gefahrenschwelle bedeutsam.[41] Schließlich tragen rechtlich unmittelbare Verschärfungen des polizeilichen und strafprozessualen Eingriffsrechts zum Verschleifen von Prävention und Repression bei.[42]

Eine andere mögliche Ursache für das Verschleifen der Grenzen zwischen präventivem und repressivem Handeln sind informationstechnische Entwicklungen, die sich in diesem Bereich gewissermaßen disruptiv auf das Recht auswirken.[43] So betonte bereits *Alfred Stümper* die Rolle technischer Entwicklungen, als er 1975 die Unterscheidung zwischen präventiver und repressiver polizeilicher Tätigkeit grundlegend in Frage stellte.[44] Neue Technologien können grundsätzlich zu einer Konvergenz unterschiedlicher Regelungsgegenstände führen und einen Anpassungsdruck auf das Recht ausüben.[45] Gegebenenfalls können Anpassungen im Sinne der praktischen Anwendbarkeit und Rechtsstaatlichkeit der Regelungen geboten sein.[46]

Ein Bereich, in dem technologische Entwicklungen konkret eine Rolle dabei spielen, dass die Grenzen zwischen Prävention und Repression verwischen, ist die Gewinnung von Informationen durch heimliche Überwachungsmaßnahmen. Aufgrund des Ausbaus der Ermächtigungen zur verdeckten Überwachung[47] und der wachsenden technischen Möglichkeiten hat dieser Bereich zuletzt verstärkt Aufmerksamkeit erhalten.[48] Mit den wachsenden technischen Möglichkeiten zur Überwachung und der Auswertung der daraus gewonnenen Daten nehmen auch die Fälle zu, in denen eine klare Trennung von Prävention und Repression schwerfällt. Die Polizei hat bei der verdeckten Informationsgewinnung faktisch oftmals die Wahl zwischen präventiven und repressiven Befugnissen, die ein ähnliches Vorgehen erlauben, wenn sich zugleich der Verdacht einer bereits begangenen Straftat und die Gefahr weiterer Rechtsgutsverletzungen begründen lassen.[49] So ließe sich etwa die Telekommunikationsüberwachung eines Drogenhändlers, der bereits Geschäfte abgewickelt hat, aber auch noch weitere „Deals" plant, sowohl mit einer repressiven als auch mit einer präventiven Zielrichtung begründen.

Die in diesem Fall gleichermaßen einschlägigen Ermittlungsbefugnisse aus der Strafprozessordnung und den Polizeigesetzen haben allerdings teilweise unterschiedliche

---

[41] Vgl. *Bäcker*, Kriminalpräventionsrecht, S. 541 f., der im Ergebnis vorschlägt, das das kriminalpräventive Strafrecht aus den polizeirechtlichen Ermächtigungen zu verbannen.
[42] *Gärditz*, S. 8.
[43] Vgl. *Weßlau*, S. 48.
[44] *Stümper*, Kriminalistik 1975, 49 (53).
[45] *Bizer*, in: FS Kilian, S. 39 (54).
[46] *Bizer*, in: FS Kilian, S. 39 (54).
[47] Vgl. *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 14.
[48] Vgl. *Brodowski*, S. 344 ff. m.w.N.
[49] Vgl. mit diversen Beispielen *Kniesel*, Die Polizei 2018, 265 (269 f.).

Voraussetzungen. Tendenziell sind Eingriffe im präventiven Bereich unter etwas niedrigeren Voraussetzungen möglich, da hier noch die Möglichkeit zur Verhinderung von Schäden besteht. Für repressive (Ermittlungs-)Maßnahmen sind umgekehrt tendenziell stärkere Sicherungsvorkehrungen erforderlich.[50] Zudem ist bei einem repressiven Tätigwerden die Sachleitungsbefugnis der Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens" zu beachten. Im Gegensatz dazu handelt die Polizei bei präventiven Tätigkeiten auf Grundlage der Polizeigesetze eigenverantwortlich.

Angesichts der faktisch oftmals bestehenden Möglichkeit, zwischen Befugnissen aus dem präventiven und repressiven Bereich zu wählen, erscheint es naheliegend, dass sich die Polizei für die Befugnisse entscheiden wird, die niedrigere Anforderungen stellen. Damit kann die Polizei eine Art „Befugnisshopping"[51] betreiben und sich für eine Rechtsgrundlage ihrer Wahl entscheiden.[52] Dem steht auch nicht ein etwaiger Vorrang des Strafverfahrensrechts[53] oder Gefahrenabwehrrechts[54] entgegen. Einem solchen möglichen Vorrang hat zuletzt der 2. Strafsenat des Bundesgerichtshofs eine Absage erteilt.[55] In seiner Entscheidung zu legendierten Kontrollen sprach er sich im Zusammenhang mit der Durchsuchung eines Fahrzeugs nach Betäubungsmitteln als echter doppelfunktionaler Maßnahme[56] für eine weitgehende Wahlmöglichkeit zwischen präventivem und repressivem Tätigwerden aus. Der 2. Strafsenat entschied, dass es „weder einen allgemeinen Vorrang der Strafprozessordnung gegenüber dem Gefahrenabwehrrecht noch umgekehrt" gebe.[57] Auch bei Vorliegen eines Anfangsverdachts im Sinne von § 152 Abs. 2 StPO sei „ein Rückgriff auf präventiv-polizeiliche Ermächtigungsgrundlagen rechtlich möglich."[58]

[50] Vgl. *Forgó/Hawellek/Knoke/Stoklas*, in: Corrales/Fenwick/Forgó, S. 251 (258 f.).

[51] *Brodowski*, S. 355.

[52] *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 15; *Gusy*, StV 1991, 499; *Puschke*, S. 169.

[53] Dafür *W. Müller/Römer*, NStZ 2012, 543 (546 f.); mit Einschränkungen auch *Roggan*, GSZ 2018, 52 (56).

[54] Dafür *Kniesel*, ZRP 1987, 377 (378); *Tegtmeyer*, KritV 1989, 213 (220); *G. Wolf*, Kriminalistik 1975, 389 (391 f.).

[55] BGH NStZ 2017, 651 (654 Rn. 27).

[56] Bei der Durchsuchung „beabsichtigte die Polizei nicht nur, die Betäubungsmittel zwecks Gefahrenabwehr aus dem Verkehr zu ziehen, sondern verfolgte daneben auch das Ziel der Beweissicherung in einem potentiellen Strafverfahren"; BGH NStZ 2017, 651 (653 Rn. 20).

[57] BGH NStZ 2017, 651.

[58] BGH NStZ 2017, 651 (654 Rn. 25).

2. Zuordnung informationsordnender Tätigkeiten

Die beschriebenen Schwierigkeiten bei der Zuordnung polizeilicher Tätigkeiten zum präventiven oder repressiven Bereich kommen bei informationsordnenden Tätigkeiten besonders stark zum Vorschein.

So werden Daten meist nicht mit Blick auf eine konkrete Situation der Strafverfolgung oder Gefahrenabwehr gespeichert, in der sie verwendet werden sollen. Es ist zwar vorstellbar, dass eine Speicherung nur an ein konkretes Verfahren geknüpft ist, dessen Zweck dann hierfür maßgeblich ist. In der Regel dient die Speicherung von Informationen in kriminalbehördlichen Informationsressourcen aber zumindest auch der Vorbereitung künftiger Verfahren. Das vorhandene Wissen der Behörden soll für die Zukunft gesammelt und aufbewahrt werden.[59] Auf die Funktion der kriminalbehördlichen Informationsressourcen als Instrumente zur Vorsorge wird sogleich näher eingegangen.[60]

Zum Zeitpunkt ihrer Speicherung sind die Informationen in kriminalbehördlichen Systemen für potentiell viele Zwecke relevant.[61] So können es die gespeicherten Informationen ermöglichen, Beziehungen zwischen unterschiedlichen – abgeschlossenen und noch laufenden – Verfahren herzustellen. Sie können auch dazu dienen, neue Verdachtsmomente zu generieren und zu der Aufdeckung bisher noch nicht bekannt gewordener Straftaten beizutragen. Darüber hinaus sind abstraktere Verwendungen möglich: Informationen können dazu eingesetzt werden, übergreifende „Erkenntnisse zu sammeln, die für die Aufklärung erst künftig zu erwartender Straftaten von Bedeutung sind“ oder für die allgemeine Gefahrenabwehr genutzt werden.[62]

Ähnlich vielseitig nutzbar wie die Informationen sind auch die Dateien und Systeme, in denen sie gespeichert werden. In der Regel sind diese nicht so gestaltet, dass sie ausschließlich zur Erfüllung eines bestimmten einzelnen Zweckes dienen. Dies wäre beispielsweise dann der Fall, wenn die Polizei eine Datei betreiben würde, um Informationen über Hooligans nur dafür zu speichern, um von diesen ausgehende Straftaten zu verhindern. Solche Ressourcen mit spezifisch festgelegten präventiven oder repressiven Zwecken sind selten. In der Praxis dienen viele Informationsressourcen dazu, um sowohl präventive als auch repressive Zwecke zu erfüllen. Die meisten Dateien bei der Polizei sind in diesem Sinne so genannte Mischdateien.[63] Dabei kann es sich konkret

[59] *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 33; vgl. auch *Bäcker*, Kriminalpräventionsrecht, S. 494; *Siebrecht*, JZ 1996, 711.

[60] Siehe unten B. II.

[61] Vgl. *Kniesel*, in: Bull, S. 105 (109); speziell zu INPOL *Siebrecht*, JZ 1996, 711; *Zöller*, S. 171.

[62] *Siebrecht*, JZ 1996, 711; *Zöller*, S. 171.

[63] *Singelnstein*, in: MüKo-StPO, 2019, Vorbemerkung zu § 483 Rn. 4; vgl. auch *Bäcker*, Kriminalpräventionsrecht, S. 71; *Rudolph*, S. 96.

um Dateien wie die in *Fall 5* beschriebene Falldatei „Hass und Hetze im Internet“ oder die Datei „Gewalttäter Sport“ handeln.

Insbesondere in dem für die alltägliche Arbeit sowie für die vorliegende Untersuchung besonders relevanten INPOL-System werden Daten auch unabhängig von konkreten laufenden Verfahren bevorratet. Eine klare Trennung von Speicherungen zu präventiven und repressiven Zwecken erfolgt in dem System nicht. Dies ist bereits in der technischen und organisatorischen Konzeption des 1972 eingeführten und 2003 grundlegend reformierten INPOL[64] angelegt. Hierbei wurden präventive und repressive Verwendungszwecke nicht getrennt, sondern zusammengedacht.[65] Dies hing zum Teil auch mit den – teilweise mittlerweile überwundenen – Schwierigkeiten zusammen, die Aufgabenkategorie der „vorbeugenden Verbrechensbekämpfung“ klar dem präventiven oder repressiven Bereich zuzuordnen. Die Vermengung von präventiven und repressiven Zwecken bei der Arbeit mit INPOL wurde seit jeher kritisiert.[66]

Ein Modell kriminalbehördlicher Informationssysteme, das klar zwischen der Verfolgung präventiver und repressiver Zwecke unterscheidet, wurde immer wieder gefordert.[67] Es hat sich aber praktisch nie durchgesetzt.[68] Auch in den Plänen zur Neuordnung der polizeilichen Informationsordnung durch das Programm Polizei 20/20 ,das unter anderem die Schaffung eines Informationsverbundes vorsieht, spielt die Abgrenzung von Speicherungen zu präventiven und repressiven Zwecken keine Rolle.[69]

Der Umsetzung eines solchen dichotomischen Modells steht entgegen, dass es wahrscheinlich redundante Speicherungen von Daten durch die Endnutzer*innen der Systeme erfordern würde. Sollte die zukünftige Nutzung von Daten zu präventiven und repressiven Zwecken ermöglicht werden, müssten sie zwei Mal gespeichert bzw. zumindest markiert werden – einmal für jede Zweckrichtung. Dies ginge mit einem erhöhten Aufwand bei der Nutzung der Systeme einher. Die Notwendigkeit redundanter Speicherungen durch die Anwender*innen hat sich in der Praxis bereits als Hindernis bei der Nutzung kriminalbehördlicher Informationssysteme und als ein die Informationsqualität potentiell mindernder Faktor herausgestellt.[70] Die Polizei sieht eine Trennung von Daten in polizeilichen Informationssystemen nach der Verwendung für präventive

[64] Siehe zu der Entstehungsgeschichte des Systems unten B. III.
[65] *Sehr*, Kriminalistik 1999, 532.
[66] *Siebrecht*, JZ 1996, 711 (712).
[67] Deutscher Richterbund, DRiZ 1986, 110; *Zöller*, S. 173; vgl. auch *Matheis*, S. 106.
[68] Vgl. *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, § 481 Rn. 3.
[69] Siehe zu Polizei 20/20 unten B. III. 3.
[70] Redundante Speicherungen sind oftmals durch die Inkompatibilität der Informationssysteme von Bund und Ländern notwendig; vgl. BT-Drs. 18/11163, S. 84; BMI, Polizei 2020, S. 2.

und repressive Zwecke teilweise auch deswegen nicht für notwendig an, weil diese aufgrund der Regelung für Mischdateien in § 483 Abs. 3 StPO ohnehin insgesamt dem Polizeirecht unterliegen würden.[71]

Durch die technische Entwicklung der kriminalbehördlichen Informationsressourcen scheint sich die Zuordnungsproblematik aktuell tendenziell noch zu verschärfen. Schon bei der Führung polizeilicher Kriminalakten[72] in Papierform war die Zuordnung der Speicherung von Informationen zum präventiven oder repressiven Tätigkeitsbereich regelmäßig unklar.[73] In den polizeilichen Informationssystemen ist eine saubere Unterscheidung der beiden Tätigkeitsbereiche nicht angelegt. Die aktuell nachvollziehbaren Wünsche der Kriminalbehörden, Informationen aus ihren Beständen noch stärker als bisher zu verknüpfen,[74] lassen es unwahrscheinlicher denn je erscheinen, dass die Unterscheidung der beiden Handlungsbereiche eingehalten werden kann.

B. Kriminalbehördliche Informationsressourcen

Dieser Abschnitt nimmt die Informationsressourcen in den Blick, auf die sich die informationsordnenden Tätigkeiten beziehen bzw. in denen sie sich abspielen. Er konzentriert sich also auf die kriminalbehördliche Informationsordnung im gegenständlichen Sinne. Er dient dazu, einen breiten Überblick über den Ist-Zustand der vorhandenen Dateien und Systeme zu geben.

Dafür wird zunächst dargestellt, welche Arten von kriminalbehördlichen Informationsressourcen derzeit existieren und wie diese eingesetzt werden (I.). Es wird betrachtet, inwiefern es sich bei den Informationssystemen und Datenbanken um Instrumente der Vorsorge handelt (II.). Darauf wird die Entwicklung der polizeilichen (III.) sowie der staatsanwaltschaftlichen Informationsressourcen (IV.) untersucht. Schließlich wird herausgearbeitet, welche Rolle kriminalbehördliche Informationsressourcen in der Sicherheitsarchitektur der Bundesrepublik Deutschland (V.) und der Europäischen Union (VI.) spielen.

---

[71] Vgl. BVerfGE 120, 378 (422); siehe hierzu näher zu § 483 Abs. 3 StPO unten Teil 2 A. III. 1. a. bb).

[72] Bzw. nach später verwendeter Terminologie „kriminalpolizeilicher personenbezogener Sammlungen“; vgl. dazu und zum Begriff *Ahlf*, Polizeiliche Kriminalakten, S. 6 ff.; *Ahlf*, KritV 1988, 136 (137); *Schoreit*, NJW 1985, 169 (170).

[73] So sahen etwa die 1981 erlassenen Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien, GMBl. Nr. 7/1981, S. 119 ff.) keine Unterscheidung zwischen Speicherungen zu präventiven und repressiven Zwecken vor; vgl. dazu *Ahlf*, Polizeiliche Kriminalakten, S. 15 f. *Denninger*, CR 1988, 51 (56); *Rachor*, S. 158 ff.; *Schoreit*, CR 1986, 224 (225).

[74] Siehe dazu im Einzelnen unten Teil 2 B. I.

I. Das System der kriminalbehördlichen Informationsressourcen

Wie bereits eingangs festgestellt, betreiben die Polizeien und Staatsanwaltschaften eine Vielzahl von Informationssystemen. Wie viele Systeme mit welchem Inhalt und zu welchen Zwecken in Bund und Ländern genau im Einsatz sind, ist praktisch kaum nachzuvollziehen.[75] Aus öffentlich zugänglichen Quellen sind noch am ehesten Informationen über die beim Bundeskriminalamt vorhandenen Informationsressourcen zu erhalten.[76] Das Bundeskriminalamt ist als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen (Art. 87 Abs. 1 Satz 2 GG, § 2 Abs. 1 BKAG) der wichtigste Akteur für den Betrieb polizeilicher Informationsressourcen in Deutschland.[77]

Dass der Komplex der kriminalbehördlichen Informationsressourcen nicht nur für Forschende schwer überschaubar ist, zeigt die Auswertung der für diese Untersuchung geführten Interviews. Einige der befragten Mitarbeiter*innen der Datenschutzaufsicht sowie polizeiliche Anwender*innen gaben an, selbst Schwierigkeiten dabei zu haben, die kriminalbehördliche Informationsordnung vollständig zu überblicken. Ein*e Mitarbeiter*in einer Datenschutzbehörde berichtete:

> „Es ist für einen Nichtpolizeibeamten schwierig, diese ganze Systematik zu durchblicken. Es gibt Dienstanweisungen und es gibt tolle Schaubilder, aber das ist – wenn man keinen polizeilichen Hintergrund hat – schwer zu erfassen. Und wenn man dann Ausdrucke bekommt von Ermittlungsakten oder Kriminalakten, war mein Eindruck immer, die sind sehr inhomogen. Man muss sich also regelrecht durchkämpfen." (DSA1)

Mehrere der interviewten polizeilichen Anwender*innen erklärten, keinen Überblick über sämtliche aktive polizeiliche Informationsressourcen zu haben. Sie betonten aber, dass der Kreis der Systeme, die man kennen müsse, an die jeweils bekleidete Stelle und ausgeübte Tätigkeit gebunden sei (POL1, POL2). Ein*e Interviewpartner*in sagte:

> „Ich traue mir nicht zu, zu behaupten, dass ich einen vollständigen Überblick über alle Quellen hätte, oder über alle Datenbestände, die es bei uns im Land so gibt, geschweige denn bundesweit. Ich denke, es ist immer die Frage, in welchem Bereich bin ich gerade tätig? Und in dem Bereich kriegt man dann

[75] Vgl. mit einem Überblick der polizeilichen Informationssysteme und der verwendeten Software auf Bundesebene (Stand 2016) BT-Drs. 18/8596, S. 1 ff.

[76] Vgl. BT-Drs. 20/6633 (Stand: April 2023); BT-Drs. 19/15346, S. 14 ff. (Stand: November 2019); BT-Drs. 17/14735, S. 9 ff. (Stand: 2013); BT-Drs. 17/2803, S. 13 ff. (Stand: 2010); BT-Drs. 16/13563, S. 12 ff. (Stand: 2009); BT-Drs. 16/2875, S. 10 ff. (Stand: 2006).

[77] Siehe näher zu der Stellung des Bundeskriminalamts und den Möglichkeiten zum Ausbau seiner Aufgaben und Befugnisse unten Teil 3 A. II.

> durch Erfahrungswerte oder auch Learning-by-doing, Einweisung von lebensälteren oder dienstälteren Kollegen und so den Überblick [...], so dass man da das größtmögliche Potential ausschöpfen kann." (POL1)

Da es selbst polizeilichen Anwender*innen schwerfällt, die aktiven Informationssysteme in ihrer Gesamtheit zu erfassen, überrascht es nicht, dass die Verknüpfbarkeit bzw. Interoperabilität der polizeilichen Systeme auf Bundes- und Landesebene eine praktische Herausforderung darstellt. Auf diese wird im weiteren Verlauf der Untersuchung näher einzugehen sein.[78]

Eine Beschreibung sämtlicher kriminalbehördlicher Informationsressourcen ist im Ergebnis kaum zu leisten. Zum Verständnis der Materie trägt es allerdings auch mehr bei, die kriminalbehördliche Informationsordnung in ihrer Systematik erschließen.

Es ist zunächst zwischen polizeilichen und staatsanwaltschaftlichen Informationsressourcen zu differenzieren. Obwohl vor allem viele von der Polizei erhobene und gespeicherte Daten auch für die Staatsanwaltschaften relevant sind, sind die Systeme der Polizeien und Staatsanwaltschaften weitgehend voneinander abgeschottet. Die Ursachen hierfür werden im Zusammenhang mit der Entwicklung der kriminalbehördlichen Informationsordnung näher betrachtet.[79] Die Informationssysteme der Polizei sind jenen der Staatsanwaltschaften außerdem in struktureller und technischer Hinsicht überlegen. Sie weisen weit größere Datenbestände auf, auch wenn es um die Speicherung von Informationen zu Zwecken der Strafverfolgung geht.[80] Dass die polizeilichen Bestände mit mehr Daten gefüllt sind, dürfte darauf beruhen, dass die Polizei durch ihre Tätigkeit näher am straf- und gefahrenabwehrrechtlich relevanten Geschehen und damit auch an den relevanten Informationen ist. Dass ihre Systeme technisch und strukturell weiter entwickelt sind als jene der Staatsanwaltschaften, dürfte unter anderem daran liegen, dass sich die Polizei durch ihr frühes und intensives Engagement beim Einsatz der elektronischen Datenverarbeitung einen technischen Vorsprung gegenüber den Staatsanwaltschaften verschaffte.[81] Auch heute wendet die Polizei mehr Mittel für die Weiterentwicklung ihrer Informationssysteme auf als die Staatsanwaltschaften. Die aus all dem resultierende polizeiliche Dominanz in der Informationsordnung ist der Grund dafür, weshalb in Zentrum des Interesses dieser Untersuchung vor allem die polizeilichen Informationssysteme stehen.

---

[78] Siehe unten Teil 2 A. I. und B. I.

[79] Siehe unten III. und IV.

[80] Vgl. Arbeitskreis AE, S. 119; *Puschke*, S. 170; *Schaefer*, NJW 1998, 3178; *Singelnstein*, in: FS Rogall, S. 725 (729); *Zöller*, S. 177.

[81] Siehe dazu näher unten III.

Die kriminalbehördliche Informationsordnung besteht aktuell im Wesentlichen aus voneinander getrennten Informationssammlungen, die meist als Dateien bezeichnet werden. Die Zwecke und die Ausgestaltung dieser Dateien legen Errichtungsanordnungen fest, die die Exekutive als Verwaltungsvorschriften erlässt.[82] Der Funktionsweise nach lässt sich zwischen internen Dateien, die nur von einer Stelle betrieben werden und nur für diese zugänglich sind, und Dateien, an denen sich mehrere Stellen beteiligen, unterscheiden. Die internen Dateien von Kriminalbehörden dienen in erster Linie zur Erfüllung ihrer eigenen Aufgaben und zu Zwecken der Vorgangsverwaltung.[83] Das Bundeskriminalamt betreibt als interne Systeme zu Zwecken der Strafverfolgung vor allem so genannte Amtsdateien.[84] Von diesen Dateien existierten im Jahr 2019 innerhalb der Abteilungen Schwere und Organisierte Kriminalität und Staatsschutz 377;[85] im Jahr 2023 waren es 549.[86] Die in *Fall 5* beschriebene fiktive Falldatei „Hass und Hetze im Internet" beispielsweise könnte als eine solche Amtsdatei betrieben werden. Das Bundeskriminalamt könnte diese zur Erfüllung seiner Aufgaben im Bereich Staatsschutz nutzen.

Mehrere Polizeibehörden verbindende Systeme sind bislang in Verbunddateien und Zentraldateien organisiert. Verbunddateien sind „von einer Zentralstelle geführte Dateien, in die die Teilnehmer selbst auf Stromwegen unmittelbar einspeichern und aus denen sie Daten unmittelbar abrufen können"[87]. Als führende Zentralstellen kommen im polizeilichen Zusammenhang bei bundesweiten Dateien vor allem das Bundeskriminalamt und bei landesweiten Dateien vor allem die Landeskriminalämter in Betracht.[88] INPOL-neu ist als das derzeit wichtigste polizeiliche Informationssystem mit dem Bundeskriminalamt als Zentralstelle in Verbunddateien organisiert.[89] Auf die Entwicklung von INPOL wird sogleich näher eingegangen.[90] Die von der Öffentlichkeit

[82] *Graulich*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. E Rn. 431.

[83] Darunter ist „die rein formale Begleitung" von Vorgängen zum Nachweis ihres Eingangs, ihrer Bearbeitung, ihres Ausgangs und ihres Verbleibs zu verstehen; BT-Drs. 13/1550, S. 37 (zu § 30 Abs. 2 BKAG 1997).

[84] Vgl. BT-Drs. 16/13563, S. 17 ff.; BT-Drs. 16/2875, S. 19 ff.; *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 32.

[85] BT-Drs. 19/15346, S. 3.

[86] BT-Drs. 20/6633, S. 2.

[87] *Petri*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 391; vgl. zu dem Begriff auch BT-Drs. 13/1550, S. 24; *Arzt*, NJW 2011, 352; *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 30.

[88] Das Zollkriminalamt führt darüber hinaus das Zollfahndungsinformationssystem INZOLL.

[89] Vgl. §§ 7; 11 – 13 BKAG aF.

[90] Siehe unten III.

sowie in Rechtsprechung[91] und Literatur[92] am meisten beachteten Verbunddateien sind allerdings die „Gewalttäter"-Dateien. Die bekannteste von ihnen ist die Datei „Gewalttäter Sport", die fachlich bei der Zentralen Informationsstelle Sporteinsätze (ZIS) in Nordrhein-Westfalen verortet ist, aber technisch vom Bundeskriminalamt als Zentralstelle betrieben wird.[93] Auch die in *Fall 1* referenzierte Falldatei Rauschgift ist eine Verbunddatei.

Zentraldateien unterscheiden sich von Verbunddateien dadurch, dass hier nur die Zentralstelle selbst die Daten eingibt – und nicht die Teilnehmenden.[94] Es kann sich hierbei um Daten handeln, die die Zentralstelle selbst erhoben hat, oder um Daten, die zunächst von Teilnehmenden erhoben und dann an die Zentralstelle übermittelt wurden.[95] Zentraldateien beim Bundeskriminalamt werden nicht Bestandteil von INPOL. Das Bundeskriminalamt nutzt Zentraldateien beispielsweise, um Publikationen und Akteur*innen aus bestimmten Phänomenbereichen zu katalogisieren bzw. aufzulisten.[96] Die Behörde führte im Jahr 2019 allein innerhalb der Abteilung Schwere und Organisierte Kriminalität 116 Zentral- und 32 Verbunddateien.[97]

Aktuell steht das System der kriminalbehördlichen Informationsordnung im polizeilichen Bereich vor einem grundlegenden Umbruch. Dieser könnte die etablierte Aufteilung der Informationsordnung in Dateien auf lange Sicht hinfällig machen. Durch die Umsetzung des Programmes Polizei 20/20 soll ein neues „Datenhaus" der deutschen Polizei entstehen, das zu einer stärkeren Zentralisierung des Informationswesens führt. Vereinfacht lässt sich das „Datenhaus" als einheitliche Struktur verstehen, in der Daten wie in einem Silo abgelagert werden. Es erfolgt keine weitere Strukturierung auf einer untergeordneten Ebene mehr wie dies bisher durch Dateien geschieht. Dadurch sollen Daten besser miteinander verknüpfbar und leichter erschließbar werden. Eine nähere Befassung mit dem Programm Polizei 20/20 und dem neuen „Datenhaus" erfolgt im Zusammenhang mit der Untersuchung der tatsächlichen Entwicklung der polizeilichen Informationsordnung.[98]

---

[91] Vgl. nur BVerwG NJW 2011, 405 ff.; OVG Lüneburg BeckRS 2009, 31332; OVG Magdeburg BeckRS 2012, 57512; OVG Münster DVBl. 2013, 1460 ff.

[92] Vgl. nur *Henseler*, NWVBl. 2015, 53 ff.; *Kehr*, passim; *Ruch/Feltes*, NK 2016, 62 ff.; *Spiecker gen. Döhmann/Kehr*, DVBl. 2011, 930 ff.; *Steinat*, passim.

[93] Siehe näher zu der tatsächlichen Entwicklung dieser Datei unten Teil 2 D. I. 1.

[94] Vgl. BT-Drs. 13/1550, S. 24; *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 28; *Petri*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 391.

[95] *Petri*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 391.

[96] BT-Drs. 19/15346, S. 15 ff.; mit weiteren Beispielen *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 28.

[97] BT-Drs. 19/15346, S. 3.

[98] Siehe unten III. 3.

II. Kriminalbehördliche Informationsressourcen als Vorsorgeinstrumente

Die Einrichtung kriminalbehördlicher Informationsressourcen und die Speicherung von Daten hierin dienen zu einem erheblichen Maße Vorsorgezwecken.[99] Daten werden regelmäßig nicht nur mit Blick auf eine unmittelbare Anschlussverwendung in Informationssystemen und Datenbanken abgelegt, sondern auch, um Tätigkeiten in der Strafverfolgung und Gefahrenabwehr vorzubereiten, die weit in der Zukunft liegen können. Dies veranschaulichen die am Anfang der Untersuchung geschilderten Beispielfälle. In *Fall 1* und *Fall 2* werden Konstellationen beschrieben, in denen Daten zur Unterstützung einer möglichen zukünftigen Strafverfolgung von Personen in den Bereichen der Drogenkriminalität und der Sexualdelikte gespeichert werden. Besonders im Kontext der Strafverfolgung sollen die bevorrateten Informationen die Erfolgsaussichten künftiger Verfahren verbessern, indem sie neue Ermittlungsansätze liefern oder vorhandene Ansätze unterstützen.[100] Daten finden auch Eingang in Informationsressourcen, um übergreifende Wissensgrundlagen für Kriminalbehörden zu schaffen. Die Ressourcen können dazu dienen, um Abbilder krimineller Phänomene festzuhalten oder gezielt Informationen über bestimmte Milieus zu sammeln.[101]

Im Sicherheitsbereich insgesamt ist seit Jahren ein zunehmendes Bemühen nachzuvollziehen, durch rechtliche Regelungen und hoheitliches Handeln die Verletzung von Rechtsgütern frühzeitig zu verhindern und Risiken zu minimieren, anstatt erst an späterer Stelle – etwa zur Abwehr einer konkreten Gefahr – in Kausalverläufe einzugreifen oder im Falle von Straftaten auf ihre nachträgliche Verfolgung zu setzen.[102] Dieses Bemühen lässt sich als Ausdruck eines übergreifenden Vorsorgeprinzips[103] verstehen, das nicht nur in der Sicherheitsgewährleistung, sondern auch in anderen Bereichen staatlichen Handelns zum Tragen kommt.[104] Die staatlichen Informationsressourcen spielen bei den Bemühungen um mehr Vorsorge eine wichtige Rolle. So war immer wieder zu

[99] Vgl. auch *Knemeyer*, in: FS Rudolf, S. 483 (489); *Siebrecht*, JZ 1996, 711 (713); *Zöller*, S. 86 f.

[100] Vgl. *Zöller*, RDV 1997, 163 (165).

[101] *Kötter*, S. 184; vgl. auch *Albers*, Determination, S. 129.

[102] Vgl. *Garland*, S. 306 ff.; *Kunz/Singelnstein,* S. 329 ff.; *Legnaro*, KrimJ 2018, 123 f.; *Singelnstein*, in: Brunhöber, S. 41 ff.; *Zedner,* Theoretical Criminology 11 (2007), 261 ff.

[103] Vgl. dazu *Park*, S. 211; *Voßkuhle*, in: FS Würtenberger, S. 1101 (1108); *Waechter*, JZ 2002, 854 (855); *R. Wolf*, Leviathan 15 (1987), 357 (388).

[104] Vgl. *Volkmann*, JZ 2004, 696 (700); *Hoffmann-Riem*, S. 18 f. Siehe zu den Ursprüngen des Vorsorgeprinzips in dem Begriff der Daseinsvorsorge *Ossenbühl*, NVwZ 1986, 161 (162); zum Ausdruck des Vorsorgeprinzips im Umwelt- und Technikrecht *Preuß*, in: Grimm, Staatsaufgaben, S. 523 (538 f.); *Spiecker gen. Döhmann*, in: Funke/Lachmayer, S. 181 (195).

beobachten, dass sicherheitsbehördliche Informationssysteme nach sicherheitsrelevanten Ereignissen wie Terroranschlägen neu geschaffen oder ausgebaut wurden.[105]

Neben der allgemeinen Tendenz zu mehr vorsorgendem Handeln ist auch ein Trend zur personenbezogenen Prävention festzustellen.[106] Hierbei steht das Individuum, von dem Schäden für Rechtsgüter auszugehen drohen, im Zentrum des Interesses. Im Zusammenhang mit der Nutzung kriminalbehördlicher Informationsressourcen soll besonders die Registrierung von potentiell gefährlichen Personen in Datenbanken frühzeitig Schäden vorbeugen.[107] So lässt sich etwa die Pflege der Gewalttäter-Dateien als Ausdruck eines zunehmenden Bestrebens zur personenbezogenen Prävention verstehen.

Der vorsorgende Charakter kriminalbehördlicher Informationsressourcen und ihrer Nutzung steht in einem Zusammenhang mit technologischen Entwicklungen. Schon bevor Polizei und Staatsanwaltschaften die elektronische Datenverarbeitung hierfür nutzten, bevorrateten sie Informationen oftmals, um sich für die Abwehr von Gefahren und die Verfolgung von Straftaten in der Zukunft zu rüsten.[108] Allerdings spricht viel dafür, dass die neuen technischen Möglichkeiten die Tendenz zum vorsorgenden bzw. präventiv ausgerichteten Handeln bei den Kriminalbehörden im Allgemeinen und speziell im Zusammenhang mit ihren Informationsressourcen verstärkt haben.[109]

Der Zusammenhang zwischen technologischen Entwicklungen und der Stärkung von Vorsorgetendenzen lässt sich aus einer sozio-technischen Dynamik erklären: Welche Erwartungen an die staatliche Sicherheitsgewährleistung bestehen und wie diese Aufgabe wahrgenommen wird, ist unter anderem von den hierfür zur Verfügung stehenden Mitteln abhängig. Technologische Entwicklungen erweitern das Repertoire der verfügbaren Mittel. Der technische Fortschritt ist dabei nicht bloß ein Ausdruck gesellschaftlicher Entwicklungen und Bedürfnisse. Er ermöglicht und verstärkt diese Entwicklungen und Bedürfnisse auch. Neue technische Möglichkeiten zum präventiven Rechtsgüterschutz können also die Erwartungen hieran steigern sowie eine Entwicklung zu mehr Prävention beschleunigen. Die Technik ist mit den Worten von

---

[105] Siehe unten V.

[106] Zum Begriff der personenbezogenen Prävention *Rusteberg*, in: Münkler, S. 233 (234 f.); vgl. zu der Tendenz zur Personalisierung der Risikobewältigung allgemein *Bäcker*, in: Kulick/Goldhammer, S. 147 (161 ff.); *Hanschmann*, KJ 2017, 434 (436 ff.); *Samour*, in: Kulick/Goldhammer, S. 49 f.; *Weßlau*, S. 42; vgl. speziell im Zusammenhang mit der nachrichtendienstlichen Beobachtung *Linzbach*, GSZ 2022, 7 ff.

[107] *Schulze-Fielitz*, in: FS Schmitt Glaeser, S. 407 (412 f.).

[108] Vgl. *Schoch*, Der Staat 43 (2004), 347 (353); *Trute*, in: GS Jeand'Heur, S. 403.

[109] Siehe zu der Verstärkung von Tendenzen zu präventiv ausgerichtetem Handeln durch technologische Entwicklungen *Baldus*, Die Verwaltung 2014, 1 (7); *Narr*, Bürgerrechte & Polizei/CILIP 76 (3/2003), 6 (7 f.); *Poscher*, Die Verwaltung 2008, 345 (347); *Roßnagel/Wedde/Hammer/Pordesch*, S. 52 („Prävention und IuK-Technik gehen eine symbiotische Verbindung ein.").

Tobias Singelnstein nicht nur „bloßes Hilfsmittel einer ohnehin in Gang gesetzten Entwicklung", sondern „konstitutiv für den Wandel".[110]

Die Einrichtung und Nutzung kriminalbehördlicher Informationsressourcen macht den Wandel zu mehr Prävention durch technische Entwicklungen anschaulich. Schon die Einführung der elektronischen Datenverarbeitung hat den Charakter informationsordnender Tätigkeiten sowie ihre Rechtsgrundlagen grundlegend verändert. Im Jahr 1968 postulierte der spätere BKA-Präsident *Horst Herold*, dass die elektronische Datenverarbeitung die Polizei in die Lage versetze, „ihr Augenmerk immer stärker der Verbrechensvorbeugung und Verbrechensverhütung als der [...] wichtigsten Form der Verbrechensbekämpfung zuzuwenden"[111]. *Herold* verband damit die Vision, kriminelles Verhalten mit Hilfe der elektronischen Datenverarbeitung praktisch vorauszuberechnen.[112] Dafür setzte er eine ausreichend breite Datenbasis in einer neu zu schaffenden polizeilichen Informationsordnung voraus. Der Einsatz elektronischer Datenverarbeitung, der auf der Grundlage dieser Erwartungen erfolgte, war mitursächlich dafür, dass die Vorsorge[113] umfassend als polizeiliche Aufgabe geregelt wurde.[114] Dies geschah zunächst unter dem Begriff der vorbeugenden Verbrechensbekämpfung.[115] In den 1970er-Jahren fand diese neue Aufgabe Eingang in einzelne polizeirechtliche Regelwerke.[116] Flächendeckend wurde sie allerdings erst infolge des Vorentwurfes zur Änderung des Musterentwurfes eines Polizeigesetzes von 1986 (VE ME PolG 1986) in den

[110] *Singelnstein*, in: FS Rogall, S. 725 (736).

[111] *Herold*, in: Taschenbuch für Kriminalisten, S. 240 (243).

[112] *Herold*, in: Taschenbuch für Kriminalisten, S. 240 (243). Ähnliche Visionen findet heute in Anwendungen Ausdruck, die unter dem Schlagwort „Predictive Policing" diskutiert werden; vgl. hierzu aus juristischer Sicht nur *Gless*, in: GS Weßlau, S. 165 ff.; *Hofmann*, S. 130 ff.; *Rademacher*, AöR 142 (2017), 366 ff.; *Singelnstein*, NStZ 2018, 1 ff.; *Trute/Kuhlmann*, GSZ 2021, 103 ff.; *Wischmeyer*, in: Kulick/Goldhammer, S. 193 (195 ff.); zur Entwicklung in den USA *Ferguson*, Washington University Law Review 94 (2017), 1115 ff. Zwar werden in Deutschland vorwiegend noch Maßnahmen diskutiert, um anhand nichtpersonenbezogener Daten Prognosen für zukünftiges strafbares Verhalten zu erstellen. Es erscheint aber nur eine Frage der Zeit, bis hier einzelne Personen und persönliche Verhaltensweisen in den Vordergrund rücken.

[113] Die Vorsorge hat als polizeiliche Aufgabe eine lange Tradition, fand aber bis dahin nur vereinzelt ausdrückliche Regelung; so etwa in der preußischen Verordnung wegen verbesserter Einrichtung der Provinzial-Behörden vom 30. April 1815 (GS, S. 85 ff.), die „die Vorsorge zur Abwendung allgemeiner Beschädigungen" in § 13 Nr. 2 zu den Aufgaben der Polizei zählte.

[114] Vgl. zu der technologischen Prägung dieser Aufgabe *Rachor*, S. 26; *Wellbrock*, CR 1986, 149 (154 f.).

[115] Dieser Begriff ist mit Blick auf den engen Verbrechensbegriff in § 12 Abs. 1 StGB unglücklich; vgl. zur Geschichte des Begriffs *Rachor*, S. 10 ff.

[116] Nach § 5 Abs. 1 BKAG 1973 sollte „[d]ie vorbeugende Verbrechensbekämpfung [...] Sache der Länder" bleiben; sie wurde in diesem Zusammenhang als vollständig präventive Aufgabe eingeordnet; vgl.

Polizeigesetzen eingeführt.[117] Heute verwenden die Polizeigesetze hierfür im Wesentlichen den Begriff der vorbeugenden Bekämpfung von Straftaten.[118]

Mit der Menge der verfügbaren Daten und der Weiterentwicklung von Technologien zu ihrer Speicherung und Auswertung, ist auch das Potential von Datenbanken und Informationssystemen, einen effektiven Beitrag zur Prävention zu leisten, kontinuierlich gestiegen.[119] Die kriminalbehördliche Informationsordnung ist eine notwendige Basis für andere präventive Tätigkeiten. So können Daten effizienter und vielseitiger ausgewertet werden, wenn sie richtig geordnet und gespeichert werden. Im Zusammenhang mit der personenbezogenen Prävention erscheint die massenhafte Bevorratung von Daten mit modernen Hilfsmitteln besonders vielversprechend, um darauf aufbauend Prognosen über das zukünftige Verhalten einer Person zu erstellen.[120] Diese Prognosen folgen als Form des Risikomanagements einer für die neue Kriminalpolitik charakteristischen Versicherungslogik.[121] Die Bevorratung von Daten fördert außerdem einzelfallübergreifende und überindividuelle Präventionsansätze wie etwa raumbezogene Analysen oder die Generierung von Lagebildern.[122]

III. Die Entwicklung der polizeilichen Informationsordnung

In ihrer gut fünfzigjährigen Geschichte ist die EDV-gestützte[123] polizeiliche Informationsordnung kontinuierlich gewachsen. Ihre Entwicklung wird im Folgenden in drei Phasen geschildert: Der ersten Blütezeit der EDV bei der Polizei von Anfang der 1970er-Jahre bis zum Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (1.), einer darauf folgenden Phase der Verrechtlichung und gescheiterten Neukonzipierung der Informationsordnung (2.) sowie einem seit Anfang der 2010er-Jahre nachzuvollziehenden Neuanlauf, in dem die Informationsordnung zu einem

BT-Drs. 7/178, S. 10. Vgl. auf Landesebene im Zusammenhang mit der polizeilichen Informationsverarbeitung § 27 Abs. 2 PolG BremPolG vom 21. März 1983 (BremGBl., S. 141). Außerdem fand sich die Aufgabe in § 10 Abs. 1 Nr. 2 Musterentwurf eines Polizeigesetzes von 1976 (ME PolG 1976); vgl. dazu *F. Sydow*, ZRP 1977, 119 (124).

[117] Vgl. *Kniesel/Vahle*, DÖV 1987, 953 (955 f.); siehe näher zum VE ME PolG 1986 und der Kritik am Konzept der vorbeugenden Verbrechensbekämpfung in diesem Zusammenhang unten Teil 3 B. III. 2.

[118] Art. 54 Abs. 2 Satz 1 BayPAG; § 42 Abs. 3 ASOG Bln; § 39 Abs. 4 BbgPolG; § 36 Abs. 2 HbgPolDVG; § 20 Abs. 6 Satz 1 HSOG; § 37 Abs. 1 SOG MV; § 23 Abs. 6 PolG NRW; § 52 Abs. 2 Satz 1 POG RP; § 43 Abs. 2 Satz 1 SächsPolG; § 23 Abs. 1 SOG LSA.

[119] *Bäcker*, Kriminalpräventionsrecht, S. 69.

[120] Vgl. *Rusteberg*, Föderale Sicherheitsarchitektur, S. 44.

[121] Vgl. hierzu *Kunz/Singelnstein*, S. 327 f. m.w.N.; *Lageson*, S. 65.

[122] Vgl. zu raumbezogenen Aspekten *Hofmann*, S. 86 ff.; *Singelnstein*, NStZ 2018, 1 (2).

[123] Die Betrachtung beschränkt sich hier auf die polizeiliche Informationsordnung unter dem Eindruck der elektronischen Datenverarbeitung; vgl. zu der Geschichte der Polizei als historischem „Prozess der zunehmenden Fähigkeit zur Informationsgewinnung und -verarbeitung" *Heinrich*, S. 99 f.

neuen „Datenhaus“ umgestaltet werden soll (3.). In all diesen Phasen nehmen das polizeiliche Informationssystem INPOL und seine Weiterentwicklung eine zentrale Rolle ein.

1. 1970 bis 1983: Technikeuphorie und erster Einsatz von INPOL

Eine erste „Vorphase“ der computerisierten polizeilichen Informationsordnung lässt sich vom Beginn des Einsatzes der elektronischen Datenverarbeitung in der Verwaltung Ende der 1960er-Jahre bis zu der Etablierung entsprechender Technologien beim Bundeskriminalamt Anfang der 1970er-Jahre abstecken.[124] Polizeibehörden erprobten in den 1960er-Jahren erstmals Möglichkeiten der Automatisierung kriminalpolizeilicher Datenverarbeitungen. Schon bevor die EDV sich flächendeckend bei der Polizei etablierte, setzen einzelne Organisationseinheiten entsprechende Anwendungen ein.[125] Insgesamt herrschte beim Einsatz der EDV in der polizeilichen Informationsordnung anfangs allerdings noch Zurückhaltung. Es fehlten die notwendigen finanziellen und personellen Mittel, um größere Sprünge zu machen.[126]

Dies änderte sich in der ersten Phase der EDV-gestützten Informationsordnung, die sich von Anfang der 1970er-Jahre bis zum Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983[127] eingrenzen lässt. Sie war von den ersten großen EDV-Anwendungen geprägt, die bei der Polizei zum Einsatz kamen. Vor allem das Bundeskriminalamt setzte stark auf die damals neuen Technologien. Die EDV wurde als innovatives Mittel gesehen, um den inneren Unruhen in dieser Zeit und wachsenden terroristischen Bedrohungen zu begegnen. Noch am Ende der 1960er-Jahre war das Bundeskriminalamt in diesem Zusammenhang heftiger Kritik hinsichtlich seiner Funktionsfähigkeit ausgesetzt gewesen.[128] Der Einsatz der Informationstechnik im Bundeskriminalamt und die damit verbundenen Innovationen werden bis heute stark mit der Person von *Horst Herold* verbunden, der *Paul Dickopf* im September 1971 als Präsiden-

[124] Vgl. zu den ersten Überlegungen zum Einsatz elektronischer Datenverarbeitung im kriminalpolizeilichen Meldedienst *Mangold*, S. 67 ff.; zum Stand der Informatisierung am Anfang der 1970er-Jahre *Heinrich*, S. 163 ff.

[125] Vgl. zur Stadtpolizei München *M. Schreiber*, Die Polizei 1967, 71 f.; zu den Tätigkeiten der Arbeitsgruppe „Elektronik“ im Bundeskriminalamt seit 1966 *Dickopf/Holle*, S. 114 ff.; *Mangold*, S. 79 ff.; *Schramm*, in: BKA, Datenverarbeitung, S. 13 ff.; im Überblick *Bergien*, Zeithistorische Forschungen, 2017, 258 (264 ff.) m.w.N.

[126] *Abbühl*, S. 122 m.w.N.

[127] BVerfGE 65, 1.

[128] Vgl. *Abbühl*, S. 123 m.w.N.

ten der Behörde ablöste. Während *Dickopf* als technikskeptisch galt und sich einer Nutzung der EDV eher entgegen stellte,[129] galt *Herold* als „Computer-Enthusiast“[130] und räumte dem Einsatz von Computertechnik einen hohen Stellenwert ein.[131] Auch über den Aspekt der Informationsordnung hinaus erlebte das Bundeskriminalamt in dieser Zeit einen Aufschwung. Die Behörde wuchs und wurde mit immer mehr Aufgaben betraut.[132] Dies geschah zum Teil als Reaktion auf die terroristischen Anschläge der Roten Armee Fraktion in dieser Zeit und zum Teil aus einem allgemeinen Bestreben der damaligen Bundesregierung heraus, die Verwaltungsstrukturen des Bundes zu stärken. Eine Rolle dabei, dass das Bundeskriminalamt in dieser Zeit florierte, spielte aber auch das Aufkommen der Computertechnik.[133]

Anfang der 1970er-Jahre erhielt das Bundeskriminalamt die Funktion einer Zentralstelle für den elektronischen Datenverbund der deutschen Polizeien,[134] welche ihm gesetzlich ausdrücklich durch eine Reform des BKAG im Jahr 1973[135] zugewiesen wurde.[136] Bereits 1972 nahm das zentrale Rechenzentrum des Bundeskriminalamts seine Tätigkeit auf und das INPOL-System mit seiner Funktion zur Personenfahndung ging erstmals in Betrieb. Bis zu diesem Zeitpunkt hatte noch das Deutsche Fahndungsbuch – ein umfangreiches Druckwerk – als primäres Hilfsmittel bei der Fahndung gedient. Die Inbetriebnahme von INPOL steigerte die Aktualität und die Menge der zur Verfügung stehenden Fahndungsdaten innerhalb kurzer Zeit erheblich.[137] Als Ziel von INPOL gab das Bundeskriminalamt schon zu dieser Zeit aus, es zu „ermöglichen, Informationen bundesweit jeder interessierten Polizeibehörde unkompliziert und schnell zur Verfügung zu stellen.“[138] INPOL war der erste Baustein für ein umfassendes „ge-

[129] *Bergien*, Zeithistorische Forschungen, 2017, 258 (263 f.).

[130] *Bergien*, Zeithistorische Forschungen, 2017, 258 (265) m.w.N.; vgl. auch *Herold* im Interview mit *Cobler*, Transatlantik 11/1980, 29 (40).

[131] Vgl. dazu *Harnischmacher/Semerak*, S. 197; *Klink*, in: FS Herold, S. 65 (87, 92); *Schwinghammer*, KrimJ 1980, 241 (246 ff.); *H. Albrecht*, S. 301.

[132] *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (7) spricht von einer „Boom-Phase“ des Bundeskriminalamts.

[133] *Abbühl*, S. 146; *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (7).

[134] Vgl. dazu *Schweppe*, S. 49.

[135] Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes in der Fassung vom 29. Juni 1973, BGBl. I, S. 704 ff.

[136] Siehe näher zu der gesetzlichen Aufgabe des BKA als Zentralstelle und deren Entwicklung im Laufe der Zeit unten Teil 3 A. II. 1.

[137] *Abbühl*, S. 149 f.

[138] *Lodde*, in: BKA, Datenverarbeitung, S. 25.

meinsames Informations- und Auskunftssystem für die gesamte Polizei in der Bundesrepublik mit dem Bundeskriminalamt als Zentralstelle“[139]. Durch die Ergänzung von Dateien und Anwendungen entwickelte sich INPOL in der Folgezeit kontinuierlich weiter. 1974 erhielt es eine Funktion der Sachfahndung und wurde 1975 um die Funktion des elektronischen Aktennachweises erweitert.[140]

Inzwischen sind zahlreiche weitere Dateien und Funktionen hinzugekommen. Die grundlegende Funktionsweise von INPOL hat sich dabei nicht geändert. Das System basiert auf einer autonomen Funktion der Informationssysteme der Polizeien des Bundes und der Länder. INPOL ist bis heute in Dateien gegliedert,[141] für deren Errichtung eine Anordnung unter Festlegung der Zwecke der Datenspeicherung erforderlich ist.[142] Die Bedeutung von INPOL für die polizeiliche Arbeit ist immens.[143]

Der Einsatz der EDV erfolgte in der hier beschriebenen ersten Phase zunächst zur Bewältigung konkreter Probleme und einer „Informationsflut“ bei der Polizei.[144] Die Anwender*innen versprachen sich von den neuen Technologien der Datenverarbeitung, einer zunehmenden Masse von Informationen Herr zu werden.[145] Die einzelnen polizeilichen Stellen entwickelten ihre Anwendungen auf eigene Faust, woraus eine starke Fragmentierung der polizeilichen EDV-Strukturen resultierte. Es entstanden zahlreiche einzelne Systeme, die nicht miteinander vernetzt oder kompatibel waren. Dass die Verteilung der Systeme und der darin abgelegten Daten auf unterschiedliche Polizeistellen praktisch zugleich zu einer Art „informationeller Gewaltenteilung“[146] führte, stellte sich dabei eher als unbeabsichtigter Nebeneffekt dar denn als gezielte

[139] Ständige Konferenz der Innenminister und -senatoren des Bundes und der Länder, Programm für die innere Sicherheit in der Bundesrepublik Deutschland, Teil I, Beilage zu GMBl. Nr. 31/1972, S. 9; vgl. zur Bedeutung von INPOL für die Informatisierung der Polizei insgesamt auch *Heinrich*, S. 166 f.

[140] Vgl. zum Ausbaustand von INPOL im Jahr 1978 *Wiesel/Gerster*, S. 53 ff.

[141] Vgl. zu den wichtigsten Dateien im alten INPOL *Zöller*, S. 141 ff.

[142] Vgl. hierzu § 34 BKAG aF.

[143] Vgl. BMI, Polizei 2020, S. 16; *Ogorek*, ZRP 2023, 86 f.; *Rusteberg*, Föderale Sicherheitsarchitektur, S. 64.

[144] *Bergien*, Zeithistorische Forschungen, 2017, 258 (264); *Busch/Funk/Kauß/Narr/Werkentin*, S. 115; *Schweppe*, S. 49; vgl. auch *Boge*, Kriminalistik 1982, 619; *Herold* im Interview mit *Cobler*, Transatlantik 11/1980, 29 (36); *Herold*, Universitas 1976, 63 ff.

[145] Ähnliche Erwägungen existierten bei der Informationsverarbeitung zu juristischen Zwecken. So vertrat *Spiros Simitis* die Auffassung, ein zunehmender Einsatz der elektronischen Datenverarbeitung im juristischen Bereich sei geboten, um einer „Informationskrise“ des Rechts entgegenzuwirken, die durch eine unüberschaubare Flut rechtlicher Regelungen ausgelöst werde; *Simitis*, S. 56, 107; vgl. dazu auch *Fiedler*, JuS 1970, 603.

[146] Vgl. zu der „informationellen Gewaltenteilung“ als Aspekt der datenschutzrechtlichen Zweckbindung unten Teil 3 D. III. 3.

Maßnahme zum Datenschutz. Das Datenschutzrecht stand zu diesem Zeitpunkt überhaupt erst am Anfang seiner Entwicklung. Eine größere Rolle für den Aufbau der polizeilichen Informationssysteme spielten organisatorische Aspekte und Kompetenzvorgaben. Angesichts der Fragmentierung der Informationssysteme der Polizei in Bund und Ländern sind schon in dieser frühen Phase erste Bemühungen zur Zentralisierung der EDV-Struktur festzustellen. *Horst Herold* bemerkte, dass nicht eine „Zentralisation der Organisation" nötig sei, sondern die „Zentralisierung der wechselseitigen Informationsmöglichkeiten" verschiedener Polizeistellen.[147] Dies lässt sich als eine Forderung nach einer verbesserten informationellen Vernetzung der Polizeien verstehen. Sie führte zu dieser Zeit allerdings nicht zu nachvollziehbaren Ergebnissen.

Nach den raschen Fortschritten in den 1970er-Jahren begann die Entwicklung von INPOL zu Beginn der 1980er-Jahre zu stocken.[148] Als Gründe hierfür werden einerseits die technischen Leistungsgrenzen des Systems und andererseits die steigende Sensibilität für den Datenschutz in dieser Zeit angeführt.[149] Nach dem Aufblühen der polizeilichen Informationsordnung in den 1970er-Jahren war die Folgezeit stark von der rechtlichen Einordnung der geschaffenen Anwendungen[150] und anderen Themen wie der Bekämpfung der Organisierten Kriminalität[151] geprägt.

2. 1983 bis 2010: Verrechtlichung und INPOL-Neukonzeption

Einen Einschnitt in die Entwicklung der polizeilichen Informationsordnung bedeutete das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983.[152] Mit der Anerkennung des Rechtes auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG machte es eine rechtliche Regelung für sämtliche Verarbeitungen personenbezogener Daten der Polizei und anderer Behörden erforderlich.[153] Dies galt auch für Datenverarbeitungen im Zusammenhang mit polizeilichen Informationssystemen wie INPOL. Grundlage für den Betrieb von INPOL waren zunächst von der

[147] *Herold*, in: Göppinger/Witter, S. 208 (231); vgl. dazu *Harnischmacher/Semerak*, S. 197; *Schwinghammer*, KrimJ 1980, 241 (246); ähnlich schon *Herold*, in: Taschenbuch für Kriminalisten, S. 240 (246 ff.); für dezentrale Systeme hingegen *Schweinoch*, Die Polizei 1984, 292.

[148] *Abbühl*, S. 161; *Küster*, in: FS BKA, S. 107 (114); *Kennhöfer*, Kriminalistik 1987, 182; vgl. zu dem von der Innenministerkonferenz beschlossenen Konzept für die Fortentwicklung des polizeilichen Informationssystems INPOL vom 12. Juni 1981 *Heinrich,* S. 180 ff.; *Schweinoch*, Die Polizei 1984, 292; *Wiesel*, Kriminalistik 1986, 587.

[149] *Abbühl*, S. 161; vgl. auch *Heinrich*, S. 102; *Nogala*, S. 62 ff.

[150] Vgl. *Bull*, iur 1986, 287 (293).

[151] *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (7).

[152] BVerfGE 65, 1.

[153] Siehe näher unten C. III. 1. a.

Innenministerkonferenz beschlossene Richtlinien und Datei-Errichtungsanordnungen gewesen.[154] Erst im Jahr 1997 sollten im Rahmen einer grundlegenden Reform des BKAG,[155] der mehrere gescheiterte Versuche vorangegangen waren,[156] die Vorgaben des Volkszählungsurteils umgesetzt[157] und eine gesetzliche Grundlage für INPOL geschaffen werden (§§ 7 ff. BKAG 1997)[158].

Während die Regelung von Rechtsgrundlagen für das bisherige System noch nicht abgeschlossen war, wurde 1992 bereits die Entwicklung seines Nachfolgers INPOL-neu offiziell angestoßen. Die Arbeitsgemeinschaft der Innenminister der Länder setzte hierfür durch den Arbeitskreis II „Innere Sicherheit" eine Projektgruppe ein. Ein erstes fachliches Grobkonzept für INPOL-neu lag im November 1992 vor.[159] Dieses Konzept analysierte anhand einer Beschreibung des Zustandes des bisherigen Systems dessen Schwachstellen und entwickelte daraus Anforderungen an ein moderneres Informationssystem, das das alte INPOL ersetzen sollte.[160]

An dem bisherigen INPOL wurden grundlegende Mängel festgestellt, was unter anderem seine technische Leistungsfähigkeit betraf.[161] Als ein zentrales Problem wurde die Notwendigkeit der redundanten sowie sehr aufwändigen Erfassung und Speicherung von Daten genannt.[162] Diese Notwendigkeit brachte die Aufteilung von INPOL in einzelne Systeme von Bund und Ländern mit sich.[163] Bisweilen schreckte sie Nutzer*innen des Systems von der Eingabe von Daten ab, weil sie einen zusätzlichen Arbeitsaufwand bedeutete.[164] Weitere Probleme bestanden bei operativen Auswertungen sowie bei der Integration der alten, für INPOL verwendeten Software in moderne EDV-Systeme.[165] Letztlich war das aus den frühen 1970er-Jahren stammende INPOL-

---

[154] GMBl. Nr. 7/1981, S. 114 ff., 119 ff.; vgl. dazu *Abbühl*, S. 149; *Dix*, JURA 1993, 571 (574); *Zöller*, S. 140.

[155] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten vom 7. Juli 2997; BGBl. I, S. 1650 ff.; vgl. zu den Inhalten der Reform im Einzelnen *Lersch*, in: FS Herold, S. 35 (40 ff.); *W. Schreiber*, NJW 1997, 2137 ff.

[156] Vgl. *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (8).

[157] Vgl. BT-Drs. 13/1550, S. 19.

[158] Die für die Speicherung von Daten im Rahmen der Funktion als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen zentralen Regelungen fanden sich dabei in §§ 8, 9 BKAG 1997. Den Betrieb von INPOL regelten §§ 11-13 BKAG 1997.

[159] *Busch*, Bürgerrechte & Polizei/CILIP 76 (3/2003), 12.

[160] *Sehr*, Kriminalistik 1999, 532.

[161] *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (10); *Sehr*, Kriminalistik 1999, 532.

[162] *Busch*, Bürgerrechte & Polizei/CILIP 76 (3/2003), 12 (14); *Zöller*, S. 149, vgl. auch *Rublack*, DuD 1999, 437; *Sehr*, Kriminalistik 1999, 532.

[163] *Abbühl*, S. 169.

[164] *Sehr*, Kriminalistik 1999, 532.

[165] Vgl. *Rublack*, DuD 1999, 437; *Sehr*, Kriminalistik 1999, 532; *Zöller*, S. 149.

Konzept, das auf einer veralteten Technologie für Großrechenanlagen beruhte, mittlerweile aus der Zeit gefallen.[166]

Ziel der Entwicklung von INPOL-neu war ein oberflächenloses System, das sich aus dem Vorgangsbearbeitungssystemen der Polizeien der Länder und des Bundes speiste. Beim Bundeskriminalamt sollte die zentrale Kommunikationsschnittstelle liegen, auf die die Teilnehmer*innen[167] des Systems von ihren Arbeitsplätzen aus sollten zugreifen können.[168] Hier sollte ein gemeinsamer „Datenpool" von Bundeskriminalamt und Landespolizeien entstehen.[169] Dieser sollte es ermöglichen, die Datensätze von INPOL nicht in den jeweiligen einzelnen Anwendungen, sondern in einer zentralen Datenbank zu speichern.[170] Der zentrale Datenpool sollte dabei über ein komplexes System von Zugriffsberechtigungen erschlossen werden.[171] Dieses Berechtigungssystem sollte auch die Vereinbarkeit von INPOL-neu mit den datenschutzrechtlichen Grundprinzipien der Zweckbindung und Erforderlichkeit sicherstellen.[172] Der Datenpool sollte vor allem das geschilderte Problem der Notwendigkeit einer redundanten Datenerfassung lösen.[173] Er sollte auch eine weitergehende Verknüpfung der bisher vorhandenen Informationen als bisher und eine ganzheitliche Betrachtung von Phänomenen der Kriminalität ermöglichen.[174]

Konzeptionell sollte INPOL-neu mit seinem Datenpool eine Verschlankung gegenüber dem bisherigen INPOL-System herbeiführen. Letztlich konnte diese Konzeption aber nicht verhindern, dass INPOL nach der Reform wieder anwuchs. Das Bundeskriminalamt hatte zunächst die Vorstellung, den „Datenpool" nur grob in „Teilmengen

[166] *Busch*, Bürgerrechte & Polizei/CILIP 76 (3/2003), 12 (13).

[167] Der Teilnehmerkreis sollte dabei jenem von INPOL-alt entsprechen, ein Zugriff der Staatsanwaltschaften war weiterhin nicht vorgesehen; *Rublack*, DuD 1999, 437 (438).

[168] *Rublack*, DuD 1999, 437 (438); *Sehr*, Kriminalistik 1999, 532 (533).

[169] Vgl. *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (10); *Petri*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 120; *Rublack*, DuD 1999, 437 (438); *Sehr*, Kriminalistik 1999, 532 (534); *Zöller*, S. 152.

[170] *Abbühl*, S. 169.

[171] *Heinrich*, S. 219 f. In den Berechtigungsbereichen sollte dabei zwischen Grundinformation, Fallinformationen, besonders schützenswerte Informationen aus einzelnen Phänomenbereichen wie der Organisierten Kriminalität und Geldwäsche sowie vereinzelte Sonderbereiche unterschieden werden; vgl. dazu näher *Rublack*, DuD 1999, 437 (439).

[172] *Rublack*, DuD 1999, 437 (438 f.).

[173] *Heinrich*, S. 220; *Rublack*, DuD 1999, 437 (438).

[174] *Sehr*, Kriminalistik 1999, 532 (534); vgl. auch *Petri*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 120.

aufzuspalten und lediglich für diese umfassende Errichtungsanordnungen vorzulegen“[175]. Dem wurde allerdings aus datenschutzrechtlichen Gründen eine Absage erteilt.[176] Aus diesem Grund sollte das System auch künftig an dem eher kleinteiligen Aufbau in delikt- und phänomenorientierte Dateien festhalten, von dem man sich eigentlich verabschieden wollte.[177] Letztlich hat die Strukturierung von INPOL in Dateien noch bis heute Bestand.

Praktisch begegnete die Einrichtung von INPOL-neu erheblichen Schwierigkeiten.[178] Der Prozess zur Umsetzung des Systems nahm deutlich mehr Zeit in Anspruch als geplant. 1995 lag ein erstes technisches Grobkonzept für INPOL-neu vor.[179] Ab Oktober 1996 arbeitete eine Bund-Länder-Projektgruppe an seiner Umsetzung.[180] Nachdem 1998 mit der Programmierung begonnen worden war, gelang es jedoch nicht, die Umsetzung des Konzepts wie geplant abzuschließen.[181] Die ursprünglich für Ende 1999 bzw. Anfang 2000 geplante[182] Einführung des Systems musste zunächst verschoben werden. Auch ein Probelauf im Frühjahr 2001 war nicht von Erfolg gekrönt, so dass es zu einer weiteren Verschiebung kam.[183] Das ursprüngliche Konzept wurde in der Folge aufgegeben und INPOL-neu in einer reduzierten Form realisiert.[184] Im Jahr 2003 ging INPOL-neu als bundesländerübergreifendes Informationssystem der Polizeien beim Bundeskriminalamt an den Start.[185] Das System ist in die Bereiche INPOL-Zentral/Bund und INPOL-Land aufgeteilt und sternförmig angelegt.[186] Die Datenbestände der Länder basieren auf eigenständigen EDV-Systemen und sind mit der zentralen Datenverarbeitung beim Bundeskriminalamt verbunden.

Das reduzierte INPOL-neu konnte seine ursprünglichen Versprechen nur sehr eingeschränkt einlösen. Eine umfassende Kompatibilität der polizeilichen Informationssysteme wurde nicht erreicht. Das problematische Erfordernis, Daten redundant einzugeben, besteht auch in dem neuen System fort.[187] Eine echte Zentralisierung erfolgte

[175] *Rublack*, DuD 1999, 437 (439).
[176] *Rublack*, DuD 1999, 437 (439).
[177] Vgl. *Sehr*, Kriminalistik 1999, 532 (533).
[178] Ausführlich dazu *Heinrich*, S. 221 ff.
[179] *Rublack*, DuD 1999, 437.
[180] Vgl. dazu *Sehr*, Kriminalistik 1999, 532 (536).
[181] Vgl. *Gadorosi*, Kriminalistik 2003, 402; *Rublack*, DuD 1999, 437 (438).
[182] *Rublack*, DuD 1999, 437 (438).
[183] Der Spiegel 15/2001, S. 19; *Abbühl*, S. 170; *Zöller*, S. 153.
[184] Vgl. *Abbühl*, S. 170 f.
[185] Vgl. *Busch*, Bürgerrechte & Polizei/CILIP 76 (3/2003), 12.
[186] Vgl. *Abbühl*, S. 149.
[187] BT-Drs. 18/11163, S. 84; *Gadorosi*, Kriminalistik 2003, 402 (407).

nicht. Die Gesamtphilosophie von INPOL-neu war vorerst gescheitert.[188] Diverse bereits mit INPOL-neu verbundene Ziele finden sich nunmehr in dem Konzept eines neuen „Datenhauses" für die Polizei wieder, das sogleich näher betrachtet wird.[189] Dieses Projekt soll zur Bewältigung ähnlicher Herausforderungen dienen wie seinerzeit INPOL-neu und eine Homogenisierung sowie Zentralisierung der polizeilichen Informationsordnung herbeiführen.[190] Die Probleme bei der Einrichtung von INPOL-neu nachzuvollziehen, erscheint daher besonders wichtig, um die aktuellen Entwicklungen kritisch würdigen zu können.

Ein erhebliches Hindernis bei der Einführung von INPOL-neu war die Komplexität der bereits bestehenden Ländersysteme. Die Entwicklung anschlussfähiger Systeme in den Ländern bereitete unerwartete Herausforderungen.[191] Es gelang nicht, die Umstellung aller Informationssysteme in Bund und Ländern wie geplant synchron in einem kleinen Zeitfenster zu realisieren.[192] Ein Grund für diese Schwierigkeiten mag in einer mangelhaften Koordination zwischen Bund und Ländern bei der Anpassung der Informationssysteme gelegen haben.[193] Es ist aber auch zu bezweifeln, dass alle Länder nach ihren besten Möglichkeiten an der Umstellung mitwirkten. Die Umstellung begegnete auf Landesebene mitunter erheblichen Widerständen, da die Polizeien der Länder durch die aufwändige Einrichtung eigener Informationssysteme teils bereits Tatsachen geschaffen hatten, bevor eine Einigung über die Einrichtung und Funktionsweise von INPOL erfolgte.[194]

3. Seit 2010: Der Weg zum neuen „Datenhaus"

Eine dritte – noch andauernde – Phase der Entwicklung der kriminalbehördlichen Informationsordnung lässt sich seit Anfang der 2010er-Jahre nachvollziehen. Diese Phase ist von einem Bedürfnis geprägt, vorhandene Datenbestände besser als bisher miteinander zu verknüpfen, was im Zusammenhang mit den operativen Bedürfnissen der Kriminalbehörden noch näher zu thematisieren sein wird.[195] Eine größere Diskussion über die Defizite bei der Verknüpfbarkeit von Datenbeständen bei der Polizei – und auch

---

[188] Vgl. *Sehr*, Kriminalistik 1999, 532 (536); anders *Gadorosi*, Kriminalistik 2003, 402 (404), der relativierend von einer konsequenten Orientierung an der ursprünglichen Grundphilosophie spricht.

[189] Siehe unten 3.

[190] Vgl. im Zusammenhang mit INPOL-neu *Rublack*, DuD 1999, 437; *Sehr*, Kriminalistik 1999, 532 (533).

[191] *Liborius*, Kriminalistik 1999, 686; *Rublack*, DuD 1999, 437 (438); *Sehr*, Kriminalistik 1999, 532 (536).

[192] *Gadorosi*, Kriminalistik 2003, 402.

[193] *Liborius*, Kriminalistik 1999, 686.

[194] Vgl. *Abbühl*, S. 148 f.; *Heinrich*, S. 223.

[195] Siehe unten Teil 2 B.

anderen Sicherheitsbehörden – löste zuletzt die Aufdeckung der NSU-Terrorzelle im November 2011 aus.[196] In der Folge beschloss die Innenministerkonferenz die frühzeitige Einführung des Polizeilichen Informations- und Analyseverbunds (PIAV),[197] durch den im polizeilichen Informationsverbund gespeicherte Daten aufbereitet und ausgewertet werden können.[198] Der PIAV befindet sich seit März 2017 in einem Wirkbetrieb, der kontinuierlich ausgebaut wird.[199]

Mittlerweile sind die Bemühungen um den Ausbau des PIAV in dem Projekt Polizei 20/20[200] aufgegangen,[201] durch das die polizeiliche Informationsordnung grundsätzlich reformiert werden soll. Im Zentrum dieses Vorhabens steht ein neues „Datenhaus", das langfristig INPOL-neu ersetzen soll. In dem Konzept des Datenhauses finden sich viele Wünsche wieder, die bereits mit der Einführung von INPOL-neu verknüpft waren. Rechtliche Impulse für eine Umgestaltung der polizeilichen Informationsordnung lieferten das Urteil des Bundesverfassungsgerichts zum BKAG vom 20. April 2016[202] sowie die im Rahmen der europäischen Datenschutzreform am 27. April 2016 verabschiedete Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (JI-Richtlinie).[203]

Im Folgenden wird zunächst erörtert, wie das neue Konzept der polizeilichen Informationsordnung rund um das „Datenhaus" entstanden ist (a.) und wie seine Struktur geplant ist (b.). Anschließend wird bestehende Kritik an diesem Vorhaben aufgegriffen und eine eigene kritische Würdigung vorgenommen (c.).

a. Entstehung des neuen Konzepts

Als wichtiger rechtlicher Ausgangspunkt für die Entwicklung des neuen Konzepts der polizeilichen Informationsordnung gilt das Urteil des Bundesverfassungsgerichts zum

[196] Siehe dazu auch unten V.

[197] IMK, Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 193. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder, S. 32.

[198] Vgl. *Burczyk*, Bürgerrechte & Polizei/CILIP 121 (4/2020), 16 (19).

[199] BKA, Meldung vom 7. März 2017, abrufbar unter https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/170307_PIAV.html.

[200] Das Programm hieß zunächst Polizei 2020, wurde dann aber umbenannt. Die Nennung einer Jahreszahl im Titel wurde im Nachhinein als unglücklich angesehen, da das Jahr 2020 nicht als Zeitpunkt der Umsetzung des Programmes vorgesehen war; Behörden Spiegel vom 1. März 2021, abrufbar unter https://www.behoerden-spiegel.de/2021/03/01/zwischen-anspruch-und-wirklichkeit/. Der neue Titel bezieht sich offenbar auf die 20 teilnehmenden Polizeibehörden und spielt auf die normale Sehschärfe 20/20 nach dem Snellen-Index an.

[201] BMI, Polizei 2020, S. 22, 28.

[202] BVerfGE 141, 220.

[203] Siehe näher zu dieser unten C. III. 1. b.

BKAG vom 20. April 2016.[204] In dieser Entscheidung äußerte sich das Gericht grundsätzlich zu den Voraussetzungen und Grenzen verdeckter polizeilicher Informationsbeschaffung.[205] Auch wenn sich die Entscheidung unmittelbar vor allem auf Aspekte der Informationsgewinnung bezog, ist sie auch von Bedeutung für die rechtliche Bewertung von informationsordnenden Tätigkeiten.[206] Das Bundesverfassungsgericht unterschied in seinen Ausführungen zwischen Ermittlungsbefugnissen, die Datenerhebungen gestatten, und Regelungen zur weiteren Verwendung dieser Daten. Für das Speichern und Ordnen von Daten sind letztere Ausführungen relevant. Hier äußerte sich das Gericht insbesondere zu den Voraussetzungen der Zweckbindung und Zweckänderung von personenbezogenen Daten. Die Voraussetzungen für eine Zweckänderung knüpfte es dabei an den Grundsatz der hypothetischen Datenneuerhebung, der im Detail später zu betrachten sein wird.[207]

Von politischer Seite waren die entscheidenden Anstöße für die Neukonzeption der polizeilichen Informationsordnung die am 30. November 2016 von der Innenministerkonferenz verabschiedete Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit und das Programm Polizei 20/20. Die Saarbrücker Agenda gab das übergreifende Ziel aus, eine gemeinsame, moderne und einheitliche Informationsarchitektur der deutschen Polizeien zu schaffen.[208] Die in Bund und Ländern jeweils eigenständig eingerichteten Informationsstrukturen wurden hierbei als Hindernisse für den Informationsaustausch ausgemacht. Als konkrete Ziele nannte die Agenda unter anderem einen verbesserten Zugriff auf relevante Informationen für polizeiliche Anwender*innen, eine einfache und anwenderfreundliche Informationstechnik sowie eine einheitliche Entwicklung von polizeilichen IT-Angeboten für Bund und Länder.

In der Folge schuf der Bundesgesetzgeber mit dem Gesetz zur Neugestaltung des Bundeskriminalamtsgesetzes vom 8. Juni 2017[209] die Rahmenbedingungen für die neue polizeiliche Informationsordnung auf Seiten des Bundeskriminalamts. Die Regelungen hierzu orientierten sich an dem Urteil des Bundesverfassungsgerichts zum BKAG vom 20. April 2016. Der Grundsatz der hypothetischen Datenneuerhebung wurde so zur gesetzlichen Voraussetzung für die Weiterverarbeitung von personenbezogenen Daten

[204] Vgl. BT-Drs. 18/11163, S. 2.

[205] Gegenstand des Urteils waren die Regelungen des BKAG zur Übertragung der Aufgabe der Abwehr von Gefahren des internationalen Terrorismus. Das Gericht erklärte hierbei einzelne Vorschriften des BKAG für verfassungswidrig und nichtig.

[206] Vgl. zu der Bedeutung für das Sicherheitsrecht insgesamt *Rusteberg*, KritV 2017, 25 (29).

[207] Siehe unten Teil 3 C. II. 3.

[208] Saarbrücker Agenda zur Informationsarchitektur der Polizei als Teil der Inneren Sicherheit vom 30. November 2016, abrufbar unter https://www.medienservice.sachsen.de/medien/medienobjekte/110307/download.

[209] BGBl. I 2017, S. 1354 ff.

gemacht, womit er auch für informationsordnende Tätigkeiten maßgeblich wurde. Die Landesgesetzgeber folgten teilweise diesem Beispiel und schufen ähnliche Regelungen in ihren Polizeigesetzen.[210]

Der Bundesgesetzgeber nahm den Standpunkt ein, dass „[d]ie bestehende IT-Architektur des Bundeskriminalamtes, insbesondere das polizeiliche Informationssystem INPOL, [...] für die Umsetzung der Vorgaben aus dem Urteil des Bundesverfassungsgerichts vom 20. April 2016 nicht ausgelegt und daher grundlegend neu zu strukturieren“[211] sei. Diese Annahme legte daraufhin auch das Programm Polizei 20/20 zugrunde.[212] Bei näherer Betrachtung erweist sich die Annahme, dass das Urteil des Bundesverfassungsgerichts eine derart drastische Umstellung der polizeilichen Informationsordnung erforderte, aber als unzutreffend. Die Entscheidung des Gerichts bezog sich auf die Verarbeitung von Daten aus verdeckten Überwachungsmaßnahmen; die hier formulierten Grundsätze sind nicht ohne Weiteres auf andere Bereiche der Datenverarbeitung übertragbar.[213] Im Übrigen gaben auch die eher allgemeinen datenschutzrechtlichen Vorgaben der JI-Richtlinie an die polizeiliche Informationsordnung[214] keinen Anlass zu einer weitreichenden Änderung ihrer Struktur.[215]

Nach Verabschiedung des neuen BKAG konkretisierte im Januar 2018 ein White Paper zu dem Programm Polizei 20/20 die Pläne zur Neukonzeption der Informationsordnung.[216] Als strategische Ziele des Programmes nennt es die Verbesserung der Verfügbarkeit polizeilicher Informationen, die Erhöhung der Wirtschaftlichkeit des polizeilichen Informationswesens und die Stärkung des Datenschutzes durch Technik.[217] Als eine Maßnahme zur Umsetzung dieser Ziele und einen zentralen Bestandteil des Programmes beschreibt das White Paper ein neues „gemeinsames Datenhaus der deutschen Polizei“[218]. Das „Datenhaus“ soll eine stärkere Zentralisierung des polizeilichen Informationswesens bewirken. Vorgesehen ist eine „zentrale Datenhaltung im Bundeskriminalamt“[219] in einem von diesem zu diesem Zweck zur Verfügung gestellten[220] Sys-

[210] Siehe etwa § 15 BWPolG; § 20 HSOG; § 23 PolG NRW; § 51 POG RP; § 13b SOG LSA.
[211] BT-Drs. 18/11163, S. 2.
[212] BMI, Polizei 2020, S. 3.
[213] Dazu im Einzelnen unten Teil 3 C. II. 3 b.
[214] Siehe dazu näher unten C III. 1. b.
[215] So auch BfDI, Stellungnahme BKAG 2018, S. 2.
[216] BMI, Polizei 2020.
[217] BMI, Polizei 2020, S. 8 ff.
[218] BMI, Polizei 2020, S. 11.
[219] BT-Drs. 18/11163, S. 2; vgl. auch BMI, Polizei 2020, S. 2.
[220] Vgl. § 29 Abs. 1 Satz 2 BKAG.

tem. Dies soll zu einer leichteren Verfügbarkeit und Abfrage von Daten führen als bisher.[221] Eine Verknüpfung von Daten aus verschiedenen Beständen soll vereinfacht werden.[222] Die zentrale Datenhaltung beim Bundeskriminalamt soll allerdings nicht zu einer Verantwortlichkeit des Bundeskriminalamts für die Speicherung führen; „der Datenbesitz und damit die Verantwortung für die Daten" sollen „weiterhin bei den jeweiligen Polizeien des Bundes und der Länder verbleiben." [223]

Mit diesen Plänen und dem seit Mai 2018 geltenden BKAG wurde eine grundlegende Veränderung der polizeilichen Informationsordnung angestoßen. Ob, wann und wie das „Datenhaus" umgesetzt wird, ist allerdings schwer einzuschätzen. Die Erfahrungen mit vergangenen Projekten zur Restrukturierung der polizeilichen Informationsordnung legen eher eine vorsichtige Prognose nahe. Besonders die holprige Umsetzung von INPOL-neu, mit der ähnliche Ziele verfolgt wurden wie mit dem neuen „Datenhaus", kann hier als mahnendes Beispiel dienen.[224] Fest steht, dass die bisherige Informationsordnung rund um INPOL jedenfalls mittelfristig von praktischer Bedeutung bleiben wird. Es ist geplant, die neue Informationsordnung in einem schrittweisen Transformationsprozess einzuführen.[225] Dabei sollen die bisherigen Systeme zumindest solange aufrecht erhalten werden, wie dies zur Sicherung der Funktionsfähigkeit der Polizei erforderlich ist.[226] Bemerkenswert ist, dass der Transformationsprozess derart offen angegangen wird, dass kein konkretes Zieldatum für die Umstellung anvisiert wurde.[227] Zwar schätzte die Gesetzesbegründung zum BKAG 2018 noch einen Zeitraum von ca. fünf Jahren „für die Erneuerung der INPOL-Systemlandschaft"[228], in dem Konzept Polizei 2020 erfolgt aber keine Festlegung auf einen bestimmten Zeitraum.[229] Mittlerweile heißt es von Seiten des BMI, dass die Zielarchitektur im Jahr 2030 erreicht werden soll.[230] Die flexible Zeitplanung erweckt insgesamt en Eindruck, dass hier Lehren aus der umständlichen Umstellung von INPOL auf INPOL-neu gezogen wurden, bei dem der Zeitplan immer wieder angepasst werden musste.

---

[221] Vgl. BT-Drs. 18/11163, S. 76; BMI, Polizei 2020, S. 2; siehe zu dem Ziel der Verfügbarkeit von Daten im Einzelnen unten Teil 2 A. I.

[222] Vgl. *Rusteberg*, Föderale Sicherheitsarchitektur, S. 65; siehe zu dem Ziel der Verknüpfbarkeit von Daten im Einzelnen unten Teil 2 B. I.

[223] BMI, Polizei 2020, S. 2; vgl. auch BT-Drs. 18/11163, S. 2.

[224] Siehe dazu oben 2.

[225] BMI, Polizei 2020, S. 16.

[226] BMI, Polizei 2020, S. 16.

[227] Vgl. BMI, Polizei 2020, S. 16.

[228] BT-Drs. 18/11163, S. 81.

[229] Vgl. BMI, Polizei 2020, S. 16; BT-Drs. 19/25651, S. 2, 4 („Zeitraum von ca. zehn Jahren").

[230] BMI, Programm P20, abrufbar unter https://www.bmi.bund.de/DE/themen/sicherheit/programm-p20/programm-p20-node.html.

b. Struktur des „Datenhauses"

Das neue polizeiliche „Datenhaus" soll aus zwei Teilen bestehen, für die jeweils bereits rechtliche Grundlagen existieren: Einem einheitlichen Informationssystem des Bundeskriminalamts und einem allgemeinen Informationsverbund der Polizeien der Länder. Das neue einheitliche Informationssystem des Bundeskriminalamts dient zur Erfüllung der eigenen Aufgaben der Behörde und ist in § 13 BKAG in recht allgemeiner Form geregelt.[231] Mit diesem einheitlichen Informationssystem nimmt das Bundeskriminalamt an dem allgemeinen polizeilichen Informationsverbund nach § 29 BKAG teil. Für den Informationsverbund stellt es als Zentralstelle gemäß § 29 Abs. 1 BKAG ein Verbundsystem zur Verfügung. Damit sollen ein einheitlicher technischer Standard der Datenverarbeitung gewährleistet und bisherige Kompatibilitätsprobleme überwunden werden.[232] Gemäß § 29 Abs. 2 Satz 1 BKAG hat das Verbundsystem dabei die gleichen Grundfunktionen zu erfüllen, die nach § 13 Abs. 2 BKAG auch für das einheitliche Informationssystem des BKAG vorgesehen sind.

Für die Teilnehmer*innen, deren Systeme an den Informationsverbund angeschlossen sind,[233] ist zwischen zwei Kategorien von Daten zu unterscheiden: Einerseits verbundrelevanten Daten, auf die alle anderen Teilnehmer*innen des Verbundes zugreifen können und andererseits Daten ohne Verbundrelevanz, die nur für den jeweiligen „Datenbesitzer" sichtbar sind.[234] In dem Verbund sollen die Daten im Wesentlichen nach Themen geordnet werden.[235] Die wohl größte Neuerung im Vergleich zu der bisherigen Informationsordnung ist, dass der neue Informationsverbund auf einen Strukturierung in Dateien verzichten soll. Der Begriff „Datenhaus" ist vor diesem Hintergrund ein wenig verwirrend, weil er eine strukturelle Trennung des Informationsverbundes in „Räume" nahelegt, wie es sie in einem Haus als Gebäude üblicherweise existieren. Ein Begriff wie „Datensilo" oder „Datensee"[236] wäre passender. Der Verzicht auf eine Strukturierung in Dateien soll die Verknüpfbarkeit verschiedener Informationen erleichtern.[237] So sollen sich dadurch etwa Informationen zu einer einzelnen Person, die in verschiedenen Dateien gespeichert sind, leichter auffinden und zusammenführen lassen. *Fall 5* veranschaulicht beispielhaft die Interessen an einer dateiübergreifenden Auswertung polizeilicher Daten: Hier sollen die Inhalte mehrerer Dateien miteinander

[231] Siehe unten C. II. 2.
[232] Vgl. *Graulich*, KriPoZ 2017, 278 (279).
[233] Siehe hierzu § 29 Abs. 3 BKAG.
[234] BMI, Polizei 2020, S. 11.
[235] BT-Drs. 18/11163, S. 109.
[236] Dieser Begriff wird im Zusammenhang mit Europol verwendet; siehe unten VI.
[237] BMI, Polizei 2020, S. 5.

abgeglichen werden, um die Identität von Personen aufgrund verwendeter Pseudonyme, Bilder und Sprachmuster festzustellen.

Im neuen „Datenhaus" soll auch die Notwendigkeit entfallen, Daten mehrfach zu erfassen.[238] Wenn die Polizei Daten erhebt, die für mehrere Systeme relevant sind, kann das dazu führen, dass sie einzeln in diese eingepflegt werden müssen, weil die Systeme unterschiedliche technische Standards hierfür vorsehen. Es handelt sich um ein altes Problem der Informationsordnung, das auch in der Konzeption von INPOL-neu hervorgehoben, aber bisher nicht gelöst wurde.[239]

c. Kritik am „Datenhaus" und seinen Grundlagen

Die geplante neue Informationsordnung ist Gegenstand von Kritik und wirft Fragen auf. Zunächst wird das Fehlen eines konzeptionellen Fundamentes bemängelt.[240] Auf rechtlicher Ebene ist unklar, welche Befugnisnormen des BKAG für einzelne Schritte des Umgangs mit personenbezogenen Daten innerhalb des neuen „Datenhauses" maßgeblich sind.[241] Dies gilt besonders für das Verhältnis der §§ 12, 16, 18 und 19 BKAG, auf deren Voraussetzungen noch näher einzugehen sein wird.[242]

Unklar ist auch, ob und wie der technische und rechtliche Rahmen der neuen themenbezogenen Informationsordnung ein hinreichendes Datenschutzniveau gewährleisten kann. Die Gesetzesbegründung zum BKAG 2018 kündigt einen Wandel von einem vertikalen zu einem horizontalen Datenschutzkonzept in der neuen polizeilichen Informationsordnung an.[243] Was dies im Einzelnen bedeuten soll, ist bislang nicht eindeutig nachvollziehbar.[244] Das vertikale Datenschutzkonzept bezeichnet die bisher praktizierte Speicherung von Informationen in Dateien.[245] Die bisherige Ordnung in Dateien basierte auch maßgeblich auf datenschutzrechtlichen Erwägungen, da diese technisch eine klare Abgrenzung verschiedener Informationsbestände ermöglichten.[246] Nach den Zwecken und der Gestaltung einer Datei richten sich auch die Art und das Ausmaß der Datenverarbeitung, die darin stattfindet. Diese Zwecke werden wiederum von exekutiv erlassenen Errichtungsanordnungen bestimmt.

Der Maßstab der Errichtungsanordnungen würde in dem neuen „Datenhaus" wegfallen. Allerdings soll der Zugriff auf Daten hier durch differenzierte Berechtigungen

---

[238] BT-Drs. 18/11163, S. 75.
[239] Siehe oben 2.
[240] *Bäcker*, Verfassungsblog vom 8. Juni 2017; vgl. auch BfDI, 26. Tätigkeitsbericht 2015-2016, S. 107.
[241] *Bäcker*, Verfassungsblog vom 8. Juni 2017.
[242] Siehe unten C. III. 1. b.
[243] BT-Drs. 18/11163, S. 75 f., 98 f.
[244] *Graulich*, KriPoZ 2017, 278 (286 f.).
[245] BT-Drs. 18/11163, S. 75.
[246] Für eine Beibehaltung der Dateiordnung BfDI, 26. Tätigkeitsbericht 2015-2016, S. 109.

geregelt werden, so dass jede*r Teilnehmer*in nur auf bestimmte Inhalte des „Datenhauses“ zugreifen könnte, denen eine Verbundrelevanz zukommt. Die konkreten Zugriffsrechte sollen sich nach dem Grundsatz der hypothetischen Datenneuerhebung richten, wie ihn das Bundesverfassungsgericht in seinem Urteil zum BKAG formuliert hat und er in § 12 BKAG einfachgesetzlich umgesetzt wurde.[247] Dieser Grundsatz ist damit auch die Grundlage des horizontalen Datenschutzkonzeptes,[248] dessen Details noch nicht ganz klar sind. Der Grundsatz der hypothetischen Datenneuerhebung und seine einfachgesetzliche Umsetzung werden an späterer Stelle ausführlich gewürdigt.[249] Etwas vereinfacht gesagt können danach Daten zu neuen Zwecken verarbeitet werden, wenn vergleichbar schwerwiegende Straftaten verfolgt oder verhindert bzw. vergleichbar bedeutsame Rechtsgüter geschützt werden sollen wie bei der ursprünglichen Erhebung der Daten (§ 12 Abs. 2 BKAG). Hinzu treten muss ein konkreter Anlass für die Verarbeitung im Einzelfall.

Den Zugriff auf Daten an differenzierte Voraussetzungen zu knüpfen, die mit den Umständen ihrer Erhebung zusammenhängen, erfordert die Kennzeichnung und Kategorisierung der Daten. Nur bei Kennzeichnung der Zwecke und Umstände, zu und unter denen Daten gespeichert wurden, kann die Rechtmäßigkeit ihrer Weiterverarbeitung überprüft werden. Die Kennzeichnung dient damit weitgehend zur Sicherstellung der Funktionen, die für Dateien bisher die Errichtungsanordnung erfüllte. § 14 Abs. 1 BKAG regelt die notwendige inhaltliche Kennzeichnung, Abs. 2 der Vorschrift sieht eine Suspendierung der Weiterverarbeitung von nicht gekennzeichneten Daten vor. Die Funktionsfähigkeit des neuen „Datenhauses“ wird es erfordern, auch die bereits in großen Mengen vorhandenen „Altdaten“ zu kennzeichnen. Dies dürfte die Polizeien auch ressourcenmäßig vor Herausforderungen stellen. Es bleibt abzuwarten, ob eine flächendeckende Kennzeichnung und Verwendung von Altdaten umgesetzt werden wird.

Das Wegfallen der Errichtungsanordnungen könnte schließlich ein Stück weit durch Verzeichnisse der Verarbeitungstätigkeiten kompensiert werden, die die für die Datenverarbeitung im „Datenhaus“ Verantwortlichen datenschutzrechtlich zu führen haben (§ 70 BDSG; § 80 BKAG). Ein Verarbeitungsverzeichnis hat unter anderem Angaben zu den Zwecken der Datenverarbeitung zu enthalten (§ 70 Abs. 1 Satz 2 Nr. 2 BDSG; § 80 Abs. 2 BKAG). Ähnlich wie eine Errichtungsanordnung soll das Verarbei-

[247] BMI, Polizei 2020, S. 11.
[248] BT-Drs. 18/11163, S. 98 f.
[249] Siehe unten Teil 3 C. II. 3.

tungsverzeichnis es der Datenschutzaufsicht ermöglichen, eine Kontrolle der Verarbeitungen personenbezogener Daten durchzuführen.[250] Es dient aber eher zum Überblick über sämtliche Verarbeitungsvorgänge und regelt anders als die Errichtungsanordnung nicht den näheren Umgang mit Informationssystemen in Form einer Verwaltungsvorschrift.[251] Daher ist zu bezweifeln, ob Verarbeitungsverzeichnisse die Funktionen von Errichtungsanordnungen umfassend übernehmen können.[252]

Es ist kritisch zu hinterfragen, ob sich die ehrgeizigen Ziele der Reform der polizeilichen Informationsordnung vorrangig durch die neuen rechtlichen Vorgaben erreichen lassen. Bei der Umgestaltung des polizeilichen Informationswesens sind technische und administrative Aspekte von erheblicher Bedeutung.[253] Dass eine Umsetzung der formulierten Ziele aufwändige technische Maßnahmen erfordert, erkennt auch die Gesetzesbegründung an.[254] Die Erfolgsaussichten der technischen Umsetzung sind dabei schwer abzusehen. Ähnliches gilt für den administrativen Umgang mit der neuen Informationsordnung, der sich ebenfalls als umständlich darstellen dürfte. Der Zugriff auf den Informationsverbund durch seine Teilnehmer*innen wird detailgenau zu organisieren sein. Bei dem inhaltlich orientierten „Datenhaus" wird anders als bei primär an Organisationseinheiten orientierten Systemen öfter ein Bedarf bestehen, die Berechtigung des einzelnen Zugriffs zu prüfen.[255] Schon in dem bisherigen System der Informationsordnung wurden administrative und organisatorische Defizite bemängelt.[256]

Auffallend ist schließlich, dass die aktuelle Reform der Informationsordnung der Polizei in ihren Zielen und Strukturen zahlreiche Übereinstimmungen mit den größtenteils gescheiterten Bemühungen um die Fortentwicklung von INPOL um die Jahrtausendwende aufweist.[257] Die vorgesehene Struktur des neuen „Datenhauses" erinnert in Grundzügen an den „Datenpool", der ursprünglich mit INPOL-neu geschaffen werden sollte. Auch dieser sollte das alte INPOL-Dateiensystem ersetzen. Die Notwendigkeit redundanter Datenspeicherungen zu beseitigen war damals wie heute ein zentrales Ziel. Der Zugriff auf die Daten sollte ebenfalls auf Grundlage eines abgestuften Berechtigungssystems erfolgen. Das Ziel der besseren Verknüpfbarkeit durch das neue „Da-

[250] *Greve*, NVwZ 2017, 737 (742); *Schwichtenberg*, in: Kühling/Buchner, 3. Aufl. 2020, § 70 BDSG Rn. 2.
[251] Vgl. *M. Müller/Schwabenbauer,* in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 1045.
[252] Zweifelnd auch *Petri,* in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 458.
[253] Vgl. *Graulich*, KriPoZ 2017, 278 (279).
[254] BT-Drs. 18/11163, S. 2, 80, 85.
[255] Vgl. BT-Drs. 18/11163, S. 81.
[256] Vgl. BfDI, Stellungnahme BKAG 2018, S. 4.
[257] Siehe dazu oben 2.

tenhaus“ ähnelt dem mit INPOL-neu verfolgten Ideal der „ganzheitlichen Kriminalitätsbetrachtung“.[258] Die Hürden, an denen INPOL-neu in seiner ursprünglich geplanten Form scheiterte, bestehen heute fort. Die Informationssysteme der Länder sind weiterhin komplex und nicht miteinander kompatibel. Widerstände von Seiten der Landespolizeien bei dem Vorhaben einer weitgehenden Zentralisierung wären zumindest nicht überraschend. Es bleibt abzuwarten, ob und unter welche Bedingungen es diesmal gelingen wird, die Widerstände zu überwinden.

IV. Die Entwicklung der staatsanwaltschaftlichen Informationsordnung und ihr Verhältnis zur Polizei

Auch die Staatsanwaltschaften betreiben auf elektronische Datenverarbeitung gestützte Informationssysteme. Ihre Entwicklung kam aber deutlich später in Gang als bei den Polizeien.[259] Die ersten Systeme wurden in den späten 1970er- und frühen 1980er-Jahren eingerichtet.[260] Erst in den 1990er-Jahren hielt die elektronische Datenverarbeitung in der Informationsordnung der Staatsanwaltschaften auf breiter Basis Einzug.[261] Hierbei standen und stehen bis heute Dateien zur Vorgangsverwaltung[262] im Vordergrund.[263]

Den Knotenpunkt der staatsanwaltschaftlichen Informationsordnung bildet das Zentrale Staatsanwaltschaftliche Verfahrensregister bzw. staatsanwaltschaftliche Informationssystem.[264] Dieses wurde im Wesentlichen in den 1980er-Jahren politisch vorbereitet[265] und nach einem ersten Regelungsvorschlag Ende der 1980er-Jahre[266] durch das

[258] Vgl. zum ganzheitlichen Ansatz der Kriminalitätsbekämpfung *Ziercke*, Kriminalistik 2005, 700 (702 ff.).

[259] Vgl. *Ringwald*, ZRP 1988, 178.

[260] Eine Vorreiterstellung nahm hierbei das Land Schleswig-Holstein ein; vgl. *Ernesti*, NStZ 1983, 57; *Rebmann/Schoreit*, NStZ 1984, 1 (2).

[261] *Janovsky*, JurPC 1996, 30; *König/Voigt*, in: GS Weßlau, S. 181 (183).

[262] Hierunter fällt die Bearbeitung von Akten durch die Geschäftsstellen der Staatsanwaltschaft; BT-Drs. 12/989, S. 45 f.

[263] BfDI, Stellungnahme BKAG 2018, S. 17.

[264] Siehe hierzu *Hoffmann*, ZRP 1990, 55 ff.; *Lemke*, NStZ 1995, 484 ff.; *Rudolph*, S. 197 ff.; *S. Schneider*, NJW 1996, 302 ff.

[265] Vgl. Beschlüsse der 57. Justizministerkonferenz 1986, TOP 15; zur Geschichte im Überblick *Groß*, JurPC 1996, 24 f.

[266] Referentenentwurf einer gesetzlichen Regelung für ein länderübergreifendes staatsanwaltschaftliches Informationssystem vom 22. Dezember 1988, abgedruckt in StV 1989, 178.

Gesetz zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze vom 28. Oktober 1994[267] rechtlich geregelt.[268] Das 1999 zunächst bei der Dienststelle Bundeszentralregister des Generalbundesanwalts eingerichtete System führt mittlerweile das Bundesamt für Justiz (§ 492 Abs. 1 StPO). Es enthält Eintragungen über strafrechtliche Ermittlungsverfahren, die unter anderem die Identität des Beschuldigten, die zuständige Stelle und das Aktenzeichen sowie die Tatvorwürfe betreffen (§ 492 Abs. 2 StPO).[269] Ziel des Registers ist es, die Informationsbestände der Staatsanwaltschaften zu vernetzen und es ihnen zu ermöglichen, ihre Maßnahmen zu koordinieren.[270] Es umfasst nach Angaben des Bundesamts für Justiz etwa 30 Millionen Einträge.[271]

Eine darüber hinaus gehende Stärkung und Modernisierung der staatsanwaltschaftlichen Informationsordnung wurde immer wieder angekündigt,[272] bisher aber nicht in größeren Schritten realisiert. Einen Einschnitt könnte die Einführung der elektronischen Akte in Strafsachen bedeuten. Ab dem 1. Januar 2026 sollen neu anzulegende Akten nur noch elektronisch zu führen sein.[273] Mit der elektronischen Akte wird voraussichtlicher ein großer, zu Strafverfolgungszwecken auswertbarer Datenbestand geschaffen,[274] dessen Nutzung und ihre Grenzen rechtlich näher zu untersuchen sein werden.[275]

In der Gesamtschau sind die Informationssysteme der Staatsanwaltschaften den polizeilichen Anwendungen bislang in struktureller und technischer Hinsicht sowie in der

---

[267] BGBl I, S. 3186.

[268] Zunächst in § 474 StPO; vgl. zu der damals nicht verwirklichten Überlegung, das System im Zusammenhang mit den später eingeführten Vorschriften zur Datenspeicherung zu regeln *Hoffmann*, ZRP 1990, 55 (58 f.).

[269] Siehe zu den registrierten Daten im Einzelnen *Singelnstein*, in: MüKo-StPO, 2019 § 492 Rn. 2 ff.

[270] BT-Drs. 12/6853, S. 3, 37; *S. Schneider*, NJW 1996, 302 (303); *Wittig*, in: BeckOK-StPO, 47. Ed. 2023, § 492 Rn. 2; vgl. auch *Kestel*, StV 1997, 266.

[271] https://www.bundesjustizamt.de/DE/Themen/Gerichte_Behoerden/ZStV/ZStV_node.html.

[272] Vgl. nur *Lemke*, NStZ 1995, 484 ff.; *Zöller*, S. 178.

[273] Artikel 2 Nr. 1 Gesetz zur Einführung der elektronischen Akte in der Justiz und zur weiteren Förderung des elektronischen Rechtsverkehrs vom 5. Juli 2017; BGBl. I, S. 2208 (2214).

[274] Vgl. BT-Drs. 18/9416, 69 f.; *Singelnstein*, in: FS Rogall, S. 725 (733); *Singelnstein*, in: Hoffmann-Riem, Big Data, S. 179; *König/Voigt*, in: GS Weßlau, S. 181.

[275] Herausforderungen bringen unter anderem die Manipulationsanfälligkeit elektronischer Daten und die Grenzen der Zulässigkeit maschineller Abgleiche mit sich; vgl. *König/Voigt*, in: GS Weßlau, S. 181 (190 f.). Neben Fragen von Datenschutz und Datensicherheit stellen sich aber auch solche im Zusammenhang mit den Funktionen der Aktenführung im Strafverfahren, die unter anderem dem Schutz von Beschuldigtenrechten dienen; vgl. im Zusammenhang mit den Grundsätzen der Aktenklarheit, Aktenwahrheit und Aktenvollständigkeit *von Stetten*, ZRP 2015, 138; zum Beweiswert der elektronischen Akte BT-Drs. 18/9416, S. 31; zum Grundsatz rechtlichen Gehörs *Wojtech*, NJW-Spezial 2012, 632; zu Löschungspflichten *Spatscheck/Dovas/Feldle*, NStZ 2022, 705 ff.

Größe ihrer Datenbestände weit unterlegen, auch wenn es um die Speicherung von Informationen zu repressiven Zwecken geht.[276] Die Dominanz der polizeilichen Informationsordnung beruht darauf, dass die Polizei durch ihre Tätigkeit näher an den relevanten Daten ist und sich durch ihr frühes und intensives Engagement beim Einsatz der elektronischen Datenverarbeitung einen deutlichen technischen Vorsprung gegenüber den Staatsanwaltschaften verschaffte.[277]

Aufgrund der faktischen Überlegenheit der polizeilichen Informationssysteme gegenüber jenen der Staatsanwaltschaft ist das Verhältnis beider Institutionen zueinander in diesem Bereich angespannt. Dies gilt schon seit den 1970er-Jahren, als die Frage um den staatsanwaltschaftliche Zugriff auf INPOL als Aspekt einer breiter geführten Diskussion[278] um das sich wandelnde Verhältnis von Staatsanwaltschaft und Polizei auf den Plan trat. In der ursprünglichen Konzeption von INPOL war vorgesehen, dass auch die Staatsanwaltschaften Zugriff auf das System haben sollten.[279] Die Polizei schottete ihre Informationssysteme dann jedoch zunehmend gegenüber der Justiz und anderen Stellen ab.[280] Den Staatsanwaltschaften blieben in der Folge Rechte zu der Eingabe und für den Abruf von Daten aus INPOL verwehrt,[281] obwohl nicht nur viele Daten in diesem System aus der Strafverfolgung stammten, sondern auch für diese Aufgabe weiterverwendet werden sollten.

Versuche, die elektronischen Informationsressourcen von Polizei und Justiz miteinander zu verbinden, sind immer wieder gescheitert. So versandete in den 1970er-Jahren das von den Konferenzen der Justiz- und Innenminister*innen initiierte Vorhaben, Staatsanwaltschaften und Polizeien gegenseitig an ihren Informations- und Kommunikationssystemen zu beteiligen.[282] Dies setzte die Staatsanwaltschaften unter Druck, eine

[276] Vgl. Arbeitskreis AE, S. 119; *Puschke*, S. 170; *Schaefer*, NJW 1998, 3178; *Singelnstein*, in: FS Rogall, S. 725 (729); *Zöller*, S. 177.

[277] Siehe oben III.

[278] Vgl. nur Bericht des Unterausschusses des Arbeitskreises II „Öffentliche Sicherheit und Ordnung" der Innenministerkonferenz über das „Verhältnis Staatsanwaltschaft – Polizei" vom 1. Dezember 1972; abgedruckt bei *Schubert*, S. 419 (425 f.).

[279] Vgl. *Lilie*, ZStW 106 (1994), 625 (632); *K. Merten*, NStZ 1987, 10 (11); *Ringwald*, S. 17 f.

[280] Vgl. *Ernesti*, NStZ 1983, 57; *K. Merten*, NStZ 1987, 10 (11).

[281] Vgl. *Wolter*, in: FS Rolinski, S. 273 (274); *Zöller*, S. 172. Ausnahmen bildeten probeweise eingerichtete Anschlüsse für die Staatsanwaltschaften München und Frankfurt am Main; vgl. *Herold*, in: BKA, Polizei und Justiz, S. 79 (80).

[282] Gesamtbericht der von den Konferenzen der Justizminister/-senatoren und Innenminister/-senatoren eingesetzten „Gemeinsamen Kommission" über die Neugestaltung des Verhältnisses „Staatsanwalt – Polizei" vom 13. Mai 1975, Leitsatz 1; abgedruckt bei *Schubert*, S. 489 (490); vgl. dazu *Ernesti*, NStZ 1983, 57; *Herold*, in: BKA, Polizei und Justiz, S. 79.

eigene Informationsordnung aufzubauen.[283] Durch das Gesetz zur effektiveren Nutzung von Dateien im Bereich der Staatsanwaltschaften vom 10. September 2004[284] wurde den Staatsanwaltschaften zumindest ein Recht zum automatisierten Abruf bestimmter Daten[285] vom Bundeskriminalamt eingeräumt.[286] Die Herstellung einer „einheitlichen digitalen Kommunikation zwischen Justiz und Polizei von Bund und Ländern" sieht die Konferenz der Justizministerinnen und Justizminister weiterhin als wichtige Aufgabe an.[287] Konkrete und erfolgversprechende Vorhaben, eine einheitlichere Kommunikation oder bessere Vernetzung zu erreichen, zeichnen sich aber nicht ab.

V. Die kriminalbehördliche Informationsordnung als Bestandteil der Sicherheitsarchitektur der Bundesrepublik Deutschland

Die Existenz und Funktionsfähigkeit kriminalbehördlicher Datenbanken und Informationssysteme gelten als Voraussetzungen dafür, dass Polizei und Staatsanwaltschaften handlungsfähig sind und ihre Aufgaben erfüllen können.[288] Diese Informationsressourcen sind ein wichtiger Bestandteil der Sicherheitsarchitektur der Bundesrepublik Deutschland. Aus kriminologischer Sicht lassen sie sich als Instrumente der sozialen Kontrolle einordnen, die im Zusammenhang mit einer umfassenden Infrastruktur zur vorbeugenden Kontrolle von Kriminalität betrachtet werden können.[289] Die Zusammenhänge kriminalbehördlicher Informationsressourcen mit den Informationsressourcen anderer Sicherheitsbehörden und ihre Stellung in der Sicherheitsarchitektur sind für die vorliegende Untersuchung unter anderem aufgrund der zunehmenden Vernetzungen der Sicherheitsbehörden und ihrer Systeme bedeutsam.

Der Begriff der Sicherheitsarchitektur ist unscharf.[290] Diese Untersuchung versteht darunter eine Organisation staatlicher Stellen, die auf möglichst umfassende Weise Si-

[283] Vgl. allerdings bereits mit Zweifeln an der Umsetzung *Schoreit*, DRiZ 1986, 54 (56).
[284] BGBl. I, S. 2318.
[285] Zu Personenfahndung, DNA-Analyse und Haft; vgl. hierzu BT-Drs. 15/1492, S. 8.
[286] § 29 Abs. 6 Satz 2 BKAG; ehemals § 11 Abs. 4 Satz 2 BKAG.
[287] 90. Konferenz der Justizministerinnen und Justizminister 2019, Beschluss zu TOP II. 14., Digitale Zusammenarbeit von Polizei und Justiz.
[288] Vgl. *Roggan/Bergemann*, NJW 2007, 876 ff.
[289] Vgl. *Singelnstein/Stolle*, S. 11 ff. (zu Begriff und Wandel sozialer Kontrolle), 82 f. (zu sicherheitsbehördlichen Datensammlungen).
[290] Vgl. zu dem Begriff *Kugelmann*, Die Verwaltung 2014, 25; *Rusteberg*, in: Gusy/Kugelmann/Würtenberger, S. 113 (114); *Würtenberger/Tanneberger*, in: Riescher, S. 97.

cherheit gewährleisten sollen und dafür mit entsprechenden Aufgaben und Befugnissen ausgestattet sind.[291] Diese Organisation ist in hohem Maße von dem Austausch und der Speicherung von Informationen geprägt und abhängig. Neben den kriminalbehördlichen Datenbanken und Systemen spielen hierbei Informationsbestände anderer staatlicher Stellen – wie etwa Nachrichtendiensten – eine wichtige Rolle. Auch private Datenbestände werden zunehmend in die staatliche Sicherheitsarchitektur einbezogen. Dies zeigt sich beispielsweise an den seit vielen Jahren umstrittenen Verpflichtungen von Telekommunikationsanbietern, Verkehrsdaten auf Vorrat zu speichern, um diese in der Folge etwa für Zwecke der Strafverfolgung verwenden zu können. Auch die in *Fall 5* beschriebene Verpflichtung von Anbietern Sozialer Netzwerke nach dem Netzwerkdurchsetzungsgesetz, bestimmte potentiell strafbare Inhalte an das Bundeskriminalamt zu melden, ist ein Beispiel dafür, wie private Datenbestände durch infrastrukturelle Verpflichtungen zum Gegenstand der staatlichen Sicherheitsarchitektur gemacht werden können.

Welche Rolle das Sammeln und Ordnen von Informationen für die Gewährleistung von Sicherheit insgesamt spielt, wurde in der Politik und Fachöffentlichkeit in jüngerer Vergangenheit immer wieder nach Ereignissen diskutiert, die Verletzlichkeiten offenlegten. So warfen die Terroranschläge vom 11. September 2001 unter anderem ein Schlaglicht auf Defizite der Informationssysteme von Sicherheitsbehörden, deren unzureichende Verknüpfung miteinander kritisiert wurde.[292] 9/11 gab dem Einsatz neuer Technologien zur Sicherheitsgewährleistung insgesamt einen Schub.[293] Der internationalen terroristischen Bedrohung sollte eine neue Sicherheitsarchitektur entgegengesetzt werden, die unter anderem eine verstärkte Vernetzung, mehr Zentralisierung[294] und mehr Prävention versprach.[295] Besonders im Zusammenhang mit der Terrorismusbe-

[291] Der Begriff der Sicherheitsarchitektur wird regelmäßig genutzt, um die Struktur der Behörden zu beschreiben, die im föderalen System Aufgaben zur Gewährleistung der öffentlichen Sicherheit wahrnehmen. Hierbei werden verschiedene „Säulen" nach Aufgaben und Behörden ausgemacht; vgl. *Gusy*, VerwArch 101 (2010), 309 (322 f.); *Löffelmann*, GSZ 2018, 85 (86). In einem ähnlichen Sinne werden die Begriffe „Sicherheitsnetz" und „Sicherheitssystem" verwendet; vgl. *Volkmann*, NVwZ 2009, 216

[292] National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, 2004, S.408 ff.; vgl. zu der folgenden Diskussion in Deutschland *Abbühl*, S. 242; *Mehde*, JZ 2005, 815 (816).

[293] Vgl. mit zahlreichen Beispielen *S. Kaufmann*, in: Gusy/Kugelmann/Würtenberger, S. 3 (15 f.).

[294] Siehe zu Möglichkeiten einer weiteren Zentralisierung der kriminalbehördlichen Informationsordnung unten Teil 3 A.

[295] Vgl. *Abbühl*, S. 221; *Gusy*, VerwArch 101 (2010), 309 (322); *Kötter*, S. 292; *Kugelmann*, Die Verwaltung 2014, 25 (51); *Mehde*, JZ 2005, 815 (816); *Ziercke*, in: Pitschas/Stolzlechner, S. 63 (67) (mit dem Vorschlag zur Schaffung eines institutionalisierten Informationsboards, an dem alle Sicherheitsbehörden unter Leitung des Bundeskriminalamts beteiligt sind).

kämpfung kam es international wie auch in Deutschland zu einer Ausweitungen staatlicher Informationssysteme.[296] 2006 wurde die Antiterrordatei eingeführt[297] und in diesem Zusammenhang erstmals eine gesetzliche Grundlage für die Verknüpfung von Daten aus polizeilichen und nachrichtendienstlichen Beständen geschaffen.[298] Das Bedürfnis nach der Vernetzung der Informationsbestände unterschiedlicher Stellen in der Sicherheitsarchitektur kam dazu in der Schaffung von „Informationsdrehscheiben" zum Ausdruck. Das seit Dezember 2004 operierende Gemeinsame Terrorismusabwehrzentrum (GTAZ)[299] und das seit April 2011 aktive Nationale Cyber-Abwehrzentrum (NCAZ)[300] sind Beispiele für derartige informelle Zusammenarbeiten zwischen Behörden, durch die relevante Informationen ausgetauscht werden sollen.

Auf europäischer Ebene führten die terroristischen Anschläge von Madrid 2004, London 2005 und Paris 2015 zu neuen Impulsen in der Diskussion um die Sicherheitsarchitektur und die Informationsverarbeitung in diesem Zusammenhang.[301] Speziell in Deutschland löste die Aufdeckung der NSU-Terrorzelle in Zwickau im November 2011 Kontroversen über den Umgang mit Informationen durch Sicherheitsbehörden und die strukturellen Defizite hierbei aus.[302] Neben den Verfassungsschutzbehörden stand dabei die Polizei im Fokus. Kritisiert wurde unter anderem die fehlende Interoperabilität verschiedener Informationssysteme, die wichtige Ermittlungen behindern könne.[303] Die Ereignisse und ihre Aufarbeitung führten insgesamt zu Forderungen nach einer weiteren Vernetzung und Zentralisierung der Sicherheitsbehörden. Diese Forderungen mündeten im November 2012 darin, dass das Bundesinnenministerium ein Gemeinsames Terrorismus- und Extremismusabwehrzentrum (GETZ) nach dem

[296] Vgl. BVerfGE 120, 378 (410 f.); *Saurer*, NVwZ 2005, 275 (279 f.) (zum Ausländerzentralregister); *Zöller*, JZ 2007, 763 (767 ff.).

[297] Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder vom 22. Dezember 2006; BGBl. I 2006, S. 3409; vgl. hierzu *Stubenrauch*, S. 18 ff.

[298] Aus diesem Grund wurde die Antiterrordatei vor dem Hintergrund des verfassungsrechtlichen Gebotes der organisatorischen Trennung von Polizei und Nachrichtendiensten kritisiert; *Roggan/Bergemann*, NJW 2007, 876 ff.; *Zöller*, JZ 2007, 763 (770); anders *Stubenrauch*, S. 61 f. Ob und auf welcher Grundlage sich ein derartiges Trennungsgebot unmittelbar aus dem Grundgesetz herleiten lässt und welche Reichweite es hat, ist allerding umstritten; vgl. hierzu *Baumann*, DVBl. 2005, 798 (799 ff.); *Denninger*, ZRP 1981, 231 f.; *Nehm*, NJW 2004, 3289 ff.; *Roewer*, DVBl. 1986, 205 ff.; *Wolff*, DÖV 2009, 597 (601 f.).

[299] Dieses wird aufgrund einer unzureichenden Trennung zwischen polizeilichen und nachrichtendienstlichen Aktivitäten sowie einer fehlenden Rechtsgrundlage kritisiert; vgl. *Zöller*, JZ 2007, 763 (767).

[300] Vgl. dazu *Schöndorf-Haubold*, in: 47. ATÖR, S. 149 (158 ff.).

[301] Vgl. KOM(2010) 385 endg., S. 2.

[302] Vgl. *Gusy*, ZRP 2012, 230.

[303] BT-Drs. 17/14600, S. 862.

Vorbild des GTAZ einrichtete.[304] Dazu wurde das Bundesamt für Verfassungsschutz mit neuen Befugnissen zur zentralen Datenauswertung[305] und Einführung von Datenbanksystemen[306] ausgestattet sowie seine Stellung gegenüber den Ländern gestärkt.[307] Zuletzt hat die Diskussion um die Sicherheitsarchitektur in der Bundesrepublik durch den Anschlag auf den Berliner Breitscheidplatz im Jahr 2016 Antrieb erhalten.[308] Bei dessen Aufarbeitung wurden unter anderem Mängel im Informationsaustausch und der Koordination zwischen Sicherheitsbehörden – namentlich Polizei und Verfassungsschutzämtern – thematisiert.[309]

Im Ergebnis spielten kriminalbehördliche – und dabei vor allem polizeiliche –Informationsressourcen in den Diskussionen um die Sicherheitsarchitektur der Bundesrepublik in den letzten Jahrzehnten kontinuierlich eine Rolle. Dabei ging es allerdings in erster Linie um die Vernetzung polizeilicher Informationsbestände mit jenen von anderen Sicherheitsbehörden. In den übergreifenden Diskussionen kamen immer wieder Bedürfnisse nach der Schaffung neuer Möglichkeiten zur Verknüpfung von Informationen und ihrer systemübergreifenden Auswertung zum Ausdruck. Diese Tendenzen werden im Kontext der kriminalbehördlichen Informationsordnung näher zu untersuchen sein.[310]

VI. Die kriminalbehördliche Informationsordnung in der europäischen Sicherheitsarchitektur

Schließlich spielt die Einrichtung und Vernetzung von Informationssystemen eine wichtige Rolle in der Sicherheitsarchitektur der Europäischen Union – auch angesichts ihrer geringen Kompetenzen im Sicherheitsbereich.[311] Im Raum der Freiheit, der Si-

[304] Bundesamt für Verfassungsschutz, Presseinformation zum Start des Gemeinsamen Extremismus- und Terrorismusabwehrzentrums zur Bekämpfung des Rechtsextremismus/-terrorismus, des Linksextremismus/-terrorismus, des Ausländerextremismus/-terrorismus und der Spionage/Proliferation vom 15. November 2012.

[305] § 5 Abs. 2 Satz 1 BVerfSchG.

[306] § 6 BVerfSchG.

[307] Durch das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015; BGBl. I, S. 1938; vgl. dazu *Bergemann*, NVwZ 2015, 1705 ff.; *Marscholleck*, NJW 2015, 3611 ff.

[308] Vgl. etwa BT-Drs. 19/7424.

[309] BT-Drs. 19/30800, S. 1132.

[310] Siehe unten Teil 2 B.

[311] Vgl. *von Arnauld*, JA 2008, 327; *Möstl*, EuR 2009, Beiheft 3, 33 (49); *Schöndorf-Haubold*, S. 70 ff.; allgemein zu Informationssystemen als Bausteinen des europäischen Verwaltungsverbunds *J.-P. Schneider*, NVwZ 2012, 65 ff.; speziell im Kontext der Terrorismusbekämpfung *Balzacq*, JCMS 2008, 75 (83 ff.).

cherheit und des Rechts existiert eine stetig wachsende Anzahl von Informationsressourcen und Datenbanken.[312] Diese sind in hohem Maße standardisiert[313] und lassen sich als vernetztes Gesamtsystem betrachten.[314] Daneben lassen sich Bemühungen nachvollziehen, den Austausch und die Vernetzung von Informationen aus Systemen der Mitgliedstaaten zu fördern. Die kriminalbehördlichen Informationsressourcen auf Ebene der Europäischen Union werden im Folgenden vor allem in ihren Bezügen zu der nationalen Informationsordnung beleuchtet.

Im Kontext der Strafverfolgung sind als unionseigene Systeme primär das Schengener Informationssystem (SIS) sowie das Europol-Informationssystem von Interesse. Das SIS lässt sich als Grundstein der europäischen Sicherheitsinformationsordnung begreifen. Seiner Einrichtung liegt maßgeblich der Gedanke zugrunde, Sicherheitsrisiken zu kompensieren, die durch den Wegfall der Kontrollen der Binnengrenzen in der Europäischen Union entstanden.[315] Das SIS wurde seit 1995 auf Grundlage von Art. 92 ff. des Schengener Durchführungsübereinkommens vom 19. Juni 1990 (SDÜ)[316] betrieben und auf Grundlage des Ratsbeschlusses 2007/533/JI[317] durch das Schengener Informationssystem der zweiten Generation (SIS II) mit erweiterten Funktionalitäten abgelöst.[318] Das SIS II ist ein zentralisierter Informationsverbund und dient in erster

[312] Vgl. zur Übersicht Wissenschaftlicher Dienst des Europäischen Parlaments, Europäische Informationssysteme im Bereich Justiz und Inneres, 2017; KOM(2016) 205 endg., S. 6 ff.; KOM(2010) 385 endg., S. 4 ff.

[313] Vgl. zu den Vor- und Nachteilen der Standardisierung *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 202 f.

[314] *F. Meyer*, in: Kugelmann/Rackow, S. 41 (50).

[315] Vgl. KOM(2016) 205 endg., S. 3; *Aden*, dms 2014, 55 (61); *Middel*, S. 87; *J.-P. Schneider*, NVwZ 2012, 65.

[316] Übereinkommens vom 19. Juni 1990 zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 zwischen den Regierungen der Staaten der Benelux-Wirtschaftsunion, der Bundesrepublik Deutschland und der Französischen Republik betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen; BGBl. II 1993, S. 1013.

[317] Der Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. EU L 205, S. 63) dient als Rechtsgrundlage des Betriebs zum Zwecke der polizeilichen und justiziellen Zusammenarbeit in Strafsachen und wird auf nationaler Ebene durch Art. 1 Gesetz zum Schengener Informationssystem der zweiten Generation für anwendbar erklärt. Weitere Rechtsgrundlagen für den Betrieb des SIS II sind Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) (ABl. EU L 381, S. 1) und Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. EU L 381, S. 4).

[318] Vgl. zur Entstehung Beschluss des Exekutivausschusses vom 7. Oktober 1997 bezüglich der Entwicklung des SIS (ABl. EG 2000 L 239, S. 442); Beschluss 2001/886/JI des Rates vom 6. Dezember 2001

Linie als Fahndungssystem zur unionsweiten Ausschreibung von Personen und Gegenständen (z.B. Fahrzeugen) zu Zwecken von Strafverfolgung und Prävention.[319] Der Zugriff ist Polizei-, Grenzkontroll-, Zoll- und Justizbehörden für Zwecke von Strafverfahren sowie Europol und Eurojust gestattet.

Im Kontext dieser Untersuchung von größerem Interesse als das SIS sind aufgrund ihrer Bezüge zu nationalen informationsordnenden Tätigkeiten in der Strafverfolgung allerdings die Informationsressourcen des 1995 gegründeten und seit 1999 tätigen Europäischen Polizeiamtes (Europol).[320] Rechtsgrundlage für die Datenverarbeitung durch Europol ist seit Mai 2017[321] die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 (Europol-VO).[322]

Aufgaben von Europol sind unter anderem Erhebung, Speicherung, Verarbeitung, Analyse und Austausch von Informationen zur Unterstützung mitgliedstaatlicher Tätigkeiten auf dem Bereich der Strafverfolgung (Art. 88 Abs. 2 lit. a AEUV; Art. 4 Abs. 1 lit. a Eurpol-VO[323]). Die Tätigkeiten von Europol in den genannten Bereichen sollen dabei mitgliedsstaatliche Aktivitäten ergänzen, nicht aber ersetzen.[324] Das Amt lässt sich vereinfacht als eine Art „Dienstleistungsorganisation für die nationalen Strafverfolgungsbehörden im Bereich des Informationsaustausches und der Informationsverarbeitung“[325] verstehen. Damit ist die Funktion von Europol zumindest teilweise mit der Zentralstellenfunktion des Bundeskriminalamts nach Art. 87 Abs. 1 Satz 2 GG, § 2

über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. EG L 328, S. 1).; Verordnung (EG) Nr. 2424/2001 des Rates vom 6. Dezember 2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. EG L 328, S. 4); KOM(2003) 771 endg.; KOM(2010) 385 endg., S. 7.

[319] Vgl. zu der Funktionsweise des Systems im Einzelnen *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. N Rn. 205 ff.; *Schöndorf-Haubold*, S. 71 ff.; zum Ausbau in den letzten Jahren *Monroy*, Bürgerrechte & Polizei/CILIP 121 (4/2020), 67 ff.

[320] Vgl. zu der Geschichte von Europol *Ruthig*, in: Böse, Europäisches Strafrecht, 2013, § 20 Rn. 5 ff.

[321] Zuvor waren Rechtsgrundlagen von Europol von 1995 bis 2009 die Europol-Konvention (Übereinkommen aufgrund von Artikel K.3 des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts vom 27. November 1995, ABl. EG C 316, S. 2) sowie von 2010 bis April 2017 der Europol-Beschluss (Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamts, ABl. EU L 121, S. 37); vgl. zu der Entwicklung der Rechtsgrundlagen *Tolmein*, StV 1999, 108.

[322] ABl. EU L 135, S. 53; vgl. zu der Entstehung der VO *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 102. Die Verordnung regelt dabei nur die Datenverarbeitung durch Europol selbst und betrifft nicht direkt die Datenverarbeitung der mitgliedstaatlichen Stellen.

[323] Ähnlich bereits Art. 3 Abs. 1 Nr. 1 und Nr. 2 Europol-Konvention sowie Art. 5 Abs. 1 lit. a Europol-Beschluss.

[324] *Röben*, in: Grabitz/Hilf/Nettesheim, 78. EL 2023, Art. 88 AEUV Rn. 15; *Müller-Wille*, JCMS 2008, 57 ff.

[325] *Felgenhauer*, in: FG Hilger, S. 75 (77); ähnlich *Schöndorf-Haubold*, S. 59.

BKAG vergleichbar, das in diesem Zusammenhang ebenfalls als technischer Dienstleister für andere Polizeibehörden fungiert.[326]

Mit der Europol-VO sollten die Tätigkeiten von Europol auf den Gebieten der Informationssammlung und Informationsanalyse gestärkt werden. Ein Anliegen der Verordnung war es, Europol zu einem „Knotenpunkt des Informationsaustauschs zwischen den Strafverfolgungsbehörden der Mitgliedstaaten“[327] weiterzuentwickeln. Dies bedeutet auch einen Schritt zur Zentralisierung der Informationsverarbeitung bei Europol.[328] Um die Funktion eines Knotenpunkts zu erfüllen, sollte unter anderem eine Datenverarbeitungsarchitektur geschaffen werden, in der sich Zusammenhänge zwischen vorhandenen Daten leichter als bisher erkennen und analysieren lassen.[329] Dies entspricht dem Ziel einer besseren Verknüpfbarkeit von Daten, das auch auf nationaler Ebene zunehmend betont und verfolgt wird.[330] Um den Umbau der Datenverarbeitungsarchitektur zu ermöglichen, entschied man sich auch für eine möglichst technikoffene Regelung in der Europol-VO.[331] Anders als ihre Vorgängerregelungen[332] enthält die Europol-VO keine spezifischen Vorgaben mehr dafür, welche Informationssammlungen das Amt in welcher Form zu führen hat. Bisher war die Auswertung von Informationen durch Europol nur in spezifischen Analysedateien zulässig, deren Betrieb jeweils den Erlass einer Errichtungsanordnung voraussetzte.[333] Diese Notwendigkeit fällt mit der Europol-VO weg.

Die neue Datenverarbeitungsarchitektur auf Grundlage der Europol-VO soll einem „Konzept zur integrierten Datenverwaltung“[334] folgen. Es soll die bisherige Ordnung

[326] *Middel*, S. 93; siehe näher zur Zentralstellenfunktion des Bundeskriminalamts unten Teil 3 A. II. 1.

[327] KOM(2013) 173 endg., S. 6, 8; ErwGr 3 Europol-VO; vgl. auch ErwGr 12 f. Europol-VO sowie schon Europäischer Rat, Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger (2010/C 115/01), ABl. EU C 114, 1 (20).

[328] *Sikora*, in: Brings-Wissen/Ferreau, S. 59 (66).

[329] KOM(2013) 173 endg., S. 8.

[330] Siehe dazu näher unten Teil 2 B. I.

[331] KOM(2013) 173 endg., S. 8; *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 108.

[332] Vgl. Art. 6 ff. Europol-Konvention, Art. 10 ff. Europol-Beschluss.

[333] Vgl. Art. 10, 12 Europol-Konvention, Art. 14, 16 Europol-Beschluss.

[334] Begründung des Rates: Standpunkt (EU) Nr. 8/2016 des Rates in erster Lesung im Hinblick auf den Erlass einer Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI (2016/C 169/02), ABl. EU C 169, S. 60 (62); EURPOL, Programming Document 2019 – 2012, S. 12, 33.

in Dateien auflösen, dadurch eine bessere Verknüpfbarkeit von Informationen ermöglichen und eine redundante Datenspeicherung vermeiden.[335] Dieses Konzept will Europol durch eine zentrale Informationsressource – einen „Datensee" („data lake")[336] – umsetzen. Die bisher wichtigste Informationssammlung des Amtes, das dezentral organisierte Europol-Informationssystem,[337] soll daneben zunächst weiterbetrieben werden. Zur Ausschöpfung des „Datensees" bestehen auch Pläne, Methoden künstlicher Intelligenz und maschinellen Lernens einzusetzen.[338] Schließlich sollen Interoperabilität und Verknüpfbarkeit verschiedener Systeme auf EU-Ebene verbessert werden.[339] Insgesamt weisen die Pläne rund um einen „Datensee" viele Gemeinsamkeiten mit dem Projekt zur Schaffung eines gemeinsamen „Datenhauses" der deutschen Polizeien auf. In beiden Projekten soll eine neue Informationsordnung ohne Dateien geschaffen werden, in der keine redundanten Datenerfassungen mehr notwendig sind und Informationen sich besser verknüpfen lassen.

Durch die neuen Möglichkeiten zur Verknüpfung von Daten, die in dem „Datensee" zur Verfügung stehen würden, würden auch neue Risiken für die Informationssubjekte entstehen. Diese sollen durch strengere Datenschutzregelungen als bisher abgefedert werden.[340] Dazu soll eine Begrenzung des Umfangs der Datenverarbeitung nach dem verfolgten Zweck und Regelungen über den Zugang zu Daten gehören.[341] Es soll ein Prinzip des „eingebauten Datenschutzes"[342] umgesetzt werden. Was damit im

[335] Begründung des Rates: Standpunkt (EU) Nr. 8/2016 des Rates in erster Lesung im Hinblick auf den Erlass einer Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI (2016/C 169/02), ABl. EU C 169, S. 60 (62); vgl. dazu *Coudert*, European Data Protection Law Review 2017, 313 ff.

[336] Europol, 2018 Consolidated Annual Activity Report, S. 6, 9, 24, 72 f.

[337] Vgl. Art. 7 ff. Europol-Konvention, Art. 11 ff. Europol-Beschluss; zur Funktionsweise *Felgenhauer*, in: FG Hilger, S. 75 (79); *Ruthig*, in: Böse, Europäisches Strafrecht, 2013, § 20 Rn. 46 ff.; *Schöndorf-Haubold*, S. 76 ff.; *Weßlau*, in: AE Europol, S. 318 (327 ff.).

[338] Europol, Programming Document 2019 – 2012, S. 33.

[339] Europol, Programming Document 2019 – 2012, S. 38.

[340] Vgl. KOM(2013) 173 endg., S. 6; *Priebe*, EuZW 2016, 894 (895).

[341] Vgl. Begründung des Rates: Standpunkt (EU) Nr. 8/2016 des Rates in erster Lesung im Hinblick auf den Erlass einer Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI (2016/C 169/02), ABl. EU C 169, S. 60 (62).

[342] KOM(2013) 173 endg., S. 8.

Detail gemeint ist, ist ähnlich unklar wie bei dem Konzept des „horizontalen Datenschutzes", das für das deutsche „Datenhaus" angestrebt wird.[343] Jedenfalls fallen die Regelungen über Informationsverarbeitung und Datenschutz in der Europol-VO detaillierter aus als in ihren Vorgängerregelungen.[344]

C. Rechtliche Grundlagen

Dieser Abschnitt stellt die rechtlichen Grundlagen der kriminalbehördlichen Informationsordnung im Überblick dar. Er dient dazu, die geltenden normativen Soll-Vorgaben für diesen Bereich zusammenzufassen. Auf die hier eingeführten rechtlichen Rahmenbedingungen wird im Zusammenhang mit den spezifischen Anforderungen an die Informationsordnung näher einzugehen sein. Außerdem soll die Zusammenfassung an dieser Stelle als Grundlage dazu dienen, später Möglichkeiten zur Fortbildung des Informationsordnungsrechts zu untersuchen.

Es werden zunächst die kompetenzrechtlichen Grundlagen des Informationsordnungsrechts dargestellt (I.). Darauf werden die rechtlichen Vorgaben für den Betrieb und die Funktionsfähigkeit kriminalbehördlicher Informationssysteme erörtert (II.). Es folgt ein Überblick über die Rechte derjenigen, über die Daten in den kriminalbehördlichen Informationssystemen verarbeitet werden (III.). In diesem Zusammenhang werden auch die eingriffsrechtlichen Vorgaben für informationsordnende Tätigkeiten betrachtet.

I. Kompetenzrechtliche Weichenstellungen

Um die gesetzlichen Regelungsstrukturen nachvollziehbar zu machen, bedarf es einer Betrachtung des kompetenzrechtlichen Rahmens der kriminalbehördlichen Informationsordnung. Schon seit jeher sind die föderalen Strukturen der Bundesrepublik Deutschland und die Kompetenzordnung des Grundgesetzes prägend für die Organisation der staatlichen Datenverarbeitung.[345] Für die kriminalbehördliche Informationsordnung gilt insofern keine Ausnahme. Zu Beginn der EDV-Ära war die Kompetenzordnung eine wesentliche Ursache dafür, dass die Polizeien jeweils eigene Informationssysteme entwickelten.[346]

---

[343] Siehe oben III. 3. c.

[344] Vgl. zu der Entwicklung der Datenschutzstandards bei Europol insgesamt zu der Geschichte von Europol *Ruthig*, in: Böse, Europäisches Strafrecht, 2013, § 20 Rn. 15.

[345] Vgl. *Gurlit*, NJW 2010, 1035 (1038).

[346] Siehe oben B. III. 1.

Wer welche Datenflüsse kontrolliert, gestaltet sich auch heute noch als Machtfrage,[347] die durch die gesetzgeberischen und behördlichen Zuständigkeiten zu klären ist. Die Zuständigkeiten für die Gesetzgebung stecken auch den Rahmen der Möglichkeiten für eine Umstrukturierung der Rechtsgrundlagen für die kriminalbehördliche Informationsordnung ab.[348]

Die Aufteilung der Kontrolle über die Informationsflüsse durch die Kompetenzordnung hat schließlich eine freiheitssichernde Funktion für die Betroffenen.[349] Sie stellt sicher, dass staatliche Stellen personenbezogene Informationen nicht beliebig zusammen speichern sowie miteinander verknüpfen können und führt zu einer „informationellen Gewaltenteilung".[350]

Für die Frage, welcher Gesetzgeber Regelungen über welche informationsordnenden Tätigkeiten treffen darf, ist die Unterscheidung von Regelungskompetenzen für das Recht der Gefahrenabwehr und das Recht der Strafverfolgung relevant (1.). Vor allem im Zusammenhang mit den Möglichkeiten einer weiteren behördlichen Zentralisierung ist außerdem die Zentralstellenkompetenz für das polizeiliche Auskunfts- und Nachrichtenwesen nach Art. 87 Abs. 1 Satz 2 GG (2.) zu betrachten.

1. Gefahrenabwehr und Strafverfolgung

Während die Gesetzgebungskompetenzen für die Bereiche der Strafverfolgung und Gefahrenabwehr nach dem Grundgesetz prinzipiell voneinander getrennt sind (a.), verlaufen die Grenzen im Recht der Europäischen Union fließender (b.). Im Folgenden werden die Kompetenzen und ihre Relevanz für informationsordnende Tätigkeiten näher betrachtet.

a. Kompetenzordnung des Grundgesetzes

In der Kompetenzordnung des Grundgesetzes ist es angelegt, dass grundsätzlich zwischen Regelungen über präventive und repressive Tätigkeiten der Kriminalbehörden zu unterscheiden ist.[351] Dies ist auch für Regelungen über informationsordnende Tätigkeiten zu beachten, wenngleich die Grenzen zwischen Prävention und Repression bei diesen in der Praxis – wie bereits herausgestellt wurde –[352] verwischen können.

---

[347] *Bergien*, Zeithistorische Forschungen, 2017, 258 (265 f.).

[348] Siehe unten Teil 3 B.

[349] Siehe zu der freiheitssichernden Funktion der Kompetenzordnung *Bäcker*, DÖV 2011, 840 (841); *Gärditz*, AöR 144 (2019), 81 (83); *Gärditz*, S. 3 f., 239 f.

[350] Siehe zur informationellen Gewaltenteilung als Ausfluss der Zweckbindung unten Teil 3 D. III. 3.

[351] Vgl. *Danne*, S. 165 ff.; *Knemeyer*, in: FS Rudolf, S. 483.

[352] Siehe oben A. III.

Nach dem Grundgesetz liegen die Gesetzgebungskompetenzen bei den Ländern, soweit sie nicht ausdrücklich dem Bund zugewiesen sind (Art. 70 Abs. 1 GG). Dementsprechend liegt die Zuständigkeit für das Recht der Gefahrenabwehr mangels anderweitiger Regelungen zunächst bei den Ländern.[353] Dies hat historische Gründe. Sowohl die alliierten Besatzer als auch die Verfasser des Grundgesetzes wollten eine Dezentralisierung der Gefahrenabwehr erreichen.[354]

Für den Bereich der Strafverfolgung dagegen folgen aus der konkurrierenden Gesetzgebungskompetenz für das gerichtliche Verfahren aus Art. 74 Abs. 1 Nr. 1 GG weitgehende Regelungsmöglichkeiten des Bundes. Das Recht des gerichtlichen Verfahrens umfasst die Gesamtheit der Rechtsnormen über die „verfahrensmäßige Behandlung von Streitfällen durch die Gerichte“[355] einschließlich des Strafprozessrechts. Unstreitig ist auch das unmittelbare Vorfeld des Strafverfahrens von der Gesetzgebungskompetenz aus Art. 74 Abs. 1 Nr. 1 GG gedeckt, so dass das strafprozessuale Ermittlungsverfahren auf dieser Grundlage vom Bund geregelt werden konnte.[356]

Generell ist hinsichtlich der Regelungskompetenzen zwischen einzelnen Phasen der Verarbeitung von Informationen zu unterscheiden. Für die Informationsordnung maßgeblich sind primär die Speicherung und Ordnung von Daten. Regelungen über diese Schritte der Datenverarbeitung sind kraft Sachzusammenhangs durch den Gesetzgeber zu treffen, der auch für die Regelungen über die Erhebung der Daten zuständig ist.[357] Dies bedeutet vereinfacht, dass die Speicherung von Daten, die zunächst zu Zwecken der Strafverfolgung erhoben wurden, vom Bundesgesetzgeber und die Speicherung von Daten, die zunächst zu Zwecken der Gefahrenabwehr erhoben wurden, vom Landesgesetzgeber zu regeln ist.

---

[353] Vgl. zu der Bundesgesetzgebungskompetenz für die öffentliche Fürsorge aus Art. 74 Abs. 1 Nr. 7 GG als möglicher Grundlage eines „Präventionsgesetzes“ für diverse staatliche und gesellschaftliche Einrichtungen *Ostendorf*, in: FS Grünwald, S. 419 (429 f.); *Pitschas*, DÖV 2002, 221 (228 f.)

[354] Vgl. zu den bundesrechtlichen Kompetenztiteln zur Prävention *Gärditz*, S. 240 ff.

[355] *Uhle*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 74 Rn. 118.

[356] *Uhle*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 74 Rn. 119; *O. Müller*, StV 1995, 602 (604); *Siebrecht*, JZ 1996, 711 (714); *W. Schenke*, JR 1970, 48 (51); kritisch hierzu aus normativ-funktionaler Sicht *Brodowski*, S. 503 ff.; vgl. zum verfassungshistorischen Hintergrund *Gärditz*, S. 314 ff.

[357] Vgl. BVerfGE 125, 260 (314); BVerfGE 133, 277 (319 f.); BVerfGE 154, 152 (235); *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 33.

b. Unionsrechtlicher Kontext

Im europäischen Kontext spielt die Unterscheidung zwischen präventiven[358] und repressiven Tätigkeiten eine nur untergeordnete Rolle.[359] Dies gilt auch für informationsordnende Tätigkeiten. Das Unionsrecht unterscheidet zwischen polizeilicher und justizieller Zusammenarbeit (Art. 82 ff., 87 ff. AEUV), allerdings nicht im Einzelnen zwischen Tätigkeiten und Aufgaben im präventiven und repressiven Bereich. Es vereint den präventiven und repressiven Rechtsgüterschutz in einem integrierten Ansatz.[360]

Die polizeiliche Zusammenarbeit nach Art. 87 Abs. 1 AEUV erfasst neben der Verfolgung auch die Verhütung von Straftaten. Ähnlich umfasst der in Art. 88 Abs. 1 AEUV geregelte Auftrag von Europol gleichermaßen die „Verhütung und Bekämpfung“[361] von Kriminalität.[362] Auch aus den Dokumenten der Europäischen Union wird deutlich, dass der Tätigkeitsbereich der Strafverfolgung (als Übersetzung von „law enforcement“) nicht gleichbedeutend mit einem repressiven Tätigwerden ist und insbesondere die Verhütung von Straftaten erfasst,[363] die nach deutschem Rechtsverständnis dem präventiven Tätigkeitsbereich zuzuordnen wäre. So nehmen auch Datenbanken und Informationssysteme auf EU-Ebene die Strafverfolgung nicht isoliert in Bezug, sondern schließen auch präventive Zwecke mit ein.[364]

In einem ähnlichen Sinne enthält Art. 8 JI-Richtlinie für die kriminalbehördliche Datenverarbeitung Vorgaben, die ebenso für den Bereich der Gefahrenabwehr wie für den Bereich der Strafverfolgung gelten. Zwar sind diese recht unspezifisch und erforderten keine grundlegende Anpassung der vor Geltung der JI-Richtlinie bestehenden Regelungen im deutschen Gefahrenabwehr- und Strafverfolgungsrecht.[365] Allerdings weist Art. 8 JI-Richtlinie zumindest in die Richtung gemeinsamer Vorgaben für die Datenverarbeitung in beiden Bereichen.

Unter Berücksichtigung der europäischen Ebene scheinen unterschiedliche Regelungen für die Speicherung von Daten zu präventiven und repressiven Zwecken den

---

[358] Vgl. zum unklaren Bedeutungsgehalt des Begriffes der Prävention im Unionsrecht *Schöndorf-Haubold*, S. 130.

[359] *Brodowski*, S. 469; *Möstl*, EuR 2009, Beiheft 3, 33 (50); *Schöndorf-Haubold*, S. 29 f.; vgl. grundlegend zu den Kategorien Prävention und Repression im Recht der Europäischen Union *Gärditz*, in: AE Eurpol, S. 192 ff.

[360] *Gärditz*, in: AE Eurpol, S. 192 (209) m.w.N.

[361] Zu der unterschiedlichen Bedeutung dieser Begriffe auf europäischer Ebene im Vergleich zum nationalen Recht *Paeffgen*, in: AE Eurpol, S. 173 (176 ff.).

[362] Vgl. zu der Vermengung repressiver Aufgabenbereiche bei Europol bereits *Tolmein*, StV 1999, 108 (110).

[363] KOM(2012) 735, S. 3.

[364] Vgl. *Brodowski*, S. 459.

[365] Vgl. *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (69); siehe näher unten III. 1. b.

Zielen der kriminalbehördlichen Informationsordnung eher im Wege zu stehen. So stellte die Kommission fest, dass einem „effizienten Informationsaustausch [...] Abweichungen bei der Unterscheidung zwischen polizeilicher, zollbehördlicher und justizieller Zusammenarbeit“ abträglich sind.[366]

2. Zentralstellenkompetenz

Für das Recht der kriminalbehördlichen Informationsordnung ist weiter die Zentralstellenkompetenz für das polizeiliche Auskunfts- und Nachrichtenwesen nach Art. 87 Abs. 1 Satz 2 GG relevant. Dieser ermöglicht es, durch Bundesgesetz Zentralstellen unter anderem für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei einzurichten. Das polizeiliche Auskunfts- und Nachrichtenwesen umfasst „das Sammeln, Auswerten und Weitergeben von Informationen zur Gefahrenabwehr und Strafverfolgung“[367]. Hierunter fallen unter anderem die im Rahmen dieser Untersuchung als informationsordnende Tätigkeiten bezeichneten Handlungen.[368] Die Gesetzgebungskompetenzen, die mit den Verwaltungskompetenzen in Art. 87 Abs. 1 Satz 2 GG korrespondieren, regelt Art. 73 Abs. 1 Nr. 10 GG.[369]

Eine Notwendigkeit zur Differenzierung zwischen präventiven und repressiven Tätigkeiten der Polizei ergibt sich im Rahmen des polizeilichen Auskunfts- und Nachrichtenwesens nicht. Weder aus Art. 87 Abs. 1 Satz 2 GG noch aus der einfachgesetzlichen Umsetzung der Regelung in § 2 Abs. 1 BKAG, der von der Unterstützung bei der „Verhütung und Verfolgung von Straftaten“ spricht, folgt eine Einschränkung der Tätigkeiten der Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen auf präventive Aufgaben.[370]

Derzeit füllt das Bundeskriminalamt nach § 2 Abs. 1 BKAG die Funktion der Zentralstelle aus. Im weiteren Verlauf der Arbeit wird näher zu untersuchen sein, inwiefern Möglichkeiten einer weiteren Zentralisierung der Informationsordnung beim Bundeskriminalamt bestehen.[371]

---

[366] KOM(2005) 490 endg., S. 3.

[367] *Ibler*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 87 Rn. 129; vgl. auch VG Düsseldorf BeckRS 2011, 45746; *Abbühl*, S. 86; *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BKAG Rn. 7; *Hermes*, in: Dreier, GG, 3. Aufl. 2018, Art. 87 Rn. 50.

[368] Siehe oben A. I.

[369] Siehe näher unten Teil 3 A. II. 2.

[370] Vgl. zum BKAG 1973 *Riegel*, DVBl. 1982, 720 (723).

[371] Siehe unten Teil 3 A.

II. Vorgaben für den Betrieb von Informationsressourcen

Einer der Schwerpunkte der vorliegenden Untersuchung sind die Anforderungen an Informationsressourcen aus kriminalbehördlich-operativer Sicht. Im Zusammenhang mit diesen wird näher zu untersuchen sein, inwiefern sie mit rechtlichen Anforderungen an die Informationsordnung korrespondieren oder jenen widersprechen. An dieser Stelle wird herausgearbeitet, ob eine Pflicht zum Betrieb von kriminalbehördlichen Informationssystemen besteht (1.) und ein Überblick gegeben, welche Anforderungen das Recht an ihre Funktionen stellt (2.).

1. Pflichten zum Betrieb von kriminalbehördlichen Informationsressourcen

Wie bereits erörtert, lassen sich kriminalbehördliche Informationsressourcen als Instrumente zur Vorsorge begreifen,[372] die unter anderem dazu dienen, sich auf die Abwehr von Gefahren für die öffentliche Sicherheit und zukünftige Maßnahmen in der Strafverfolgung vorzubereiten. In diesem Zusammenhang stellt sich die Frage, ob sich rechtlich eine Pflicht herleiten lässt, kriminalbehördliche Informationsressourcen generell oder in einer bestimmten Form zu betreiben. Auf verfassungsrechtlicher Ebene könnten die staatlichen Pflichten zur Gewährleistung der öffentlichen Sicherheit und einer funktionstüchtigen Strafrechtspflege den Betrieb von Informationsressourcen gebieten.

Die Pflicht zur Gewährleistung einer funktionstüchtigen Strafrechtspflege beruht auf dem Rechtsstaatsprinzip.[373] Zur Verwirklichung von Gerechtigkeit im Rechtsstaat besteht ein Bedürfnis nach einer wirksamen Strafverfolgung.[374] Als „wesentlicher Auftrag eines rechtsstaatlichen Gemeinwesens" verfassungsrechtlich anerkannt ist die Aufklärung schwerer Straftaten.[375]

Zum Teil wird aus dem verfassungsrechtlich anerkannten Interesse an einer funktionierenden Strafrechtspflege abgeleitet, dass der Staatsanwaltschaft zumindest aktuelle Ermittlungsdaten zur Verfügung stehen müssten.[376] Dies leuchtet zunächst ein, da eine funktionierende Strafrechtspflege im Allgemeinen und eine Aufklärung schwerer Straftaten im Besonderen ohne die Bevorratung gewisser Ermittlungsdaten kaum vorstellbar sind. In welcher Form die Bevorratung zu erfolgen hat, auf welchem Stand die

---

[372] Siehe oben B. II.

[373] Vgl. dazu nur BVerfGE 33, 367 (383); BVerfGE 53, 152 (160); BVerfG NJW 1987, 1929; kritisch zu diesem Begriff *Hassemer*, StV 1982, 275 (277 ff.).

[374] BVerfGE 33, 367 (383).

[375] BVerfGE 29, 183 (194); BVerfGE 33, 367 (383); BVerfGE 109, 279 (336).

[376] *Rebmann/Schoreit*, NStZ 1984, 1 (4).

Daten sein müssen, in welcher Art von Systemen sie gespeichert werden und wie einfach sie verfügbar sein müssen, lässt sich aus der Pflicht zur Gewährleistung einer funktionstüchtigen Strafrechtspflege in ihrer vagen Kontur allerdings nicht folgern.

Ähnlich schwierig ist es, eine Pflicht zum Betrieb kriminalbehördlicher oder anderer sicherheitsbehördlicher Informationsressourcen aus der staatlichen Aufgabe der Gewährleistung von Sicherheit herzuleiten, die gewissermaßen das Fundament der Legitimation des modernen Staats-Leviathans bildet.[377] Anders als in diversen historischen und aktuellen Verfassungstexten[378] ist eine staatliche Verpflichtung zur Gewährleistung von Sicherheit im Grundgesetz nicht ausdrücklich festgeschrieben.[379] Nach dem Grundgesetz ergibt sich eine Aufgabe staatlicher Sicherheitsgewährleistung jedoch aus den Schutzpflichten, die aus den einzelnen Grundrechten hergeleitet werden.[380] Ein eigenständiges „Supergrundrecht" auf Sicherheit existiert nicht.[381]

Dass die Kriminal- und Sicherheitsbehörden gewisse Informationssysteme betreiben und Daten speichern müssen, damit der Staat seinen Schutzpflichten in der Realität nachkommen kann, dürfte sich kaum bestreiten lassen. Die kriminalbehördlichen Informationsressourcen sind ein wichtiger Bestandteil der Sicherheitsarchitektur der Bundesrepublik Deutschland[382] und aus dem Alltag der Strafverfolgung und Gefahrenabwehr nicht wegzudenken. Aus den grundrechtlichen Schutzpflichten einigermaßen konkrete Vorgaben herzuleiten, für welche Zwecke, in welcher Form und bei welchen Stellen der Staat sicherheitsrelevante Informationen mit und ohne Personenbezug vorhalten muss, ist jedoch schwer.

---

[377] *F.-X. Kaufmann*, in: Grimm, Staatsaufgaben, S. 15 (20 f.); *Kötter*, S. 92; vgl. zu der Entwicklung der Staatsaufgabe Sicherheit *Möstl*, S. 4 ff.; *Park*, S. 11; *Preuß*, in: Grimm, Staatsaufgaben, S. 523 (524 ff.) jeweils m.w.N.; vgl. zu Ideengeschichte und staatstheoretischem Fundament *Dietlein*, S. 21 ff.; *Isensee*, S. 3 ff.; *Robbers*, S. 27 ff.

[378] So etwa Art. 3 Virginia Declaration of Rights vom 12. Juni 1776; Art. 2 Satz 2 Erklärung der Menschen- und Bürgerrechte vom 26. August 1789; vgl. auch Art. 3 AEMR; siehe zu den Rechten auf Sicherheit aus Art. 5 Abs. 1 Satz 1 EMRK und Art. 6 GRCh *Schöndorf-Haubold*, S. 28.

[379] Eine entsprechende Formulierung von Art. 2 Abs. 1 GG war aber im parlamentarischen Rat erwogen worden; vgl. dazu *Matz*, in: Häberle, Entstehungsgeschichte der Artikel des Grundgesetzes, 2. Aufl. 2010, S. 1 (62); *Kötter*, S. 117; vgl. zu der ausschließlichen Gesetzgebungskompetenz für die Zusammenarbeit der Sicherheitsbehörden aus Art. 73 Abs. 1 Nr. 10 GG als Verfassungsentscheidung für die innere Sicherheit *Götz*, in: Isensee/Kirchhof, Handbuch des Staatsrechts IV, 3. Aufl. 2006, § 85 Rn. 23; *Pitschas*, JZ 1993, 858 (859).

[380] Vgl. nur BVerfGE 39, 1 (41 ff.); BVerfGE 46, 160 (164); BVerfGE 49, 24 (53); BVerfGE 53, 30 (57); *Bethge*, DVBl. 1989, 841 (848); *Isensee*, S. 27 ff.; *Möstl*, S. 15, 25 ff.

[381] Vgl. dazu *Kniesel*, Die Polizei 1991, 185 (186); *Kowalczyk*, S. 22; *Denninger*, in: Hohmann, S. 127 (129). Einfachgesetzlich ergibt sich eine Pflicht zur Gewährleistung der öffentlichen Sicherheit aus den Aufgabenzuweisungen der Polizeigesetze.

[382] Siehe oben B. V.

Die Schutzpflichten erscheinen im Zusammenhang mit der kriminalbehördlichen Informationsordnung ebenso schwer operationalisierbar wie das Interesse an der Gewährleistung einer funktionierenden Strafrechtspflege. Dies hängt unter anderem damit zusammen, dass es um die Bereitstellung von Ressourcen zur Vorsorge geht. Zwar ist anzunehmen, dass grundrechtliche Schutzpflichten auf der Ebene der Vorsorge zur Gefahrenabwehr und Strafverfolgung durchaus relevant sein können.[383] Der Zusammenhang zwischen der Errichtung und Nutzung kriminalbehördlicher Informationssysteme und konkret abzuwendenden Gefährdungen von Rechtsgütern ist aber regelmäßig so entfernt, dass grundrechtliche Schutzpflichten hier keine Wirkung entfalten können. Es ist kaum eine Konstellation vorstellbar, in der die Errichtung und Nutzung einer Datenbank sich gerade als die konkrete Maßnahme aufdrängt, um ein bestimmtes Rechtsgut schützen zu können. So lässt sich beispielsweise in *Fall 5* kaum sagen, ob gerade die Einrichtung der Falldatei „Hass und Hetze im Internet" die gebotene Handlung ist, um den öffentlichen Frieden und die Ehre der Nutzer*innen im Rahmen von Diskussionen in sozialen Medien zu schützen.

Es besteht ein weiter staatlicher Handlungsspielraum[384] bei der Einrichtung und Ausgestaltung von Informationsressourcen, die zum präventiven und repressiven Rechtsgüterschutz beitragen sollen. Ansatz für die genauere Bestimmung einer Pflicht zur Bereithaltung von Informationen können dabei nur konkretere Schutzgüter und Gefährdungslagen sein.[385] So ließe sich etwa diskutieren, ob der Staat Datenbanken mit Informationen über (potentielle) Terrorist*innen bereithalten muss, um die Allgemeinheit vor Anschlägen schützen und die Verantwortlichen strafrechtlich verfolgen zu können. Die Bereitstellung von Datenbanken und Speicherung von Informationen darin wäre in diesem Fall im Kontext der Maßnahmen zum Schutz vor terroristischen Anschlägen insgesamt zu beurteilen. Im Sinne des verfassungsrechtlichen Untermaßverbotes müssten hierfür jedenfalls Mindestanforderungen erfüllt werden und die getroffenen staatlichen Maßnahmen dürften ihr Ziel nicht evident verfehlen.[386] In den Bereichen der Strafverfolgung und Gefahrenabwehr ist aufgrund der stetigen Bemühungen um den Ausbau der Informationsressourcen angesichts neuer Bedrohungen eine derartige Unterschreitung des Mindestschutzes nicht zu befürchten.

---

[383] Vgl. *Middel*, S. 39; *Pietrzak*, JuS 1994, 748 (750); *Unruh*, S. 78.

[384] Vgl. zur Erweiterung des Handlungsspielraums bei sich nicht notwendigerweise realisierenden Gefahren *E. Klein*, NJW 1989, 1633 (1637).

[385] In diese Richtung auch *Albers* in: Spiecker gen. Döhmann/Collin, S. 50 (64).

[386] Vgl. BVerfGE 56, 54 (80); BVerfGE 88, 203 (254 f., 262 f.); *O. Klein*, JuS 2006, 960 (961).

Nicht präzise zu bestimmen ist auch, in welchem Ausmaß der Staat im Rahmen der Informationsordnung[387] – und darüber hinaus – dazu verpflichtet ist, moderne Technologien zur Sicherheitsgewährleistung einzusetzen.[388] Wie weit Schutzpflichten zum Einsatz von Informationstechnologien gehen, ist im Einzelnen noch kaum untersucht.[389] Zwar erscheint es plausibel, dass sich der Staat zur Erfüllung seines Auftrags zum Schutz von Rechtsgütern modernen technischen Hilfsmitteln nicht verschließen darf, allerdings wird auch hier eine genauere Bestimmungen etwaiger Verpflichtungen nur im Zusammenhang mit konkreten Schutzgütern und Gefährdungslagen sowie der Gesamtheit der ergriffenen Maßnahmen möglich sein.

Jedenfalls faktisch hängt es auch von den Erwartungen der Bürger*innen ab, inwieweit sich der Staat durch die Errichtung von Informationsressourcen und den Einsatz komplexer technischer Hilfsmittel um die öffentliche Sicherheit sowie eine funktionierende Strafrechtspflege bemüht. Ob sich diese Erwartungen auf normativer Ebene heranziehen lassen, um die konkrete Reichweite der Schutzpflichten zu bestimmen, ist hingegen fraglich.[390] Hierfür ließe sich anführen, dass ein wesentlicher Grund für die Anerkennung grundrechtlicher Schutzpflichten darin liegt, die Gehorsamspflicht der Bürger*innen und ihre Unterwerfung unter das staatliche Gewaltmonopol zu kompensieren.[391] Weil die Bürger*innen sich dem Staat unterordnen, müssen sie durch ihn geschützt werden. Vor diesem Hintergrund erscheint es nur konsequent, bei der Bestimmung des notwendigen rechtlichen Schutzes ihre Erwartungen zu berücksichtigen.

Eine einheitliche gesamtgesellschaftliche Erwartung, wie Informationsressourcen für die (Vorbereitung von) Strafverfolgung und Gefahrenabwehr ausgestaltet zu sein haben, wird sich allerdings nur schwer ermitteln lassen. Generell ist die Annahme verbreitet, dass in der modernen Gesellschaft die Erwartungen an den Staat steigen, zu Sicherheitszwecken Wissen zu generieren und Informationen zu gewinnen.[392] Dies findet

[387] Vgl. zu der staatlichen Sammlung von Informationen zu Sicherheitszwecken als Erfüllung einer Schutzpflicht BayVerfGH NVwZ 1996, 166. Dass die Generierung staatlichen Wissens generell zur Erfüllung einer staatlichen Schutzpflicht dienen kann, zeigt etwa BVerfGE 53, 30 (59 f.), wonach verschiedene informationsbezogene Aspekte des atomrechtlichen Genehmigungsverfahrens der staatlichen Pflicht zum Schutz von Leben und körperlicher Unversehrtheit Rechnung tragen; vgl. auch *Albers* in: Spiecker gen. Döhmann/Collin, S. 50 (63 f.).

[388] Vgl. *Roßnagel/Wedde/Hammer/Pordesch*, S. 159; *Martínez Soria*, DÖV 2007, 779.

[389] Vgl. *Albers* in: Spiecker gen. Döhmann/Collin, S. 50 (63 f.).

[390] Vgl. in diese Richtung *Gusy*, DÖV 1996, 573 (574); *Bull*, in: Bull, S. 15 ff.; *F.-X. Kaufmann*, in: Grimm, Staatsaufgaben, S. 15 ff.

[391] *Isensee*, S. 23 ff.; *E. Klein*, NJW 1989, 1633 (1635 f.).

[392] Vgl. *Schwabenbauer*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 1; *Volkmann*, JZ 2004, 696 (700).

beispielsweise in der von *Gilles Deleuze*[393] festgestellten Entwicklung hin zu einer Kontrollgesellschaft Ausdruck, die mit einem verstärkten Anspruch der „Vorbeugung von Verstößen durch eine permanente, das Individuum einbeziehende Kontrolle“[394] verbunden ist. In diesem Sinne wird ein wachsendes Präventionsbedürfnis auch als Ursache dafür angeführt, dass der Staat in immer größerem Maße Informationen sammelt und ordnet.[395]

Die Erwartungen der Bürger*innen, wie der Staat die Aufgabe der Sicherheitsgewährleistung wahrnimmt, sind dabei zugleich von technologischen Entwicklungen geprägt.[396] Dies wirkt sich auch auf die kriminalbehördliche Informationsordnung als Instrument zur Vorbereitung von Strafverfolgung und Gefahrenabwehr aus. Technische Entwicklungen und gesellschaftliche Erwartungen führen dazu, dass eine komplexe Informationsordnung als Instrument der Sicherheitsgewährleistung gestaltet wird. Rechtlich ist ein Rahmen dafür zu schaffen, dass die Informationsordnung ihre Aufgaben erfüllen kann.

Schließlich lassen sich neben den grundrechtlichen Schutzpflichten auch aus anderen verfassungsrechtlichen Vorgaben nur schwerlich Rückschlüsse darauf ziehen, ob und in welcher Form eine kriminalbehördliche Informationsordnung zu errichten und einzurichten ist. Eine allgemeine Pflicht oder Aufgabe, Informationen zu bevorraten,[397] enthält das Grundgesetz nicht. Art. 87 Abs. 1 Satz 2 GG scheint das Ziel eines funktionierenden polizeilichen Auskunfts- und Nachrichtenwesens zumindest zu implizieren.[398] Allerdings handelt es sich hierbei in erster Linie um eine Kompetenznorm und nicht etwa um ein Staatsziel. Art. 87 Abs. 1 Satz 2 GG legitimiert die hierin genannten Aufgaben zwar auch verfassungsrechtlich, eine Pflicht zu ihrer Wahrnehmung – im

---

[393] *Deleuze*, in: Deleuze, Unterhandlungen, S. 254 ff.

[394] *Singelnstein*, in: FS Rogall, S. 725 (735); vgl. auch *Jones*, Punishment & Society 2000, 5 (8 ff.); *S. Kaufmann*, in: Gusy/Kugelmann/Würtenberger, S. 3 (12 f.).

[395] *Grimm*, KritV 1986, 38 (45).

[396] Vgl. *Grimm*, KritV 1986, 38.

[397] In diese Richtung wurde teilweise BVerfGE 65, 1 (3) interpretiert, wo von einer zu respektierenden „Pflicht des Staates [...], die für rationales und planvolles staatliches Handeln erforderlichen Informationen zu beschaffen“ die Rede ist. Hieraus wurde zum Teil eine Aufgabe der Informationsvorsorge hergeleitet; vgl. *Rogall*, S. 54 f.; *Scholz/Pitschas,* S. 103 f.; *Vogelgesang*, S. 190 f.; ähnlich auch *Ernst*, S. 98 f. („Informationsvorhaltung“). Dieses Konzept ist allerdings abzulehnen, da es in erster Linie dazu zu dienen schien, dem vom Bundesverfassungsgericht anerkannten Recht auf informationelle Selbstbestimmung einen Auftrag staatlicher Informationsvorsorge entgegenzusetzen, um dieses zu „neutralisieren“ (*Denninger*, in: Hohmann, S. 127 (128)). Auch die verfassungsrechtliche Herleitung der Informationsvorsorge überzeugt methodisch nicht; vgl. *Albers*, Determination, S. 99; *Albers* in: Spiecker gen. Döhmann/Collin, S. 50 (64); *Weßlau*, S. 169.

[398] *Möstl*, Stellungnahme BKAG 2018, S. 5; vgl. im Zusammenhang mit der rechtsstaatlich gebotenen Verfolgung von Straftaten auch BVerwG NJW 1990, 2765 (2766).

Allgemeinen oder in einer bestimmten Art und Weise – lässt sich aus der Vorschrift hingegen nicht ableiten.[399]

Im Ergebnis legen verschiedene einfache Gesetze den Betrieb von bestimmten Informationsressourcen durch die Kriminal- und Sicherheitsbehörden fest bzw. legitimieren diesen.[400] Eine Notwendigkeit zum Betrieb derartiger Systeme in einer spezifischen Form ergibt sich aber nicht aus höherrangigem Recht. Wollte man ein notwendiges Mindestmaß des Betriebs kriminalbehördlicher Informationsressourcen aus den Pflichten zur Gewährleistung einer funktionierenden Strafrechtspflege und den grundrechtlichen Schutzpflichten herleiten, wäre dieses aktuell jedenfalls nicht unterschritten.

2. Anforderungen an die Funktionen von Informationssystemen

Nur wenige gesetzliche Vorschriften legen Anforderungen an die Funktionen von kriminalbehördlichen Informationssystemen fest. Ein Beispiel hierfür ist die Regelung über das Informationssystem des Bundeskriminalamtes in § 13 BKAG. Abs. 2 der Vorschrift beschreibt die Grundfunktionen des Systems für die Strafverfolgung und Gefahrenabwehr in recht allgemeiner Form. Dazu gehören unter anderem die Unterstützung bei polizeilichen Ermittlungen, bei Ausschreibungen und Fahndungen, bei der Erstellung von strategischen Analysen und Statistiken sowie die Durchführung von Abgleichen von personenbezogenen Daten. Die Aufzählung dieser Funktionen ist allerdings nicht abschließend, sondern als regelbeispielhaft zu verstehen.[401] § 29 Abs. 2 Satz 1 BKAG schreibt für den allgemeinen polizeilichen Informationsverbund, für den das BKA als Zentralstelle gemäß § 29 Abs.1 BKAG ein Verbundsystem zur Verfügung stellt, vor, dass auch dieser die in § 13 Abs. 2 BKAG geregelten Grundfunktionen zu erfüllen hat. Eine mit § 13 Abs. 2 BKAG beinahe wortlautgleiche Regelung findet sich außerdem für die Funktionen eines von der Polizei in Sachsen-Anhalt zu betreibenden Informationssystems in § 13c SOG LSA.

Im Übrigen finden sich im Polizei- und Datenschutzrecht Anforderungen an die Qualität von Daten, die in kriminalbehördlichen Informationsressourcen bereitgehalten werden. Diese Anforderungen sind aber eher allgemein gehalten.[402] Vor allem das Unionsrecht verlangt auch eine zwischenbehördliche Verfügbarkeit von Daten.[403] Im nationalen Recht ist dieser Aspekt noch nicht ausdrücklich geregelt.

---

[399] *Burgi*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 87 Rn. 54; *Sachs*, in: Sachs, GG, 9. Aufl. 2021, Art. 87 Rn. 33 f.

[400] Vgl. § 1 Abs. 1 ATDG (für die Antiterrordatei); § 1 Abs. 1 RED-G; § 13 Abs. 1 BKAG.

[401] BT-Drs. 18/11163, S. 109; *Eichenhofer*, in: Barczak, BKAG, 2023, § 13 Rn. 16.

[402] Siehe näher unten Teil 2 C. III.

[403] Siehe unten Teil 2 A. III. 3.

III. Individualschützende Vorgaben

Neben den Anforderungen an den Betrieb und die Funktionen kriminalbehördlicher Informationssysteme sind auch die rechtlichen Vorgaben zum Schutz derjenigen zu betrachten, über die Informationen in der kriminalbehördlichen Informationsordnung gespeichert sind. Diese werden in erster Linie aus dem Datenschutzrecht hergeleitet (1.). Aber auch der Diskriminierungsschutz sowie die rechtsstaatliche Unschuldsvermutung sind für im Rahmen der kriminalbehördlichen Informationsordnung relevant (2.).

1. Datenschutzrecht

Aus dem Datenschutzrecht folgen die am stärksten ausgeprägten Vorgaben für den Schutz von Individuen im Zusammenhang mit der kriminalbehördlichen Informationsordnung. Hier sollen zunächst die verfassungsrechtlichen Grundlagen des Datenschutzes skizziert werden (a.). Diese Vorgaben finden konkret Niederschlag in den Befugnissen zur Speicherung und Strukturierung von Daten in den Polizeigesetzen und der Strafprozessordnung (b.). Schließlich werden die Funktionen und Leistungsgrenzen des Datenschutzrechts im Zusammenhang mit der kriminalbehördlichen Informationsordnung betrachtet (c.).

a. Verfassungsrechtliche Grundlagen

Die einfachgesetzlichen Regelungen zur kriminalbehördlichen Informationsordnung sind stark von datenschutzrechtlichen Vorgaben geprägt, deren Wurzeln im Verfassungsrecht liegen. Im deutschem Recht ist hierfür das vom Bundesverfassungsgericht in seinem Volkszählungsurteil 1983[404] aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitete Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts maßgeblich. Dieses schützt im Ausgangspunkt die „Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[405]. Dazu gehört es nach dem Bundesverfassungsgericht auch, dass die Bürger*innen wissen können müssten, „wer was wann und bei welcher Gelegenheit über sie weiß.“[406]

[404] BVerfGE 65, 1. Wichtige Aspekte des verfassungsrechtlichen Datenschutzes entwickelte das Bundesverfassungsgericht zuvor bereits in der Mikrozensus-Entscheidung aus dem Jahr 1969; BVerfGE 27, 1 ff.

[405] BVerfGE 65, 1 (43).

[406] BVerfGE 65, 1 (43).

Der Schutz durch das Recht auf informationelle Selbstbestimmung knüpft unmittelbar an den Umgang mit jeder Art von personenbezogenen Daten an.[407] Zur Bestimmung des Begriffes „personenbezogene Daten" kann auf die gesetzliche Definition zurückgegriffen werden. Nach Art. 4 Nr. 1 DSGVO, § 46 Nr. 1 BDSG sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen".[408] Hinsichtlich der betreffenden Daten ist es unerheblich, welcher Aussagegehalt ihnen zukommt, solange ein Personenbezug vorhanden ist. Der Grad der „Privatheit" einer Information spielt keine Rolle – es gibt in diesem Sinne kein „belangloses" Datum mehr.[409]

Der weite Schutzumfang des informationellen Selbstbestimmungsrechts ist einer durch die moderne Datenverarbeitung geschaffenen abstrakten Gefährdungslage geschuldet.[410] Diese Gefährdungslage kann nach dem Bundesverfassungsgericht „bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann."[411] Dies kann der Fall sein, wenn aus solchen Informationen „weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch Eingriffe in seine Verhaltensfreiheit mit sich bringen können"[412]. Zur Beschreibung der Gefährdung durch die Verknüpfung von Informationen wird oftmals auf das Risiko der Erstellung von „Persönlichkeitsprofilen" oder „Persönlichkeitsbildern" verwiesen.[413] Die realen Beeinträchtigungen der freien Entfaltung der Persönlichkeit, die sich aus dem Umgang mit einzelnen personenbezogenen Daten ergeben, sind nur schwer zu erfassen. Sie folgen aus der tatsächlichen oder auch nur möglichen Verwendung der Daten in unterschiedlichen Zusammenhängen.[414]

Einen ähnlichen Schutzgehalt wie das informationelle Selbstbestimmungsrecht weist das Recht auf Achtung des Privatlebens in Art. 8 Abs. 1 EMRK auf, auf das der

---

[407] BVerfGE 65, 1 (42); vgl. auch *Albers*, Informationelle Selbstbestimmung, S. 280.

[408] Ähnlich die Definition in § 3 Abs. 1 BDSG a.F., wonach personenbezogene Daten „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" sind.

[409] BVerfGE 65, 1 (45).

[410] Vgl. *Benda*, DuD 1984, 86 (88).

[411] BVerfGE 120, 274 (312).

[412] BVerfGE 120, 274 (312).

[413] *Di Fabio*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 2 Abs. 1 Rn. 174 ff.; *Singelnstein*, NStZ 2012, 593 (599).

[414] *Albers*, Informationelle Selbstbestimmung, 2005, S. 240; vgl. auch *Weichert*, NJW 2001, 1463 (1465 f.).

Europäische Gerichtshof für Menschenrechte seine Rechtsprechung zum Datenschutzrecht stützt. Im Recht der Europäischen Union ergibt sich ein Recht auf den Schutz personenbezogener Daten aus Art. 8 GRCh und Art. 16 Abs. 1 AEUV.[415] Aufgrund ihrer Weite sind die Rechtspositionen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, Art. 8 EMRK und Art. 8 GRCh nur schwer abstrakt voneinander abzugrenzen.[416] Auf europäischer Ebene rückte der Datenschutz etwas später in den Fokus als in Deutschland. Mittlerweile haben sich der Europäische Gerichtshof für Menschenrechte und der Europäische Gerichtshof allerdings ausführlich mit Fragen des Datenschutzes befasst. Dies gilt besonders im Zusammenhang mit der sicherheitsbehördlichen Informationsordnung. Besonders die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Art. 8 EMRK ist stark von kriminal- und sicherheitsbehördlichen Datenverarbeitungen geprägt.[417] Sie bildete bis zum Inkrafttreten der GRCh im Jahre 2009 die Grundlage der Rechtsprechung des Europäischen Gerichtshofs zum Datenschutzrecht.[418]

In der kriminalbehördlichen Informationsordnung werden personenbezogene Daten auf vielfältige Weise verarbeitet. Die abstrakten Risiken, vor denen das Recht auf informationelle Selbstbestimmung bzw. das Datenschutzgrundrecht schützen sollen, lassen sich anhand der kriminalbehördlichen Informationsordnung nahezu idealtypisch veranschaulichen: Dass Daten über Bürger*innen in polizeilichen und staatsanwaltschaftlichen Systemen gespeichert und strukturiert werden, bekommen diese noch nicht unmittelbar zu spüren. Diese Schritte bereiten aber den Boden für potentiell ernstzunehmende Beeinträchtigungen, die aus dem Abruf (vgl. *Fall 1*), der Verknüpfung (vgl. *Fall 3*) und sonstigen Verwendungen der Daten folgen können. Die grundsätzliche Forderung des Bundesverfassungsgerichts, dass Bürger*innen wissen können

[415] Vgl. dazu nur *Britz*, EuGRZ 2009, 1 ff.; *Drackert*, S. 98 ff.; *Marsch*, passim; *Reinhardt*, AöR 142 (2017) 528 ff.

[416] Mit Ansätzen für eine Abgrenzung *Albers*, Informationelle Selbstbestimmung, S. 297; *Gusy*, in: FG Hilger, S. 117 (119 ff.); *Marsch*, S. 14 ff. m.w.N.; *Siemen*, S 133.

[417] Bereits die erste wichtige datenschutzrechtliche Entscheidung befasste sich im Jahr 1987 mit der Speicherung personenbezogener Daten in einem geheimpolizeilichen Register; EGMR (Kammer), Urteil vom 26. März 1987, Leander gegen Schweden, No. 9248/81; vgl. danach besonders EGMR (Große Kammer), Urteil vom 4. Mai 2000, Rotaru gegen Rumänien, No. 28341/95; EGMR (Große Kammer), Urteil vom 4. Dezember 2008, S. u. Marper gegen Vereinigtes Königreich, No. 30562/04 und 30566/04 = NJOZ 2010, 696 ff.; EGMR (4. Sektion), Urteil vom 13. November 2012, M.M. gegen Vereinigtes Königreich, No. 24029/07; EGMR (5. Sektion), Urteil vom 18. April 2013, M.K. gegen Frankreich, No. 19522/09; EGMR (1. Sektion), Urteil vom 24. Januar 2019, Catt gegen Vereinigtes Königreich, No. 43514/15 = NVwZ 2020, 377 ff.; EGMR (1. Sektion), Urteil vom 13. Februar 2020, Gaughran gegen Vereinigtes Königreich, No. 45245/15.

[418] Vgl. *Marsch*, S. 7 ff.

müssten, „wer was wann und bei welcher Gelegenheit über sie weiß“[419], erscheint im Kontext der kriminalbehördlichen Informationsordnung nur schwer umsetzbar, wie etwa *Fall 4* veranschaulicht. Jedenfalls bedürfen die Speicherung und Ordnung ebenso wie andere Schritte der Verarbeitung von personenbezogenen Daten aufgrund der damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht einer einfachgesetzlichen Rechtfertigung. Hierfür existieren Befugnisse im Polizei- und Strafprozessrecht, auf die sogleich eingegangen wird.

b. Befugnisse zur Informationsordnung

Die verfassungsrechtlichen Anforderungen an den Datenschutz finden im Zusammenhang mit der kriminalbehördlichen Informationsordnung vor allem Niederschlag in den Befugnissen zur Speicherung und Strukturierung von Informationen. Im Polizeirecht finden sich derartige Befugnisse auf Landes- wie auf Bundesebene. Die Strafprozessordnung sieht in ihrem achten Buch Befugnisse zur Speicherung und Strukturierung von Daten vor. Die durch das StVÄG 1999 vom 2. August 2000[420] eingeführten §§ 474 ff. StPO dienten ähnlich wie die Regelungen zur Datenverarbeitung in den Polizeigesetzen zur Umsetzung der Vorgaben aus dem Volkszählungsurteil des Bundesverfassungsgerichts.[421] Im Einzelnen sollen die Befugnisse und ihre Voraussetzungen im Zusammenhang mit den Anforderungen an die kriminalbehördliche Informationsordnung betrachtet werden.[422]

Der unionsrechtliche Rahmen für die Befugnisse zur Speicherung und Strukturierung von Daten durch Kriminalbehörden ergibt sich aus der JI-Richtlinie. Sie enthält umfassende Vorgaben für die Verarbeitung von personenbezogenen Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten sowie der

---

[419] BVerfGE 65, 1 (43).

[420] BGBl. I, S. 1253 ff.; vgl. zu der (Vor-)Geschichte der Regelungen Referentenentwurf eines Strafverfahrensänderungsgesetzes 1988, abgedruckt in StV 1989, 172 ff.; BT-Drs. 12/989, S. 45 ff., 60; BT-Drs. 13/194; S. 8, 10 ff.; BT-Drs. 13/9718, S. 22 ff.; BT-Drs. 14/1484, S. 25 ff.; BT-Drs. 14/2595, S. 29 f.; BT-Drs. 14/2886, S. 4 f.; BT-Drs. 14/3525, S. 2 f.; im Überblick *Hilger*, NStZ 2000, 561 (562); *Pollähne*, GA 2006, 807 (809 ff.).

[421] BT-Drs. 14 /1484, S. 1. Zuvor waren ähnliche Regelungen in Nr. 182 ff. RiStBV enthalten gewesen. Die Einführung der §§ 474 ff. StPO war rechtspolitisch hoch umstritten und langwierig; vgl. *Brodersen*, NJW 2000, 2536 f.; *Hassemer*, in: Institut für Kriminalwissenschaften Frankfurt a. M., S. 101 (110 ff.); *Matheis*, S. 106 ff.; *Wolter*, StV 1989, 358 ff. Eine nähere gesetzliche Regelung für die Aufbewahrung von Informationen in Akten im Bereich der (Straf-)Justiz wurde in den 1990er-Jahren verstärkt diskutiert; vgl. BfD, 16. Tätigkeitsbericht 1995-1996, S. 47; 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung vom 9./10. März 1995 zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich; *Hilger*, in: FS Meyer-Goßner, S. 755 ff. Die aufgestellten Forderungen, etwa nach einer gesetzlich fixierten Aufbewahrungsdauer, fanden jedoch in den folgenden Reformen der Strafprozessordnung wenig Berücksichtigung.

[422] Siehe unten Teil 2 A. III. 1.

Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, durch die hierfür zuständigen Behörden (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 JI-Richtlinie). Damit erfasst die Richtlinie unter anderem die polizeiliche Datenverarbeitung zu präventiven und repressiven Zwecken, was unter anderem die Speicherung von Daten in Informationssystemen mit einschließt.[423] Auch die Datenverarbeitung der Staatsanwaltschaften zu Zwecken der Strafverfolgung ist erfasst.

Die im Jahr 2016 verabschiedete Richtlinie war bis zum 6. Mai 2018 im mitgliedstaatlichen Recht umzusetzen (Art. 63 Abs. 1 JI-Richtlinie), was in Deutschland jedoch nicht durchgehend reibungslos gelang.[424] Sie stellt einen großen Schritt zur Europäisierung der Regelungen über die kriminalbehördliche Datenverarbeitung dar, die bisher im Wesentlichen national geprägt waren.[425] Für die Regelungen von Befugnissen für informationsordnende Tätigkeiten sind vor allem die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten aus Art. 4 JI-Richtlinie und die Vorgaben für die Rechtmäßigkeit der Datenverarbeitung aus Art. 8 JI-Richtlinie von Interesse.

Die Grundsätze des Datenschutzrechts haben ihre Wurzel in dem europäischen Datenschutzgrundrecht aus Art. 8 GRCh.[426] Sie sind für den Anwendungsbereich der Richtlinie in deren Art. 4 niedergelegt und wurden im deutschen Recht durch eine beinahe wortlautgleiche Übernahme dieser Vorschrift umgesetzt.[427] Nach Art. 4 Abs. 1 lit. a JI-Richtlinie sehen die Mitgliedstaaten vor, dass personenbezogene Daten im Anwendungsbereich der Richtlinie auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden. Es ist vorzusehen, dass die Daten für festgelegte, eindeutige und rechtmäßige Zwecke verarbeitet werden (Art. 4 Abs. 1 lit. b JI-Richtlinie) und in Bezug auf diese Zwecke nicht übermäßig sind (Art. 4 Abs. 1 lit. c JI-Richtlinie).

Diese Vorgaben konkretisiert wiederum Art. 8 Abs. 1 JI-Richtlinie. Nach dieser Vorschrift sehen die Mitgliedstaaten vor, dass eine Datenverarbeitung nur dann rechtmäßig ist, wenn und soweit diese Verarbeitung für die Erfüllung einer Aufgabe erforderlich ist, die im Rahmen des Anwendungsbereiches der Richtlinie von einer hierfür

---

[423] Nicht von der JI-Richtlinie erfasst erscheint hingegen die sonderordnungsbehördliche Gefahrenabwehr. Der Zusatz „einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" lässt sich so verstehen, dass Datenverarbeitungen zu diesen Zwecken nur dann vom Anwendungsbereich der JI-Richtlinie erfasst sind, wenn ein Bezug zu den zuvor genannten „Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung" besteht; vgl. *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (66 f.); *Hornung/Schindler/J. Schneider*, ZIS 2018, 566 (572).

[424] Siehe zur Umsetzung auf Bundesebene *Aden*, vorgänge 2018, 93 (98 ff.); *Singelnstein*, NStZ 2020, 639 ff. (speziell zur Umsetzung in der StPO) sowie auf Landesebene *Arzt*, SächsVBl. 2019, 345 ff.; *Golla*, KriPoZ 2019, 238 ff.

[425] Vgl. *Albers*, in: Seckelmann, S. 509 (518); *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (64).

[426] Vgl. *Johannes/Weinhold*, § 1 Rn. 123.

[427] Vgl. § 47 BDSG; für das Landesrecht beispielhaft § 37 DSG NRW.

zuständigen Behörde wahrgenommen wird, und die Verarbeitung auf Grundlage des Unionsrechts oder des Rechts der Mitgliedstaaten erfolgt. Hieraus lässt sich allerdings kaum etwas für informationsordnende Befugnisse der Kriminalbehörden ableiten, das in der Ausgestaltung der einschlägigen Regelungen nach dem deutschen Datenschutzverständnis nicht bereits berücksichtigt ist.[428] Dass die Speicherung von Daten für die Erfüllung polizeilicher bzw. staatsanwaltschaftlicher Aufgaben erforderlich sein und hierfür eine Rechtsgrundlage vorhanden sein muss, ist anerkannt, seit das Bundesverfassungsgericht in seinem Volkszählungsurteil grundsätzlich jede staatliche Verarbeitung personenbezogener Daten als Grundrechtseingriff eingestuft hat. Auch die Vorgabe aus Art. 8 Abs. 2 JI-Richtlinie, wonach im Recht der Mitgliedstaaten „zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben" werden sollen, errichtet keine Vorgaben, die über den ohnehin schon bestehenden Standard hinausgehen.

c. Funktionen und Leistungsgrenzen datenschutzrechtlicher Regelungen

Vor dem Hintergrund ihrer Entstehungsgeschichte lassen sich die Befugnisse zur Speicherung und Strukturierung von Daten in den Polizeigesetzen und der Strafprozessordnung als Regelungen des Risiko(verwaltungs)rechts begreifen. Sie dienen dazu, komplexen Risiken der elektronischen Datenverarbeitung für die Persönlichkeit des Einzelnen zu begegnen[429] und sind in erster Linie eine Konsequenz des Volkszählungsurteils des Bundesverfassungsgerichts, durch das die staatliche Verarbeitung personenbezogener Daten einem Regelungsvorbehalt unterstellt wurde.

Zuvor hatte es an umfassenden gesetzlichen Regelungen für den Umgang mit personenbezogenen Daten durch die Kriminalbehörden gefehlt.[430] Datenerhebungen und -verarbeitungen wurden teilweise nicht[431] oder erst ab einer gewissen Intensität[432] als Grundrechtseingriffe eingestuft.[433] Sofern die Datenerhebung und -verarbeitung als

---

[428] Vgl. *Bäcker*, in: Hill/Kugelmann/Martini, S. 63 (69); kritisch hierzu *Wolff*, in: Kugelmann/Rackow, S. 61 (92).

[429] Vgl. *Spiecker gen. Döhmann*, in: Vesting/Korioth, S. 263 (280).

[430] Eine Ausnahme ist das Bremische Polizeigesetz vom 21. März 1983 (BremGBl., S. 141), in dem sich bereits detaillierte Regelungen zu der Verarbeitung personenbezogener Daten fanden; vgl. dazu. *Alberts*, NVwZ 1983, 585 ff.; *Scholz/Pitschas*, S. 162.

[431] So etwa *Kniesel*, Die Polizei 1983, 374 (383) (zur Datenerhebung); *Kube*, in: BKA, Polizeiliche Datenverarbeitung, S. 99 (102 ff.). Sie wurden teils als „Vorbereitungsakte" für andere Maßnahmen, die Grundrechtseingriffe bedeuteten, angesehen.; vgl. *Schwabenbauer*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 4.

[432] So etwa *Ahlf*, Die Polizei 1983, 41 (50 f.) (zur Führung von Kriminalakten); *Rebmann*, NJW 1985, 1 (3).

[433] Vgl. zum Ganzen BVerfGE 110, 33 (56); *Kowalczyk*, S. 43 ff.; *Schwabenbauer*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 4; *Stephan*, VBlBW 2005, 410.

Grundrechtseingriffe gesehen wurden, wurden sie teilweise auf die polizeilichen Generalklauseln gestützt.[434] Diese Möglichkeit wurde mitunter auch nach dem Volkszählungsurteil noch angenommen,[435] bot aber besonders aufgrund der Voraussetzung einer konkreten Gefahr keine praktisch befriedigende Möglichkeit für die verfahrensunabhängige Bevorratung personenbezogener Daten.[436]

Das Volkszählungsurteil führte zu einer Welle der Regelung von Befugnissen zur polizeilichen und sicherheitsbehördlichen Datenverarbeitung, die oft als Phase der „Verrechtlichung"[437] beschrieben wird[438] und erst Ende der 1990er-Jahre ihren Abschluss fand.[439] Sämtliche Polizeigesetze sowie die Strafprozessordnung wurden um Befugnisse zur Datenverarbeitung ergänzt.[440] Dass der Erlass von Regelungen zur Rechtfertigung von Datenverarbeitungen mitunter beträchtliche Zeit in Anspruch nahm, hatte erhebliche praktische Konsequenzen. Zwar ließ sich aus der Rechtsprechung des Bundesverfassungsgerichts[441] herleiten, dass die polizeiliche Datenverarbeitung innerhalb einer gewissen „Schonzeit" auch ohne die Schaffung neuer Rechtsgrundlagen erfolgen durfte, um die Funktionsfähigkeit staatlicher Einrichtungen nicht zu gefährden

[434] VG Darmstadt DVBl. 1979, 743; vgl. hierzu auch *Rudolph*, S. 51 ff.; *Siebrasse*, S. 25.

[435] So etwa VGH Mannheim NJW 1987, 3022; VGH München NJW 1984, 2235 (2237 f.); *Denninger*, CR 1988, 51 (56 f.); *Götz*, NVwZ 1987, 858 (859); *Honnacker*, CR 1986, 287 (289); *Pitschas/Aulehner*, NJW 1989, 2353 (2357); dagegen aber BayVerfGH NJW 1986, 915 (916); VG München BeckRS 1987, 31156431.

[436] Vgl. VG Frankfurt am Main NJW 1987, 2248 (2249); *Ahlf*, KritV 1988, 136 (146); *Denninger*, CR 1988, 51 (57).

[437] Der Begriff der Verrechtlichung lässt sich in Anbetracht der Tatsache kritisieren, dass die nach dem Volkszählungsurteil erlassenen Regelungen zum polizeilichen Aufgabenbereich und der polizeilichen Datenverarbeitung teilweise auch über die Festschreibung bisheriger Praktiken hinausgingen; vgl. *Gusy*, StV 1993, 269 (270 f.); *Kugelmann*, Die Verwaltung 2014, 25 (30); *Poscher*, Die Verwaltung 2008, 345 (347); *Wegener*, VVDStRL 2016, S. 293 (298 f.); anders hingegen *Möstl*, DVBl. 2007, 581 (585). Regelmäßig wurde dieser Begriff auch kritisch im Sinne einer übermäßigen Formalisierung und Bürokratisierung verwendet; vgl. *Pitschas/Aulehner*, NJW 1989, 2353 (2356); vgl. auch allgemein kritisch gegenüber eine „Hyperverrechtlichung" aufgrund einer Ausweitung des Vorbehalts des Gesetzes *Kloepfer*, JZ 1984, 685 (689); ähnlich *Rogall*, S. 8.

[438] Siehe zu dieser Phase in der Entwicklung der kriminalbehördlichen Informationsordnung oben B. III. 2.

[439] Vgl. dazu nur *Götz*, NVwZ 1990, 725 ff.; *Götz*, NVwZ 1998, 679; *Möstl*, DVBl. 2007, 581 (582); Riegel, DVBl. 1987, 325 (326 ff.); *Riegel*, Die Polizei 1991, 1 ff.; *Trute*, in: GS Jeand'Heur, S. 403. Den Reformen der Polizeigesetze diente zu wesentlichen Teilen der VE MPolG als Vorlage. Als Generalklausel für die Datenspeicherung, -veränderung und -nutzung sah § 10a VE MPolG 1986 vor, dass diese zulässig ist, sofern sie zur Erfüllung polizeilicher Aufgaben erforderlich ist.

[440] Forderungen wie von *Götz*, NVwZ 1990, 725 (726), die Informationsverarbeitung außerhalb des eigentlichen polizeilichen Fachrechts zu regeln, setzten sich nicht durch.

[441] Vgl. nur BVerfGE 33, 1 (12 f.); BVerfGE 41, 251 (267); BVerfG NJW 1980, 35 (37).

(„Übergangsbonus“).[442] Allerdings vertraten Mitte bis Ende der 1980er-Jahre mehrere Gerichte die Auffassung, dass bestehende kriminalbehördliche Sammlungen personenbezogener Daten (nach einer verstrichenen Übergangsfrist) zu löschen seien.[443]

Die infolge des Volkszählungsurteils geschaffenen Befugnisse zur Datenverarbeitung haben ihre Gestalt im Wesentlichen bis heute behalten. Teils erfuhren sie schon unmittelbar nach ihrem Erlass heftige Kritik. Sie seien zu unspezifisch und würden im Grunde nur die Aussagen des Volkszählungsurteils wiederholen.[444] Besonders im polizeirechtlichen Diskurs werden die Regelungen, die die Speicherung von und den weiteren Umgang mit Informationen festlegen, bisweilen als Fremdkörper betrachtet. Ihre von der Kategorie der Gefahr abweichenden Voraussetzungen werden als Zeichen einer „Erosion der Gefahrenschwelle“[445] oder Entgrenzung des Polizeirechts gedeutet.[446] Stimmen in der Literatur sehen die polizeirechtliche Dogmatik in ihrer klassischen Form[447] als ungeeignet an, um Erscheinungen der Informations- und Risikogesellschaft Herr zu werden sowie die neuen Regelungen zum Umgang mit Informationen einzuordnen.[448]

Die Annahme einer Entgrenzung polizeilicher oder kriminalbehördlicher Befugnisse aufgrund der neuen Einordnung der informationellen Dimension erscheint als Missverständnis.[449] Sie erweckt den Eindruck, die informatorischen Befugnisse führten zu einer Störung des Systems der Eingriffsbefugnisse insgesamt. Die informatorische

---

[442] Vgl. BayVerfGH NJW 1986, 915 (916); *Götz*, NVwZ 1990, 725 (729); *Kniesel*, in: Bull, S. 105 (115 f.); *Kniesel/Vahle*, DÖV 1987, 953 (954).

[443] VG Frankfurt am Main NJW 1987, 2248 f.; VG Hannover CR 1987, 250 ff.; VG München BeckRS 1987, 31156431; vgl. zum Verfassungsschutzamt Niedersachsen VG Hannover NVwZ 1987, 826 ff.; anders VGH Mannheim NJW 1987, 2762 ff. (zur Aufbewahrung erkennungsdienstlicher Unterlagen); OLG Frankfurt am Main NJW 1989, 47 ff. (für die Zentralen Namenskartei der Staatsanwaltschaft, für das das Gericht zwar das Fehlen einer Rechtsgrundlage bemängelte, aber zu dem Ergebnis kam, dass der „[gesetzlose] Zustand noch für eine gewisse Übergangszeit hinzunehmen“ sei).

[444] *Aulehner*, S. 8.

[445] *Trute*, in: GS Jeand'Heur, S. 403 (407); dem folgend *Middel*, S. 336.

[446] Vgl. *Gärditz*, S. 7; *Götz*, NVwZ 1998, 679; *Wegener*, VVDStRL 2016, S. 293 (297 ff.).

[447] Die klassische, aus dem liberalen Rechtsstaat des späten 19. und frühen 20. Jahrhunderts stammende polizeirechtliche Dogmatik charakterisieren unter anderem die Trennung polizeilicher Aufgaben und Befugnisse, der Gefahrenbegriff als Anknüpfung für polizeiliches Handeln, die Bestimmtheit der polizeilichen Schutzgüter und die Störerverantwortlichkeit. Grundlegend hierfür waren die Kreuzberg-Urteile des Preußischen Oberverwaltungsgerichts vom 10. Juni 1880 (Preuß VwBl. 1879/80, S. 401 ff.) und 14. Juni 1882 (PrOVGE 9, 353 = DVBl. 1985, 219 ff.), die unter anderem die Aufgabe der polizeilichen Gefahrenabwehr von der Aufgabe der Wohlfahrtspflege abgrenzten; vgl. dazu nur *Di Fabio*, S. 30 ff.; *Preu*, S. 326 ff.; *Rusteberg*, in: Brings-Wiesen/Ferreau, S. 191 (193 f.). Dem klassischen Polizeirecht des liberalen Rechtsstaats wird heute regelmäßig ein vom Gedanken des Präventionsstaats geprägtes Konzept des Polizeirechts entgegengesetzt; *Schoch*, Der Staat 43 (2004), 347 (350); zu dem Gedanken des Präventionsstaats grundlegend *Denninger*, KJ 1988, 1 (10 ff.); vgl. auch *Grimm*, NJW 1989, 1305 (1310 f.); *Kötter*, S. 192.

[448] *Park*, S. 4; *Schoch*, Der Staat 43 (2004), 347 (350).

[449] Ähnlich *Möstl*, DVBl. 2007, 581 (585); *Rusteberg*, in: Brings-Wiesen/Ferreau, S. 191 (193).

Tätigkeit wirkt aber nicht derart in andere Bereiche ein, dass die Anlassschwelle in diesen erodieren könnte. Gerade die informationsordnenden Befugnisse können in dem System der Eingriffsbefugnisse eigenständig eingeordnet werden, da informationsordnende Tätigkeiten eine eigenständige Relevanz haben und sich leicht von anderen kriminalbehördlichen Tätigkeiten abgrenzen lassen.[450] Sie finden in einem Bereich statt, der lange überhaupt nicht als regelungsbedürftig angesehen wurde und daher auch nicht mit der hergebrachten polizeirechtlichen Dogmatik einzufangen ist.

Faktisch nahmen Kriminalbehörden schon immer informationsordnende Tätigkeiten vor, die sich nie zutreffend als Teil der klassischen Gefahrenabwehr oder Strafverfolgung ansehen ließen, die gesetzlich geregelt war.[451] Ein Regelungsbedarf entstand erst infolge der technologischen Entwicklung der elektronischen Datenverarbeitung und der Vorgaben aus dem Volkszählungsurteil. In der Folge waren die betreffenden Tätigkeiten rechtlich neu einzuordnen. Mit der damit einhergehenden Erweiterung des Polizei- und Strafprozessrechts waren und sind auch Grundannahmen für diese Gebiete kritisch zu überprüfen. Im Zusammenhang mit den informatorischen Befugnissen der Polizei ist etwa die Annahme, dass die Polizei nur im Gefahrenbereich Befugnisse hat und Befugnisse im Vorfeld von Gefahren den Nachrichtendiensten vorbehalten sind, schon lange nicht mehr haltbar.[452] Jedenfalls im informatorischen Bereich lässt sich die Gefahrenabwehr nicht mehr „als Normalzustand des Polizei- und Ordnungsrechts begreifen“[453].

Insofern sind die datenschutzrechtlichen Elemente im Polizeirecht und Strafprozessrecht weniger Symptome einer Entgrenzung als notwendige Ergänzungen, um informationelle Tätigkeiten in rechtsstaatlichen Bahnen zu halten.[454] Fraglich ist aber, ob die geltenden Befugnisse zur Speicherung und Strukturierung von Daten ihre Rolle als risikorechtliche Korrektive ausfüllen können. Der Schutzgehalt des Datenschutzrechts ist unspezifisch. Es ist nicht darauf ausgelegt, nach der Relevanz und dem Aussagegehalt von personenbezogenen Informationen in verschiedenen Zusammenhängen zu differenzieren. Dass es nach der bekannten Aussage des Bundesverfassungsgerichts „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses‘ Datum

[450] Siehe dazu bereits oben A. I. und II.

[451] Vgl. *Albers*, Determination, S. 27; *Rusteberg*, in: Brings-Wiesen/Ferreau, S. 191 (195).

[452] *Wolff*, DVBl. 2015, 1076 (1080).

[453] *Rusteberg*, in: Brings-Wiesen/Ferreau, S. 191 (193).

[454] So auch *Schwan*, in: Hohmann, S. 276 (285), nach dem die datenschutzrechtlichen Regelungselemente im Polizeirecht als Ansatz zu begreifen sind, um „die polizeiliche Datenverarbeitung in Einklang zu bringen mit dem überkommenen rechtsstaatlichen Polizeirecht, aus dem diese in jüngerer Zeit infolge des allzu zügellosen Einsatzes moderner Informationstechnologien ausgebrochen ist.“

mehr" gibt,[455] weist zutreffend auf die Risiken der Verknüpfung und Auswertung von Informationen hin, bedeutet aber nicht, dass Daten und Informationen in unterschiedlichen Zuständen und Phasen stets gleich behandelt werden sollten. Die vom Bundesverfassungsgericht vorgegebene Prämisse hat zu einer vereinfachten, nicht sonderlich kontextbezogenen Betrachtung des Datenschutzrechts geführt.[456] In der vorherrschenden Betrachtung des Datenschutzrechts genießt die ursprüngliche Beschaffung bzw. Erhebung von Daten mehr Aufmerksamkeit als die logisch nachgeschalteten Phasen der Speicherung und Auswertung.

Dass sich das Datenschutzrecht damit schwertut, spezifische Risiken in den Blick zu nehmen, hängt mit seinem Charakter als Vorfeldrecht sowie seiner instrumentellen Schutzfunktion zusammen. Das Recht auf informationelle Selbstbestimmung ist nach der Rechtsprechung des Bundesverfassungsgerichts als Vorfeldschutz konzipiert. Es „flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit", indem es „ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen" lässt.[457] Eine Gefährdung des Rechtes auf informationelle Selbstbestimmung könne „bereits im Vorfeld konkreter Bedrohungen von Rechtsgütern entstehen."[458] Schon um die Intensität eines Eingriffs durch die Erhebung und Speicherung personenbezogener Daten zu bestimmen, bedarf es daher einer Prognose der Konsequenzen ihrer späteren Verwendung.[459]

Sowohl nach deutschem als auch nach europäischem Verständnis lässt sich das Datenschutzrecht auf einer instrumentellen Schutzebene mit weiteren Rechtspositionen bzw. Gehalten aufladen,[460] um den Risiken der Datenverarbeitung in einem bestimmten Kontext – wie etwa der kriminalbehördlichen Informationsordnung – zu begegnen. Es zielt mit den Worten von *Nikolaus Marsch* „nicht selbstzweckhaft auf den Schutz von Daten ab", sondern dient „dem Schutz einer Vielzahl anderer Rechte und Interessen"[461]. Es lässt sich damit als Grundgerüst zum Schutz der Interessen von Informationssubjekten begreifen,[462] das aber eines spezifischen Ausbaus bedarf.

---

[455] BVerfGE 65, 1 (45).

[456] *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 50 f.

[457] BVefGE 118, 168 (184 f.); BVerfGE 120, 378 (397); ähnlich BVerfGE 120, 274 (311 f.).

[458] BVerfGE 120, 378 (397).

[459] *Spiecker gen. Döhmann*, in: Vesting/Korioth, S. 263 (280).

[460] *Marsch*, S. 109; *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 561 (568, 573 f.); *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, S. 167 (178); *Rouvroy/Poullet*, in: Gutwirth/Poullet/De Hert/de Terwangne/Nouwt, S. 45 (50); vgl. kritisch bzgl. einer Instrumentalität zugunsten anderer Freiheiten *Franzius*, ZJS 2015, 259 (266).

[461] *Marsch*, S. 87.

[462] Vgl. *Masing*, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 467 (491).

Im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung lässt sich eine funktionale Offenheit bereits seit seiner Anerkennung durch das Bundesverfassungsgericht nachvollziehen.[463] Dies ist auch vor dem Hintergrund der Entwicklungsoffenheit des verfassungsrechtlichen allgemeinen Persönlichkeitsrechts konsequent. Das Bundesverfassungsgericht stellte im Volkszählungsurteil fest, dass es „keinen Anlaß zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung" gebe.[464]

Während die Konzeption des Datenschutzrechts als Vorfeldrecht und ausfüllungsbedürftigem Instrument einerseits den Vorteil einer strukturellen Offenheit mit sich bringt, neigt es andererseits dazu, einfachgesetzlich leicht aufgeweicht zu werden. Dies zeigt sich konkret bei der Anwendung der Befugnisse zur Informationsordnung in den Polizeigesetzen und der Strafprozessordnung. Diese setzen tatbestandlich im Wesentlichen voraus, dass eine Datenverarbeitung für die Erfüllung polizeilicher Aufgaben oder die Zwecke des Strafverfahrens erforderlich ist. Hieraus werden nur geringe Anforderungen für die Speicherung und Weiterverwendungen von Daten abgeleitet. Es wird als ausreichend angesehen, dass Informationen eine potentielle Relevanz für eine spätere polizeiliche Tätigkeit haben. Angesichts moderner Hilfsmittel zur Auswertung fällt es dabei immer leichter, die Relevanz auch scheinbar belangloser Informationen zu begründen.

Zwar ließen sich aus den Kriterien der Erforderlichkeit und Verhältnismäßigkeit in den Befugnissen zur Informationsordnung theoretisch auch strengere Voraussetzungen für die Speicherung und Weiterverarbeitung von personenbezogenen Daten ableiten. Dafür dürfte es sich aber empfehlen, namentlich den Maßstab der Verhältnismäßigkeit durch weitere Rechtspositionen aufzuladen.

2. Weitere individualschützende Rechtspositionen

Gerade angesichts der begrenzten Möglichkeiten, spezifische Risiken, die aus der Speicherung und Strukturierung von Daten folgen können, allein mit dem Instrumentarium des Datenschutzrechts zu handhaben, sollen im Folgenden auch andere Rechtspositionen in den Blick genommen werden, die im Zusammenhang mit der kriminalbehördlichen Informationsordnung relevant für den Schutz von Individuen sind. Konkret werden die Vorgaben des Diskriminierungsschutzes (a.) und der Unschuldsvermutung (b.) behandelt.

---

[463] Vgl. *Scholz/Pitschas*, S. 71 f.
[464] BVerfGE 65, 1 (44 f.).

a. Diskriminierungsschutz

Art. 3 Abs. 3 GG und Art. 21 Abs.1 GRCh regeln auf verfassungsrechtlicher Ebene Diskriminierungsverbote, die für informationsordnende Tätigkeiten der Kriminalbehörden relevant werden können. Demnach sind Diskriminierungen – also negative Behandlungen anhand sozialer Kategorien[465] – unter anderem aufgrund des Geschlechtes, der „Rasse", der Herkunft, der Sprache, der religiösen und politischen Anschauungen sowie der Behinderung einer Person grundsätzlich unzulässig.

Der verfassungsrechtliche Diskriminierungsschutz weist Schnittmengen mit dem Datenschutz auf. Beide Gebiete dienen der „Absicherung der Offenheit des Vorgangs der Wahrnehmung von Persönlichkeit"[466]. Während dem Datenschutz unter anderem der Gedanke zugrunde liegt, den Einzelnen vor der Erstellung von umfassenden Persönlichkeitsprofilen zu schützen, soll das Antidiskriminierungsrecht davor schützen, dass die Wahrnehmung einer Person von einem stereotypen Persönlichkeitsbild bestimmt wird.[467] Teilweise zielen datenschutzrechtliche Regelungen direkt auf einen Schutz vor Diskriminierung im Rahmen von Datenverarbeitungen.[468] Dies gilt etwa für den Schutz besonderer Kategorien personenbezogener Daten, der u.a. in Art. 10 JI-Richtlinie geregelt ist und ähnliche Merkmale erfasst wie die verfassungsrechtlichen Diskriminierungsverbote. Die Befugnisse zur Verarbeitung personenbezogener Daten bieten im Rahmen von Interessenabwägungen Raum, Wertungen des Diskriminierungsschutzes zu berücksichtigen. Auch die verfassungsrechtlichen Gewährleistungen des Datenschutzes ermöglichen es, derartigen Gesichtspunkten Rechnung zu tragen. So prüfte etwa der Europäische Gerichtshof für Menschenrechte in seinem Marper-Urteil Beeinträchtigungen des Diskriminierungsverbots aus Art. 14 EMRK im Zusammenhang mit der sicherheitsbehördlichen Datenbevorratung nicht gesondert, sondern im Rahmen des Rechtes auf die Achtung des Privatlebens aus Art. 8 EMRK.[469]

Aus Art. 3 Abs. 3 GG, der eine Benachteiligung wegen der genannten Merkmale verbietet, lässt sich für das Verwaltungshandeln ein grundsätzliches Verbot folgern, an

---

[465] Vgl. zum Begriff der Diskriminierung *Drackert*, S. 30; *Scherr*, in: Scherr/El-Mafaalani/Yüksel, S. 39 (46 ff.) m.w.N.

[466] *Britz*, S. 52. In diesem Sinne fand die Gefahr sozialer Etikettierung bereits im Volkszählungsurteil des Bundesverfassungsgerichts Anklang; BVerfGE 65, 1 (49).

[467] *Britz*, S. 57; *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 561 (572 f.).

[468] *Marsch*, S. 94; *Tzanou*, IDPL 2013, 88 (91 f.); vgl. aber auch zu Konflikten zwischen datenschutzrechtlichen Regelungen und Diskriminierungsschutz im Zusammenhang mit der Generierung diskriminierungsrelevanten Wissens *Tischbirek*, in: Münkler, S. 67 (84 f.).

[469] EGMR (Große Kammer), Urteil vom 4. Dezember 2008, S. u. Marper gegen Vereinigtes Königreich, No. 30562/04 und 30566/04 § 127 ff. = NJOZ 2010, 696 (703).

diese Merkmale anzuknüpfen.[470] Hierfür bedarf es einer Rechtfertigung, die sich aus kollidierendem Verfassungsrecht oder besonders schwerwiegenden Gründen ergeben kann.[471] Ein grundsätzlich verbotenes Anknüpfen soll dann vorliegen, wenn im Hinblick auf ein bestimmtes Ergebnis bzw. als Voraussetzung für eine Rechtsfolge auf eines der Merkmale abgestellt wird.[472] Eindeutig geklärt ist die Reichweite des Anknüpfungsverbotes aus Art. 3 Abs. 3 GG allerdings nicht. Bezogen auf informationsordnende Tätigkeiten der Kriminalbehörden stellt sich die Frage, ob bereits ein Speichern oder Strukturieren von Daten eine unzulässige Anknüpfung darstellen kann. Diese soll im Zusammenhang mit den Voraussetzungen für informationsordnende Tätigkeiten näher untersucht werden.[473]

Die Anforderungen des Diskriminierungsschutzes lassen sich nicht nur auf den Umgang mit Daten anwenden, die unmittelbar in Art. 3 Abs. 3 Satz 1 genannte Informationen enthalten, sondern auch auf den tendenziell häufigeren Fall einer verdeckten bzw. mittelbaren Diskriminierung. Hierbei wird nicht direkt an ein in Art. 3 Abs. 3 Satz 1 GG genanntes Merkmal angeknüpft, im Ergebnis aber die gleiche Wirkung erzielt.[474] So können in kriminalbehördlichen Informationsressourcen scheinbar unverfängliche Informationen eindeutig auf Merkmale schließen lassen, die verfassungsrechtlich besonders geschützt sind. Wenn die Polizei beispielsweise die Merkmale „Land- und Stadtstreicher" und „wechselt häufig Aufenthaltsort" in Informationssystemen verwendet und diese Angaben sich auf ganz unterschiedliche Personen beziehen

[470] *Fehling*, in: FS Würtenberger, S. 669 (684); *Kischel*, in: BeckOK-GG, 55. Ed. 2023, Art. 3 Rn. 212; *Schwabenbauer,* in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 375; siehe zu der umstrittenen Frage, ob es sich um ein Begründungs- oder Anknüpfungsverbot handelt nur *Boysen*, in: von Münch/Kunig, GG, 7. Aufl. 2021, Art. 3 Rn. 125 ff.; *Baer/Markard*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 3 Rn. 426 jeweils m.w.N. Die Rechtsprechung des Bundesverfassungsgerichts weist in die Richtung eines Anknüpfungsverbotes; BVerfGE 85, 191 (206); BVerfGE 97, 35 (43); BVerfGE 114, 357 (364).

[471] *Kischel*, in: BeckOK-GG, 55. Ed. 2023, Art. 3 Rn. 214.

[472] *Boysen*, in: von Münch/Kunig, GG, 7. Aufl. 2021, Art. 3 Rn. 126; *Kischel*, in: BeckOK-GG, 55. Ed. 2023, Art. 3 Rn. 212a.

[473] Siehe unten Teil 1 A. III. 1. b. aa).

[474] Vgl. zu der Unterscheidung der Kategorien von Diskriminierung *Tischbirek*, in: Münkler, S. 67 (69 f.); zum Ursprung der Figur der mittelbaren Diskriminierung im US-amerikanischen Recht *Koch/Nguyen*, EuR 2010, 364 (365 f.).

können, aber praktisch fast nur im Zusammenhang mit Sinti und Roma genutzt werden,[475] liegt hierdurch faktisch eine grundsätzlich unzulässige Anknüpfung an die ethnische Herkunft vor.[476] In derartigen Fällen können bei der Anwendung des allgemeinen Gleichheitssatzes (Art. 3 Abs. 1 GG) die strengeren Anforderungen aus Art. 3 Abs. 3 GG angewandt werden.[477] Ein anderes Ergebnis würde die Wertungen der Diskriminierungsverbote unterlaufen. Verbotene Diskriminierungswirkungen ließen sich dann verdeckt erreichen.[478]

Eine derartige mittelbare Diskriminierung kann auch dann vorliegen, wenn Informationen in Datenbanken in Verknüpfung miteinander auf Merkmale aus Art. 3 Abs. 3 GG schließen lassen – so etwa, wenn der Wohnort einer Person kombiniert mit weiteren persönlichen Merkmalen einen klaren Rückschluss auf ihre ethnische Herkunft zulässt. Auch in diesem Fall lassen sich erhöhte Anforderungen an die Rechtfertigung für eine Verarbeitung der Daten begründen. Derartige, auf Korrelationen basierende Diskriminierungen kommen jedoch auf komplexe Art zustande und sind schwer aufzudecken.[479] Der Diskriminierungsschutz erscheint hier außerdem noch nicht bei der Speicherung der Daten, sondern erst bei ihrer Verknüpfung relevant.

Insgesamt sind mögliche Verbesserungen des rechtlichen Diskriminierungsschutzes im Angesicht neuer digitaler Technologien aktuell Gegenstand einer breiten juristischen Diskussion. Vor allem im Zusammenhang mit dem Einsatz lernfähiger Systeme wird den verfassungsrechtlichen Diskriminierungsverboten aus Art. 21 Abs.1 GRCh und Art. 3 Abs. 3 GG eine erhöhte Bedeutung beigemessen und ein Bedarf zur Schärfung ihrer Dogmatik festgestellt.[480] Der Einsatz derartiger Systeme ist auch für die kriminalbehördliche Informationsordnung relevant. Eine Überlegung ist es, den rechtlichen Schutz perspektivisch eher auf die technischen Strukturen zu beziehen, durch die eine Diskriminierung zustande kommt als auf einzelne Akte der Diskriminierung. Aus einer staatlichen Pflicht zum Schutz vor Diskriminierung könnten sich strukturelle Gebote für die Gestaltung technischer Systemen ableiten lassen.[481] Dieser Gedanke ist nachvollziehbar, da technische Arrangements diskriminierende Effekte verfestigen

[475] Vgl. zu dieser Praxis *Schröder*, in: Grundrechte-Report 2015, S. 38 (39); zur Verwendung der genannten Merkmale in den Informationssystemen der Polizei Baden-Württemberg LT-Drs. BW 15/5841, S. 3.

[476] *Tischbirek/Wihl*, JZ 2013, 219

[477] *Tischbirek/Wihl*, JZ 2013, 219 (222); vgl. auch *Fehling*, in: FS Würtenberger, S. 669 (682 f.).

[478] *Fehling*, in: FS Würtenberger, S. 669 (675); *Koch/Nguyen*, EuR 2010, 364 (365, 374).

[479] *Tischbirek*, in: Münkler, S. 67 (79).

[480] *Wischmeyer*, AöR 143 (2018), 1 (27); vgl. auch *Hacker*, CMLR 2018, 1143 ff.; *Kischel*, in: BeckOK-GG, 55. Ed. 2023, Art. 3 Rn. 218a ff.; *Tischbirek*, in: Münkler, S. 67 (77 ff.).

[481] Vgl. *Wischmeyer*, AöR 143 (2018), 1 (28 ff.).

können.[482] Im Rahmen der kriminalbehördlichen Informationsordnung erschiene es beispielsweise im Sinne des Diskriminierungsschutzes plausibel, problematische Merkmale schon auf der Ebene der Einrichtung von Systemen von der Speicherung und Verarbeitung auszuschließen.[483]

b. Unschuldsvermutung

Ebenfalls von Relevanz für informationsordnende Tätigkeiten ist die unter anderem[484] nach Art. 6 Abs. 2 EMRK gewährleistete rechtsstaatliche Unschuldsvermutung. Die Unschuldsvermutung als Element eines fairen Verfahrens[485] schützt nicht nur vor Schuldspruch und Strafe, sondern auch vor Nachteilen, die diesen „gleichkommen, denen aber kein rechtsstaatliches prozessordnungsgemäßes Verfahren zur Schuldfeststellung vorausgegangen ist“[486]. Die Unschuldsvermutung steht in einer gewissen Nähe zum Diskriminierungsschutz, da sie verhindern will, dass „strafgleiche oder strafähnliche Diskriminierungswirkungen den mangels gesetzlichen Nachweises der Schuld als unschuldig geltenden Bürger treffen.“[487]

Es fragt sich, ob auch durch die Speicherung von Daten in Informationssystemen auf Grundlage des Strafverfahrensrechts[488] Nachteile entstehen können, die Schuldspruch oder Strafe gleichkommen. Dies könnte etwa dann der Fall sein, wenn Personen durch die Speicherung Attribute zugewiesen werden, die geeignet sind, den unzutreffenden Eindruck zu erwecken, dass die betreffenden Personen Straftäter seien.

---

[482] Vgl. *Dolata/Werle*, in: Dolata/Werle, S. 15 (18 f.), der dies am Beispiel der von *Winner*, Daedalus 109 (1/1980), 121 (123 f.) verbreiteten Geschichte eines New Yorker Stadtbaumeisters erläutert, der niedrige Brücken über den Straßen nach Long Island errichten ließ, um weniger wohlhabende Personen, die den Busverehr nutzten, vom Strand fernzuhalten; vgl. zu der interpretativen Flexibilität dieser Geschichte *Joerges,* Leviathan 27 (1999), 43 ff.

[483] Vgl. *Von Lewinski*, in: Seckelmann, S. 107 (119 f.).

[484] Vgl. zur Verortung der Unschuldsvermutung im Rechtsstaatsprinzip des Grundgesetzes BVerfGE 74, 358 (370); *Kühl*, S. 10 f.; *Stuckenberg*, S. 50 f.

[485] EGMR (4. Sektion), Urteil vom 5. Juli 2001, S. u. Phillips gegen Vereinigtes Königreich, No. 41087/98 § 40; *Harrendorf/König/Voigt*, in: Meyer-Ladewig/Nettesheim/von Raumer, EMRK, 5. Aufl. 2023, Art. 6 Rn. 194.

[486] BVerfG NJW 2002, 3231; ähnlich *Kestel*, StV 1997, 266 (268).

[487] *Kühl*, S. 19 f.

[488] Vgl. zum sachlichen Anwendungsbereich der Unschuldsvermutung auch über das Straf(verfahrens)recht hinaus *Stuckenberg*, S. 63 ff.; speziell zur Geltung im Zusammenhang mit komplexen Datenauswertungen zu Zwecken der Gefahrenabwehr *Kipker*, S. 42 ff.

Unter welchen Umständen eine Eintragung in einer kriminalbehördlichen Informationsressource einen so gravierenden Nachteil begründet, dass sie einem Schuldspruch gleichkommt, ist schwer zu beurteilen.[489] Die Zuweisung von Attributen in der kriminalbehördlichen Informationsordnung entfaltet jedenfalls keine physischen oder materiellen Auswirkungen, die mit jenen einer strafgerichtlichen Verurteilung vergleichbar wären. Als Vergleichsmaßstab mit der Strafe kann aber auch auf die sozialethische Deklassierungswirkung einer Handlung abgestellt werden.[490] In diesem Sinne wird das mit ihr verbundene soziale Unwerturteil als spezifisches Charakteristikum der Strafe angesehen.[491] Freilich ist auch die sozialethische Desklassierungswirkung einer Handlung schwer messbar. Die belastenden Wirkungen einer Strafe sind komplex. Im Vordergrund stehen hierbei in der Regel berufliche Beeinträchtigungen, psychische Belastungen und Rufschädigungen.[492]

Unter diesen Gesichtspunkten erscheint es nur in Ausnahmefällen denkbar, dass eine Eintragung in einem kriminalbehördlichen Informationssystem in ihrer sozialethischen Deklassierungswirkung einmal mit einer Strafe vergleichbar ist. Eine Eintragung in einem polizeilichen Informationssystem kann sich in einzelnen Fällen auf die Ausübung oder Ergreifung eines Berufes auswirken. Dies zeigt *Fall 4,* in dem eine für die Einstellung notwendige Sicherheitsüberprüfung aufgrund einer Eintragung in einer polizeilichen Datenbank scheitert. Psychische Belastungen und Rufschädigungen, die mit jenen, die aus Strafen folgen können, vergleichbar sind, sind bei derartigen Eintragungen aber kaum denkbar. Hier spricht schon der Umstand, dass die Inhalte kriminalbehördlicher Informationsressourcen nicht publik gemacht werden, stark gegen eine Vergleichbarkeit mit Strafen.[493] Allerdings können durch die Nutzung der Informationsressourcen zumindest im Einzelfall nachteilige Effekte entstehen, die dazu führen, dass das Informationssubjekt wie ein verurteilter Straftäter behandelt wird. So kann beispielsweise eine gewichtige Stigmatisierungswirkung entstehen, wenn eine Person auf Grundlage einer Eintragung regelmäßig als potentieller Gefährder oder Intensivtäter angesprochen wird. In derartigen Fällen könnte die Unschuldsvermutung zumindest wertungsmäßig Berücksichtigung finden, wenn es gilt, die Zulässigkeit der Speicherung von Daten zu beurteilen.

---

[489] Vgl. *Stuckenberg*, in: FG Hilger, S. 25 (44 f.) sowie generell zu der Schwierigkeit, die Strafähnlichkeit zu definieren *Stuckenberg*, ZStW 111 (1999), 422 (431 f.) m.w.N.

[490] So *Kühl*, S. 14 ff.

[491] Vgl. nur BVerfGE 96, 245 (249); *Frisch*, NStZ 2016, 16 (19 f.); *Putzke*, in: MüKo-StPO, 2019, § 3 Rn. 2.

[492] Vgl. *Heger*, in: Lackner/Kühl/Heger, StGB, 30. Aufl. 2023, § 46 Rn. 36a; *von Heintschel-Heinegg*, in: BeckOK-StGB, 57. Ed. 2023, § 46 Rn. 5.

[493] Vgl. *Rachor*, S. 93 f. Anders ist die Situation etwa in den USA zu beteiligen, wo besonders Strafakten wesentlich leichter der Öffentlichkeit zugänglich sind als in Deutschland; vgl. *Lageson*, S. 6 ff.

Die Speicherung von Informationen in der kriminalbehördlichen Informationsordnung unterscheidet sich auch von anderen polizeilichen und staatsanwaltschaftlichen Handlungen in Ermittlungsverfahren, die teilweise zwangsläufig mit einer Stigmatisierung des Betroffenen verbunden, aber für die Durchführung des Verfahrens notwendig sind.[494] Die vorsorgliche Speicherung von Informationen hat ein weniger konkretes Ziel vor Augen als die Klärung eines Verdachts oder die Abwehr einer Gefahr. Eine gewichtige Stigmatisierung lässt sich hier schwieriger rechtfertigen.

In der Rechtsprechung wird das Risiko einer Stigmatisierung von Informationssubjekten durch die Speicherung und Bevorratung von Daten in kriminalbehördlichen Datenbanken im Zusammenhang mit der Unschuldsvermutung teilweise bereits berücksichtigt. Am deutlichsten geschieht dies durch den Europäischen Gerichtshof für Menschenrechte, während das Bundesverfassungsgericht[495] und der Europäische Gerichtshof[496] im Zusammenhang mit den Risiken staatlicher Datensammlungen eher auf die mit diesen verbundenen Einschüchterungseffekte abstellen, ohne diese je genauer zu erklären. In der Rechtssache Marper betonte der Europäische Gerichtshof für Menschenrechte das Risiko der Stigmatisierung und führte aus, dass die Speicherung von Daten nach einem Freispruch zwar nicht gleichbedeutend mit einem Verdacht hinsichtlich der Unschuld der Informationssubjekte sei, gleichwohl aber „ihre eigene Wahrnehmung, sie würden nicht als unschuldig behandelt, dadurch verstärkt, dass ihre Daten wie bei verurteilten Straftätern auf unbegrenzte Zeit gespeichert werden, während die solcher Personen, die nie einer Straftat verdächtig waren, vernichtet werden müssen."[497]

Der Europäischen Gerichtshof für Menschenrechte argumentierte dazu in der Rechtssache Khelili dafür, den aus Art. 8 EMRK folgenden Schutz personenbezogener Daten im Zusammenhang mit polizeilichen Datenbanken durch die Unschuldsvermutung aufzuladen.[498] In dem Fall war eine Frau über 18 Jahre lang in einer polizeilichen Datenbank als Prostituierte geführt worden, weil bei ihr verdächtige Visitenkarten aufgefunden worden waren. Verurteilt worden war Frau Khelili nie. Die Attribution in der Datenbank aber legte ein strafbares Verhalten nahe. Dies sah das Gericht „insbeson-

[494] Vgl. *Amelung*, NJW 1979, 1687 (1688 f.); *Kühl*, S. 25; *Kühne*, NJW 1979, 617.

[495] BVerfGE 120, 378 (430); BVerfGE 65, 1 (43); BVerfGE 100, 313 (381).

[496] EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights, Rn. 37.

[497] EGMR (Große Kammer), Urteil vom 4. Dezember 2008, S. u. Marper gegen Vereinigtes Königreich, No. 30562/04 und 30566/04 § 122 = NJOZ 2010, 696 (702).

[498] EGMR (2. Sektion), Urteil vom 18. Oktober 2011, Khelili gegen Schweiz, No. 16188/07; vgl. zu Überschneidungen von Art. 6 II und Art. 8 EMRK auch EGMR (Große Kammer), Urteil vom 12. Juli 2013, Allen gegen Vereinigtes Königreich, No. 25424/09 § 92 = NJOZ 2014, 1834 (1836) m.w.N.

dere im Hinblick auf das überragende Prinzip der Unschuldsvermutung“ als Verletzung von Art. 8 EMRK an.[499] Auch wenn die Attribution in der Datenbank nicht einem Schuldspruch oder einer Strafe gleichkam, sah sich das Gericht veranlasst, auf die Unschuldsvermutung zu verweisen.

Es überzeugt, Art. 6 Abs. 2 EMRK zumindest wertungsmäßig zu berücksichtigen, wenn die Speicherung in kriminalbehördlichen Informationsressourcen geneigt ist, schwerwiegende Stigmatisierungswirkungen zu entfalten. Dies wird aber nur in wenigen Fällen gegeben sein. Die Unschuldsvermutung kann das Schutzbedürfnis der Betroffenen dann besser abbilden, als dies (allein) durch die Regelungen des Datenschutzes möglich ist.[500] Ihr Schutzgehalt ist vor dem Hintergrund der dynamischen technologischen Entwicklung zu verstehen, aufgrund derer Zuschreibungen von Schuld oder Fehlverhalten unter Umständen automatisiert möglich werden können.[501] Die Wertung aus der Unschuldsvermutung lässt sich konkret bei der Prüfung einer Verletzung des Rechts auf informationelle Selbstbestimmung berücksichtigen. Die Speicherung von Informationen über einen freigesprochenen Angeklagten kann schon für Zwecke der weiteren Strafverfolgung ungeeignet oder jedenfalls nicht erforderlich und damit unverhältnismäßig sein.

Zwischenergebnis

Die informationsordnenden Handlungen der Kriminalbehörden – also das Errichten und Ausgestalten von Informationssystemen sowie das Speichern und Strukturieren von Daten darin – sind von hoher Relevanz für die Strafverfolgung und ihre Vorbereitung. Ganz trennscharf voneinander abgrenzen lassen sich Tätigkeiten zu Zwecken von Strafverfolgung und Gefahrenabwehr im Rahmen der kriminalbehördlichen Informationsordnung allerdings nicht. Sowohl die Gestaltung der Systeme als auch die Speicherung von Daten darin können vielfältigen Zwecken dienen, die in der Praxis nicht unbedingt von vornherein eindeutig festgelegt werden. Dieser Umstand steht im Konflikt mit der Kompetenzordnung des Grundgesetzes, die prinzipiell getrennte Regelungen über kriminalbehördliche Tätigkeiten im präventiven und repressiven Bereich verlangt.

---

[499] EGMR (2. Sektion), Urteil vom 18. Oktober 2011, Khelili gegen Schweiz, No. 16188/07 § 68.

[500] Vgl. mit einem ähnlichen Schluss bezogen auf das allgemeine Persönlichkeitsrecht *Kühl*, S. 20. BfDI, 26. Tätigkeitsbericht 2015-2016, S. 109 sieht es hingegen sogar als „Kernanliegen“ des Datenschutzes, die Unschuldsvermutung zur Geltung zu bringen.

[501] Vgl. dazu *Hu*, Florida Law Review 67 (2016), 1735 ff.; *Lageson*, S. 65.

Wie Daten gespeichert und geordnet werden, beeinflusst ihre folgende Verwendung in konkreten Verfahren. Die Verarbeitungsschritte der Informationsordnung stehen in einem notwendigen Zusammenhang mit der vorgelagerten erstmaligen Gewinnung und der nachgelagerten späteren Auswertung von Daten. Sie sind daher auch mit Blick auf diese Tätigkeiten zu bewerten. Die hohe tatsächliche Relevanz von informationsordnenden Handlungen gebietet es aber auch, sie eigenständig zu würdigen.

Die Systeme, in denen sich informationsordnende Tätigkeiten abspielen, sind wichtige Säulen der nationalen und europäischen Sicherheitsarchitektur. Seit der Einführung der ersten EDV-gestützten kriminalbehördlichen Informationsressourcen in den 1970er-Jahren hat ihre Bedeutung kontinuierlich zugenommen. Die Verwendung der Informationssysteme hat stark vorsorgenden Charakter. Am Beispiel der kriminalbehördlichen Informationsordnung lässt sich auch exemplarisch nachvollziehen, dass technische Entwicklungen – wie hier die Einführung und Weiterentwicklung der elektronischen Datenverarbeitung – eine Tendenz zum vorsorgenden Handeln verstärken können.

Dominant sind innerhalb der kriminalbehördlichen Informationsordnung bereits seit ihren Anfangszeiten polizeiliche Informationsressourcen wie INPOL, während die Systeme der Staatsanwaltschaften nur eine Nebenrolle spielen. Dies gilt auch für die Speicherung von Daten zu Zwecken der Strafverfolgung und ihrer Vorbereitung. Die wichtigste Institution im Zusammenhang mit dem Betrieb der Informationssysteme ist das Bundeskriminalamt, das als Zentralstelle für den elektronischen Datenverbund der deutschen Polizeien fungiert. Dennoch werden die meisten einzelnen Informationssysteme von Polizeibehörden der Länder betrieben. Insgesamt stellt sich die polizeiliche Informationsordnung als ein organisch gewachsenes Gefüge von Systemen dar, die nur sehr eingeschränkt miteinander kompatibel sind.

Die getrennte Entwicklung der jeweiligen polizeilichen Informationssysteme ist dabei nicht etwa datenschutzrechtlichen Gründen geschuldet, sondern primär den Machtinteressen der jeweiligen Stellen. An diesen Interessen scheiterten frühe Bemühungen einer stärkeren Zentralisierung der Informationsordnung. Auch der Anfang der 2000er-Jahre unternommene Versuch, die Informationssysteme der Polizeien durch das Projekt INPOL-neu in einem zentralen „Datenpool“ miteinander zu verknüpfen, war nicht von Erfolg gekrönt. Das aktuell laufende Projekt zum Aufbau eines neuen „Datenhauses“ der deutschen Polizei im Rahmen des Programmes Polizei 20/20 greift die für INPOL-neu formulierten Ziele wieder auf. Seine Erfolgsaussichten sind allerdings zweifelhaft. Die rechtlichen Grundlagen für die neue Informationsordnung erscheinen unklar. Dazu werfen die administrative und technische Dimension der Umsetzung Fragen auf.

Bemühungen zur Herstellung einer besseren Interoperabilität und Vernetzung von Informationssystemen lassen sich auch auf europäischer Ebene nachvollziehen. Mit dem neuen „Datenhaus“ der deutschen Polizei konzeptionell eng verwandt ist die neue Informationsordnung von Europol in Form eines „Datensees“ („Data Lake“). Diese wendet sich ebenfalls von der Strukturierung des polizeilichen Informationswesens in Dateien ab und soll eine bessere Verknüpfbarkeit von Informationen ermöglichen.

Die im Vergleich zur Polizei weniger weit entwickelte Informationsordnung der Staatsanwaltschaften harrt indes einer Modernisierung. Die Unterlegenheit der staatsanwaltschaftlichen Informationsordnung beruht nicht nur auf der Nähe der Polizei zu den relevanten Daten in der Phase ihrer Erhebung, sondern auch auf dem früheren und intensiveren technischen Engagement der Polizeien. Aufgrund der überlegenen Informationsressourcen der Polizei besteht ein Konflikt zwischen polizeilicher und staatsanwaltschaftlicher Informationsordnung, der auch das Verhältnis der beiden Institutionen insgesamt berührt.

Im Verhältnis zu ihrer tatsächlichen Bedeutung sind die rechtlichen Anforderungen an die informationsordnenden Tätigkeiten der Kriminalbehörden nicht sonderlich ausgeprägt. Welche Funktionen die einschlägigen Informationssysteme zu erfüllen haben, ist kaum geregelt. Im Wesentlichen stecken die Befugnisse zur Verarbeitung von personenbezogenen Daten, die infolge des Volkszählungsurteils des Bundesverfassungsgerichts geregelt wurden, den rechtlichen Rahmen für informationsordnende Tätigkeiten ab. Die JI-Richtlinie der Europäischen Union hat für die informationsordnenden Befugnisse insofern nicht zu beachtenswerten neuen Anforderungen geführt. Die Befugnisse in den Polizeigesetzen und der Strafprozessordnung machen die Rechtmäßigkeit der Speicherung von Daten im Kern davon abhängig, ob diese für die Erfüllung der Aufgaben der Behörden erforderlich ist. Die zu erfüllende Aufgabe wird dabei regelmäßig die Vorbereitung auf künftige Verfahren sein.

Die Befugnisse zur Datenverarbeitung einschließlich der Speicherung und Strukturierung lassen sich als risikorechtliche Korrektive betrachten, um informationelle Tätigkeiten der Kriminalbehörden in rechtsstaatlichen Bahnen zu halten. Sie lassen sich nur eingeschränkt mit herkömmlichen kriminalbehördlichen Befugnissen vergleichen. Aufgrund des eher unspezifischen Schutzgehaltes des Datenschutzrechts bzw. des Rechts auf informationelle Selbstbestimmung ist nicht immer ganz klar, wovor die informationsordnenden Befugnisse die von der Datenverarbeitung betroffenen Personen schützen sollen. Da Daten nicht selbstzweckhaft geschützt werden, ließe sich der datenschutzrechtliche Schutz allerdings mit anderen Gehalten aufladen, die die Schutzbedürfnisse im Kontext der kriminalbehördlichen Informationsordnung spezifischer erfassen – so etwa Wertungen des Diskriminierungsschutzes und der Unschuldsvermutung.

Teil 2

Anforderungen an die kriminalbehördliche Informationsordnung

Dieser Teil der Untersuchung befasst sich mit den Anforderungen, die die Anwender*innen der kriminalbehördlichen Informationsordnung an ihre Ausgestaltung und ihre Funktionen stellen. Er verfolgt primär das Ziel, die Soll-Zustände der Informationsordnung aus kriminalbehördlich-operativer Sicht festzustellen. Diese werden mit den geltenden rechtlichen Vorgaben unter Berücksichtigung der Interessen der Personen, über die Daten in kriminalbehördlichen Systemen gespeichert werden, zu einem integrierten Soll-Zustand zusammengeführt. Der im ersten Teil der Arbeit festgestellte Ist-Zustand wird mit dem integrierten Soll-Zustand abgeglichen. Im weiteren Verlauf der Arbeit werden auf Grundlage dieses Abgleichs Möglichkeiten untersucht, Ist und Soll durch rechtliche Regelungen einander anzunähern.

Aus der Betrachtung der Praxis haben sich vor allem drei Anforderungen an kriminalbehördliche Informationssysteme als wesentlich herausgestellt: Die schnelle und einfache Verfügbarkeit von Informationen (A.), die Verknüpfbarkeit von Informationsbeständen (B.) sowie die Aktualität und Richtigkeit von Daten (C.).[1]

Im Zusammenhang mit den einzelnen Anforderungen wird erstens untersucht, welche spezifischen Erwartungen Anwender*innen aus Kriminalbehörden an die Funktionen ihrer Informationssysteme haben. Diese Erwartungen sind unter anderem aus behördlichen Dokumenten, Leitfäden und politischen Papieren nachzuvollziehen.[2] Zudem greift die Untersuchung auf drei leitfadenorientierte Interviews zurück, in denen Mitarbeiter*innen unterschiedlicher Polizeibehörden ihre aktuelle Bedarfe und Herausforderungen bei ihrer Arbeit mit Informationssystemen schilderten.[3]

Zweitens wird untersucht, welche Implikationen die von den Anwender*innen erwünschten Funktionen der Systeme für die Personen haben, über die Daten gespeichert sind bzw. werden. Hierbei stehen die Risiken im Vordergrund, die sich aufgrund des

---

[1] Ähnlich *Gusy/Eichenhofer*, S. 104, die die „Vollständigkeit, Verfügbarkeit und Aktualität der Daten" als wesentliche Anforderungen nennen. Während sich Vollständigkeit und Aktualität als Aspekte der Datenqualität einordnen lassen, berücksichtigt diese Zusammenfassung nicht die gerade aktuell hohe Bedeutung der Verknüpfbarkeit von Daten.

[2] Vgl. *Grutzpalk*, in: Grutzpalk, S. 8 (9).

[3] Codes POL1-POL3.

technischen Wandels der Informationssysteme ergeben. Auch hier greift die Untersuchung neben Erkenntnissen aus Literaturquellen auf eigene empirische Forschung zurück: Um die aktuellen Risiken, die aus der Verwendung kriminalbehördlicher Informationsressourcen folgen, einschätzen zu können, wurden fünf Mitarbeiter*innen unterschiedlicher Datenschutzaufsichtsbehörden interviewt, die mit der Kontrolle entsprechender Systeme befasst sind.[4] Die Datenschutzaufsichtsbehörden nehmen die Interessen der von Datenverarbeitungen betroffenen Personen wahr, denen es in der Praxis schwerfällt, die Vorgänge zu durchschauen und sich rechtlich dagegen zur Wehr zu setzen.

Drittens werden die einfachrechtlichen Rahmenbedingungen, die bezüglich der einzelnen Anforderungen bestehen, in die Betrachtung mit einbezogen. Die Regelungen hegen die Funktionen der kriminalbehördlichen Informationssysteme einerseits ein und begrenzen sie. Dies geschieht vor allem im Interesse der in den Systemen gespeicherten Personen. Andererseits stellen rechtlich-normative Vorgaben auch Anforderungen an die Informationssysteme auf und sichern deren Funktionen ab.

Nach der Untersuchung der drei zentralen Anforderungen an die Informationsordnung wird beleuchtet, wie sich diese zueinander verhalten und welche gemeinsamen Herausforderungen bei ihrer Erfüllung bestehen (D.). Die Anforderungen werden in der Praxis unterschiedlich gewichtet und stehen teilweise im Konflikt zueinander. Dass sie derzeit nicht durchgehend erfüllt werden, ist möglicherweise auf strukturelle Probleme der Informationsordnung zurückzuführen, welche näher zu untersuchen sind.

A. Die schnelle und einfache Verfügbarkeit von Informationen

Die erste wesentliche Anforderung an die Informationsordnung aus kriminalbehördlich-operativer Sicht besteht darin, dass hierin abgelegte Informationen für ihre Anwender*innen schnell und einfach verfügbar sein sollen.

[4] Codes DSA1-DSA5.

*I. Anforderungen aus Sicht der Anwender*innen*

Die Verfügbarkeit setzt voraus, dass die auf der operativen Ebene tätigen Personen ohne unnötige Zwischenschritte auf Informationen zugreifen können, die in kriminalbehördlichen Systemen gespeichert sind.[5] Dazu gehört nicht nur der technisch störungsfreie, sondern auch der möglichst einfache und anwenderfreundliche Zugriff. Durch die bestmögliche Verfügbarkeit sollen im Ergebnis kommunikativer Aufwand[6] bei der Erlangung relevanter Informationen erspart und operative Vorgänge beschleunigt werden. Die Anforderung der schnellen und einfachen Verfügbarkeit bezieht sich sowohl auf Informationen, die bei der eigenen Behörde vorliegen als auch auf Informationen aus den Systemen anderer Behörden.

Auch die im Rahmen dieser Untersuchung interviewten Anwender*innen polizeilicher Datenbanken betonten die Wichtigkeit der Verfügbarkeit von Daten. Sie nannten Hürden bei dem Zugang zu Daten als einen besonders verbesserungsbedürftigen Aspekt der kriminalbehördlichen Informationsordnung. Dabei bezogen sie sich sowohl auf den Abruf von Informationen aus den Systemen ihrer eigenen Behörden als auch auf die Informationsressourcen anderer Stellen.

Die Anforderungen an die Verfügbarkeit von Informationen haben sich im Laufe der Zeit durch technologische Entwicklungen stark verändert. Die elektronische Datenverarbeitung hat dazu geführt, dass ein sekundenschneller Abruf aktueller Informationen möglich wurde und heute von den Anwender*innen kriminalbehördlicher Systeme auch eingefordert wird. Wie einschneidend die Veränderungen waren, lässt sich an dem Abruf von Fahndungsdaten bei der Polizei veranschaulichen: Bevor INPOL in den 1970er-Jahren als Fahndungssystem eingeführt wurde,[7] waren die hier abgelegten Daten nur in einem gedruckten Fahndungsbuch verfügbar. Die Fahndungsdaten wurden erhoben und durchliefen einen komplizierten Redaktionsprozess, bevor das Fahndungsbuch in den Druck ging und schließlich an die Beamt*innen vor Ort geschickt wurde. Es handelte sich um ein 600 bis 1.500 Gramm schweres Werk, das unter Umständen schon veraltet sein konnte, wenn die Anwender*innen es erstmals in den Händen hielten und darin blätterten, um Daten abzugleichen.[8] Die Nutzung des elektronischen INPOL gestaltete sich schon deutlich einfacher: Polizist*innen auf Streife hatten zwar keinen direkten Zugriff auf das System, konnten Informationen daraus aber per

[5] Vgl. zu dem Ziel der Verfügbarkeit von informationstechnischen Systemen und Daten im IT-Sicherheitsrecht *Bedner/Ackermann*, DuD 2010, 323 (326). *Möstl*, SIAK-Journal 2/2010, 61 versteht den Aspekt der Datenverfügbarkeit weiter im Zusammenhang mit der Frage, „was Sicherheitsbehörden wissen dürfen und wann ihnen welche Ermittlungsmethoden zur Verfügung stehen."

[6] Vgl. zu der Ersparnis kommunikativen Aufwands als Ziel der Informations- und Kommunikationstechnik *Halfmann*, in: Schulte/Schröder, Handbuch des Technikrechts, 2. Aufl. 2011, S. 93 (96).

[7] Siehe hierzu oben Teil 1 B. III. 1.

[8] Vgl. *Busch/Funk/Kauß/Narr/Werkentin*, S. 117; *Herold*, Universitas 1976, 63 (66 f.).

Funk abrufen.[9] Das bedeutete für die Anwender*innen nicht nur eine erhebliche Zeitersparnis,[10] sondern machte auch aktuellere Daten verfügbar als der Umgang mit dem Fahndungsbuch. Heute ist ein direkter Abruf von INPOL durch Anwender*innen auf Streife möglich. Die mobile Verfügbarkeit von Daten soll allerdings weiter verbessert werden: Wesentliche polizeifachliche Anwendungen sollen bald durchgängig auf mobilen Endgeräten verfügbar sein.[11] Auf diese Art gewissermaßen einen polizeilichen „App-Store" zu schaffen, ist eine Bestrebung des Programms Polizei 20/20.

Ein besonderer Aspekt der Anforderung der Verfügbarkeit von Informationen ist jener der zwischenbehördlichen Verfügbarkeit. Nicht nur der Zugriff auf Informationen, die innerhalb der eigenen Stelle liegen, soll schnell und einfach möglich sein, sondern auch der unkomplizierte Austausch relevanter Informationen zwischen Kriminal- und Sicherheitsbehörden wird zunehmend als wichtig angesehen. Dass Politik und Kriminalbehörden diesen Aspekt betonen, hängt auch mit konkreten sicherheitsrelevanten Ereignissen zusammen.[12] So stellten sich bei der Aufklärung der Mordserie der terroristischen Gruppierung Nationalsozialistischer Untergrund (NSU) Mängel bei der zwischenbehördlichen Verfügbarkeit von Informationen heraus. In seinem Bericht forderte der zu diesem Themenkomplex eingesetzte Untersuchungsausschuss, es dürfe „nicht nochmals vorkommen, dass Zeit und Kraft dafür verloren gehen, unterschiedliche Systeme [...] während einer laufenden Ermittlung zu verknüpfen."[13] Die „Maßnahmen, die Interoperabilität der Datensysteme zu schaffen," müssten „zügig zu einem guten, verfassungsrechtlich einwandfreien Ergebnis geführt werden."[14] Dieser Gedanke wurde in der Begründung des Entwurfes eines neuen BKAG aufgegriffen.[15] Es ist eines der zentralen Ziele der aktuellen Umstellung der polizeilichen Informationsordnung,[16] die Datenbestände der Polizeien besser verfügbar zu machen. Polizeibeamte müssten „mit einer gezielten Recherche oder Abfrage insbesondere in Kontrollsituationen zuverlässig alle vorhandenen Datenquellen erreichen, um Personen zu erkennen und herauszufiltern, Anschläge zu verhindern und polizeiliche Lagen effektiv zu bewältigen"[17], heißt es in der Begründung zu den Rechtsgrundlagen für den neuen Informationsverbund der Polizei im BKAG.

[9] Vgl. *Lilie*, ZStW 106 (1994), 625 (631).
[10] Vgl. *Busch/Funk/Kauß/Narr/Werkentin*, S. 128.
[11] BMI, Polizei 2020, S. 14.
[12] Siehe oben Teil 1 B. V.
[13] BT-Drs. 17/14600, S. 862.
[14] BT-Drs. 17/14600, S. 862.
[15] BT-Drs. 18/11163, S. 76; vgl. dazu *Graulich*, KriPoZ 2017, 278 (286).
[16] Siehe dazu oben Teil 1 C. 3.
[17] BT-Drs. 18/11163, S. 84.

Während die aktuellen Bemühungen um das Programm Polizei 20/20 die zwischenbehördliche Verfügbarkeit von Informationen unter Polizeibehörden betreffen, lassen sich in der gesamten Entwicklung der EDV-gestützten kriminalbehördlichen Informationsordnung auch Probleme beim Zugriff der Staatsanwaltschaften auf polizeiliche Informationsbestände nachvollziehen. Lange Zeit konnten die Staatsanwaltschaften etwa keine Informationen aus INPOL abrufen oder in das System eingeben.[18] Dabei sind die dort gespeicherten Informationen, die zu erheblichen Teilen aus der Strafverfolgung stammen und auch hierfür weiterverwendet werden sollten, für die staatsanwaltschaftliche Arbeit potentiell sehr relevant. Der fehlende staatsanwaltschaftliche Zugriff auf polizeiliche Systeme kann ein Ermittlungsverfahren erheblich beeinflussen.[19] Er kann auf der einen Seite dazu führen, dass ein Ermittlungsverfahren zunächst auf Grundlage von Informationen, die sich dem Zugriff der Staatsanwaltschaft entziehen, möglicherweise zu Unrecht betrieben wird. Auf der anderen Seite kann der fehlende Zugriff dazu führen, dass der Staatsanwaltschaft Anhaltspunkte für Straftaten entgehen und gebotene Ermittlungsverfahren nicht eingeleitet oder weitergeführt werden.[20]

II. Implikationen für Betroffene

Für die Betroffenen ist schon der Umstand, dass persönliche Informationen über sie in kriminalbehördlichen Ressourcen gespeichert werden und abrufbar sind, von Bedeutung. Sie können durch das Vorhandensein der Daten stigmatisiert und kriminalisiert werden.

Auf der ersten Stufe der Beeinträchtigungen steht die Stigmatisierung als eine Beschädigung der Identität, die nicht notwendigerweise offen zutage tritt. Ein Stigma lässt sich mit *Erving Goffman* als eine Form der Diskrepanz zwischen der virtualen und tatsächlichen sozialen Identität einer Person begreifen, welche durch Zuschreibungen entsteht.[21] Die Zuschreibung von problematischen persönlichen Eigenschaften kann in kriminalbehördlichen Informationsressourcen auf vielerlei Art erfolgen. Ein Beispiel hierfür ist die Eintragung von ermittlungsunterstützenden Hinweisen, durch die Personen in polizeilichen Dateien mit Attributen wie „Rocker", „politisch motivierter Straftäter", „gewalttätig" oder „geisteskrank" belegt werden.[22] Die ermittlungsunter-

[18] Siehe oben Teil 1 B. IV.
[19] *Lilie*, ZStW 106 (1994), 625 (632).
[20] Arbeitskreis AE, S. 122.
[21] *Gofffman*, S. 11.
[22] LT-Drs. BW 15/5841, S. 4; BfDI, 26. Tätigkeitsbericht 2015-2016, S. 111; LfDI Berlin, Jahresbericht 2012, S. 55 f.

stützenden Hinweise haben die früher vergebenen personengebundenen Hinweise abgelöst, die vorrangig dem Schutz der Polizei und der Betroffenen dienten – etwa durch den Vermerk einer Suizidgefahr.[23] Zum Teil wurde die Vergabe problematischer Attribute – wie etwa „Landstreicher", „Prostitution" oder „Fixer" – im Laufe der Zeit eingestellt, es finden sich aber noch entsprechende Zuschreibungen in alten Datenbeständen.[24] Die Kriterien für die Vergabe ermittlungsunterstützender Hinweise sind nicht öffentlich bekannt.[25] Eine Offenlegung wäre aber im Sinne des Persönlichkeitsschutzes der Betroffenen geboten. Es ist nicht erkennbar, inwiefern eine Offenlegung der Kriterien, nach denen ermittlungsunterstützende Hinweise vergeben werden, zu konkreten Beeinträchtigungen polizeilichen Handelns führen sollte, die nicht angesichts der Bedeutung des Persönlichkeitsschutzes hingenommen werden müssten.[26]

Problematische Eigenschaften können Personen im Übrigen nicht nur durch individuelle Eintragungen zugeschrieben werden. Es kann auch schon in der Struktur eines Informationssystems angelegt sein, dass die darin erfassten Personen stigmatisiert werden. So beruhen beispielsweise viele Eintragungen in der Datei „Gewalttäter Sport" nicht auf Ermittlungsverfahren oder Verurteilungen wegen „Gewalttaten" wie Delikten gegen Leib oder Leben oder Formen der Nötigung.[27] Auch nach ihrer inneren Logik ist eine Eintragung in der Datei „Gewalttäter Sport" nicht zwangsläufig gleichbedeutend mit einer Einstufung als gewalttätige Person.[28] Dennoch erweckt eine solche

[23] Vgl. BayLT-Drs. 17/8030, S. 1.

[24] *Schröder*, in: Grundrechte-Report 2015, 38 (40).

[25] BfDI, 26. Tätigkeitsbericht 2015-2016, S. 111. Für den INPOL-Verbund existiert ein Leitfaden für die Vergabe von personengebundenen Hinweisen des Bundeskriminalamts, der auf einem Beschluss des Facharbeitskreises II (Innere Sicherheit) der Innenministerkonferenz beruht und als Verschlusssache eingestuft ist; LT-Drs. BW 15/5841, S. 2.

[26] Vor diesem Hintergrund überzeugt es nicht, dass ein Begehren auf Herausgabe des Leitfadens für die Vergabe von personengebundenen Hinweisen des Bundeskriminalamts nach dem IFG mit der Begründung abgelehnt wurde, dass „[v]on der Kenntnis der Vergabekriterien [...] polizeiliche Maßnahmen [...] abgeleitet [werden], die bei Bekanntwerden der Kriterien vorhersehbar bzw. absehbar wären." Eine Einstellung der Betroffenen auf das Verhalten der Polizei könne „den Erfolg der Maßnahme beeinträchtigen und zu Gefährdungen von Leben oder Gesundheit von Menschen führen."; Der Polizeipräsident in Berlin, Antwortschreiben auf eine Anfrage nach dem Berliner Informationsfreiheitsgesetz vom 30. September 2013, abrufbar unter https://fragdenstaat.de/anfrage/leitfaden-fur-die-vergaben-von-personengebundenen-hinweisen-poliksinpol/12438/anhang/ifg_polpbln_20130930.pdf.

[27] Stand 2021 war der häufigste Speicherungsgrund (ein Verdacht auf) Landfriedensbruch nach § 125 StGB (3.324 Speicherungen); BT-Drs. 19/26771, S. 2. Es lagen dazu eine Vielzahl von Speicherungen zu Delikten wie Beleidigung nach § 185 StGB (314 Speicherungen), Hausfriedensbruch nach § 123 StGB (457 Speicherungen) oder Verstößen gegen das Versammlungsgesetz (240 Speicherungen) vor, die sich jedenfalls nach dem allgemeinen Sprachgebrauch nicht mit Gewalttätigkeit gleichsetzen lassen; vgl. auch *Ruch/Feltes*, NK 2016, 62 (70).

[28] So ist in dieser Datei – ähnlich wie in anderen Informationsressourcen – die Möglichkeit eines gesonderten Hinweises vorgesehen, dass Personen als gewalttätig gelten; vgl. OVG Münster DVBl. 2013, 1460 (1461).

Eintragung zumindest einen starken äußeren Anschein, dass eine Person mit Gewalttaten in Verbindung steht bzw. sich einer entsprechenden Straftat schuldig gemacht hat.[29]

Dieser Anschein ist geeignet, dem Ansehen einer Person erheblich zu schaden. In diesem Sinne sah auch das OVG Münster in der Bezeichnung Gewalttäter ohne Vorliegen tatsächlicher Anhaltspunkte für die Begehung entsprechender Taten zurecht einen rechtswidrigen Eingriff in das allgemeine Persönlichkeitsrecht.[30] Die stigmatisierende Benennung der Datei, die die gespeicherten Inhalte nicht richtig bezeichnet, greift empfindlich in die Rechte der Betroffenen ein, ohne das dies zur Erfüllung eines legitimen Zweckes erforderlich wäre. Zumindest eine Umbenennung der Dateien „Gewalttäter Sport" erscheint daher – sollten nicht die Speicherungsgründe angepasst werden – zwingend geboten.[31]

Das Vorliegen eines Stigmas setzt nicht voraus, dass eine problematische Zuschreibung Dritten bekannt ist.[32] So kann eine Person beispielsweise durch das Vorhandensein von ermittlungsunterstützenden Hinweisen in einer polizeilichen Datenbank auch dann stigmatisiert sein, wenn die Speicherung lange zurückliegt und die auf polizeilicher Seite beteiligten Akteure sich nicht mehr an die Hinweise erinnern. Allein die Möglichkeit, dass in kriminalbehördlichen Ressourcen vorhandene Informationen in künftige Entscheidungsverfahren mit einbezogen werden, ist problematisch. Folgerichtig nimmt die Verwaltungsrechtsprechung im Rahmen von Fortsetzungsfeststellungsklagen ein Rehabilitationsinteresse bei der Speicherung von beeinträchtigenden Informationen in kriminalbehördlichen Systemen an, selbst wenn diese nicht an die Öffentlichkeit gelangt sind.[33] Auch in der frühen Rechtsprechung des Bundesverwaltungsgerichts fällt eine Sensibilität für die Risiken der Stigmatisierung durch kriminalbehördliche Datenspeicherungen auf: Polizeibehörden dürften nach dem Menschenbild des Grundgesetzes „nicht jedermann als potentiellen Rechtsbrecher betrachten und auch nicht jeden, der sich irgendwie verdächtig gemacht hat (‚aufgefallen ist') oder bei der Polizei angezeigt worden ist, ohne weiteres ‚erkennungsdienstlich behandeln'"[34]. Es sei „in Betracht zu ziehen, daß die Aufbewahrung von erkennungsdienstlichen Unterlagen

[29] Vgl. VG Hamburg BeckRS 2013, 52593.

[30] OVG Münster DVBl. 2013, 1460 (1461).

[31] Die Bund-Länder-Arbeitsgruppe Überprüfung und Anpassung der beim Bundeskriminalamt geführten Datei Gewalttäter Sport gab in ihrem Abschlussbericht (S. 6) an, die Möglichkeit einer Umbenennung der Datei aus diesem Grund geprüft zu haben. Eine Änderung sei aber nicht angezeigt, da der Dateiname bundesweit etabliert und bekannt sei. Gerade dieser Umstand spricht aber für Stigmatisierungseffekte und dafür, den Namen der Datei zu ändern.

[32] *Goffman*, S. 56 ff., S. 94 ff.

[33] OVG Saarlouis BeckRS 2012, 58861.

[34] BVerwG NJW 1967, 1192.

die persönliche Sphäre des Betroffenen schon allein wegen des Bewußtseins stark berühren kann, von der Kriminalpolizei als möglicher künftiger Rechtsbrecher betrachtet zu werden. Sie kann unter Umständen dadurch dem guten Ruf und der Unbescholtenheit der betreffenden Person abträglich sein, daß diese Tatsache durch die – kriminalpolizeilich gerechtfertigte – Verwertung der internen Unterlagen bekannt wird."[35] Weniger überzeugend ist das Begriffsverständnis in der Rechtsprechung des Bundesverfassungsgerichts, das davon ausgeht, dass Informationen erst über die Ermittlungsbehörden hinaus bekannt werden müssen, um eine stigmatisierende Wirkung entfalten zu können.[36]

Die Stigmatisierung durch die Zuschreibung von Eigenschaften ist stets mit Blick auf ihre Folgeeffekte zu betrachten. Einer dieser Effekte ist die Kriminalisierung von Individuen. Betroffene können durch die Zuschreibung von Tatsachen oder Wertungen in Informationsressourcen in Verdacht geraten, Straftaten begangen zu haben oder zu bestimmten Straftaten zu neigen. Gewisse Attribute können direkt kriminelle Verhaltensweisen implizieren (z.B. „Gewalttäter"[37], „Einbrecher", „Drogenhändler") oder solche nahelegen (z.B. „wechselt häufig den Aufenthaltsort"). Wenn Personen auf diese Art Rollen zugeschrieben werden, kann daraus resultieren, dass sie diese Rollen akzeptieren und übernehmen. Es erfolgt unter Umständen eine Etikettierung im Sinne des kriminologischen Labeling Approach.[38] Mithin kann die Zuweisung eines Attributs in einem kriminalbehördlichen Informationssystem im Extremfall zur „selbsterfüllenden Prophezeiung" werden.[39]

Dafür muss sich die Attribution nach außen manifestieren. Im Zusammenhang mit der kriminalbehördlichen Informationsordnung ist dies vorstellbar, wenn die Speicherung bestimmter Informationen dazu führt, dass eine Person kontinuierlich kontrolliert und als verdächtig behandelt wird. Zwar darf die Tatsache, dass eine Person in einer Datei eingetragen ist oder eine Speicherung zu ihr in einem Informationssystem vorhanden ist, nicht schon für sich genommen dazu führen, dass eine Maßnahme gegen sie erfolgt, ein Verdacht angenommen oder eine Gefahrenprognose bejaht wird.[40] Es ist

[35] BVerwG NJW 1967, 1192 (1193).
[36] Vgl. BVerfGE 115, 320 (351 f.)
[37] Vgl. dazu näher *Ruch/Feltes*, NK 2016, 62 (69).
[38] Vgl. zu dieser von *Howard Saul Becker* (Outsiders, 1963) und im deutschsprachigen Raum von *Fritz Sack* (vgl. *Sack*, KJ 1971, 384 (385 ff.)) geprägten kriminologischen Theorie *Eisenberg/Kölbel*, § 8 Rn. 1 ff.; *Neubacher*, S. 117; *Kunz/Singelnstein*, S. 168 ff.; *Singelnstein/Stolle*, S. 130 ff.; zum Labeling durch Eintragungen in Strafregister *Morgenstern*, ZStW 131 (2019), 625 (635 f.).
[39] Vgl. *Neubacher*, S. 117.
[40] Vgl. OVG Bremen BeckRS 2010, 46388; VG Hamburg BeckRS 2013, 52593; VGH Kassel BeckRS 2017, 103690; *Arzt/Eier*, DVBl. 2010, 816 (819); *Spiecker gen. Döhmann/Kehr*, DVBl. 2011, 930.

jedoch zu beobachten, dass gewisse Einträge in Informationssystemen in der polizeilichen Praxis in diese Richtung verwendet werden.[41] So werden zum Beispiel Jugendliche, die in Datenbanken als „Intensivtäter" geführt werden, auf dieser Grundlage von der Polizei angesprochen.[42]

Eine weitere Fallgruppe, in der Personen auf mitunter schwachen Tatsachengrundlagen Stigmatisierungen erfahren und unter Umständen langfristig wie Kriminelle behandelt werden, ist die Speicherung in Rauschgiftdateien. Dies veranschaulicht beispielhaft *Fall 1*, in dem eine Person aufgrund ihrer Eintragung in einer Rauschgiftdatei darauf angesprochen wird, ob sie illegale Betäubungsmittel bei sich führt. Mehrere im Rahmen dieser Untersuchung befragte Mitarbeiter*innen der Datenschutzaufsicht gaben an, dass sie auch auf Grundlage geringfügiger Verstöße gegen das Betäubungsmittelgesetz längerfristige Speicherungen in entsprechenden Dateien festgestellt hätten. Ein*e Befragte*r äußerte:

> „Wir haben es im Bereich der Rauschgiftkriminalität gesehen, bei der Prüfung. Dass dann teilweise Personen gespeichert waren, weil sie irgendwo angetroffen wurden und einen Joint geraucht hatten, in einer Wohnung. Und sich dann in so einer bundesweiten Datenbank wiederfinden. Wo man dann auch die Erstkonsumenten leichter Drogen erfasst hat, obwohl die eigentlich in so einer bundesweiten Datenbank nichts zu suchen haben." (DSA4)

Ein*e andere*r Interviewpartner*in berichtete, dass es im Zusammenhang mit Verstößen gegen das Betäubungsmittelgesetz in dem betreffenden Bundesland regelmäßig zu präventiv begründeten Datenspeicherungen mit einer Löschfrist von zehn Jahren kommen würde (DSA2). Derartige Datenspeicherungen führen typischerweise zu äußerlich manifestierten Stigmatisierungen, wenn die betroffenen Personen in Verkehrskontrollen angehalten werden und einen Drogentest absolvieren müssen, weil eine Abfrage von Daten in einem polizeilichen Informationssystem ergibt, dass bereits wegen möglichen Verstößen gegen das Betäubungsmittelgesetz gegen sie ermittelt wurde (vgl. *Fall 1*). Die Struktur dieser Systeme begünstigt es im Ergebnis offenbar, dass Betroffene auch aufgrund (des Verdachts) geringer Verstöße langfristig eine spezielle polizeiliche Behandlung erfahren.

Durch den Einsatz der elektronischen Datenverarbeitung und neuer mobiler Technologien, die Informationen leichter verfügbar machen als bisher, werden die möglichen Effekte von Stigmatisierungen verstärkt.[43] Das Risiko einer Kriminalisierung

---

[41] *Spiecker gen. Döhmann/Kehr*, DVBl. 2011, 930.

[42] *H. E. Müller*, in: Strafverteidigertag, S. 169 (184 ff.); vgl. auch *Jasch*, KJ 2014, 237 (243 f.); vgl. zur Einordnung der Gefährderansprache *Hebeler*, NVwZ 2011, 1364 ff.; *Kreuter-Kirchhof*, AöR 139 (2014), 257 ff.; *Kießling*, DVBl. 2012, 1210 ff.

[43] Vgl. *Lageson/Maruna*, Punishment & Society 2018, 113 (117).

wächst, je schneller und leichter Daten abrufbar sind und je eher sie routinemäßig abgerufen werden. Besteht eine einfache Zugriffsmöglichkeit für einen breiten Personenkreis, wiegt schon das bloße Vorhandensein belastender Daten in der kriminalbehördlichen Informationsordnung schwerer, als wenn diese nur für einen engen Personenkreis unter strengen Voraussetzungen zugänglich sind. Die aktuelle Priorität, speziell die Verfügbarkeit von Daten zu verbessern, könnte daher auch die Risiken für die Betroffenen erhöhen.

Schließlich ist zu berücksichtigen, dass mit der einfachen und schnellen Verfügbarkeit von Daten das Risiko zunehmen kann, dass diese missbräuchlich abgerufen werden.[44] In den letzten Jahren waren vermehrt Fälle nachzuvollziehen, in denen Polizist*innen illegal Daten aus Informationssystemen abriefen.[45] Oft erfolgten unzulässige Datenabfragen aus privatem Interesse. So beklagte etwa die Berliner Datenschutzbeauftragte im Frühjahr 2019 öffentlich, Polizisten würden häufig zu privaten Zwecken auf Datenbanken zugreifen, etwa „um Informationen über Nachbarn zu bekommen oder den Schwager zu ärgern“[46]. Während der bloße Abruf aus Neugier noch keinen Straftatbestand verwirklicht, fällt der Abruf mit Absicht zur Schädigung einer Person unter die Straftatbestände der Landesdatenschutzgesetze.[47]

III. Rechtliche Rahmenbedingungen

Die rechtlichen Rahmenbedingungen für die Verfügbarkeit von Daten ergeben sich in erster Linie aus den Voraussetzungen für ihre Speicherung (1.) und ihren Abruf (2.). Als Vorgabe für den zwischenbehördlichen Zugriff auf Daten von besonderem Interesse ist der Grundsatz der Verfügbarkeit aus dem Recht der Europäischen Union (3.).

1. Die Speicherung

Die Speicherung ist die Grundvoraussetzung dafür, dass Daten zum Abruf zur Verfügung stehen. Im Folgenden wird zunächst auf die Grundvoraussetzungen der Datenspeicherung (a.) und dann auf problematische Fallgruppen der Speicherung (b.) eingegangen, in denen besondere Voraussetzungen gelten.

---

[44] Vgl. hierzu *Golla*, JB InfoR 2019, 199 (212 ff.).

[45] Vgl. etwa LfDI Baden-Württemberg, Pressemitteilung vom 18. Juni 2019, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten/; LfDI Berlin, Jahresbericht 2018, S. 55 f.; LfD Bremen, 1. Jahresbericht nach der Europäischen Datenschutzgrundverordnung 2018, S. 23.

[46] Tagesspiegel, Datenschutzbeauftragte kritisiert Berliner Polizei, 28.03.2019, abrufbar unter https://www.tagesspiegel.de/berlin/pannen-missbrauch-und-lecks-datenschutzbeauftragte-kritisiert-berliner-polizei/24157448.html.

[47] So etwa §§ 70 i.V.m. 29 BlnDSG.

a. Grundvoraussetzungen der Datenspeicherung

Die Voraussetzung zur Speicherung von Daten in kriminalbehördlichen Informationssystemen sind im Polizeirecht auf Landes- und Bundesebene (aa)) sowie im Strafprozessrecht (bb)) geregelt.

aa) Voraussetzungen im Polizeirecht

Die Polizeigesetze der Länder erlauben die Speicherung personenbezogener Daten in Akten oder Dateien, soweit dies zur Erfüllung polizeilicher Aufgaben, zu einer zeitlich befristeten Dokumentation[48] oder zur Vorgangsverwaltung[49] erforderlich ist.[50] Die Erfüllung polizeilicher Aufgaben umfasst dabei sowohl die Verwendung von Daten in konkreten Verfahren als auch die Vorsorge bzw. Vorbereitung kommender Verfahren.

Zum Teil enthalten die Befugnisse zur Speicherung ausdrücklich die Voraussetzung, dass die Daten rechtmäßig erhoben wurden.[51] Dabei ist auch die Speicherung von zu Strafverfolgungszwecken erhobenen Daten zur Gefahrenabwehr – teils auch in der problematischen Begrifflichkeit der vorbeugenden Bekämpfung von Straftaten[52] – gestattet.[53] Zuletzt wurden in einigen Landespolizeigesetzen Regelungen zur Umsetzung

[48] Der Zweck der Dokumentation bezieht sich auf abgeschlossene Vorgänge und soll unter anderem ihrem Nachweis im Rahmen von gerichtlichen Verfahren dienen; *Petri,* in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 870.

[49] Die Vorgangsverwaltung erfasst die formale Begleitung von Vorgängen zum Nachweis ihres Eingangs, ihrer Bearbeitung, ihres Ausgangs und ihres Verbleibs („Veraktung"); BT-Drs. 13/1550, S. 37 (zu § 30 Abs. 2 BKAG 1997); vgl. auch *Petri,* in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 865; OVG Lüneburg NdsVBl. 2008, 323 f. Die Zulässigkeit der Speicherung ist damit in der Regel auch an den Ablauf dieser Verfahren gebunden und entfällt regelmäßig mit ihrem Abschluss. Nicht in allen Polizeigesetzen ist der Speicherungszweck der Vorgangsverwaltung ausdrücklich erwähnt; vgl. zu der fehlenden Notwendigkeit hierfür OVG Lüneburg BeckRS 2013, 47085.

[50] Art. 54 Abs. 1 BayPAG; § 42 Abs. 1 Satz 1 ASOG Bln; § 39 Abs. 1 BbgPolG; § 50 Abs. 1 Satz 1 BremPolG; § 36 Abs. 1 HmbPolDVG; § 20 Abs. 1 HSOG; §§ 36 Abs. 1 Satz 1, 38 SOG MV; § 38 Abs. 1 Satz 1 NPOG; §§ 22 Abs. 1, 23 Abs. 1 PolG NRW; § 52 Abs. 1 POG RP; § 25 SPolG i.V.m. § 23 Abs. 1 Satz 1 SPolDVG; § 43 Abs. 1 Satz 1 SächsPolG; § 22 Abs. 1 Satz 1 SOG LSA; § 188 Abs. 1 Satz 1 SchlHLVwG; § 40 Abs. 1 TH PAG.

[51] § 42 Abs. 1 Satz 1 ASOG Bln; § 39 Abs. 1 BbgPolG; § 50 Abs. 1 Satz 1, Abs. 4 Satz 1, Abs. 5 BremPolG; § 38 Abs. 1 Satz 1 NPOG; § 22 Abs. 1 PolG NRW; § 40 Abs. 1 TH PAG; vgl. zu den Möglichkeiten der Weiterverarbeitung rechtswidrig erlangter Daten *W. Schenke*, in: FG Hilger, S. 225 (239 ff.); mit Überlegungen zu einem allgemeinen Rechtmäßigkeitsvorbehalt für die Weiterverarbeitung von Daten in Informationssystemen *Stubenrauch*, S. 149 f.

[52] Art. 54 Abs. 2 Satz 1 BayPAG; § 42 Abs. 3 ASOG Bln; § 39 Abs. 2 Satz 1 BbgPolG; § 50 Abs. 4 BremPolG; § 36 Abs. 2 HbgPolDVG; § 20 Abs. 6 Satz 1 HSOG; § 37 Abs. 1 SOG MV; § 23 Abs. 6 PolG NRW; § 52 Abs. 2 Satz 1 POG RP; § 25 SPolG i.V.m. § 23 Abs. 4 Satz 1, Abs. 5 Satz 1 SPolDVG; § 43 Abs. 2 Satz 1 SächsPolG; § 23 Abs. 1 SOG LSA.

[53] § 39 Abs. 2 Satz 1 BbgPolG; § 39 Abs. 3 NPOG; § 189 Abs. 1 Satz 4 SchlHLVwG; § 40 Abs. 2 TH PAG.

des vom Bundesverfassungsgericht formulierten Grundsatzes der hypothetischen Datenneuerhebung verankert.[54] Erstmals geschah dies allerdings in § 12 BKAG, der Bedingungen für sämtliche Weiterverarbeitungen[55] von Daten nach ihrer erstmaligen Erhebung im Anwendungsbereich des BKAG enthält.[56] Nach den Kategorien der hypothetischen Datenneuerhebung ist die Speicherung personenbezogener Daten in einem Informationssystem regelmäßig eine zweckändernde Nutzung, die im Anwendungsbereich des BKAG an dessen § 12 Abs. 2 zu messen ist. Die Voraussetzungen für eine „weitere Nutzung" im Sinne von § 12 Abs. 1 BKAG, dass die Speicherung seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter erfolgt, wird regelmäßig nicht zu erfüllen sein. Aufgrund der Multipolarität der Informationsordnung, also dem Umstand, dass einzelne Informationsressourcen zur Erfüllung mehrerer Zwecke dienen,[57] wird es oftmals an den Voraussetzungen der Erfüllung derselben Aufgabe scheitern.

Nach § 12 Abs. 2 BKAG kann das Bundeskriminalamt zur Erfüllung seiner Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn mindestens vergleichbar schwerwiegende Straftaten verhütet, aufgedeckt oder verfolgt oder vergleichbar bedeutsame Rechtsgüter geschützt werden sollen und sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten ergeben oder zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.

Für die Speicherung von Daten im Informationssystem des Bundeskriminalamts sehen §§ 16, 18 und 19 BKAG besondere Regelungen vor.[58] § 16 BKAG stellt allgemeine Voraussetzungen für die Weiterverarbeitung von Daten im Informationssystem des Bundeskriminalamts auf. Nach Abs. 1 der Vorschrift kann das Bundeskriminalamt „personenbezogene Daten nach Maßgabe des § 12 im Informationssystem weiterverar-

[54] § 15 BWPolG; § 20 HSOG; § 36 SOG MV; § 23 PolG NRW; § 51 POG RP; § 13b SOG LSA.

[55] Unter diesen weiten Begriff fällt die Speicherung von Daten ebenso wie ihre Auswertung und weitere Nutzungsschritte nach der erstmaligen Erhebung; vgl. BR-Drs. 109/17, S. 104.

[56] Die Geltung von § 12 BKAG als allgemeiner Grundsatz ergibt sich schon aus seiner systematischen Stellung zu Beginn von Abschnitt 2 Unterabschnitt 2 („Weiterverarbeitung von Daten") BKAG. Dies entspricht auch dem Willen des Gesetzgebers; vgl. BT-Drs. 18/11163, S. 92. Für die Weiterverarbeitung von Daten im Informationssystem des BKAG ergibt sich die Geltung von § 12 BKAG auch direkt aus § 16 Abs. 1 BKAG („nach Maßgabe des § 12").

[57] Siehe oben Teil 1 A. III. 2.

[58] Für Unklarheit sorgt hier der Begriff „Weiterverarbeiten". Dieser legt nahe, dass sich die Regelung nur auf der Speicherung nachgelagerte Verwendungen von Daten bezieht.

beiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist und soweit dieses Gesetz keine zusätzlichen besonderen Voraussetzungen vorsieht."[59] § 16 Abs. 2 BKAG trifft eine besondere Regelung zur Weiterverarbeitung von Daten in einer Personenfahndungsdatei.[60] Zentral für die Strafverfolgungsvorsorge ist Abs. 3 der Vorschrift. Demnach kann das Bundeskriminalamt „personenbezogene Daten, die es bei der Wahrnehmung seiner Aufgaben auf dem Gebiet der Strafverfolgung erlangt hat, unter den Voraussetzungen der §§ 18 und 19 BKAG im Informationssystem für Zwecke künftiger Strafverfahren weiterverarbeiten." Die Formulierung „Zwecke künftiger Strafverfahren" ist hierbei gleichbedeutend mit der Vorsorge für künftige Strafverfolgung zu verstehen.[61] §§ 18 und 19 BKAG stellen spezifische Anforderungen für die Weiterverarbeitung – einschließlich der Speicherung – von Daten zu bestimmten Personen auf.

§ 18 BKAG trifft eine Regelung zur Zulässigkeit der Weiterverarbeitung von Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen.[62] Nach Abs. 1 der Vorschrift ist die Weiterverarbeitung von Daten zu diesen Personen zur Erfüllung der Aufgaben des Bundeskriminalamtes grundsätzlich zulässig. Abs. 2 legt näher fest, welche Arten von Daten auf dieser Grundlage weiterverarbeitet werden dürfen. Eine Weiterverarbeitung von personenbezogenen Daten ist nach Abs. 3 unter bestimmten Bedingungen auch möglich, um festzustellen, ob es sich bei einer Person um einen Verurteilten, Beschuldigten, Tatverdächtigen oder eine sonstige Anlassperson handelt („Prüffälle"). Nach Abs. 4 ist die Verarbeitung von Daten zum Nachweis von Personen, die einer richterlich angeordneten Freiheitsentziehung unterliegen, zulässig – er bildet damit die Grundlage für Speicherungen in einer Haftdatei.[63] Nach

[59] Damit hat § 16 Abs. 1 BKAG einen potentiell überaus weiten Anwendungsbereich. Isoliert betrachtet gestattet die Regel ihrem Wortlaut nach die Bevorratung sämtlicher Daten zumindest zu den Zwecken, zu denen sie ursprünglich erhoben wurden; vgl. kritisch hierzu *Bäcker*, Stellungnahme BKAG 2018, S. 4 f.; *Eichenhofer*, in: Barczak, BKAG, 2023, § 16 Rn. 6.

[60] Danach ist die Weiterverarbeitung von personenbezogenen Daten im Informationssystem zulässig, „soweit dies erforderlich ist zur Fahndung und polizeilichen Beobachtung oder gezielten Kontrolle, wenn das Bundeskriminalamt oder die die Ausschreibung veranlassende Stelle nach dem für sie geltenden Recht befugt ist, die mit der Ausschreibung für Zwecke der Strafverfolgung, des Strafvollzugs, der Strafvollstreckung oder der Abwehr erheblicher Gefahren vorgesehene Maßnahme vorzunehmen oder durch eine Polizeibehörde vornehmen zu lassen."

[61] BT-Drs. 13/1550 S. 34; *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 16 BKAG Rn. 27.

[62] Kritisch zu der Bestimmtheit der Regelung zur Erfassung sonstiger Anlasspersonen *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 18 BKAG Rn. 6; zum Kreis der erfassten Personen insgesamt *Eichenhofer*, in: Barczak, BKAG, 2023, § 18 Rn. 4 f.

[63] *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 18 BKAG Rn. 37.

Abs. 5 ist die Weiterverarbeitung unzulässig, wenn ein Beschuldigter rechtskräftig freigesprochen wird, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt wird oder das Verfahren nicht nur vorläufig eingestellt wird, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.

§ 19 BKAG regelt die Zulässigkeit der Weiterverarbeitung von Daten zu anderen Personen als jenen, die als Täter einer vergangenen oder künftigen Straftat in Betracht kommen. Nach Abs. 1 der Vorschrift kann das Bundeskriminalamt zur Erfüllung seiner Aufgaben Daten von Personen weiterverarbeiten, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass sie als Zeugen für die Strafverfolgung oder als Opfer einer künftigen Straftat in Betracht kommen, dass sie mit Verurteilten, Beschuldigten oder Tatverdächtigen in Verbindung stehen und sie Kenntnis über bestimmte relevante Umstände haben oder es sich um Hinweisgeber und sonstige Auskunftspersonen handelt. Die Vorschrift verlangt für die Zulässigkeit der Verarbeitung außerdem, dass sie zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich ist. Damit regelt die Vorschrift gleichzeitig einen Anlass zum präventiven („Verhütung") als auch zum repressiven Tätigwerden („künftige Verfolgung").[64] Außer in dem Fall von Personen, die mutmaßlich mit Verurteilten, Beschuldigten oder Tatverdächtigen in Verbindung stehen (§ 19 Abs. 1 Satz 1 Nr. 3 BKAG), verlangt § 19 Abs. 1 Satz 3 BKAG eine Einwilligung der Betroffenen für die Zulässigkeit der Datenverarbeitung. Die Vorschrift begründet im Vergleich zu § 18 Abs. 1 BKAG insgesamt deutlich höhere Anforderungen. Auch hier ist die Möglichkeit der Weiterverarbeitung auf bestimmte Arten von Daten begrenzt. Abs. 2 regelt die Weiterverarbeitung von Daten von Vermissten, unbekannten Personen und unbekannten Toten und ermöglicht damit die Einrichtung entsprechender Dateien. Nach Abs. 3 der Vorschrift ist eine Weiterverarbeitung von personenbezogenen Daten unter bestimmten Bedingungen auch möglich, um festzustellen, ob es sich Personen die in Abs. 1 und Abs. 2 genannten Eigenschaften aufweisen.

[64] Kritisch hierzu *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 19 BKAG Rn. 5; *Eichenhofer*, in: Barczak, BKAG, 2023, § 19 Rn. 2.

bb) Voraussetzungen im Strafprozessrecht

§ 481 Abs. 1 Satz 1 StPO enthält eine allgemeine Öffnungsklausel[65] für die Verwendung von Daten aus Strafverfahren zu allen in den Polizeigesetzen genannten Zwecken.[66] Hierunter fällt die Vorbereitung der Gefahrenabwehr als Aspekt der vorbeugenden Verbrechensbekämpfung[67] und damit auch die Speicherung von Daten in entsprechenden Informationssystemen.

Daneben sind die Regelungen des zweiten Abschnitts (§§ 483 ff. StPO), die die Speicherung und Verwendung personenbezogener Daten durch Strafgerichte, Strafverfolgungsbehörden[68] und andere Stellen der Strafrechtspflege in Dateien betreffen, von besonderem Interesse. Diese ermöglichen unter anderem die Speicherung und Strukturierung von Daten in polizeilichen Dateien zum Zwecke eines konkreten Strafverfahrens (§ 483 Abs. 1 StPO)[69] und für künftige Strafverfahren (§ 484 Abs. 1 und Abs. 2 StPO)[70]. Im Wesentlichen setzen diese Befugnisse für die Datenverarbeitung zu den genannten Zwecken voraus, dass diese für die Zwecke eines konkreten Strafverfahrens (§ 483 Abs. 1 Satz 1 StPO) oder künftiger Strafverfahren (§ 484 Abs. 1 StPO) erforderlich ist.[71]

Bei der Speicherung von Daten in polizeilichen Dateien zum Zwecke eines konkreten Strafverfahrens findet nach § 483 Abs. 3 StPO das Polizeirecht Anwendung, wenn die Speicherung zusammen mit Daten erfolgt, deren Speicherung sich nach den Polizeigesetzen richtet. Das ist bei so genannten Mischdateien der Fall, die in der polizeilichen Praxis häufig vorkommen.[72] Teilweise sieht die Polizei aufgrund dieser Regelung

---

[65] Vgl. BT-Drs. 13/9718, S. 28; BT-Drs. 14/1484, S. 31; vgl. auch *Matheis*, S. 267, 289 f.

[66] In früheren Entwürfen war die Vorschrift enger formuliert und auf Zwecke der Gefahrenabwehr beschränkt gewesen; BT-Drs. 13/9718, S. 9; BT-Drs. 14/1484, S. 9; vgl. dazu *Brodersen*, NJW 2000, 2536 (2539); *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, § 481 Rn. 6; kritisch zu der Weite der Regelung *Singelnstein*, in: MüKo-StPO, 2019, § 481 Rn. 6 m.w.N.

[67] Vgl. BT-Drs. 14/1484, S. 31; *Gieg*, in: KK-StPO, 9. Aufl. 2023, § 481 Rn. 1; *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, § 481 Rn. 6.

[68] Eine Strafverfolgungsbehörde in diesem Sinne ist dabei auch die zu repressiven Zwecken handelnde Polizei; *Weßlau*, in: SK-StPO, 4. Aufl. 2013, Vor § 483 Rn. 3.

[69] Die Verarbeitung personenbezogener Daten in Akten erfasst die Regelung nicht; *Wittig*, in: BeckOK-StPO, 47. Ed. 2023, § 483 Rn. 1. Durch die Beschränkung auf das für Zwecke des Strafverfahrens Erforderliche erlaubt die Regelung regelmäßig keine Speicherung von Daten über den Abschluss des konkreten Verfahrens hinaus; BT-Drs. 14/1448, S. 32; *Zöller*, S. 216.

[70] § 484 Abs. 1 StPO legt die Grunddaten fest, die für Zwecke künftiger Strafverfahren gespeichert werden dürfen, ohne dass weitere Voraussetzungen erfüllt sein müssten. Abs. 2 der Vorschrift ermöglicht die Speicherung weiterer personenbezogenen Daten unter der zusätzlichen Voraussetzung einer Wiederholungsgefahr; vgl. dazu *Zöller*, S. 101 f.

[71] § 484 Abs. 1 StPO regelt die Voraussetzung der Erforderlichkeit nicht ausdrücklich und sie ergibt sich (anders als nach alter Rechtslage) auch nicht mehr mittelbar aus dem Regelungszusammenhang mit § 489 StPO. Jedenfalls in verfassungskonformer Auslegung der Vorschrift ist jedoch die Erforderlichkeit der Datenspeicherung zur Zweckerfüllung vorauszusetzen.

[72] Siehe oben Teil 1 A. III. 2.

eine Trennung von Daten in polizeilichen Informationssystemen nach der Verwendung für präventive und repressive Zwecke nicht für notwendig an.[73] § 484 Abs. 4 StPO sieht bei der Verarbeitung personenbezogener Daten, die für Zwecke künftiger Strafverfahren von der Polizei gespeichert werden, die Anwendung des Polizeirechts vor.

Die Befugnisse in der Strafprozessordnung zur Speicherung von Daten wurden im November 2019 an die Vorgaben der JI-Richtlinie angepasst.[74] Dabei erfolgte neben redaktionellen Änderungen[75] eine Änderung der Regelung zur Speicherung von personenbezogenen Daten für Zwecke konkreter Strafverfahren. § 483 Abs. 1 Satz 2 StPO ermöglicht die Speicherung von Daten in neuen polizeilichen Informationssystemen.[76] Informationssysteme wie das neue „Datenhaus", die nicht in Dateien gegliedert sind, fallen begrifflich nicht unter die vorherigen Speicherungsregelungen der Strafprozessordnung, die sich auf Dateien bzw. Dateisysteme als Speicherungsressourcen bezogen.[77] Für das neue Informationssystem des Bundeskriminalamts ist damit § 483 Abs. 1 Satz 2 StPO maßgeblich, soweit darin Daten für konkrete Strafverfahren gespeichert werden. Perspektivisch könnten aber auch etwa Informationssysteme von Bundespolizei und Zollfahndung unter die Regelung fallen.[78] § 483 Abs. 1 Satz 2 und 3 StPO legen Bedingungen für die Regelung dieser Informationssysteme fest. Für das Informationssystem des BKAG sind diese durch §§ 13 ff. BKAG erfüllt.[79] So müssen für dieses die Kennzeichnung der Daten, die Zugriffsberechtigungen sowie Fristen zur Prüfung, ob gespeicherte Daten zu löschen sind sowie die Speicherungsdauer der Daten geregelt sein.[80] Für die Speicherung von Daten in dem neuen Informationssystem gelten damit im Vergleich zu der Speicherung in Dateisystemen erhöhte Anforderungen.

Zudem enthält § 81b Abs. 1 Var. 2 StPO, der die Erhebung und Speicherung bestimmter Daten für die Zwecke des Erkennungsdienstes außerhalb konkreter Verfahren erlaubt, eine Befugnis zur kriminalbehördlichen Informationsordnung. Die Zwe-

[73] Vgl. BVerfGE 120, 378 (422).

[74] Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20. November 2019; BGBl. I, S. 1724; vgl. hierzu *Singelnstein*, NStZ 2020, 639 ff.

[75] So wurde etwa der Begriff Datei in den Regelungen durch den Begriff Dateisystem (zur Anpassung an das neue Informationssystem des Bundeskriminalamts) und der Begriff Verwendung durch den Begriff Verarbeitung (zur Anpassung an die unionsrechtliche datenschutzrechtliche Terminologie) ersetzt.

[76] Vgl. BR-Drs. 433/18, S. 72.

[77] Vgl. BT-Drs. 19/4671, S. 66.

[78] Vgl. BfDI, Stellungnahme StPO 2019, S. 7.

[79] Vgl. BT-Drs. 19/4671, S. 66.

[80] Die spezifischen Anforderungen an den Gehalt der Regelungen in § 483 Abs. 1 Satz 3 StPO wurden dabei im Wesentlichen aufgrund eines Vorschlags des BfDI eingefügt; vgl. BT-Drs. 19/11190, S. 9; BfDI, Stellungnahme StPO 2019, S. 5 ff.

cke des Erkennungsdienstes sind dabei ein Spezialfall der Vorbereitung auf die Strafverfolgung.[81] Die Aufbewahrung entsprechender Unterlagen ist ebenso wie die Speicherung von Daten in polizeilichen Informationssystemen keine strafprozessuale Maßnahme im klassischen Sinne, da sie nicht auf ein konkretes Verfahren bezogen ist und keinen Anfangsverdacht erfordert.[82] Einen ähnlichen vorsorgenden Charakter hat § 81g Abs. 1 Satz 1 StPO, der die Entnahme von Körperzellen zur Identitätsfeststellung in künftigen Strafverfahren erlaubt.[83]

Speziell für die Aufbewahrung und Speicherung von Akten – einschließlich elektronischer Register und Karteien[84] – der Gerichte und Staatsanwaltschaften nach Beendigung des Verfahrens gilt schließlich das Justizaktenaufbewahrungsgesetz (JAktAG), das jedoch die Bestimmung der wesentlichen Vorgaben durch eine Verordnungsermächtigung (§ 2 JAktAG) der Bundesregierung überlässt.

b. Problematische Fallgruppen

In einzelnen Fallgruppen erscheint die Speicherung von personenbezogenen Daten in kriminalbehördlichen Informationssystemen als besonders problematisch. Daher ist es notwendig, erhöhte Anforderungen an sie zu stellen. Zwei dieser Fallgruppen werden im Folgenden näher betrachtet: Die Speicherung besonders stigmatisierender und diskriminierungsträchtiger Merkmale (aa)) sowie die Speicherung von Daten zu Personen, die freigesprochen wurden oder gegen die das Strafverfahren eingestellt wurde (bb)).

aa) Speicherung besonders stigmatisierender und diskriminierungsträchtiger Merkmale

Während das Datenschutzrecht im Ausgangspunkt den Umgang mit jeglicher Art von personenbezogenen Daten als gleichermaßen relevant betrachtet, sind bestimmte Informationen naturgemäß besonders geeignet, die betroffenen Personen zu stigmatisieren und zu kriminalisieren. Praktisch kommt dies etwa bei einer Speicherung unter Kennzeichnung einer Person als „Gewalttäter" oder „Intensivtäter" in Betracht, wenn Personen in Folge der Speicherung als solche angesprochen werden. Andere Merkmale ermöglichen in besonderem Maße eine negative Behandlung anhand sozialer Kategorien – also eine Diskriminierung. Dies gilt etwa für Angaben über die Herkunft oder Religion einer Person.

---

[81] Vgl. BVerwG NJW 1983, 1338 (1339); BVerwG NJW 1983, 772; BVerwG NJW 2006, 1225 (1226); *Fuß*, in: FS Wacke, S. 305 (317); *Rudolph*, S. 39 ff.

[82] BVerwG NJW 1967, 1192; BVerwG NJW 2006, 1225 (1226); *Busch/Funk/Kauß/Narr/Werkentin*, S. 197; anders noch BVerwG NJW 1956, 234 (235); vgl. dazu auch *Gärditz*, S. 99 ff.

[83] Vgl. hierzu nur *Eisenberg/Singelnstein*, GA 2006, 168 ff.; *Gaede*, in: FS Merkel, S. 1283 ff.; *Gärditz*, S. 103 ff.; *Volk*, NStZ 1999, 165 (167).

[84] § 1 Satz 2 JAktAG.

Zumindest für bestimmte potentiell diskriminierende Angaben gilt auch rechtlich ein besonderer Schutz, der sich einerseits aus den verfassungsrechtlichen Diskriminierungsverboten aus Art. 3 Abs. 3 GG und Art. 21 Abs.1 GRCh[85] und andererseits aus dem Schutz besonderer personenbezogener Daten gemäß Art. 10 JI-RL sowie den Vorschriften zu dessen Umsetzung ergibt.

Für besondere personenbezogene Daten im Sinne von Art. 10 JI-RL – also konkret Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung – stellen § 48 Abs. 1 BDSG und entsprechenden Vorschriften der Landesdatenschutzgesetze erhöhte Anforderungen an die Verarbeitung. Ihre Speicherung, Strukturierung und sonstige Verarbeitung ist nur zulässig, wenn dies für die Aufgabenerfüllung unbedingt erforderlich ist. Durch den Zusatz „unbedingt" wird hier ein strengerer Maßstab angelegt als bei den allgemeinen Befugnissen zur Speicherung von Daten.[86] Wie genau jedoch die Prüfung der Erforderlichkeit sich durch diesen strengeren Maßstab verändert, ist nicht vollständig geklärt. Naheliegend erscheint es, den Zusatz derart zu verstehen, dass die verarbeitende Stelle von der Speicherung für die Erfüllung ihrer Aufgaben in besonderem Maße abhängig,[87] diese also hierfür „beinahe unverzichtbar"[88] ist. Dabei besteht aber weiterhin eine Einschätzungsprärogative der speichernden Behörde, die zwar einen erhöhten Aufwand für die Begründung betreiben muss, aber praktisch wahrscheinlich weiterhin in vielen Fällen wird darlegen können, warum gewisse Daten für ihre Arbeit quasi unabdingbar sind.[89]

Einige der in Art. 10 JI-RL genannten Merkmale finden sich auch in den verfassungsrechtlichen Diskriminierungsverboten aus Art. 3 Abs. 3 GG und Art. 21 Abs. 1 GRCh wieder. Namentlich gilt dies etwa für Angaben über Herkunft, politische Anschauungen bzw. Meinungen und Religion eines Menschen. Art. 3 Abs. 3 GG verbietet eine Benachteiligung wegen dieser und anderer in der Vorschrift genannter Merkmale. Daraus lässt sich für das Verwaltungshandeln ein grundsätzliches Verbot folgern, an diese Merkmale anzuknüpfen.[90] Eine Rechtfertigung für derartige Anknüpfungen

[85] Siehe hierzu oben Teil 1 C. III. 2. a.

[86] *Kampert*, in: Sydow/Marsch, 3. Aufl. 2022, § 48 BDSG Rn. 13.

[87] *Albers/Schimke*, in: BeckOK-Datenschutzrecht, 44. Ed. 2023, § 48 BDSG Rn. 26.

[88] *Schwichtenberg*, in: Kühling/Buchner, 3. Aufl. 2020, § 48 BDSG Rn. 3.

[89] Für die Einschränkung der Einschätzungsprärogative durch den Begriff „unbedingt" *F. Braun*, in: Gola/Heckmann, 3. Aufl. 2022, § 48 BDSG Rn. 9.

[90] Siehe oben Teil 1 C. III. 2. a.

kann sich nur aus kollidierendem Verfassungsrecht oder besonders schwerwiegenden Gründen ergeben.[91]

Eindeutig geklärt ist die Reichweite des Anknüpfungsverbotes aus Art. 3 Abs. 3 GG nicht. Seine Anforderungen könnten aber auch für die Speicherung und Strukturierung von Daten gelten. Ein grundsätzlich verbotenes Anknüpfen soll dann vorliegen, wenn im Hinblick auf ein bestimmtes Ergebnis bzw. als Voraussetzung für eine Rechtsfolge auf eines der in Art. 3 Abs. 3 GG genannten Merkmale abgestellt wird.[92] Werden Daten gespeichert oder strukturiert, die entsprechende Merkmale enthalten, folgen daraus noch keine Rechtsfolgen. Diese Handlungen dienen in erster Linie dazu, um künftige Maßnahmen vorzubereiten. Allerdings stellen sie die Weichen für Maßnahmen, die von einigem Gewicht für die Betroffenen sein können und unmittelbar an die in den Informationsressourcen vorhandenen Merkmale anknüpfen. Dies spricht dafür, dass bereits in der Speicherung eines Merkmals eine potentiell unzulässige Anknüpfung liegen kann.

Dass Art. 3 Abs. 3 GG für die Speicherung von Daten in sicherheitsbehördlichen Informationsressourcen relevant sein kann, hat auch das Bundesverfassungsgericht anerkannt. In seiner ersten Entscheidung zur Antiterrordatei erwähnte es den verfassungsrechtlichen Diskriminierungsschutz im Zusammenhang mit der Aufnahme religionsbezogener Merkmale in Datenbanken und begründete diesbezüglich erhöhte Anforderungen. Für die Berücksichtigung entsprechender Daten sei „von Verfassungs wegen eine zurückhaltende Umsetzung geboten."[93] Dem sei „dadurch Rechnung zu tragen, dass die Aufnahme entsprechender Angaben nicht über eine lediglich identifizierende Bedeutung hinausgeht."[94] Daraus lässt sich folgern, dass nach Art. 3 Abs. 3 Satz 1 GG geschützte Merkmale ohne besondere Rechtfertigung nicht in Datenbanken vorgehalten werden dürfen, um diese zur Grundlage einer Bewertung zu machen.

Im Ergebnis gelten damit zumindest für in Art. 10 JI-RL und Art. 3 Abs. 3 GG aufgeführte Merkmale schon bei deren Speicherung erhöhte rechtliche Anforderungen. Die Anforderungen, dass die Speicherung „unbedingt" erforderlich ist oder besonders schwerwiegende Gründe vorliegen, die sie rechtfertigen, sind allerdings wenig konkret und daher nur eingeschränkt geeignet, um kriminalbehördliche Datenspeicherungen wirksam einzugrenzen.

---

[91] *Kischel*, in: BeckOK-GG, 55. Ed. 2023, Art. 3 Rn. 214.

[92] *Boysen*, in: von Münch/Kunig, GG, 7. Aufl. 2021, Art. 3 Rn. 126; *Kischel*, in: BeckOK-GG, 55. Ed. 2023, Art. 3 Rn. 212a.

[93] BVerfGE 133, 277 (360).

[94] BVerfGE 133, 277 (360).

bb) Speicherung von Daten aus Strafverfahren nach Freispruch oder Einstellung

Weitere rechtliche Einschränkungen ergeben sich für die Speicherung von Daten, die aus abgeschlossenen Strafverfahren stammen, die mit einem Freispruch oder einer Einstellung endeten. Die Weiterverarbeitung derartiger Daten kann in Konflikt mit der Unschuldsvermutung geraten.

Das Bundesverfassungsgericht sieht die Speicherung personenbezogener Daten aus abgeschlossenen Strafverfahren allerdings regelmäßig nicht im Konflikt mit der Unschuldsvermutung: „Die weitere Aufbewahrung und Verwendung von Daten aus Strafverfahren zur vorbeugenden Straftatbekämpfung" stelle „keinen Nachteil [...] dar, der einem Schuldspruch oder einer Strafe gleichkäme", da diese nur von einem Tatverdacht, nicht aber von einer Schuldfeststellung abhängig sei.[95] Vor der Strafverfolgung oder der Speicherung von Daten zur vorbeugenden Verbrechensbekämpfung schützt die Unschuldsvermutung nicht, sofern es hierfür einen Anlass gibt. Die Datenspeicherung in den Kriminalakten kann nach der Rechtsprechung des Bundesverfassungsgerichts demnach auch zulässig sein, wenn ein Strafverfahren eingestellt wurde oder ein Freispruch erfolgt ist.[96]

Auf dieser Grundlage nimmt die verwaltungsgerichtliche Rechtsprechung an, dass die Berücksichtigung von Verdachtsgründen, die nach einer Verfahrensbeendigung durch Freispruch oder Einstellung fortbestehen, keine Schuldfeststellung oder -zuweisung darstellt, wenn und soweit sie eine Prognose stützt, dass die Speicherung von Daten für künftige Strafverfahren erforderlich sein könnte.[97] Einfachgesetzlich finden die Anforderungen Niederschlag in § 18 Abs. 5 BKAG. Demnach ist die Weiterverarbeitung von Daten zu einem Beschuldigten nur dann unzulässig, wenn er rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt wird und sich zusätzlich aus den Gründen der Entscheidung ergibt, dass er die Tat nicht oder nicht rechtswidrig begangen hat.[98]

Die verwaltungsgerichtliche Rechtsprechung und die Regelung in § 18 Abs. 5 BKAG stehen jedoch zumindest im Fall eines Freispruchs im Widerspruch zu der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte. Danach ist die Annahme eines (Rest-)Verdachts nach einem rechtskräftigen Freispruch unzulässig.[99]

---

[95] BVerfG NJW 2002, 3231 (3232).

[96] BVerfG NJW 2002, 3231 (3232).

[97] BVerwG NJW 2011, 405 (406); OVG Saarlouis ZD 2018, 233 (234).

[98] Diese Regelung entspricht im Wesentlichen § 8 Abs. 3 BKAG aF.

[99] EGMR (Kammer), Urteil vom 25. August 1993, Sekanina gegen Österreich, No. 13126/87 § 30; EGMR (3. Sektion), Urteil vom 21. März 2000, Asan Rushiti gegen Österreich, No. 28389/95 § 27 ff.;

Der Gerichtshof unterscheidet hierbei nicht danach, was sich aus den Gründen des Freispruchs zum Tatvorwurf ergibt. Auch wenn sich aus der Entscheidung noch Raum für einen Restverdacht ergibt, kommt es danach nur darauf an, dass der Freispruch das Verfahren beende und es gebieten würde, die*den Freigesprochene*n formal als unschuldig zu behandeln.[100] Dies ist angesichts des Charakters des verfahrensabschließenden Freispruchs als „Bestätigung der Unschuldsvermutung“[101] konsequent und überzeugend. Der oder dem Betroffenen steht kein wirksames Instrument zur Verfügung, seine Unschuld feststellen zu lassen und einen Restverdacht auszuräumen.[102] Der Freispruch ist gewissermaßen das höchste, was sie oder er in der Situation erreichen kann. Daher ist dem Freispruch im Strafverfahren ein hohes Gewicht beizumessen. Die oder der Freigesprochene sollte im Ergebnis durch Abschluss des Verfahrens formell mit der- bzw. demjenigen gleichgestellt werden, gegen die bzw. den von Anfang an kein Verdacht bestand. Auch der Gedanke der Resozialisierung von Freigesprochenen spricht dafür, die Annahme eines Restverdachts, auf den die Speicherung von Daten gestützt werden kann, nicht zuzulassen.[103] Daher ist im Ergebnis der Freispruch aus Mangel an Beweisen dem Freispruch wegen erwiesener Unschuld in seinen Folgen für die Datenhaltung gleichzustellen.[104]

Auch bezüglich der Einstellung von Verfahren sind § 18 Abs. 5 BKAG und die Rechtsprechung zur Annahme eines Restverdachts zumindest in praktischer Hinsicht problematisch. Zwar erscheint es nicht geboten, eine Verfahrenseinstellung nach § 170 Abs. 2 StPO einem Freispruch gleichzusetzen und damit eine Speicherung auf Grundlage eines Restverdachtes für unzulässig halten. In der Praxis wird sich aus einer Einstellung aber nur in seltenen Fällen, wie von § 18 Abs. 5 BKAG verlangt, ergeben, dass der Beschuldigte die Tat nicht oder nicht rechtswidrig begangen hat, selbst wenn ein solcher Befund ihr zugrunde lag. Dies ist unter anderem Folge von Nr. 88 RiStBV, wonach „[i]n der Mitteilung an den Beschuldigten nach § 170 Abs. 2 StPO [...] die Gründe der Einstellung nur auf Antrag und dann auch nur soweit bekannt zu geben [sind], als kein schutzwürdiges Interesse entgegensteht.“ Hieraus wird sich in der Regel keine positive Feststellung ergeben, dass der Beschuldigte die Tat nicht begangen hat.[105] Er kann

EGMR (5. Sektion), Urteil vom 25. Januar 2018, Bikas gegen Deutschland, No. 76607/13 § 44 = NJW 2019, 203 (204); vgl. dazu *Stuckenberg*, in: FG Hilger, S. 25 (48).

[100] *Harrendorf/König/Voigt*, in: Meyer-Ladewig/Nettesheim/von Raumer, EMRK, 5. Aufl. 2023, Art. 6 Rn. 197.

[101] *Tiemann*, in: KK-StPO, 9. Aufl. 2023, § 260 Rn. 25; vgl. auch *Kühl*, S. 30; *Schmitt,* in: Meyer-Goßner/Schmitt, StPO, 65. Aufl. 2022, § 260 Rn. 17.

[102] Vgl. *Stuckenberg*, in: FG Hilger, S. 25 (38).

[103] *Fuß*, in: FS Wacke, S. 305 (323).

[104] So auch BfDI, 26. Tätigkeitsbericht 2015-2016, S. 109; *Fuß*, in: FS Wacke, S. 305 (323); vgl. auch *Kestel*, StV 1997, 266 (268); *Stuckenberg*, in: FG Hilger, S. 25 (51).

[105] *Ogorek*, ZRP 2023, 86 (88).

sich damit gegenüber den Behörden nicht auf eine derartige Sachlage berufen. Auch die internen Vermerke der Behörden werden praktisch selten entsprechende Feststellungen enthalten. So umfasst die Pflicht der Staatsanwaltschaft zur Benachrichtigung der Polizei über den Ausgang des Verfahrens nach § 482 Abs. 2 Satz 1 StPO nicht die näheren Gründe für eine Einstellung.[106]

2. Der Abruf

Der Abruf von Daten erweist sich vor allem dann als rechtlich relevanter Vorgang, wenn er über die Grenzen von Behörden hinausgeht. Der Abruf von Daten aus den eigenen Systemen einer Behörde stellt, sofern personenbezogene Daten betroffen sind, zwar auch einen regelungsbedürftigen Vorgang dar. Er lässt sich aber auf die Generalklauseln zur Datenverarbeitung in den jeweils einschlägigen Gesetzen stützen.

Der Abruf von Daten aus einem System, das nicht bei der eigenen Behörde liegt, ist als zweigliedriger Vorgang sowohl von Seiten der übermittelnden als auch von Seiten der abrufenden Behörde rechtfertigungsbedürftig („Doppeltür"-Modell).[107] Die Weitergabe und der Abruf beeinträchtigen die informationelle Selbstbestimmung bzw. das Datenschutzgrundrecht der betroffenen Person und bedürfen jeweils einer Rechtsgrundlage. Die Regelungen in den Polizeigesetzen und der Strafprozessordnung machen die Zulässigkeit dieser Vorgänge – ähnlich wie bei der Speicherung von Daten – im Wesentlichen davon abhängig, ob Übermittlung und Abruf für die Erfüllung kriminalbehördlicher Aufgaben erforderlich sind.[108]

Derartige Vorgaben hegen primär die Verfügbarkeit von Daten vor allem im Sinne des Datenschutzes ein. Ihre Ziel ist es nicht, die Verfügbarkeit zu vereinfachen. Eine Regelung wie der europäische Grundsatz der Verfügbarkeit von Daten, nach dem bestimmte Daten, die in einem Mitgliedsstaat für Zwecke der Gefahrenabwehr oder für Zwecke der Strafverfolgung gespeichert sind, unter gleichberechtigten Voraussetzungen auch in allen anderen Mitgliedsstaaten verfügbar sein sollen,[109] existiert im deutschen Recht nicht. Im Sinne einer möglichst schnellen und einfachen Verfügbarkeit von Daten sind jedoch in einigen Fällen Verfahren des automatisierten Abrufs von Daten geregelt. In derartigen Fällen kann die erhebende Stelle Daten jederzeit eigenständig

[106] Siehe zu der Möglichkeit einer Schärfung der diesbezüglichen rechtlichen Vorgaben unten Teil 3 D. III. 1. b.

[107] BVerfGE 130, 151 (184); BVerfGE 141, 220 (333 f.); *Schwabenbauer,* in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 232 ff.

[108] § 25 Abs. 1 BKAG; § 32 Abs. 1 BPolG; § 477 Abs. 1 StPO; § 59 BWPolG; Art. 56 Abs. 1 Nr. 1 BayPAG; § 44 ASOG Bln; § 42 Abs. 1 BbgPolG; § 55 Abs. 1 BremPolG; § 40 HmbPolDVG; § 22 Abs. 1 HSOG; § 39b Abs. 1 SOG MV; § 41 NPOG; § 27 Abs. 1 PolG NRW; § 57 Abs. 1 POG RP; § 44 SPolDVG; § 27 Abs. 1 SOG LSA; § 192 Abs. 1 SchlHLVwG; § 41 Abs. 1 ThürPAG.

[109] Siehe unten 3.

abrufen; eine Überprüfung durch die übermittelnde Stelle findet nicht statt.[110] So sind beispielsweise die Staatsanwaltschaften nach § 29 Abs. 6 Satz 2 BKAG befugt, bestimmte Fahndungsausschreibungen, Daten über Freiheitsentziehungen und Daten aus dem DNA-Analyse-System im automatisierten Verfahren vom Bundeskriminalamt abzurufen.

Die Möglichkeiten des Abrufs von polizeilichen Daten durch die Staatsanwaltschaften waren lange umstritten.[111] Diese besondere Konstellation des Abrufs von Daten unter Kriminalbehörden ist nicht nur praktisch besonders relevant, sondern auch besonders problematisch. Über Jahre hatte die Polizei den Staatsanwaltschaften den Zugriff auf ihr wichtigstes System INPOL verwehrt, obwohl sich in dem System viele Daten fanden, die aus der Strafverfolgung stammten und auch von Relevanz für künftige Strafverfolgung und ihre Vorbereitung waren. Die Polizei argumentierte, dass der Staatsanwaltschaft deswegen kein Zugang zu INPOL gewährt werden könne, weil das System auch zu Zwecken der Gefahrenabwehr gespeicherte Daten enthalte und ein Zugriff der Staatsanwaltschaft daher unverhältnismäßig sei.[112] Diese Vermischung wurde in diesem Zusammenhang bisweilen als unvermeidbar dargestellt,[113] was aber nicht überzeugt. Es mag zwar praktisch aufwändig sein, die Speicherung von Daten zu präventiven und repressiven Zwecken zu trennen, technisch unmöglich erscheint es aber nicht.[114] Der hier erkennbare Versuch, rechtliche Wertungen mit vorgeblichen technischen Realitäten auszuhebeln, erscheint im Ergebnis bedenklich.

Die Polizei handelt bei ihrer Tätigkeit in der Strafverfolgung allein auf Grund staatsanwaltschaftlicher Kompetenz. Der Staatsanwaltschaft kommt auf diesem Bereich die

[110] *M. Müller/Schwabenbauer,* in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 888.
[111] Siehe oben Teil 1 B. IV.
[112] *Riegel*, NJW 1983, 656 (659); kritisch hierzu *K. Merten*, NStZ 1987, 10 (12); vgl. auch *Ernesti*, ZRP 1986, 57 (58).
[113] *Riegel*, NJW 1983, 656 (659).
[114] So auch *Eisenberg/Kölbel*, § 29 Rn. 59; *Wolter*, GA 1988, 49 (62); *Zöller*, S. 173.

Sachleitungsbefugnis zu. Dass die Staatsanwaltschaft als „Herrin des Ermittlungsverfahrens“[115] nicht gleichzeitig „Herrin der Daten“[116] war, wurde in diesem Zusammenhang zurecht immer wieder kritisiert[117] und die Einräumung eines gesetzlichen Zugriffsrechts gefordert.[118] Die Kontrolle von zu Zwecken der Strafverfolgung gespeicherten Daten durch die Polizei konterkariert die Sachleitungsbefugnis der Staatsanwaltschaft.

Die Diskussion um die Rechte der Staatsanwaltschaften zum Abruf polizeilicher Systeme hat unter anderem aufgrund der mittlerweile erfolgten Regelung von staatsanwaltschaftlichen Zugriffsrechten ihre frühere Intensität verloren. Allerdings bleibt es dabei, dass die Polizei in der kriminalbehördlichen Informationsordnung eine dominante Stellung innehat, die für die Staatsanwaltschaften die Verfügbarkeit von für sie relevanten Daten erschweren kann. Die aktuell laufende Neustrukturierung der polizeilichen Informationsordnung[119] könnte diese Dominanz der Polizei innerhalb der kriminalbehördlichen Informationsordnung noch einmal verstärken.[120] Die technischen Mittel zur Speicherung und Auswertung von Informationen durch die Polizei erweitern sich hierdurch voraussichtlich, ohne dass die Staatsanwaltschaften in diesen Prozess näher einbezogen werden.

3. Der Grundsatz der Verfügbarkeit im Unionsrecht

Wie bereits erwähnt, gibt es im nationalen Polizei- und Strafprozessrecht keine Regelungen, die die Verfügbarkeit von Daten über Behördengrenzen hinaus positiv absichern. Die Regelungen zu Abruf und Übermittlung dienen in erster Linie dazu, die Verfügbarkeit im Sinne der Interessen der Datensubjekte einzuschränken. Daher wird

---

[115] Vgl. generell zum problematischen Verhältnis von Polizei und Staatsanwaltschaft im Ermittlungsverfahren *Albers*, Determination, S: 70 f.; *Gössel*, GA 1980, 325 (346 f.).

[116] Kritisch zu diesem Begriff *Ringwald*, S. 54 f.

[117] BfDI, Stellungnahme BKAG 2018, S. 17; *Schaefer*, in: FS Hanack, S. 191 (196 f.); *Schweckendieck*, ZRP 1989, 125 (127); *Uhlig*, DRiZ 1986, 247 (248 f.); *Zöller*, S. 173; vgl. mit diversen Lösungsvorschlägen wie etwa der Schaffung einer Ermittlungspolizei unter der Organisationshoheit der Staatsanwaltschaft *Lilie*, ZStW 106 (1994), 625 (641 ff.). *Weßlau*, in: SK-StPO, 4. Aufl. 2013, Vor § 483 Rn. 4 sah in dem Aufbau der polizeilichen Informationsordnung als Machtinstrument einen Versuch der Polizei, „sich aus dem Weisungsverhältnis zur Staatsanwaltschaft zu lösen und die Aufgabe der zugleich präventiv und repressiv ausgerichteten Verbrechensbekämpfung eigenverantwortlich wahrzunehmen.“

[118] *Wolter*, GA 1988, 49 (61); so konkret in § 163 Abs. 4 AE-EV: „Die Staatsanwaltschaft hat jederzeit Zugang zu personenbezogenen Daten, die im Zusammenhang mit einem Strafverfahren oder einer allfälligen künftigen Strafverfolgung (§ 150 AE-EV) erlangt und gespeichert worden sind. Dies gilt auch für Daten, die in Dateien der Polizei gespeichert worden sind.“; abgedruckt bei Arbeitskreis AE, S. 16.

[119] Siehe oben Teil 1 B. III. 3.

[120] So auch *Singelnstein*, in: MüKo-StPO, 2019, Vorbemerkung zu § 483 Rn. 4.

im Folgenden ein Blick über das nationale Recht hinaus auf den Grundsatz der Verfügbarkeit aus dem Recht der Europäischen Union geworfen.[121] Dieser dient dazu, den Zugang zu Informationen über die Grenzen von Mitgliedstaaten hinaus zu gewährleisten. Der Grundsatz der Verfügbarkeit ist im Primärrecht der Europäischen Union nicht direkt verankert,[122] wird aber von mehreren Akten des Sekundärrechts gestützt.

Nach diesem Grundsatz sollen bestimmte Daten, die in einem Mitgliedsstaat für Zwecke der Gefahrenabwehr oder für Zwecke der Strafverfolgung gespeichert sind, ohne Durchführung eines Rechtshilfeverfahrens[123] auch in allen anderen Mitgliedsstaaten verfügbar sein.[124] Dabei sollen Strafverfolgungsbehörden aus anderen Mitgliedstaaten sowie Europol und Eurojust für den Datenzugriff keine höheren Anforderungen erfüllen müssen als die Behörden des Staates, in dem die Informationen gespeichert sind.[125] Der Grundsatz der Verfügbarkeit soll so als „Bindemittel" einer integrierten europäischen Informationsordnung zu Sicherheitszwecken dienen.[126] Er erscheint als „Prinzip des gleichberechtigten Zugangs" besser beschrieben denn als „Grundsatz der Verfügbarkeit", da er keine direkte Verfügbarkeit von Informationen begründet.[127] Der Zugang muss weiterhin von den jeweiligen speichernden Stellen gewährt werden.

Erstmals[128] formulierte der Rat den Grundsatz der Verfügbarkeit im Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union vom 3. März 2005.[129] Im Oktober 2005 legte die Kommission einen Vorschlag für einen Rahmenbeschluss über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit vor.[130] Eine erste rechtsverbindliche Ausprägung fand der Grundsatz

---

[121] Hierzu ausführlich *Böse*, S. 39 ff.; *Schmidt*, S. 45 ff.

[122] *F. Meyer*, in: Kugelmann/Rackow, S. 41 (48 f.). Ein gewisser Anknüpfungspunkt hierfür findet sich in dem Grundsatz der loyalen Zusammenarbeit nach Art. 4 Abs. 3 EUV; vgl. *Schöndorf-Haubold*, S. 131.

[123] Vgl. zu den Schwierigkeiten bei Rechtshilfeverfahren KOM(2005) 490 endg., S. 3; *F. Meyer*, NStZ 2008, 188 f.; *Zöller*, ZIS 2011, 64.

[124] Vgl. *Würtenberger*, in: FS Steiner, S. 948 (953 f.).

[125] KOM(2005) 490 endg., S. 7; *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 20; *Böse*, S. 40 f., 47 f.

[126] *F. Meyer*, in: Kugelmann/Rackow, S. 41 (50); vgl. auch *F. Meyer*, NStZ 2008, 188 (194) („Rahmen und Fugenmasse").

[127] Vgl. *F. Meyer*, NStZ 2008, 188 (190).

[128] Zuvor hatte die Kommission bereits im Jahr 2004 in einer Mitteilung an den Rat und das Europäische Parlament betreffend den verbesserten Zugang zu Informationen für Strafverfolgungsbehörden das Ziel eines besseren Datenzugriffs und einer Einführung „Intelligence"-gestützter Strafverfolgung auf EU-Ebene formuliert; KOM(2004) 429 endg., S. 6 ff.

[129] ABl. EU C 53, S. 1 (7 f.). Dieses enthielt den Aufruf an die Kommission, noch im gleichen Jahr eine gesetzliche Regelung hierzu zu entwickeln, die im Jahr 2008 Wirkung entfalten sollte; vgl. in der Folge den Aktionsplan des Rates und der Kommission zur Umsetzung des Haager Programms vom 12. August 2005; ABl. EU C 198, S. 1 (10).

[130] KOM(2005) 490 endg.

durch den Rahmenbeschluss 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union.[131] Nach dessen Abs. 3 stellen die Mitgliedstaaten „sicher, dass für die Zurverfügungstellung von Informationen und Erkenntnissen an die zuständigen Strafverfolgungsbehörden anderer Mitgliedstaaten Bedingungen gelten, die nicht strenger sind als die Bedingungen, die auf nationaler Ebene für die Zurverfügungstellung und Anforderung von Informationen und Erkenntnissen gelten."

Weiter geht der zunächst von sieben Mitgliedstaaten am 27. Mai 2005 in Prüm unterzeichnete Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration,[132] der mit Ratsbeschluss 2008/615/JI vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität[133] in das Recht der Europäischen Union überführt wurde. Der Prümer Vertrag erlaubt einen direkten Online-Zugriff auf bestimmte Indexdaten in Informationsressourcen der Vertragsstaaten.[134] Anders als im Zusammenhang mit dem Rahmenbeschluss 2006/960/JI ist die Verfügbarkeit von Daten aus anderen Staaten in diesem Zusammenhang nicht notwendigerweise mit einem Auskunftsersuchen verbunden.

In der Praxis werden zum Teil Defizite bei dem Austausch von Informationen und der Umsetzung des Grundsatzes der Verfügbarkeit ausgemacht.[135] Eine Rolle spielt dabei die teilweise fehlende Interoperabilität[136] der Informationssysteme der Mitgliedsstaaten sowie der Europäischen Union.[137] Die Verbesserung der Interoperabilität verschiedener Informationssysteme innerhalb der Europäischen Union ist schon seit den 2000er-Jahren ein politisches Anliegen.[138] Zuletzt wurde im Juni 2016 eine hochrangige Expertengruppe für Informationssysteme und Interoperabilität gegründet.[139] Im Mai

[131] ABl. EU L 386, S. 89. Dieser ging auf einen Vorschlag Schwedens aus dem Jahr 2004 zurück; vgl. dazu *Böse*, S. 39 f.

[132] BGBl. I 2006, S. 1458.

[133] ABl. EU L 210, S. 1; vgl. zur Umsetzung in Deutschland BGBl. I 2009, S. 2507.

[134] Vgl. dazu *Böse*, S. 43 f.; *Zöller*, ZIS 2011, 64 (66 f.).

[135] So wird nach *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 20 die Pflicht zur Weitergabe von Informationen nicht immer vorbehaltlos befolgt; vgl. auch KOM(2016) 205 endg., S. 3 ff.

[136] Hierunter wird die „Fähigkeit von Informationssystemen, Daten auszutauschen und die gemeinsame Nutzung von Informationen zu ermöglichen" verstanden; KOM(2016) 205 endg., S. 17. Dabei wird zwischen den Ebenen der technischen, semantischen, organisatorischen und rechtlichen Interoperabilität differenziert; KOM(2012) 735, S. 15.

[137] Vgl. *Ziercke*, Kriminalistik 2005, 700 (704).

[138] Vgl. KOM(2005) 597 endg.

[139] Vgl. KOM(2016) 205 endg., S. 17.

2017 legte sie ihren Abschlussbericht vor, in dem sie die Einführung neuer Instrumente[140] zur Verknüpfung von Informationen aus verschiedenen Ressourcen vorschlug.[141] Auf technischer Ebene soll die die seit Dezember 2012 tätige Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (eu-LISA)[142] die Verfügbarkeit[143] und Interoperabilität der Informationssysteme[144] sowie die Datenqualität[145] innerhalb der Systeme sicherstellen.

Die Pläne zur Herstellung der Interoperabilität der Informationssysteme und besseren Verfügbarkeit von Informationen haben eine hohe Relevanz für die Freiheitsrechte der Unionsbürger*innen.[146] Die durch die unionsweite Verfügbarkeit erleichterte Möglichkeit des Zugriffs auf personenbezogene Daten intensiviert die Beeinträchtigung des Datenschutzgrundrechts, die durch die Speicherung der Daten ohnehin erfolgt. Im Zusammenhang mit den laufenden Bemühungen zur Herstellung der Interoperabilität verschiedener Datenbanken ist auch zu beobachten, dass Daten aus Systemen, die zu Zwecken des Grenzmanagements oder anderen Zwecken dienen, der Strafverfolgung zugeführt werden können.[147] Die Ausweitung der Zwecke dieser Datenbestände ist datenschutzrechtlich kritisch zu begleiten.

B. Die Verknüpfbarkeit von Informationsbeständen

Eine weitere wichtige Anforderung an kriminalbehördliche Informationssysteme aus Sicht ihrer Anwender*innen ist es, die darin gespeicherten Daten miteinander verknüpfen zu können.

---

[140] Konkret ein Europäisches Suchportal, einen gemeinsamen Dienst für den Abgleich biometrischer Daten und einen gemeinsamen Speicher für Identitätsdaten.

[141] High-level expert group on information systems and interoperability, S. 40.

[142] Ihre Rechtsgrundlage ist die Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates vom 14. November 2018 über die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Beschlusses 2007/533/JI des Rates sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011 (eu-LISA-VO) (ABl. EU L 295, S. 99). Die Agentur war durch Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. EU L 286, S. 1) errichtet worden. Vgl. zu der Tätigkeit von eu-LISA im Überblick *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 190 ff.

[143] Art. 2 lit. e) eu-LISA-VO; vgl. auch *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 191.

[144] Art. 1 lit. b), Art. 13 eu-LISA-VO.

[145] Art. 1 lit. a), Art. 12 eu-LISA-VO

[146] Vgl. *Schöndorf-Haubold*, S. 133.

[147] Wissenschaftlicher Dienst des Europäischen Parlaments, Europäische Informationssysteme im Bereich Justiz und Inneres, 2017, S. 1; vgl. auch *Töpfer*, vorgänge 2019, 135 ff.

*I. Anforderungen aus Sicht der Anwender*innen*

Als Verknüpfbarkeit lässt sich die Möglichkeit verstehen, Querbezüge zwischen Datensätzen herzustellen, die innerhalb einer oder mehrerer Informationsressourcen vorhanden sind. Es kann hierbei um einfache Übereinstimmungen von personenbezogenen Daten wie Namen oder Geburtsdaten gehen – so wie bei dem Datenabgleich in *Fall 3*, durch den es aufgrund von übereinstimmenden Geburtsdaten und Aliasnamen zu einer Verwechslung kommt. Moderne Informationstechnologien ermöglichen es aber auch, komplexe Beziehungen zwischen Personen, Sachen, Orten und Ereignissen zu erkennen.[148] So könnte etwa versucht werden, durch die Auswertung von Daten Muster zu finden, mit Hilfe derer sich die Mitglieder terroristischer Netzwerke identifizieren oder Radikalisierungsverläufe einzelner Personen nachvollziehen lassen. Die Verknüpfung und Auswertung von Daten kann auf diese Weise dazu dienen, Anhaltspunkte für neue kriminalbehördliche Maßnahmen zu gewinnen. Hierbei geht es oftmals um Maßnahmen weit im Vorfeld konkreter Schädigungen von Rechtsgütern, die in die Kategorie der vorausschauenden Polizeiarbeit („Predictive Policing")[149] fallen.

Die Anforderung der Verknüpfbarkeit von Informationen innerhalb der Datenbestände von Kriminalbehörden ist auch ein wesentlicher Antrieb hinter den aktuellen Bemühungen um eine Neuordnung der polizeilichen Informationsordnung. Während die aktuellen Systeme eine Verknüpfung der in „voneinander isolierten Silos"[150] gespeicherten Daten schwer machen, soll das neue „Datenhaus" einen gemeinsamen Informationspool erschaffen. Durch den Verzicht auf eine Strukturierung in Dateien soll dieser Pool weitgehende Verknüpfungen der darin gespeicherten Daten zulassen.[151]

Die Erwartungen an die Verknüpfbarkeit von Daten sind bei den Kriminalbehörden auch aufgrund neuer technischer Möglichkeiten in den letzten Jahren deutlich gestiegen.[152] Dies entspricht einer allgemeinen Tendenz, die auch bei anderen öffentlichen und privaten Stellen nachzuvollziehen ist. Mitte der 2010er-Jahre wurde unter dem Schlagwort „Big Data"[153] die Analyse großer Mengen von scheinbar belanglosen Daten als bedeutsame Chance für Staat und Wirtschaft gepriesen. Die Hoffnung, durch neue Methoden der Verknüpfung und Auswertung „Datenschätze" heben zu

[148] Vgl. *Creemers/Guagnin*, KrimJ 2014, 134 (138); *Creemers*, in: Grutzpalk, S. 101 (112); in diese Richtung auch schon *Herold*, Universitas 1976, 63 (73 f.).

[149] Siehe hierzu bereits oben Teil 1 B. II.

[150] *Albers*, in: Seckelmann, S. 509 (526).

[151] Siehe dazu im Einzelnen oben Teil 1 B. III. 3. b.

[152] Vgl. BfDI, 26. Tätigkeitsbericht 2015-2016, S. 106 ff.; zum Verfassungsschutz BT-Drs. 18/4654, 18; zu entsprechenden Entwicklungen in den USA *Ferguson*, University of Pennsylvania Law Review 163 (2015), 327 (360 ff.).

[153] Vgl. näher zu diesem Begriff *Mayer-Schönberger/Cukier*, S. 13.

können, setzt sich in den aktuellen Diskussionen um den Einsatz künstlicher Intelligenz bei der Polizei fort.

Gerade im Zusammenhang mit komplexeren Datenauswertungen nimmt auch das Bedürfnis der Anwender*innen zu, Datenbestände einzubeziehen, die außerhalb der Kriminalbehörden liegen. Dies können Daten anderer Behörden, aber auch solche aus privaten Beständen oder offenen Quellen im Internet sein. *Fall 5* zeigt dieses Bedürfnis exemplarisch auf. Hier sollen aus der Verknüpfung von Daten aus kriminalbehördlichen Ressourcen und sozialen Medien im Internet Erkenntnisse für die Strafverfolgung gewonnen werden. Die Verknüpfung von Datenbeständen über mehrere Sicherheitsbehörden hinaus spielt praktisch unter anderem im Rahmen der gemeinsamen Dateien von Polizei und Nachrichtendiensten eine Rolle. Ähnlich wie das Bedürfnis nach der zwischenbehördlichen Verfügbarkeit von Informationen lässt sich auch der Wunsch nach einer zwischenbehördlichen Verknüpfbarkeit als Aspekt einer zunehmenden Vernetzung[154] im Sicherheitsbereich begreifen. Speziell nach dem 11. September 2001 haben die Bemühungen um eine bessere Vernetzung zugenommen.[155] Vernetzung bedeutet in diesem Zusammenhang die Zuwendung zu einer nicht-hierarchischen Kooperation mehrerer Stellen, die das effizientere Sammeln, Bündeln und Austauschen von Informationen ermöglichen soll.[156] Eine Vernetzung von Behörden im Sicherheitsbereich bedeutet aber auch die Abkehr von der Vorstellung, dass einzelne Behörden umfassend Sicherheit gewährleisten können.[157]

Die im Rahmen dieser Untersuchung interviewten Anwender*innen polizeilicher Informationssysteme benannten die Verknüpfbarkeit von Daten als wichtige Anforderung an ihre Informationsordnung und sahen hierbei Herausforderungen und Verbesserungsbedarf. Ein konkretes Problem, das zur Sprache kam, war die Trennung von Daten der Polizeien unterschiedlicher Länder. Ein*e Anwender*in berichtete:

---

[154] Vgl. zum Begriff der Vernetzung im rechtlichen Kontext *Albers*, in: Seckelmann, S. 509 (511); *Möllers*, in: Oebbecke, S. 285 ff.; *Pache*, VVDStRL 2007, 106 (132); *Groß*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts I, § 13 Rn. 12, zur begrifflichen Verknüpfung mit der elektronischen Informationsverarbeitung *Gusy*, in: Weidenfeld, S. 197.

[155] Vgl. *Kötter*, S. 290 m.w.N. Mit einer besseren Vernetzung wollten die Sicherheitsbehörden spiegelbildlich auf die terroristische Bedrohung durch Netzwerke wie Al-Qaida reagieren; so äußerte der ehemalige Innenminister *Otto Schily* auf der BKA-Herbsttagung 2004: „Wir müssen die Netzwerke des Terrors mit unseren eigenen Netzwerken bekämpfen." (*Schily*, in: BKA, Netzwerke, S. 5 (7)); kritisch hierzu *Stegmaier/Feltes*, APuZ 12/2007, 18 ff.; *S. Kaufmann*, in: Gusy/Kugelmann/Würtenberger, S. 3 (12 f.) sowie speziell zu dem Schluss, auf vernetzte Bedrohungen mit einer vernetzten Sicherheitsarchitektur zu reagieren *Schöndorf-Haubold*, in: 47. ATÖR, S. 149 (150).

[156] Vgl. *Gusy*, in: Weidenfeld, S. 197 (198); *Schöndorf-Haubold*, in: 47. ATÖR, S. 149 (156).

[157] *Stegmaier/Feltes*, APuZ 12/2007, 18 (21 f.).

> „[W]ir haben sehr, sehr oft das Problem, dass die Polizei nicht weiß, was die Polizei weiß. Das heißt, dass wir Informationen zu gewissen polizeilich relevanten Personen schwer verknüpfen können. Das hängt mit der Technik zusammen, dass wir unterschiedliche Datenbanken haben, dass wir unterschiedliche Datenmodelle haben, dass wir aber auch, wenn wir jetzt gerade an den Bundesland-übergreifenden Aspekt denken, datenschutzrechtliche Restriktionen haben." (POL2)

Nicht alle befragten polizeilichen Anwender*innen aber unterstützten das Anliegen, kriminalbehördliche Datenbestände weitergehend miteinander zu verknüpfen. Eine*r der Interviewten schilderte auch seine kritische Perspektive zu diesem Wunsch:

> „Aber verknüpfte Daten an sich, das ist im Prinzip auch etwas, das immer wieder kritisiert wird. Die Sicherheitsbehörden verknüpfen Daten. Und dadurch erhöhe sich quasi die Unsicherheit. Damit kann man sehr schnell in irgendwelche Verdachtsmomente reinrutschen als Bürger. Weil der Staat irgendwelche Daten miteinander verknüpft. [...] vollautomatische Systeme, die Daten nach einem Algorithmus miteinander verknüpfen. Da wäre ich als Bürger nicht für. Und als Polizist würde ich auch sagen, das verursacht wahrscheinlich viele Fehler." (POL3)

Diese Schilderung deutet Risiken an, die durch die Speicherung von personenbezogenen Daten in kriminalbehördlichen Informationssystemen entstehen bzw. verstärkt werden: Die Dekontextualisierung von Informationen und eine mögliche Kriminalisierung von Bürger*innen. Auf diese Risiken soll sogleich näher eingegangen werden.

II. Implikationen für Betroffene

Wenn Daten innerhalb der kriminalbehördlichen Informationsordnung besser miteinander verknüpfbar werden, kann dies die im Zusammenhang mit der Verfügbarkeit von Daten beschriebenen[158] Risiken der Stigmatisierung und Kriminalisierung von Betroffenen erhöhen. Die Verknüpfung von Daten kann etwa zur Folge haben, dass Personen Eigenschaften zugeschrieben werden, die für sie zu nachteiligen Folgen führen und die sie unter Umständen in der Realität nicht aufweisen. Sie kann auch dazu führen, dass sie mit anderen Personen verwechselt werden.

Durch die Verknüpfung von Informationen aus verschiedenen Quellen können zunächst Informationen erzeugt werden, die für die betroffenen Personen belastend sind. So sollen beispielsweise in *Fall 5* durch den Abgleich von Textinhalten aus verschiedenen Quellen potentielle Täter*innen anhand ihres „sprachlichen Fingerabdrucks" iden-

[158] Siehe oben A. II.

tifiziert werden. Hierdurch werden unter Umständen neue Verdachtsmomente generiert. Durch die Verknüpfung von Daten – hier in Form eines Abgleichs von Texten – kann der Verdacht der Begehung einer Straftat auf eine Person fallen, die einen ähnlichen Schreibstil wie eine andere Person hat, die tatsächlich ein Äußerungsdelikt begangen hat. Neben der Identifikation von Personen kann die Verknüpfung von Daten aus verschiedenen Quellen auch dazu dienen, Informationen zu gewinnen, die verwendet werden sollen, um Prognosen über das zukünftige Verhalten einer Person zu treffen, ihre Beziehung zu anderen Personen oder Gegenständen offenzulegen oder Lücken in Sachverhalten aufzuklären. So wäre es – unabhängig von der rechtlichen Bewertung dieses Vorgehens – in einer ähnlichen Konstellation wie in *Fall 5* denkbar, dass das Bundeskriminalamt anhand ihm vorliegender Daten aus den Nutzerprofilen von Personen, die über soziale Medien Straftaten nach § 130 StGB (Volksverhetzung) begangen haben, das Profil eines typischen „Online-Hetzers" erstellt und auf dieser Grundlage nach anderen Personen sucht, die für die Begehung derartiger Delikte in Frage kommen.

Werden vorhandene Informationen miteinander kombiniert und daraus neue Informationen erzeugt, die einer Person zugewiesen werden, können in der kriminalbehördlichen Informationsordnung Abbilder von Personen entstehen, die von ihren reellen Vorbildern abweichen.[159] Diese Abbilder sind als „Datenschatten"[160] Abstraktionen von Persönlichkeiten mit eigenen Eigenschaften. Sie lassen sich nach einem von *Friedrich Nietzsche*[161] eingeführten und von *Gilles Deleuze*[162] geprägten Begriff als „Dividuen" bezeichnen. Die betroffene Person muss von der Existenz ihres Datenschattens nicht zwangsläufig wissen.[163] Sie kann durch diese aber dennoch stigmatisiert und kriminalisiert werden, wenn die Eigenschaften des Dividuums ihr bei der Betrachtung durch die Kriminalbehörden zugerechnet werden. Konkret könnte beispielsweise eine Person durch eine Datenauswertung als potentieller „Online-Hetzer" identifiziert worden und ein entsprechender Vermerk in einer kriminalbehördlichen Datei gespeichert worden sein, obwohl sie nie Äußerungsdelikte begangen oder derartiges vorgehabt hat. Von Ermittler*innen würde die Person dennoch als potentieller Krimineller behandelt.

Neben einer Zuschreibung einzelner Eigenschaften ist es möglich, dass es durch die Verknüpfung von Daten zu einer Verwechslung von Personen kommt. In derartigen

---

[159] *Creemers*, in: Grutzpalk, S. 101 (107); *Matzner*, Surveillance & Society 2016, 197 (203); *Poster*, S. 91; vgl. auch *Franko Aas*, Punishment & Society 2004, 379 (386); *Haggerty/Ericson*, British Journal of Sociology 51 (2000), 605 (611 ff.); *Lyon*, in: Lyon, S. 13 (22).

[160] Vgl. *Gusy/Eichenhofer*, S. 157.

[161] *Nietzsche*, Menschliches, Allzumenschliches I, Nr. 57.

[162] *Deleuze*, in: Deleuze, Unterhandlungen, S. 254 (258).

[163] Vgl. *Poster*, S. 93.

Fällen wird der betroffenen Person nicht eine eigenständige Datenbankidentität zugeschrieben, sondern sie wird für eine real existierende andere Person gehalten. In *Fall 3* etwa wird eine Person nach einem Datenabgleich aufgrund der Übereinstimmung bestimmter persönlicher Merkmale für einen anderen Menschen gehalten, der per Haftbefehl gesucht wird. Der Betroffene wird auf dieser Grundlage fälschlich inhaftiert. Der an den Fall *Amad Amad* angelehnte Sachverhalt ist nicht einzigartig. Auch in den USA kam es bereits zu Verhaftungen, weil eine polizeilich kontrollierte Person übereinstimmende persönliche Merkmale mit einer gesuchten Person aufwies.[164]

Sowohl die fehlerhafte Zuschreibung von Eigenschaften als auch die Verwechslung von Personen aufgrund einer Verknüpfung von Daten beruhen darauf, dass Informationen sich bei ihrer Weiterverarbeitung außerhalb ihres ursprünglichen Kontexts befinden. Daten, die in kriminalbehördlichen Informationsressourcen gespeichert sind, können die Umstände ihrer erstmaligen Erhebung naturgemäß nicht vollständig abbilden.[165] Die Dekontextualisierung von Informationen ist ein allgemeines Phänomen bei der Nutzung automatisierter Verfahren und moderner digitaler Informationstechnologien.[166] Es ist außerdem anzunehmen, dass der zunehmende Einsatz von Anwendungen der elektronischen Datenverarbeitung durch die Polizei tendenziell zu einer Distanzierung von den Bürger*innen führt.[167] Auch die Speicherung von Wissen in Informationssystemen bedeutet einen Akt der Distanzierung von den Informationssubjekten. Dieser vollzieht sich zunächst durch eine Formalisierung der Informationen.[168] Die Formalisierung soll dazu dienen, die Verfügbarkeit, Verknüpfbarkeit und einheitliche Qualität von Informationsbeständen zu sichern sowie Arbeitsabläufe zu standardisieren. Sie begünstigt aber auch die Herauslösung der Informationen aus dem ursprünglichen Kontext ihrer Erhebung. Dies gilt besonders für die Speicherung von Daten in Systemen, die nicht der Logik von Zwecken und Narrativen folgen. Die von Polizei und Sicherheitsbehörden für ihre neuesten Informationsressourcen verwendeten Begriffe „Data Lake" (Europol)[169], „Datenpool"[170] und „Datenhaus" (jeweils Bundeskriminalamt)[171] verdeutlichen die Problematik: Informationen werden in ein Reservoir gekippt

[164] *Jacobs*, S. 143 schildert hierzu den Fall von *Michael Ainsworth*.
[165] Vgl. *Busch/Funk/Kauß/Narr/Werkentin*, S. 117; *Creemers*, in: Grutzpalk, S. 101 (116 f.).
[166] Vgl. *Augsberg*, S. 163; *Bull*, S. 34.
[167] *Ponsaers*, Policing 2001, 470 (486). Schon die Einführung von Streifenfahrzeugen und des Polizeifunks sind Beispiele für Entwicklungen, die bedingt haben, dass sich die Polizei weniger unmittelbar mit Menschen auseinandersetzen musste als ohne diese technischen Hilfsmittel; *Manning*, Crime and Justice 15 (1992), 349 (355 f.).
[168] Vgl. *Creemers*, in: Grutzpalk, S. 101 (115); *Franko Aas*, Punishment & Society 2004, 379 (381).
[169] Siehe oben Teil 1 B. VI.
[170] Siehe oben Teil 1 B. III. 2.
[171] Siehe oben Teil 1 B. III. 3.

und vermischt, ohne dass sich Herkunft und Bedeutung der einzelnen Bestandteile notwendigerweise nachvollziehen ließen. Die Speicherung und Verknüpfung von Daten in derartigen Systemen läuft Gefahr, Verbindungen von Einzelelementen ohne eindeutigen Sinnzusammenhang hervorzubringen.[172]

Gerade jüngere technische Entwicklungen drohen also das Problem der Dekontextualisierung und die darauf basierenden Risiken der Kriminalisierung und Stigmatisierung durch die Verknüpfung von Daten verstärken. Mit Methoden der künstlichen Intelligenz und des maschinellen Lernens stehen Mittel zur Verfügung, um auf komplexe Art bestehende Informationen zu verknüpfen und neue Informationen zu generieren, deren Funktionsweise einer Black Box gleicht.[173] Derartige Methoden ermöglichen es theoretisch bereits heute, dass innerhalb kriminalbehördlicher Informationssysteme Attribute eigenständig zugewiesen und Wertungen eigenständig vorgenommen werden. Es kann also prinzipiell zu einer „algorithmenbasierten Zuschreibung von Eigenschaften"[174] kommen. Erfolgt dies ohne eine wirksame Kontrolle, können daraus möglicherweise ungerechtfertigterweise Stigmatisierungen und auch konkrete Verdachtsmomente erwachsen. Selbst wenn die problematischen Ergebnisse einer automatisierten Verknüpfung von Daten einer Überprüfung am Ende nicht standhalten, können sie folgenreich für die Betroffenen sein, wenn sie zur Grundlage weiterer Datenverarbeitungen oder Maßnahmen gemacht werden.[175] Der Einsatz von Methoden künstlicher Intelligenz oder anderer neuer Technologien zur Datenauswertung erhöht nicht zwangsläufig die Wahrscheinlichkeit, dass bei der Verknüpfung von Daten oder der Zuweisung von Eigenschaften Fehler geschehen. Auch menschliche Verknüpfungen und Auswertungen von Daten lassen Raum für Fehler. Allerdings können die Risiken durch automatisierte Auswertungen ein besonderes Ausmaß annehmen, wenn massenhaft durchgeführte Prozesse keiner wirksamen Kontrolle unterzogen werden können.

Es ist schließlich zu beachten, dass Auswertungen auf Grundlage neuer technischer Methoden den Anschein erhöhter Zuverlässigkeit und Objektivität mit sich bringen können.[176] Es besteht die Gefahr, dass sich Ermittler*innen in der Praxis unkritisch auf den Output „intelligenter" Systeme verlassen. Zugleich wird für die Anwender*innen ebenso wie für die Betroffenen nicht immer nachvollziehbar sein, wie Auswertungen und Verknüpfungen mithilfe fortschrittlicher Methoden erfolgt sind.[177] Dies gilt etwa für die Generierung von Informationen durch neuronale Netze, deren Lernprozesse selbst für die Entwickler*innen nicht vollständig durchschaubar sind. So besteht die

[172] *Creemers*, in: Grutzpalk, S. 101 (117); *Rusteberg*, in: Münkler, S. 233 (256).
[173] Vgl. *Creemers*, in: Grutzpalk, S. 101 (116 f.).
[174] *Broemel/Trute*, Berliner Debatte Initial 27 (2016), 50 (57).
[175] Vgl. *Lageson*, S. 65.
[176] Vgl. *Singelnstein*, NStZ 2018, 1 (4); *Wischmeyer*, AöR 143 (2018), 1 (27).
[177] Vgl. *Gless*, in: GS Weßlau, S. 165 (171 f.).

Gefahr, dass Informationen bei ihrer Auswertung und Verknüpfung aus ihrem ursprünglichen Zusammenhang gerissen werden, ohne dass dies für die Ermittler*innen nachvollziehbar ist.

Die Schwierigkeit, die Herkunft von Daten bzw. den ursprünglichen Kontext ihrer Erhebung nachzuvollziehen, betonte auch ein Experte für polizeiliche Software in einer Studie von *Niklas Creemers* und *Daniel Guagnin*:

> „Mit der Einführung der Vorgangsbearbeitungssysteme hat sich das schleichend eingeführt, dass eben keine klassischen Akten mehr geführt werden erstmal, sondern dass das alles elektronisch geführt wird ... [und] da irgendjemand relativ unnachprüfbar [Daten eingibt, und] sie überhaupt keinen Beleg mehr dafür haben, wie das zu Stande gekommen ist. Und darauf werden dann ganze Ermittlungsverfahren aufgesetzt."[178]

Auch ein*e im Rahmen diese*r Untersuchung befragte*r Mitarbeiter*in der Datenschutzaufsicht betonte im Zusammenhang mit den tendenziell wachsenden Datenbeständen, dem Datenaustausch innerhalb der Polizei sowie der zunehmenden Verknüpfung von Daten das Risiko, dass Informationen aus dem Kontext gerissen und hierauf Entscheidungen gestützt werden könnten:

> „Diese Datenhalden und diese vielen Datenaustäusche, die bergen natürlich auch immer mehr die Gefahr, dass sowas zweckfremd verwendet wird. Oder auch aus dem Zusammenhang gerissen verwendet wird. Oder dass andere Polizeidienststellen dann auf Datenbanken zugreifen, und das für bare Münze nehmen, was da drin steht. Und darauf dann irgendwelche Entscheidungen stützen. Auch sowas passiert ja immer mal." (DSA4)

Insgesamt äußerten die im Rahmen dieser Untersuchung befragten Mitarbeiter*innen der Datenschutzaufsicht zwar grundsätzlich Verständnis für das polizeiliche Bedürfnis, zunehmend Verknüpfungen zwischen Datenbeständen herzustellen. Sie sahen entsprechende Tendenzen aufgrund der hiermit verbundenen Intransparenz und der Erschwerung der Geltendmachung von Betroffenenrechten aber auch kritisch. Exemplarisch äußerte ein*e Befragte*r:

> „Es ist, glaube ich, für die Polizei einer der wichtigsten Punkte, Daten sinnvoll miteinander zu verknüpfen. [...] Dem Grunde nach, finde ich, ist es ein zeitgemäßer Ansatz. Nur, da muss auch ein zeitgemäßer Grundrechtsschutz her. Und da muss wirklich auch geguckt werden, ob alles mit allem verknüpfbar sein kann, das kann eigentlich auch nicht sein. Da müssen schon noch, ich sage mal, Trennwälle, also Firewalls, zwischen den unterschiedlichen Da-

[178] *Creemers/Guagnin*, KrimJ 2014, 134 (145).

> tentöpfen da sein. Sonst kriegen wir auch Rechtsschutz- und Grundrechtsprobleme, weil einfach man das nicht mehr isolieren kann, wo das Problem liegt." (DSA3)

Bei der Geltendmachung von Betroffenenrechten und Rechtsschutzersuchen kann die Verknüpfung von Datenbeständen dadurch zum Problem werden, dass für den Betroffenen schwer ermittelbar ist, woher eine belastende Information stammt oder wo diese abgelegt ist. Dies deutet etwa *Fall 4* an, in dem eine Person, die ein Auskunftsrecht geltend macht, auf die „Datenbesitzerin" verwiesen wird. Aus der Sicht des Betroffenen ist aber nicht erkennbar, wer die belastenden Daten gespeichert hat und damit auch nicht, an wenn er sich wenden soll.

III. Rechtliche Rahmenbedingungen

Die Möglichkeiten zur Verknüpfung von Daten innerhalb der kriminalbehördlichen Informationsordnung ergeben sich zunächst aus den allgemeinen polizeirechtlichen und strafprozessualen Befugnissen zur Verarbeitung von personenbezogenen Daten. Die Verknüpfung von Daten, die keinerlei Personenbezug haben, ist insofern unproblematisch. Die allgemeinen Befugnisse machen die Zulässigkeit der Verknüpfung von personenbezogenen Daten – ebenso wie bei anderen Formen der Weiterverarbeitung – davon abhängig, ob sie für die Erreichung der hiermit verfolgten Zwecke der Gefahrenabwehr oder Strafverfolgung erforderlich ist.[179] Diese Befugnisse können aber nicht jede Form der Verknüpfung von Daten rechtfertigen. Als Generalklauseln können sie vor dem Hintergrund des verfassungsrechtlichen Bestimmtheitsgrundsatzes nur Maßnahmen legitimieren, die von einer geringen Eingriffsintensität sind.[180] Darüber hinaus bedarf es für Maßnahmen der Informationsverarbeitung speziellerer Befugnisse.

Eine Verknüpfung von Daten kann auf äußerst unterschiedliche Art stattfinden und dementsprechend unterschiedliche Eingriffsintensität haben. Für die Bestimmung der Eingriffsintensität einer Datenverarbeitung haben sich vor allem in der Rechtsprechung des Bundesverfassungsgerichts Kriterien herausgebildet. Zu berücksichtigen sind unter anderem die Anzahl der betroffenen Personen (Streubreite),[181] inwiefern diese einen Anlass für den Eingriff gegeben haben[182] und welche Nachteile ihnen aufgrund einer Maßnahme drohen.[183] Es ist auch zu berücksichtigen, welche Arten von Daten mit in die Verarbeitung einbezogen werden und ob diese einen besonderen

[179] Siehe oben Teil 1 C. III. 1. b.
[180] *Bäcker*, Kriminalpräventionsrecht, S. 258.
[181] BVerfGE 115, 320 (347).
[182] BVerfGE 115, 320 (347); vgl. auch BVerfGE 100, 313 (376); BVerfGE 107, 299 (318 ff.).
[183] BVerfGE 115, 320 (347 f.); vgl. auch BVerfGE 100, 313 (376); BVerfGE 109, 279 (353).

rechtlichen Schutz genießen.[184] Dies kann etwa für nach Art. 3 Abs. 3 GG geschützte Merkmale gelten.[185] Eine besondere Eingriffsintensität weist eine Verarbeitung personenbezogener Daten außerdem auf, wenn sie ein aussagekräftiges Bild über die Persönlichkeit oder das Verhalten eines Individuums erzeugt. Die „umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger“[186] ist verfassungsrechtlich unzulässig. Die Heimlichkeit einer Datenverarbeitung ist ein weiterer Umstand, der die Intensität des Eingriffs (gegenüber einer offenen Erhebung und Verarbeitung) erhöht.[187]

Für eine geringe Eingriffsintensität sprechen die den genannten jeweils entgegengesetzten Faktoren – also etwa eine geringe Streubreite der Verarbeitung, ihre Offenheit oder die Einbeziehung wenig persönlichkeitsrelevanter Daten.[188] Zuletzt urteilte das Bundesverfassungsgericht im Zusammenhang mit der grundrechtlichen Bewertung automatisierter Datenverarbeitungen außerdem, dass eine „Methode automatisierter Datenanalyse oder -auswertung umso eingriffsintensiver [ist], 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“[189] könnten. Mit letzteren Kriterien nahm das Gericht implizit Bezug auf die sich wandelnden technischen Möglichkeiten, die sich besonders durch den Einsatz von Methoden künstlicher Intelligenz ergeben.[190]

Im Rahmen der kriminalbehördlichen Informationsordnung können sowohl vergleichsweise simple als auch komplexere Verknüpfungen von Daten stattfinden und von Relevanz sein. Diese sind dementsprechend differenziert zu beurteilen. So dürfte etwa das Zusammenführen einzelner Datensätze ohne Inhalte von besonderer Persönlichkeitsrelevanz aus einem inhaltlich stark beschränkten Informationssystem nur einen geringfügigen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen bedeuten und auf Grundlage der Generalklauseln zur Datenverarbeitung zu rechtfertigen sein. Die Zusammenführung von Informationen aus unterschiedlichsten Ressourcen unter Zuhilfenahme von Methoden künstlicher Intelligenz dürfte hingegen schwerwiegende Grundrechtseingriffe bedeuten. Hierfür bedürfte es besonderer gesetzlicher Ermächtigungen, von denen bisher nur wenige existieren. Mit § 49 Abs. 1

[184] BVerfGE 115, 320 (348).
[185] Siehe hierzu oben Teil 1 C. III. 2. a.
[186] BVerfGE 115, 320 (351 f.).
[187] *Gusy/Eichenhofer*, S. 96.
[188] Vgl. *Rückert*, ZStW 129 (2017), 302 (323).
[189] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 90.
[190] Vgl. hierzu ausdrücklich BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

Var. 1 HmbPolDVG und § 25a Abs. 1 Var. 1 HSOG hat das Bundesverfassungsgericht zuletzt zwei derartige Regelungen im Polizeirecht für verfassungswidrig erklärt, weil sie Regelungen angesichts der schwerwiegenden Eingriffe, die sie ermöglichten, nicht verhältnismäßig ausgestaltet waren.[191] Insbesondere hatten sie zu niedrige Eingriffsschwellen vorgesehen. § 23 Abs. 6 PolG NRW enthält eine ähnliche Regelung, die die automatisierte Zusammenführung von Daten erlaubt.[192]

So existieren zusammengefasst zwar Befugnisse für einfache Zusammenführungen von Daten aus kriminalbehördlichen Informationsressourcen. Für komplexere Verknüpfungen und Auswertungen, die erhebliche Risiken für die Betroffenen mit sich bringen, fehlt es aber entweder an Befugnissen oder die Rechtslage ist bezüglich dieser zumindest unklar.

C. Die Aktualität und Richtigkeit von Informationen (Datenqualität)

Die dritte zentrale Anforderung an kriminalbehördliche Informationsbestände ist ihre Aktualität und inhaltliche Richtigkeit.

*I. Anforderungen aus Sicht der Anwender*innen*

Daten in kriminalbehördlichen Informationsressourcen sollten Tatsachen zutreffend wiedergeben und möglichst auf dem neuesten Stand sein. Die Richtigkeit und Aktualität von Daten ist eine grundlegende Voraussetzung, um diese weiter nutzen zu können. Besonders eine automatisierte Verknüpfung und Auswertung von Daten kann nur gelingen, wenn das zugrunde liegende Material akkurat ist. Dies drückt die in der Informationstechnik verbreitete Phrase „Garbage In, Garbage Out“[193] aus: Schlechtes Ausgangsmaterial erzeugt auch schlechte Auswertungsergebnisse. Werden Informationen bei ihrer Erhebung und Speicherung ungenau erfasst, kann dieser Mangel im weiteren Verlauf der Verarbeitung kaum noch behoben werden. Die Sicherung der Datenqualität ist jedoch nicht auf den Schritt der Erhebung und erstmaligen Speicherung der

[191] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20.

[192] Auch gegen diese ist eine Verfassungsbeschwerde anhängig; https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-NRW/2022-10-05-PolG_NRW_Palantir_Website_geschwaerzt_Punkte.pdf.

[193] Vgl. *P. Fuchs*, Kriminalistik 2018, 707 (708); *Manning*, S. 77 f.

Daten beschränkt. Ihre Aktualität und Richtigkeit ist auch im weiteren Verlauf der Verarbeitung sicherzustellen.[194]

Sämtliche im Rahmen dieser Untersuchung interviewten Anwender*innen polizeilicher Informationssysteme nannten die Gewährleistung der Datenqualität als eine wichtige Aufgabe. Hierbei thematisierten sie nicht nur die Qualität der Daten bei ihrer erstmaligen Erhebung, sondern auch die Schwierigkeit, die Daten in der Folge aktuell und richtig zu halten (POL1, POL2). Die Wahrung der Datenqualität sei zwar kein grundsätzlich neues Thema, aber die Anforderungen hieran seien im Laufe der Zeit gestiegen (POL2, POL3). Eine*r der Befragte*n beschrieb die aktuellen Herausforderungen wie folgt:

> „Wir haben [...] das Problem, dass teilweise Löschlisten nicht so wahrgenommen wurden, wie es denn hätte wirklich sein sollen. Es werden auch Fehler in der Datenhaltung gemacht, und oftmals ist es auch so, dass die Datenerfassung nicht umfassend erfolgt. Wir würden uns wünschen, dass die Kollegen teilweise mehr Daten erfassen. Das führt zu Problemen, aber das ist einfach historisch gewachsen. Man muss sehen, früher wurde das Vorgangsbearbeitungssystem nur dazu benutzt, einen Vorgang für die Staatsanwaltschaft zu generieren, und mittlerweile gibt es ganz, ganz andere Anforderungen an die Daten. Das heißt, das Thema Datenanalyse ist weit mehr in den Vordergrund gerückt, sowohl im täglichen Bereich als auch im operativen Bereich." (POL2)

Hier kommt eine aktuelle Schwierigkeit bei der Gewährleistung der Datenqualität zum Ausdruck: Um für vielfältige Zwecke auswertbar zu sein, müssen Datensätze vollständig sein und Informationen zum Kontext ihrer Erhebung enthalten. Außerdem gibt es schon lange Bemühungen, die Erhebung und Speicherung von Daten bei der Polizei möglichst stark zu standardisieren, um aussagekräftige Datensätze zu erhalten und dadurch Abgleiche dieser zu ermöglichen.[195] Aktuell hebt das Programm Polizei 20/20 die günstigen Auswirkungen einer standardisierten Verarbeitung auf die Datenqualität hervor.[196] Wie hier eine Standardisierung erreicht werden soll, die zu einer verbesserten Datenqualität führt, bleibt abzuwarten. Denn eine Standardisierung führt nicht zwangsläufig zu einer Verbesserung der Datenqualität. Sie kann auch dazu beitragen, dass die Möglichkeit, Informationen zum Kontext einer Datenerhebung zu erfassen, begrenzt wird.

---

[194] Vgl. *Ogorek*, ZRP 2023, 86 (87).

[195] Vgl. *Aden*, dms 2014, 55 (63) sowie schon *Herold*, in: Taschenbuch für Kriminalisten, S. 240 (246), der von einer „absoluten Reinheit des Datenflusses" spricht, die es zu sichern gelte.

[196] BMI, Polizei 2020, S. 8.

II. Implikationen für Betroffene

Grundsätzlich liegt es auch im Interesse der Betroffenen, dass über sie in kriminalbehördlichen Informationssystemen gespeicherte Daten richtig und aktuell sind. Durch fehlerhafte oder veraltete Daten können die Betroffenen falsch repräsentiert sowie dadurch unter Umständen stigmatisiert und kriminalisiert werden.[197] So lässt sich etwa die Speicherung eines geringfügigen Verstoßes gegen das Betäubungsmittelgesetz für acht Jahre, wie in *Fall 1* beschrieben, als Problem der Datenqualität betrachten. Die Angabe, dass der Verstoß stattgefunden hat, ist zwar sachlich richtig. Die Informationen sind aber nicht mehr aktuell. Sie weisen keine Relevanz mehr auf, die ihre weitere Speicherung legitimiert. Aufgrund ihrer nunmehr fehlenden Relevanz ist es auch nicht im Sinne der kriminalbehördlichen Anwender*innen, dass diese Daten weiter gespeichert werden. Es erscheint daher naheliegend, dass derartige Defizite bei der Datenqualität auf strukturelle Mängel beim Umgang mit der kriminalbehördlichen Informationsordnung und den stetig wachsenden Datenbeständen[198] zurückzuführen sind.

Ein*e im Rahmen dieser Untersuchung interviewte*r Mitarbeiter*in der Datenschutzaufsicht berichtete beispielhaft von Problemen bei der Sicherung der Qualität von Daten in polizeilichen Informationsressourcen und den Folgen, die daraus für Betroffene entstehen können:

> „Was häufig helfen würde, aber aus Zeitgründen oder Ressourcengründen oft nicht gemacht wird, ist das Nachfragen. Also nicht nur eine Information aus einem System abrufen und damit losrennen. Sondern, gerade wenn es keine eigene Information aus dem eigenen Land ist, auch mal nachzufragen: ‚Ist das noch aktuell?' Das würde helfen. Wir hatten zum Beispiel folgende Situation: Da wurde vom LKA eines Landes eine Warnung verschickt an alle anderen Länder und den Bund. Bezüglich einer Dolmetscherin, dass man nicht mehr mit ihr zusammenarbeiten solle, weil jetzt wegen Geheimnisverrats gegen sie ermittelt wird. Dass dann ein paar Monate später von der Staatsanwaltschaft das Verfahren eingestellt wurde, das wurde nicht mehr weitergegeben. Und wir haben dann teilweise festgestellt, dass solche Warnungen manchmal noch zehn Jahre später irgendwo aufgehoben wurden. Bei irgendeiner Behörde in irgendeinem Bundesland. Die kriegen die [Warnungen], in so einem Hefter, und haben die eben. Und wenn sich da dann mal so ein Dolmetscher bewirbt, dann kriegt der keine Antwort auf seine Bewerbung oder wird abgelehnt, und weiß gar nicht, wieso." (DSA4)

---

[197] Siehe zu den Risiken der Stigmatisierung und Kriminalisierung bereits oben B. II.
[198] Siehe zum Wachstum der Datenbestände unten D. I.

Dieser Fall veranschaulicht, dass die Sicherung der Datenqualität einen gewissen organisatorischen Aufwand bedeutet, der unter Umständen vermieden wird, um kurzfristig Ressourcen zu sparen. Auch wenn sich organisatorische Abläufe sowie technische Anwendungen entwickeln und durchsetzen sollten, mit denen die Qualität der Daten in der kriminalbehördlichen Informationsordnung verbessert würde, ist nicht ausgeschlossen, dass Probleme im Zusammenhang mit der Aktualität und Richtigkeit von Informationen auftreten, die durch eine menschliche Bewertung zu lösen sind. Die Notwendigkeit einer individuellen Bewertung von Relevanz und Kontext gespeicherter Informationen veranschaulicht auch *Fall 3*, in dem es aufgrund teilweise übereinstimmender persönlicher Merkmale von zwei Personen in einer polizeilichen Datenbank zu ihrer Verwechslung kommt.

Insgesamt haben sowohl Anwender*innen als auch Betroffene ein Interesse an der Sicherung der Qualität von Daten, die in kriminalbehördlichen Informationssystemen gespeichert sind. Ihre Interessen sind aber nicht notwendigerweise ganz deckungsgleich. Wie bereits aus der Beschreibung der Anforderungen der Anwender*innen hervorgeht, sind diese an möglichst umfassenden, aber zugleich standardisierten Datenspeicherungen interessiert, um die Möglichkeiten zur Verknüpfung und Auswertung von Daten zu verbessern. Aus Sicht der Betroffenen birgt die standardisierte Speicherung von Informationen allerdings auch das Risiko einer zu stark schematisierten Einordnung von Lebenssachverhalten.[199] Auch, wenn bei der Speicherung eines Datensatzes bestimmte Kategorien von Informationen eingegeben werden müssen, obwohl sie nicht eindeutig ermittelbar sind oder die Angaben nur aus dem genauen Kontext ihrer Erhebung heraus verständlich sind, kann dies zu Problemen führen. Eine Person kann dann durch die Angaben in einer kriminalbehördlichen Datenbank fehlerhaft repräsentiert werden.

III. Rechtliche Rahmenbedingungen

Die Datenqualität ist die einzige der hier beschriebenen drei zentralen Anforderungen an kriminalbehördliche Informationsressourcen, die im deutschen Recht ausdrücklich geregelt ist. Sie weist außerdem die Besonderheit auf, dass sie unmittelbar sowohl den Interessen der Anwender*innen kriminalbehördlicher Informationssysteme als auch den Interessen der Personen dient, über die Daten gespeichert werden. Die rechtliche Regelung beruht allerdings in erster Linie auf den Interessen der von der Verarbeitung Betroffenen. Das Datenschutzrecht stellt Anforderungen an die Datenqualität, um

[199] Vgl. etwa *Schweinoch*, Die Polizei 1984, 292 (294) im Zusammenhang mit Personenbeschreibungen.

diese davor zu schützen, dass ihnen durch die Verarbeitung falscher oder veralteter Informationen Nachteile entstehen.

Der Grundsatz der Datenqualität ergibt sich für den Bereich der Strafverfolgung und Gefahrenabwehr aus Art. 4 Abs. 1 lit. d JI-Richtlinie.[200] Danach haben Mitgliedstaaten vorzusehen, dass personenbezogene Daten „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden". Im deutschen Recht wurde dieser Grundsatz in § 47 Nr. 4 BDSG und entsprechenden Regelungen der Landesgesetze umgesetzt. Die Gesetzgeber haben sich dabei für Formulierungen entschieden, die praktisch wortgleich mit jener in Art. 4 Abs. 1 lit. d JI-Richtlinie sind.

In der JI-Richtlinie formulieren außerdem Art. 6 und Art. 7 Abs. 1 spezifische Gebote der Datenqualität. Danach haben die Mitgliedsstaaten vorzusehen, dass die von der JI-Richtlinie erfassten Behörden bei ihrer Datenverarbeitung sauber zwischen verschiedenen Kategorien von Personen (z.B. Opfern, Tätern und Zeugen) sowie faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten unterscheiden. Diese Regelungen betreffen auch die Ausgestaltung von Informationsressourcen, die Möglichkeiten für entsprechende Differenzierungen enthalten müssen. Auch diese recht allgemeinen Vorgaben haben die Gesetzgeber von Bund und Ländern praktisch durch eine wortgleiche Übernahme des Richtlinientextes umgesetzt.[201] Nähere strukturelle Vorgaben an die Speicherung und Ordnung von Daten zur Sicherung der Datenqualität finden sich in den einschlägigen Regelungen nicht.

Der Grundsatz der Datenqualität findet schließlich Niederschlag in Betroffenenrechten wie z.B. dem Recht auf Berichtigung,[202] die einer individuellen Ausübung bedürfen. Während es schon allgemein selten ist, dass Personen von ihren datenschutzrechtlichen Betroffenenrechten Gebrauch machen, erscheint die Wahrscheinlichkeit hierfür bei kriminalbehördlichen Datenspeicherungen noch einmal geringer. Diese sind für die Betroffenen regelmäßig besonders intransparent, was die Ausübung ihrer Rechte faktisch erschwert.

Schließlich enthält die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 (Europol-VO)[203] Vorgaben für die Datenqualität beim Europäischen Polizeiamt. Art. 28 ff. Europol-VO enthalten allgemeine Vorgaben zum Datenschutz („Datenschutzgarantien"). Art. 28 Abs. 1 lit. d Europol-VO legt den

[200] Vgl. zu den Wurzeln des Grundsatzes im US-amerikanischen Datenschutzrecht *Hoeren*, ZD 2016, 459 (460).

[201] Vgl. §§ 72 f. BDSG.

[202] Vgl. Art. 16 JI-Richtlinie.

[203] ABl. EU L 135, S. 53; vgl. zu der Entstehung der VO *Aden*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. M Rn. 102.

Grundsatz der Datenqualität fest, wonach personenbezogene Daten „sachlich richtig sein und auf dem neuesten Stand gehalten werden" müssen. Die Formulierung stimmt weitgehend mit jener in Art. 4 Abs. 1 lit. d JI-Richtlinie überein. In den früheren Rechtsgrundlagen von Europol war der Grundsatz der Datenqualität lediglich angedeutet, aber nicht explizit geregelt gewesen.[204] Anders als die JI-Richtlinie konkretisiert die Europol-VO die Anforderungen an die Datenqualität noch weiter. Die genaueren Vorgaben an dieser Stelle beruhen darauf, dass sich Europol auf Informationen verlassen muss, die es von mitgliedsstaatlichen Stellen und anderen Akteuren erhält.[205] Art. 29 Europol-VO sieht daher vor, dass Mitgliedsstaaten und andere Informationsquellen[206] an Europol zu übermittelnde Informationen nach Möglichkeit nach Zuverlässigkeit der Quelle und Richtigkeit der Quelle bewerten. Dafür sieht die Regelung ein konkretes Bewertungssystem vor.

D. Gemeinsame Herausforderungen und Konflikte

Wie die vorangegangene Untersuchung der Anforderungen an kriminalbehördliche Informationsressourcen gezeigt hat, stellen sich bei der Verwirklichung der jeweiligen Anforderungen teilweise die gleichen Herausforderungen. Zwei zentrale Herausforderungen und ihre Ursachen werden im Folgenden näher betrachtet. Erstens erschwert das Wachstum der kriminalbehördlichen Datenbestände die Sicherstellung der Qualität der gespeicherten Daten ebenso wie ihre Verfügbarkeit und Verknüpfbarkeit (I.). Zweitens weisen die kriminalbehördlichen Informationsressourcen Defizite bei ihrer Interoperabilität auf, die vor allem der Verfügbarkeit und Verknüpfbarkeit von Daten entgegenstehen (II.).

Freilich stellen sich bei der Verwirklichung der verschiedenen Anforderungen nicht immer ähnliche Herausforderungen. Die einzelnen Anforderungen an die kriminalbehördliche Informationsordnung können auch in Konflikt miteinander geraten. Konfliktträchtig erscheinen vor allem die Verfügbarkeit und Verknüpfbarkeit von Daten in ihrem Verhältnis zur Datenqualität. Vorgaben zur Sicherung der Datenqualität können den Bedürfnissen entgegenstehen, Informationen möglichst ohne Zwischenschritte abzurufen und miteinander zu verknüpfen. Konkret können etwa Prüfungen der Aktualität und Richtigkeit von Daten die Geschwindigkeit ihres Abrufs und ihrer Verknüpfung verringern. In der Praxis werden die untersuchten Anforderungen an die

[204] Vgl. *Felgenhauer*, in: FG Hilger, S. 75 (81).
[205] Vgl. zu den Informationsquellen von Europol Art. 17 Europol-VO.
[206] Vgl. Art. 29 Abs. 5 Europol-VO.

kriminalbehördliche Informationsordnung unterschiedlich gewichtet. Im Programm Polizei 20/20 etwa scheint der Fokus, der sich aus den öffentlich zugänglichen Materialien hierzu ergibt, eher auf Maßnahmen zur Verbesserung der Verfügbarkeit und Verknüpfbarkeit von Informationen zu liegen als auf der Datenqualität.

I. Wachstum der Datenbestände

Das Volumen der in kriminalbehördlichen Informationsressourcen abgelegten Daten nimmt stetig zu. Diese Entwicklung wird im Folgenden näher betrachtet, wobei die Datei „Gewalttäter Sport" als konkretes Beispiel für das Wachstum von Datenbeständen sowie den Umgang mit diesem Phänomen in der Praxis herangezogen wird (1.). Im Anschluss werden die möglichen Ursachen für das Wachstum untersucht (2.). Schließlich werden die Konsequenzen beleuchtet, die das Wachstum für die Anforderungen an die Informationsordnung hat (3.).

1. Das Wachstum

Die Datenbestände der Kriminalbehörden sind seit der Einführung der elektronischen Datenverarbeitung stark angewachsen.[207] Das genaue Ausmaß des Wachstums lässt sich statistisch allerdings nur schwer nachvollziehen, da hierzu keine vollständigen Zahlen für Bund und Länder bekannt sind.[208] Selbst für die Datenbestände des Bundeskriminalamts fehlt es an genauen Angaben über die vorhandenen Informationsressourcen und die darin gespeicherten Datensätze. Im Jahr 2019 erachtete die Bundesregierung die detaillierte Auflistung sämtlicher vom Bundeskriminalamt geführter Zentral- und Verbunddateien auf eine parlamentarische Anfrage hin aufgrund des damit verbundenen Aufwands für unzumutbar und machte nur unvollständige Angaben.[209]

Im Folgenden wird exemplarisch die Entwicklung der Datei „Gewalttäter Sport" betrachtet. Diese Datei existiert seit 1994,[210] ist fachlich bei der Zentralen Informationsstelle Sporteinsätze (ZIS) bei der Polizei in Nordrhein-Westfalen verortet und wird vom Bundeskriminalamt betrieben. Sie soll vor allem dazu genutzt werden, um gewalttätige Auseinandersetzungen im Zusammenhang mit Fußballspielen zu verhindern. Für eine nähere Betrachtung eignet sich die Datei deshalb, weil das öffentliche Interesse

[207] Vgl. hierzu aus früher Zeit Der Spiegel 20/1979, S. 37; *Boge*, Kriminalistik 1982, 619 (620); *Busch/Funk/Kauß/Narr/Werkentin*, S. 210; zu den bei Polizeibehörden der Länder geführten Kriminalakten *Rachor*, S. 68 ff.

[208] Vgl. *Rudolph*, S. 10.

[209] Es werden demnach innerhalb der Abteilungen Schwere und Organisierte Kriminalität und Polizeilicher Staatsschutz 38 Verbunddateien und 129 Zentraldateien geführt (Stand: November 2019); BT-Drs. 19/15346, S. 2 f, 13.

[210] Vgl. zu der Entstehungsgeschichte *Henseler*, NWVBl. 2015, 53 f.; *Kehr*, S. 48 ff. m.w.N.

an ihr hoch ist und daher verhältnismäßig viele Informationen über ihre Entwicklung zur Verfügung stehen. Hinzu kommt, dass die Entwicklung der Datei „Gewalttäter Sport" nicht nur ein Beispiel für das Anwachsen der polizeilichen Datenbestände ist. Sie zeigt auch Möglichkeiten zur Begrenzung dieses Wachstums auf.

Die Anzahl der in der Datei „Gewalttäter Sport" erfassten Personen stieg nach ihrer Errichtung zunächst rasant an, ging aber dann in den letzten Jahren wieder zurück. Während im Jahr 1998 ca. 2.300 Personen in der Datei erfasst waren,[211] waren es 2008 bereits 10.700.[212] Nachdem die Datenbestände im Jahr 2014 einen Höhepunkt erreichten,[213] wurden die Zahlen rückläufig. Im Jahr 2018 waren 10.100 Personen erfasst,[214] im Jahr 2019 9.544.[215] Zuletzt waren mit Stand vom 8. April 2021 7.485 Personen erfasst.[216] Während die Entwicklung bis in das Jahr 2014 wenig überraschend erscheint, stellt sich die Frage, wie es danach zu einem kontinuierlichen Rückgang der Zahl der erfassten Personen kam.

Der wohl entscheidende Grund für den Rückgang ist ein Beschluss des Unterausschusses Führung, Einsatz und Kriminalitätsbekämpfung der Innenministerkonferenz vom 17. Oktober 2014, in dem dieser die Auffassung äußerte, „dass die bundesweite Datei ‚Gewalttäter Sport' einen stark angewachsenen Datenbestand aufweist, der ihre Handhabbarkeit in der praktischen Dienstausübung erheblich einschränkt" und es für erforderlich erachtete, „die Datei hinsichtlich ihrer Praktikabilität, Transparenz und Zielorientierung zu überprüfen" sowie „die Erfassungs- und Speicherkriterien der Datei ‚Gewalttäter Sport' zu analysieren, um auf Dauer den Dateizweck zu gewährleisten."[217] Zugleich richtete der Unterausschuss eine Bund-Länder-Arbeitsgruppe zur „Überprüfung und Anpassung der beim Bundeskriminalamt geführten Datei ‚Gewalttäter Sport'" ein. Diese Arbeitsgruppe identifizierte anhand einer stichprobenartigen Analyse des Datenbestandes[218] Optimierungspotentiale der Datei, besonders mit Blick auf die Datenqualität. In der Folge schlug sie unter anderem eine Reduktion der Kriterien zur Erfassung von Daten vor.[219] Die Ergebnisse ihrer Überprüfung wurden bei der

[211] LT Nds-Drs. 14/374, S. 4; vgl. zum Folgejahr BT-Drs. 14/721, S. 2; zur Entwicklung insgesamt *Henseler*, NWVBl. 2015, 53.

[212] BT-Drs. 16/11934, S. 3.

[213] Mit 13.463 erfassten Personen zum 25. Februar 2014; LT NRW-Drs. 16/5205, S. 2.

[214] BT-Drs. 19/5195, S. 2.

[215] BT-Drs. 19/11842, S. 8.

[216] BT-Drs. 19/28886, S. 3.

[217] Bund-Länder-Arbeitsgruppe Überprüfung und Anpassung der beim Bundeskriminalamt geführten Datei „Gewalttäter Sport", Abschlussbericht, S. 3.

[218] Vgl. zum methodischen Vorgehen Bund-Länder-Arbeitsgruppe Überprüfung und Anpassung der beim Bundeskriminalamt geführten Datei „Gewalttäter Sport", Abschlussbericht, S. 4.

[219] BT-Drs. 19/5195, S. 6; Bund-Länder-Arbeitsgruppe Überprüfung und Anpassung der beim Bundeskriminalamt geführten Datei „Gewalttäter Sport", Abschlussbericht, S. 11.

Neufassung der Errichtungsanordnung der Datei vom 24. Mai 2018 berücksichtigt.[220] Nach dieser Anpassung kam es zu mehr Löschungen von Datensätzen als zu Neuerfassungen.[221]

Es ist zu bezweifeln, dass die Entscheidung des Unterausschusses der Innenministerkonferenz in dieser Form gefallen und die Datei „Gewalttäter Sport" auf diese Art angepasst worden wäre, wenn sich nicht ein besondere öffentliches Interesse auf diese Datei gerichtet hätte. Diese Entwicklung zeigt aber, dass ein maßvoller Umgang mit kriminalbehördlichen Informationsressourcen und eine gesteuerte Einschränkung ihres Wachstums prinzipiell möglich ist.

2. Die Ursachen

Mögliche Ursachen für das Anwachsen der kriminalbehördlichen Datenbestände sind zunächst in der technologischen Entwicklung (a.) und den rechtlichen Grundlagen der Informationsordnung (b.) zu suchen. Als weitere Ursachen (c.) kommen neue Bedrohungslagen, denen durch die Speicherung von Informationen begegnet werden soll, sowie organisatorische Defizite – wie etwa unklare Verantwortlichkeiten für die Pflege von Informationsbeständen – in Betracht.

a. Technologische Entwicklung

Auf technischer Ebene haben moderne elektronische Systeme zur Datenverarbeitung das Horten von Informationen tendenziell leichter gemacht. Begrenzte Speicherkapazitäten jedenfalls stehen der Bevorratung von Informationen kaum noch entgegen. Dass derartige Hürden entfallen, könnte auch dazu führen, dass Daten von den Anwender*innen kriminalbehördlicher Systeme weniger reflektiert abgespeichert werden als zuvor.[222] Dieser mögliche psychologische Effekt wurde allerdings empirisch noch nicht näher untersucht und belegt.

Weiter wird angenommen, dass die elektronische Datenverarbeitung zu einer verstärkten Formalisierung und Standardisierung von Dateneingaben und -speicherungen führt, was bedingt, dass Informationen vervollständigt werden (müssen), die sonst überhaupt nicht gespeichert würden.[223] Auch dies begünstigt ein Wachstum der Datenbestände. Das Phänomen, dass komplexere Informationssysteme zu einer Zunahme

[220] BT-Drs. 19/5195, S. 6.
[221] Siehe zu den Löschungen im 1. Quartal 2021 BT-Drs. 19/28369, S. 4 f.
[222] Vgl. *Creemers/Guagnin*, KrimJ 2014, 134 (140); *Ericson/Haggerty*, S. 418; *Ruch/Feltes*, NK 2016, 62 (69).
[223] *Ericson/Haggerty*, S. 419.

der erfassten Informationen führen, lässt sich bereits an frühen Formen der Aktenführung feststellen.[224] Im Zusammenhang mit der Computerisierung wurde in der Medientheorie in den 1990er-Jahren eine zunehmende „Sammelwut" digitaler Datenbestände diagnostiziert.[225] Der Wunsch, die Datenbestände zu vergrößern, entstand unter anderem durch neue Möglichkeiten zu ihrer Auswertung. Diese haben sich in den letzten Jahren deutlich weiterentwickelt. Komplexe Algorithmen sollten es möglich machen, aus Datenmassen Erkenntnisse für verschiedenste Zwecke zu extrahieren. Dies gilt auch für die Bereiche der Strafverfolgung und Gefahrenabwehr. Auf dieser Grundlage erscheinen heute tendenziell mehr Informationen als zuvor potentiell relevant, um für eine spätere Verarbeitung aufbewahrt zu werden. Die Begehrlichkeiten sind gestiegen, auch Informationen zu speichern und vorzuhalten, die möglicherweise in der Vergangenheit als unwichtig erachtet worden wären.[226] Folgt man der Logik des unerschöpflichen Auswertungspotentials großer Datenbestände, kann beinahe jede Information als relevant für eine spätere Auswertung betrachtet werden.[227]

Dadurch, dass die Verwendung komplexer datenverarbeitender Systeme zum Anwachsen der kriminalbehördlichen Datenbestände beigetragen hat, war sie auch mitursächlich für die Klage der Anwender*innen, dass diese mit zu vielen Informationen „überflutet" würden. Dies entbehrt nicht einer gewissen Ironie. Die Einführung der elektronischen Datenverarbeitung in den 1970er-Jahren war maßgeblich mit dem Versprechen verknüpft, eine „Informationsflut" zu bewältigen, die bereits ganz ohne die Verwendung von Computertechnik entstanden war.[228] Dies galt bei der Polizei ebenso wie in anderen Bereichen der öffentlichen Verwaltung.[229] Im Ergebnis haben die Systeme, die mit dem Versprechen eingeführt wurden, mehr Ordnung zu schaffen, auch zu einem organisatorischen Mehraufwand beigetragen. Sie haben das Problem der „Informationsflut" nicht gelöst, sondern nur verändert.

Bei der Betrachtung der technologischen Entwicklung als Ursache für das Wachstum der kriminalbehördlichen Datenbestände sind schließlich nicht nur die Informationsressourcen der Kriminalbehörden und ihre Funktionen zu betrachten. Es ist auch zu berücksichtigen, dass von Seiten Dritter durch die Nutzung neuer digitaler Technologien immer mehr Daten zur Verfügung stehen, die die Polizei erheben und speichern kann. Diesen Umstand benannten auch zwei der im Rahmen der Untersuchung interviewten polizeilichen Anwender*innen als wesentliche Ursache für das Wachstum der

[224] Zur Aktenführung in der preußischen Verwaltung des frühen 19. Jahrhunderts *Koselleck*, S. 663 ff.; vgl. auch *Gärditz*, Der Staat 54 (2015), 113 (115 f.).
[225] *Manovich*, S. 224 f.
[226] *Ladeur*, in: Süssenguth, S. 225 (243).
[227] *Matzner*, Surveillance & Society 2016, 197 (199).
[228] *Bergien*, Zeithistorische Forschungen, 2017, 258 (261) m.w.N.
[229] *Knackstedt/Eggert/Gräwe/Spittka*, MMR 2010, 528 m.w.N.

kriminalbehördlichen Datenbestände (POL2, POL3). So würden etwa Verdächtige und Zeug*innen schlicht immer mehr Daten „produzieren", wie ein*e Anwender*in erklärte:

> „[V]on den Daten an sich – von der Menge der Daten – betrachtet ist es ja so, dass es vor allen Dingen unser polizeiliches Gegenüber die Daten produziert. Jeder, der ein Smartphone hat, produziert ja unfassbar viele Daten – den ganzen Tag lang. So, dass wir von daher gar nicht anders können, als mehr Daten zu speichern. Weil wir auch auf der Beweismittelebene mehr Daten haben. Wir haben vor allen Dingen mit der Datenproduktion auf der gegenüberliegenden Seite zu tun. Und unsere eigenen Daten, die wir dann daraus generieren, das ist gar nicht mal so viel." (POL3)

b. Rechtliche Voraussetzungen

Auf der rechtlichen Ebene sind die niedrigen und unbestimmten Voraussetzungen für die Speicherung von Daten eine mögliche Ursache für das Wachstum der kriminalbehördlichen Datenbestände.[230] Auch ein*e für diese Untersuchung interviewte*r Mitarbeiter*in der Datenschutzaufsicht äußerte sich in diese Richtung, wobei sie sich konkret auf die – auch in *Fall 1* referenzierte – Falldatei Rauschgift bezog:

> „Wir haben [...] vorgefunden, dass da wirklich jeder Kiffer drin gespeichert wurde. Das war eine riesige Datenbank, die nach unserer Intervention dann bedeutend verringert worden ist. Und da haben wir auch gemerkt, dass die gesetzliche Voraussetzung, also die Erheblichkeitsprüfung, dass es eben länderübergreifenden Bezug oder eine erhebliche Bedeutung oder eine internationale Bedeutung hat, nicht angewendet wurde. Und dadurch wird die Datei aufgebläht und dann findet man eben nicht den Großdealer, der länderübergreifend agiert, weil der zwischen den ganzen Jugendlichen untergeht, die einmal mit Drogen erwischt worden sind. Das ist aus meiner Sicht auch ein bisschen unverständlich, weil die Polizei sich da selbst die Arbeit schwer macht." (DSA2)

Die an Minimalstandards des Datenschutzrechts orientierten Anforderungen an die Speicherung personenbezogener Daten erscheinen nicht geeignet, um das Ausmaß der Speicherung wirksam zu begrenzen. In den 1970er-Jahren existierten noch kaum einfachgesetzliche Vorgaben für den polizeilichen Datenschutz oder den Umgang mit Daten im strafprozessualen Kontext. In der Folge des Volkszählungsurteils des Bundesverfassungsgerichts wurden entsprechende Regelungen geschaffen, die im Wesentlichen

[230] Vgl. *Ruch/Feltes*, NK 2016, 62 (69).

aber nur verlangen, dass eine Datenverarbeitung für die Erfüllung des verfolgten Zwecks erforderlich ist und einen weiten Spielraum lassen.[231]

c. Weitere Ursachen

Eine weitere mögliche Ursache für das Anwachsen der Datenbestände liegt darin, dass neu auftretende Bedrohungen und Kriminalitätsphänomene ein Bedürfnis der Kriminalbehörden auslösen können, zusätzliche Informationsressourcen einzurichten oder mehr Informationen in vorhandenen Ressourcen zu speichern. Für die Schaffung neuer Informationsressourcen lässt sich dies etwa anhand der Antiterrordatei und der Rechtsextremismus-Datei nachvollziehen, deren Einrichtung unter dem Eindruck konkreter sicherheitsrelevanter Ereignisse stand. Die Errichtung der Rechtsextremismus-Datei ist im Zusammenhang mit der Aufdeckung der NSU-Terrorzelle im Jahr 2011 zu sehen, die auch Defizite bei der sicherheitsbehördlichen Datenverarbeitung aufzeigte.[232] Die Schaffung der Antiterrordatei war eine Reaktion auf Bedrohungen des internationalen Terrorismus unter dem Eindruck der Terroranschläge vom 11. September 2001.[233]

Gerade schwer ausrechenbare, aber gewichtige Bedrohungen wie jene des Terrorismus können ein verstärktes Bedürfnis zur Risikovorsorge durch Maßnahmen wie die Informationssammlung auslösen.[234] In der Praxis scheinen es die gesellschaftlichen Erwartungen und die politischen Reaktionen auf derartige Bedrohungen konkret zu erschweren, auf die neuen Informationsressourcen und die darin gespeicherten Daten zu verzichten, wenn sie einmal vorhanden sind. Auch wenn es als sehr unwahrscheinlich erscheint, dass bestimmte Daten und Informationsressourcen konkret zur Abwehr von diffusen Bedrohungen oder zur Strafverfolgung beitragen können, werden diese im Zweifel lieber weiter betrieben als abgeschafft, wie ein*e Mitarbeiter*in der Datenschutzaufsicht berichtet:

> „Zum Beispiel die Antiterrordatei und die Rechtsextremismus-Datei, sagt uns die praktische Polizei, sind rein politische Datenbanken. Die Datenbestände, die dort drin sind, haben die auch in anderen Datenbanken, weshalb sie kaum auf diese Spezialdatenbanken zugreifen. Aber natürlich hat niemand dort den Mut zu sagen: Brauchen wir gar nicht! Wahrscheinlich wäre das auch politisch schwer vermittelbar, warum man jetzt eine Rechtsextremismus-Datei

[231] Siehe oben A. III. 1. a.
[232] Siehe oben Teil 1 B. V.
[233] Vgl. näher zur Entstehungsgeschichte BVerfGE 133, 277 (293 f.); *Prügel*, ZIS 2013, 529 f.
[234] Vgl. *Ericson/Haggerty*, S. 420.

> wieder abschafft. [...] Und dann herrscht bei der Polizei, das mag möglicherweise auch mit der konservativen Einstellung der Polizei zu tun haben, eine gewisse Ängstlichkeit: Wir speichern lieber zu viele Daten und lieber ein bisschen länger, nicht dass es dann Ärger gibt mit irgendjemandem, mit der Staatsanwaltschaft oder mit der Politik, bei der Aufarbeitung zum Beispiel vom NSU-Komplex oder vom Breitscheidplatz-Attentat und so weiter. Lieber zu viel und zu lange speichern, man könnte es ja noch gebrauchen. Oder: Wir könnten ja Ärger bekommen, wenn wir es nicht machen. Das ist wirklich ein Problem." (DSA2)

Dass für die kriminalbehördliche bzw. polizeiliche Arbeit nicht mehr erforderliche Daten zu lange gespeichert bleiben, kann schließlich auch auf unklaren Verantwortlichkeiten für die Löschung dieser Daten beruhen, wie ein*e Mitarbeiter*in der Datenschutzaufsicht berichtet:

> „Die Polizei und die Staatsanwaltschaften – wenn beide zusammenarbeiten, gibt es manchmal große Probleme. Die Staatsanwaltschaft ordnet eine Telekommunikationsüberwachung an. Die Polizei führt sie durch, speichert die Bänder, wertet die dann aus für die Staatsanwaltschaft. Aber für die Löschung, also die Anweisung der Löschung, ist wieder die Staatsanwaltschaft zuständig. Sie [die Landespolizei] haben jetzt bei unserer Prüfung festgestellt, dass sie teilweise aus den 90er-Jahren noch Bänder hatten, bei der Polizei, die sie gar nicht mehr abspielen konnten. Weil die Technik gar nicht mehr da war. Aber man hatte das alles noch, weil es hat ja keiner gesagt: ‚Schmeiß es weg.' Das sind so Sachen, das hat man häufig. Wir haben viele Bereiche, wo Polizei länderübergreifend zusammenarbeitet. Wo es Kooperationen gibt, wo einer was für andere Bundesländer macht. Und immer, wenn wir so geteilte Zuständigkeiten haben, passiert es einfach schnell, dass irgendwo Daten liegen, die derjenige, der sie verwaltet, eigentlich nicht benötigt. Und derjenige, der den Auftrag gegeben hat, weiß gar nicht mehr, dass sie da sind. Oder interessiert sich nicht dafür." (DSA4)

Hieraus lässt sich der Schluss ziehen, dass die Verantwortlichkeiten für die Ordnung und Löschung von Daten jedenfalls intern eindeutig geklärt sein müssen, um Verantwortungsdiffusionen zu vermeiden.

3. Konsequenzen

Das Wachstum der kriminalbehördlichen Datenbestände wirkt sich auf die Verfügbarkeit, die Verknüpfbarkeit und die Qualität der gespeicherten Daten aus und verändert die konkreten Anforderungen an die Informationsordnung.

Dass die kriminalbehördlichen Datenbestände wachsen, kann zunächst dazu führen, dass relevante Informationen hierin schwerer auffindbar werden. Dies berichteten zwei der im Rahmen dieser Untersuchung interviewten Mitarbeiter*innen von Datenschutzaufsichtsbehörden (DSA2, DSA4). Sie gaben an, im Rahmen ihrer Kontrolltätigkeiten auf Schwierigkeiten in dieser Hinsicht gestoßen zu sein. Als konkretes Beispiel für eine Informationsressource, bei der die wachsende Datenmenge zu Problemen bei der Auffindbarkeit relevanter Informationen führe, nannte ein*e Befragte*r die Falldatei Rauschgift (DSA2). Die möglichen Probleme bei der Verfügbarkeit von Daten aufgrund wachsender Bestände sind vielgestaltig. So ist es etwa möglich, dass Abfragen aus größeren Datenbeständen weniger eindeutige Treffer hervorbringen. Wie genau das wachsende Datenvolumen Abrufe aus einzelnen Ressourcen beeinträchtigt, hängt aber konkret davon ab, welche zusätzlichen Informationen auf welche Weise darin gespeichert werden.

Die im Rahmen dieser Untersuchung befragten Anwender*innen polizeilicher Datenbanken benannten als Problem bei der Verfügbarkeit von Daten vor allem die Vielzahl von Informationsressourcen, die sie für einzelne Ermittlungen abzurufen hätten. Dieses Problem hängt mit der wachsenden Anzahl von Informationsressourcen zusammen, ist aber im Schwerpunkt ein Problem ihrer Interoperabilität und soll daher in diesem Zusammenhang näher erörtert werden.[235]

Ähnliche Probleme wie bei der Verfügbarkeit ergeben sich bei der Verknüpfbarkeit von Daten. Je größer Datenbestände werden, desto schwieriger erscheint es, diese sinnvoll auszuwerten. Die Verknüpfung verschiedener Informationsressourcen und ihrer Inhalte ist unter anderem deswegen zu einer immer größeren Herausforderung geworden, weil nicht nur die Zahl der vorhandenen Informationsressourcen, sondern auch die Menge der darin gespeicherten Daten gestiegen ist und weiter steigt.[236] Bereits in der Anfangszeit des Einsatzes der EDV-basierten polizeilichen Informationssysteme versprachen sich die Anwender*innen, durch die neue Technik einer „Informationsflut" Herr zu werden. Die neuen Systeme sollten helfen, vorhandene und neu eingehende Informationen besser zu sortieren und effektiver zu bearbeiten. Allerdings haben sich ebenfalls durch den Einsatz der EDV-Technik die vorhandenen Datenbestände vervielfacht. Heute besteht besonders die Herausforderung, aus den großen Datenmengen relevante Informationen herauszufiltern. Bei dieser Suche nach der „Nadel im Heuhaufen" sollen automatisierte Verfahren helfen. Mitunter setzen Kriminalbehörden auf den Einsatz lernfähiger Systeme, bei denen Methoden der künstlichen Intelligenz zur

[235] Siehe unten II. 1.
[236] *Thiel*, GSZ 2021, 97 (100 f.).

Anwendung kommen. Diese Systeme sollen es ermöglichen, das Potential großer Datenbestände auszuschöpfen und hieraus neue Informationen extrahieren.[237]

Schließlich kann das Wachstum der kriminalbehördlichen Datenbestände die Datenqualität beeinträchtigen. Je größer der Datenbestand ist, desto schwerer fällt die Sicherung seiner Qualität.[238] Auch die im Rahmen dieser Untersuchung interviewten Anwender*innen polizeilicher Informationsressourcen betrachteten die Sicherung der Datenqualität angesichts des Wachstums als Herausforderung. Ohne ein funktionierendes Qualitätsmanagement drohen vor allem polizeiliche Informationsressourcen zu „Datenfriedhöfen" zu werden, in denen immer weiter veraltete und praktisch nicht langfristig nutzbare Informationen abgelagert werden.

II. Fehlende Interoperabilität der Informationssysteme

Neben dem Wachstum der Datenbestände hat sich die fehlende Interoperabilität verschiedener kriminalbehördlicher Informationsressourcen als besondere Herausforderung für die kriminalbehördliche Informationsordnung herausgestellt. Auch hier soll zunächst die grundlegende Problematik erörtert werden (1.), um anschließend auf ihre Ursachen einzugehen (2.). Schließlich werden die Konsequenzen für die dargestellten Anforderungen an die Informationsordnung betrachtet (3.).

1. Defizite bei Kompatibilität und Interoperabilität

Die Kriminalbehörden in Bund und Ländern betreiben eine Vielzahl von Informationssystemen, die nur eingeschränkt miteinander kompatibel sind. Die vorhandene zersplitterte Landschaft der Informationsordnung ist das Resultat eines organischen Entwicklungsprozesses.[239] Gerne wird besonders die polizeiliche Informationsordnung zur Veranschaulichung als „verschachteltes Gebäude"[240] beschrieben, das durch – nicht mit dem Gesamtsystem abgestimmte – Anbauten immer weiter angewachsen ist.[241] Die diversen Informations- und Dateisysteme wurden in der Regel von einzelnen Akteuren zur Lösung deren spezifischer Probleme eingerichtet.[242] Die Kompatibilität mit den Systemen anderer Behörden und Überlegungen zur Zentralisierung spielten beim Aufbau der Informationsressourcen in den meisten Behörden – wenn überhaupt – nur

[237] Vgl. den aktuellen Ideen von „Big Data"-Anwendungen bereits sehr nahe *Herold*, in: Taschenbuch für Kriminalisten, S. 240 (242).

[238] *Gärditz*, Der Staat 54 (2015), 113 (115 f.).

[239] Vgl. BMI, Polizei 2020, S. 2; siehe zu der Entwicklung im Einzelnen oben Teil 1 B. III. und IV.

[240] So BKA-Präsident *Holger Münch* im Interview mit dem Deutschlandfunk vom 4. Dezember 2017; https://www.bka.de/DE/Presse/Interviews/2017/171204_InterviewMuenchDLF.html.

[241] Vgl. auch *Sehr*, Kriminalistik 1999, 532.

[242] Vgl. *Petri*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 390.

eine untergeordnete Rolle. Die Erhebung und Verarbeitung von Daten in den polizeilichen Informationssystemen des Bundes und der Länder erfolgt daher bis heute nach unterschiedlichen Standards.[243]

Nur teilweise wurden die Heterogenität und fehlende Interoperabilität der polizeilichen Informationssysteme in der Anfangszeit ihres Einsatzes in den 1970er-Jahren als Probleme ausgemacht. Das Bundeskriminalamt bemühte sich zu dieser Zeit bereits um verbindliche einheitliche Rahmenbedingungen für polizeiliche Informationssysteme.[244] Allerdings begegneten diese Bemühungen erheblichen Widerständen bei den Landesbehörden und hatten keinen durchschlagenden Erfolg.[245] Ein 1978 durch die Innenministerkonferenz beschlossenes Neuordnungskonzept für INPOL, das eine stärkere Zentralisierung vorsah, wurde nicht umgesetzt.[246]

Mittlerweile haben sich die Probleme der Heterogenität und mangelnden Interoperabilität der polizeilichen Informationssysteme weiter verschärft. Fehlende Abstimmungen bei der Identifizierung der Kompatibilitätsprobleme sowie der Entwicklung und Beschaffung der Systeme werden nach wie vor beklagt.[247] Unterschiedliche technische Standards bei der Erhebung und Speicherung von Daten werden als Grund dafür angeführt, dass Daten in mehreren Systemen redundant eingegeben und aufwändig gepflegt werden müssen, damit sie aktuell und richtig bleiben.[248]

2. Ursachen

Dass der Kompatibilität und Interoperabilität der kriminalbehördlichen Informationsressourcen von den meisten Stellen nur wenig Beachtung geschenkt wurde und wird, liegt nach bisherigen Erkenntnissen zu einem erheblichen Maße in dem Verhältnis der Behörden zueinander sowie in ihren spezifischen Eigeninteressen begründet.

Als Ursache für die frühen Widerstände gegen eine stärkere Zentralisierung der polizeilichen Informationsordnung werden Interessen der Polizeien am Schutz ihrer Zuständigkeitsbereiche und Informationsressourcen gesehen. Die Polizeien hatten erhebliche personelle und finanzielle Investitionen in ihre ersten EDV-Strukturen getätigt.[249] Der Zugriff auf Informationen und der Betrieb eigener Systeme gestaltete sich praktisch als Machtfrage. Darüber hinaus trugen auch datenschutzrechtliche Bedenken sowie haushaltsrechtliche Vorgaben dazu bei, dass in der frühen Phase der polizeilichen

[243] BT-Drs. 18/11163, S. 84.
[244] Vgl. *Abbühl*, S. 161; siehe auch oben Teil 1 B. III. 1.
[245] Kritisch dazu *Ziercke*, in: Pitschas/Stolzlechner, S. 63 (71).
[246] Vgl. *Bergien*, Zeithistorische Forschungen, 2017, 258 (269) m.w.N.
[247] Vgl. *Petri,* in: Lisken/Denninger, 6. Aufl. 2018, Kap. G Rn. 388.
[248] BT-Drs. 18/11163, S. 84; BMI, Polizei 2020, S. 2.
[249] Anschaulich *Bergien*, Zeithistorische Forschungen, 2017, 258 (265).

Informationsordnung keine umfassende Zentralisierung beim Bundeskriminalamt erfolgte.[250]

3. Konsequenzen

Die Defizite bei der Interoperabilität verschiedener Informationsressourcen wirken sich in erster Linie auf die Verfügbarkeit und Verknüpfbarkeit von Daten aus. Sie erschweren es, Daten aus anderen Behörden abzurufen und direkt mit eigenen Beständen zu verknüpfen.[251]

So erklärten auch die für diese Untersuchung interviewten Anwender*innen polizeilicher Datenbanken, dass besonders durch die fehlende Interoperabilität von Systemen die Verfügbarkeit von Daten beeinträchtigt werde (POL1, POL3). Die Notwendigkeit, sich in den Systemen jeweils einzeln anzumelden, um Daten abzurufen, erschwere die tägliche Arbeit in der Praxis. Ein*e polizeiliche*r Anwender*in berichtete:

> „Was bei uns im Land die Usability massiv stört ist, dass wir kein Single Sign-On haben. Das heißt, für jede Datenbank habe ich eigene Benutzerdaten, für die sich die Passwörter in unterschiedlichen Zyklen ändern. Sprich, ohne einen vernünftigen Passwort-Manager verliere ich irgendwann den Überblick. Weil ich mich dann für jede Anwendung neu anmelden muss, was natürlich den Benutzerkomfort massiv einschränkt." (POL1)

Die befragten Anwender*innen betonten den erheblichen Arbeitsaufwand, der durch das Fehlen eines einheitlichen Abfragesystems entstünde. Zur Veranschaulichung dienen die folgenden Zitate:

> „Ich muss jetzt immer auf verschiedene Stellen zugreifen, im Intranet. Ich habe keine einheitliche Oberfläche. Ich habe nicht einen Punkt, wo ich alle Datenbanken abfragen kann. Man hat zwar bei uns im Land eine Stelle im Intranet, wo dann die entsprechende Links drin sind. Aber nicht so, dass ich mich jetzt in einer Oberfläche anmelde und dann meine Abfragen durchführen kann. Sondern es sind jedes Mal einzelne Produkte, wo man sich einloggen muss." (POL1)
>
> „...da gibt es unglaublich viele Systeme, einzelne Systeme, um eine Person zu überprüfen. Und da muss ich jetzt eine Person überprüfen und muss die Daten des Kraftfahr-Bundesamtes abfragen. Ich muss Daten der Einwohnermeldebehörden abfragen. Ich muss Daten der Ausländerbehörde abfragen. Ich muss Daten des polizeilichen Informationsverbundes abfragen. Haben Sie

[250] Vgl. *Abbühl*, S. 161; *Bergien*, Zeithistorische Forschungen, 2017, 258 (261 ff.).
[251] Vgl. BMI, Polizei 2020, S. 2; vgl. auch *Creemers*, in: Grutzpalk, S. 101 (109 f.).

mitgezählt, wie viele Dateien das sind? Ich muss meine eigenen Daten in [Land] abfragen." (POL3)

Zwischenergebnis

Die wesentlichen Anforderungen an die kriminalbehördliche Informationsordnung aus Sicht ihrer Anwender*innen haben sich seit der Einführung von Technologien zur elektronischen Datenverarbeitung stark verändert.

Im Zusammenhang mit der Verfügbarkeit von Daten hat sich die Erwartung durchgesetzt, dass Daten innerhalb von kürzester Zeit von überall abgerufen werden können. Dies betrifft auch Daten aus der Beständen anderer als der eigenen Behörde. Vor allem aufgrund der eingeschränkten Kompatibilität der Systeme verschiedener (Polizei-)Behörden wird diese Erwartung in der Praxis nicht erfüllt. Aus Sicht der Betroffenen, über die Informationen in kriminalbehördlichen Ressourcen gespeichert sind, erscheint eine allzu leichte Verfügbarkeit der Daten als problematisch. Sie können bereits durch das Vorhandensein von Informationen in kriminalbehördlichen Informationsressourcen stigmatisiert und kriminalisiert werden. Ihre Interessen sind im Zusammenhang mit den rechtlichen Anforderungen an die Speicherung und den Abruf von Daten zu berücksichtigen, welche aktuell recht offen ausgestaltet sind.

Noch stärker als die Anforderungen an die Verfügbarkeit von Daten haben sich im Laufe der Zeit die Anforderungen an die Verknüpfbarkeit von Daten verändert. Gerade in jüngerer Vergangenheit haben die allgemeine Tendenz zu einer stärkeren Vernetzung im Sicherheitsbereich sowie technologische Entwicklungen, die auch die Auswertung scheinbar belangloser Daten attraktiv scheinen lassen, dazu beigetragen, dass der Wunsch, komplexe Verknüpfungen zwischen Daten aus den Beständen verschiedener Behörden herzustellen, allgegenwärtig ist. Auch hier sind die Realität der kriminalbehördlichen Informationsordnung und die Wünsche ihrer Anwender*innen allerdings weit voneinander entfernt. Der Verknüpfung der Datenbestände steht die Inkompatibilität der verwendeten Systeme entgegen. Auch die für komplexere Verknüpfungen notwendigen Rechtsgrundlagen sind nur in Ansätzen vorhanden. Es bedürfte hierfür spezieller Regelungen mit gehobenen Anlassschwellen sowie angemessenen prozeduralen Sicherungen. Denn durch die Komplexität der angestrebten Verknüpfungen entstehen auch komplexe Risiken für die von der Datenverarbeitung Betroffenen. Es kann nicht nur zu einer möglicherweise fehlerhaften algorithmisierten Zuschreibung von Eigenschaften, sondern auch zu Verwechslungen kommen. Derartige Fehler können für die Betroffenen äußerst folgenreich sein.

Dass Daten sich innerhalb der kriminalbehördlichen Informationsordnung sinnvoll miteinander verknüpfen lassen, erfordert, dass sie inhaltlich richtig und aktuell sind. Mängel bei der Datenqualität sind sowohl für die Betroffenen als auch für die Anwender*innen der kriminalbehördlichen Informationsordnung problematisch. Sie bedingen Risiken wie jene der Stigmatisierung und Kriminalisierung, können aber auch dazu führen, dass „falsche Fährten" entstehen, Ermittlungen fehlgeleitet und damit behördliche Ressourcen verschwendet werden. Gerade mit dem zunehmenden Wunsch, Daten miteinander zu verknüpfen, nimmt prinzipiell auch die Bedeutung der Datenqualität zu. Dennoch wird diese Anforderung an die Informationsordnung im Vergleich zu den Anforderungen der Verfügbarkeit und Verknüpfbarkeit von Daten in der Praxis weniger stark betont. Zwar existieren grundlegende rechtliche Anforderungen an die Qualität personenbezogener Daten, allerdings sind diese weitgehend unspezifisch ausgestaltet. Aus praktischer Sicht werden – vor allem von Seiten der Datenschutzaufsicht – Mängel bei der Qualität der von den Kriminalbehörden vorgehaltenen Daten beklagt.

Als gemeinsame tatsächliche Herausforderungen bei der Gewährleistung der Verfügbarkeit und Verknüpfbarkeit sowie einer ausreichenden Datenqualität stellen sich das stetige Wachstum der Menge der vorhandenen kriminalbehördlichen Informationsressourcen und der darin vorgehaltenen Daten sowie Mängel bei der Kompatibilität der Systeme miteinander heraus. Bezogen auf das Wachstum der Datenbestände lassen sich konsequente Anstrengungen, überflüssigen Informationsballast loszuwerden und die Struktur von Informationssystemen in dieser Hinsicht zu verbessern, kaum nachvollziehen. Ein Positivbeispiel ist allerdings die Überprüfung der Datei „Gewalttäter Sport" unter anderem hinsichtlich ihrer Erfassungs- und Speicherkriterien durch eine Bund-Länder-Arbeitsgruppe, welche dazu führte, dass die Menge der gespeicherten Daten abnahm und die Datenqualität sich verbesserte. Es wäre wünschenswert, wenn kritische Überprüfungen dieser Art für alle Informationsressourcen Schule machen würden. Das Problem der mangelnden Kompatibilität der Systeme zieht sich durch die gesamte Entwicklung der kriminalbehördlichen Informationsordnung. Versuche, die Kompatibilität der Systeme, etwa durch zentralisierte Lösungen, zu verbessern, sind immer wieder gescheitert. Derartige Bemühungen lassen sich aber auch heute im Rahmen des Programms Polizei 20/20 nachvollziehen.

Teil 3

Fortbildung des Rechts der kriminalbehördlichen Informationsordnung

Der dritte und abschließende Teil der Arbeit betrachtet, ob bestimmte Änderungen oder Ergänzungen der rechtlichen Regelungen zur kriminalbehördlichen Informationsordnung dazu beitragen könnten, den Anforderungen der Anwender*innen sowie den Interessen der in den Systemen gespeicherten Personen besser gerecht zu werden als bisher. Er untersucht auf Grundlage der im Verlauf der Untersuchung gewonnenen Erkenntnisse Möglichkeiten, um den Ist-Zustand der kriminalbehördlichen Informationsordnung durch rechtliche Regelungen ihrem Soll-Zustand anzunähern.

Zwar ist die Wirkungsmacht rechtlicher Vorgaben in einem Bereich, in dem technische Faktoren, Verwaltungsstrukturen und rechtliche Regelungen auf komplexe Art und Weise zusammenwirken, naturgemäß begrenzt. Das Recht sollte allerdings zumindest Leitlinien für die Handhabe der kriminalbehördlichen Informationsordnung vorgeben. Angesichts der aktuell geringen Regelungsdichte im Informationsordnungsrecht erschiene eine Konkretisierung der Vorgaben naheliegend.

Konkret werden vier Aspekte betrachtet, zu denen neue Regelungen geschaffen bzw. die bestehenden Regelungen geändert werden könnten. Erstens wird die Möglichkeit untersucht, die Informationsordnung stärker als bisher zu zentralisieren und hierfür neue Befugnisse des Bundeskriminalamtes zu schaffen (A.). Zweitens wird erwogen, ob und inwiefern das System der informationsordnenden Befugnisse im Polizei- und Strafprozessrecht etwa durch eine Ausgliederung dieser Regelungen umstrukturiert werden könnte (B.). Drittens wird mit Blick auf die konkreten Befugnisse beleuchtet, wie sich die Anlässe für informationsordnende Tätigkeiten konkreter als bisher regeln lassen könnten (C.). Viertens werden Möglichkeiten in den Blick genommen, nähere Regelungen für kriminalbehördliche Informationsressourcen zu schaffen, deren Fokus nicht auf den Vorgängen des Speicherns und Ordnens von Informationen, sondern auf der Ausgestaltung der Systeme und den Rahmenbedingungen für die Datenverarbeitung liegt (D.).

Für jeden dieser Aspekte wird beleuchtet, welchen Herausforderungen und Problemen durch eine Anpassung der rechtlichen Regelungen begegnet werden könnte. Weiter werden die verfassungsrechtlichen Möglichkeiten und Grenzen für die Anpassung untersucht. Schließlich werden konkrete Ansätze für eine mögliche rechtliche Regelung vorgestellt.

A. Stärkere behördliche Zentralisierung der Informationsordnung

Derzeit werden Informationsressourcen von einer Vielzahl von Polizeien und Staatsanwaltschaften betrieben. Überlegungen zu einer stärkeren Zentralisierung der kriminalbehördlichen Informationsordnung sind aber schon seit langer Zeit nachzuvollziehen. Dies gilt vor allem für den polizeilichen Bereich. In den 1970er-Jahren setzte sich der damalige BKA-Präsident *Horst Herold* für eine zentrale Organisation der Datenverarbeitung in einem Verbund der Polizeien nach dezentraler Erhebung der Daten ein.[1] Diese Philosophie lag auch dem 1972 umgesetzten INPOL zugrunde.[2] Die Verantwortung für den Betrieb von INPOL bzw. heute INPOL-neu liegt seit jeher beim Bundeskriminalamt als Zentralstelle für den polizeilichen Informationsverbund. Dennoch existiert daneben eine Vielzahl einzelner Informationsressourcen in Bund und Ländern.

Eine weitere Verdichtung der kriminalbehördlichen Informationsordnung beim Bundeskriminalamt als Zentralstelle könnte durch die Einführung des „neuen Datenhauses" für die Polizei im Rahmen des Programmes Polizei 20/20 erfolgen. Das Programm zielt auf eine Vereinheitlichung der Informationsarchitektur der deutschen Polizeien und eine Abschaffung der bisherigen Strukturierung von Informationen in Dateien. Das Bundeskriminalamt soll eine noch wichtigere Rolle als bisher bei der Organisation des Informationsverbundes einnehmen.[3] Rechtlich sind die Weichen hierfür bereits gestellt.[4]

Überlegungen zu einer stärkeren behördlichen Zentralisierung der kriminalbehördlichen Informationsordnung können in einem größeren Zusammenhang als Aspekt einer allgemeinen Tendenz zur Zentralisierung im Sicherheitsbereich betrachtet werden, die auch – aber nicht nur – die Polizei betrifft.[5] Nach dem zweiten Weltkrieg war der

---

[1] *Herold*, in: Göppinger/Witter, S. 208 (231); *Herold*, in: Taschenbuch für Kriminalisten, S. 240 (246 ff.) (bereits vor *Herolds* Amtszeit als BKA-Präsident erschienen); vgl. dazu auch *Busch/Funk/Kauß/Narr/Werkentin*, S. 117; *Schwinghammer*, KrimJ 1980, 241 (249).

[2] Siehe oben Teil 1 B. III. 1.

[3] Siehe im Einzelnen oben Teil 1 B. III. 3.

[4] Siehe zu der Zentralstellenfunktion nach dem BKAG 2018 unten II. 1.

[5] Vgl. zur Zentralisierung im Sicherheitsrecht *Gusy*, VerwArch 101 (2010), 309 (324); *Kugelmann*, Die Verwaltung 2014, 25 (51); *Poscher*, in: Vesting/Korioth, S. 245 (247 f.); *Roggan*, NJW 2009, 257 (262); *Schulze-Fielitz*, in: FS Schmitt Glaeser, S. 407 (414 f.); *Wolff*, DÖV 2009, 597 (599); speziell zur Terrorismusbekämpfung *Bäcker*, GSZ 2018, 213 ff.; zur Zusammenführung der Verfassungsschutzbehörden *Gärditz*, AöR 144 (2019), 81 ff.; *Gusy*, ZRP 2012, 230 f. Aus dem weiteren sicherheitsrechtlichen Blickwinkel wird unter dem Aspekt der Zentralisierung unter anderem die Annäherung von Polizei und Nachrichtendiensten diskutiert; vgl. *Mehde*, JZ 2005, 815 (817).

(Wieder-)Aufbau der Kriminalpolizei in Deutschland von dem Ziel der Dezentralisierung geprägt.[6] Dieses sowohl von den Besatzungsmächten als auch von den Ländern getragene Ziel war jedoch von Anfang an umstritten.[7] Ein Grund für aktuelle Bemühungen im Sicherheitsbereich, Aufgaben und Befugnisse bei einzelnen (Bundes-)Behörden zusammenzuführen, sind neue Bedrohungen der öffentlichen Sicherheit, unter anderem durch den internationalen Terrorismus.[8] Diese Bedrohungen setzen die vorhandenen dezentralen Strukturen in der Sicherheitsarchitektur unter Legitimationsdruck.[9] Dies gilt auch für die Informationsordnung der Kriminalbehörden und anderer Sicherheitsbehörden. Es werden immer wieder Defizite bei der Verfügbarkeit und Verknüpfbarkeit von Informationen in dezentralen Systemen ausgemacht.[10] Vereinzelt werden aber auch die Vorteile kleinteiligerer und flexibler Organisationsstrukturen betont, die großen zentralen Einrichtungen im Einzelfall überlegen sein können, wenn sie vernetzt agieren und effizient kooperieren.[11]

Die Tendenzen zur Zentralisierung im Sicherheitsbereich stehen auch in einem Zusammenhang mit technischen Entwicklungen. Dies lässt sich historisch nachvollziehen. Im 19. Jahrhundert führten Fortschritte in der Technik und im Verkehrswesen dazu, dass die Kriminalität mobil wurde.[12] Daraus resultierten Forderungen, zentrale polizeiliche Einrichtungen zu schaffen, um etwa gegen „reisende Verbrecher" vorzugehen.[13] Besonders in den 1970er-Jahren verstärkten sich Tendenzen zur Zentralisierung polizeilicher Tätigkeiten, die von informationstechnischen Entwicklungen getrieben waren. So verwies etwa die Begründung des BKAG 1973,[14] das die Funktion des Bundeskriminalamts als Zentralstelle erstmals ausdrücklich regelte und seine Aufgaben erheblich erweiterte,[15] prominent darauf, dass „[d]ie Entwicklung der Kriminalität, die durch

[6] *Abbühl*, S. 51; *Harnischmacher/Semerak*, S. 193; vgl. zu der Möglichkeit der Verankerung eines dezentralisierten Aufbaus der Polizei im Grundgesetz Stenografisches Protokoll der 5. Sitzung des Ausschusses für Zuständigkeitsabgrenzung am 29. September 1948, in: Werner, Der Parlamentarische Rat 1948–1949, Bd. 3, 1986, S. 173 (216 f.).

[7] Vgl. *Gusy*, DVBl. 1993, 1117 (1119).

[8] So führten etwa die Terroranschläge vom 11. September 2001 im Zuge der Föderalismusreform zur Einführung einer ausschließlichen Gesetzgebungskompetenz des Bundes für die Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalpolizeiamt (Art. 73 Abs. 1 Nr. 9a GG); BGBl I 2006, S. 2034. Auf dieser Grundlage wurde das BKAG zum 25. Dezember 2008 reformiert; BGBl I, S. 3083; vgl. dazu *Roggan*, NJW 2009, 257 ff.

[9] *Mehde*, JZ 2005, 815 (817).

[10] Siehe dazu im Einzelnen oben Teil 2 A. I. und B. I.

[11] Vgl. *Gusy*, VerwArch 101 (2010), 309 (327); *Poscher*, in: Vesting/Korioth, S. 245 (252).

[12] *Abbühl*, S. 13 m.w.N.

[13] Vgl. *Abbühl*, S. 13; *Ahlf*, Das Bundeskriminalamt, S. 8 f.; *H. Albrecht*, S. 9; *Dickopf/Holle*, S. 8 f., *Zirpins*, S. 14 f.

[14] Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes in der Fassung vom 29. Juni 1973, BGBl. I, S. 704 ff.

[15] Vgl. *Abbühl*, S. 130 f.; *Kubica/Leineweber*, NJW 1984, 2068.

hohe Mobilität und zunehmende internationale Zusammenarbeit der Verbrecher gekennzeichnet ist, [...] in verstärktem Maße einen raschen zentral gesteuerten Informationsaustausch erforderlich“[16] mache. Heute werden für die Notwendigkeit einer Zentralisierung sicherheitsbehördlicher Aufgaben und Befugnisse unter anderem Bedrohungen aus dem Cyberraum angeführt, die nicht vor Staats- und Landesgrenzen Halt machen.[17] Der technologische Fortschritt eröffnet eine neue Perspektive auf den dezentralen Aufbau von Sicherheitsbehörden und dessen verfassungsrechtliche Fundamente. Es stellt sich unter anderem die Frage, welche Rolle die technologische Entwicklung für die Auslegung der verfassungsrechtlichen Grundlagen der kriminalbehördlichen Informationsordnung und anderer Felder spielt.

Im Folgenden wird zunächst betrachtet, inwiefern weitere behördliche Zentralisierungen bei der Informationsordnung dazu beitragen könnten, bestehende Herausforderungen und Probleme zu lösen (I.). Darauf werden verfassungsrechtliche Grenzen der Zentralisierung untersucht (II.). Schließlich werden konkrete Möglichkeiten einer stärkeren behördlichen Zentralisierung betrachtet, namentlich eine Erweiterung der Aufgaben und Befugnisse des Bundeskriminalamts als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen (III.).

I. Beitrag zur Lösung bestehender Herausforderungen

Eine stärkere behördliche Zentralisierung der kriminalbehördlichen Informationsordnung könnte vor allem jenen Problemen abhelfen, die im Zusammenhang mit der mangelnden Kompatibilität und Interoperabilität der verwendeten Systeme stehen. Je stärker die Ausgestaltung der Informationsressourcen bei einer Stelle liegt und je souveräner diese über die Ordnung und Form der Speicherung der dort abzulegenden Daten entscheiden kann, desto wahrscheinlicher ist es, dass die Daten unter gleichen technischen Voraussetzungen zugänglich und miteinander verknüpfbar sind. Bisher wird es als wesentliches Hindernis für die leichte Verfügbarkeit und Verknüpfbarkeit von Daten angesehen, dass verschiedene Kriminalbehörden ihre Informationsressourcen unabhängig voneinander und nach unterschiedlichen technischen Maßstäben einrichten und betreiben.[18]

[16] BT-Drs. 7/178, S. 1.

[17] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde auf dieser Grundlage bereits mit neuen Befugnissen ausgestattet; Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14. August 2009; BGBl. I, S. 2821; vgl. dazu *Poscher*, in: Vesting/Korioth, S. 245 (248). Aktuell fordern das Bundeskriminalamt und der Bundesnachrichtendienst zentrale Befugnisse zur Abwehr entsprechender Gefahren; vgl. *Münch*, Kriminalistik 2019, 11 (12 ff.). Im Gegensatz zu den defensiven Befugnissen des BSI sind die Forderungen des Bundeskriminalamts und Bundesnachrichtendienstes dagegen eher offensiv ausgerichtet und zielen unter anderem auf Maßnahmen wie „Hackbacks“.

[18] Siehe oben Teil 2 D. II.

Eine zentralisierte Organisation der kriminalbehördlichen Informationsordnung könnte auch dabei helfen, die Qualität der gespeicherten Daten zu erhöhen. Dies könnte durch die zentrale Etablierung von Standards und Verfahren zur Speicherung und Überprüfung der Daten geschehen. Auf diese Weise könnte im Ergebnis ebenfalls die Verknüpfbarkeit der gespeicherten Informationen verbessert werden.

Nicht ganz unproblematisch erscheint eine stärkere Zentralisierung der kriminalbehördlichen Informationsordnung unter dem Gesichtspunkt des Datenschutzes. Die Bündelung der Entscheidungen über die Ausgestaltung der Informationsressourcen und die zunehmende Speicherung und Auswertung von Informationen bei einer einzelnen Stelle konzentriert auch die Datenmacht bei dieser. Das bestehende Nebeneinander von Informationsressourcen, die von einzelnen Kriminalbehörden geführt werden, ist zwar nicht aus Datenschutzgründen entstanden, sondern eher aufgrund der Zuständigkeiten der Behörden und ihren Machtinteressen. Es wirkt sich jedoch zugunsten des Persönlichkeitsschutzes der Informationssubjekte aus, da es auf diese Weise schwieriger ist, Informationen zu einzelnen Personen zu bündeln und zu verknüpfen als bei einer zentralen Datenhaltung.

In der Tendenz erscheint eine behördliche Zentralisierung der Informationsordnung datenschutzrechtlich problematischer als eine dezentrale Verwaltung der Informationsressourcen. Allerdings lässt sich nicht pauschal annehmen, dass eine behördliche Zentralisierung den Datenschutz schwächt. Eine belastbare Aussage wird sich erst aus dem konkreten Vergleich eines zentralisierten mit einem dezentralen Modell treffen lassen. Bei einer zentralisierten Organisation von Informationsressourcen kann es unter Umständen möglich sein, einheitliche Datenschutzstandards zu etablieren, die jene vereinzelt organisierter Systeme in der Praxis übertreffen, weil etwa die Mittel hierfür zentral effizienter eingesetzt werden. Auch gemeinsame Standards zur Sicherung der Datenqualität können im Sinne der Informationssubjekte sein. Konkret sollen für das im Rahmen des Programmes Polizei 20/20 geplante neuen „Datenhaus“ hohe Datenschutzstandards angestrebt werden. Allerdings erscheint es anhand der aktuell vorliegenden Konzepte noch zweifelhaft, ob die Vorkehrungen zum Datenschutz für den vorgesehenen Informationspool ausreichend sind.[19]

II. Rechtliche Möglichkeiten und Grenzen

Auf verfassungsrechtlicher Ebene stecken die in Art. 87 Abs. 1 Satz 2 GG geregelte Verwaltungskompetenz und die hiermit korrespondierenden Gesetzgebungskompetenzen aus Art. 73 Abs. 1 Nr. 10 GG die Möglichkeiten und Grenzen für eine behördliche

[19] Siehe oben Teil 1 B. 3. c.

Zentralisierung der kriminalbehördlichen Informationsordnung ab.[20] Demnach können durch Bundesgesetz Zentralstellen unter anderem für das polizeiliche Auskunfts- und Nachrichtenwesen sowie für die Kriminalpolizei eingerichtet werden. Auf dieser Grundlage hat der Gesetzgeber die Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und die Zentralstelle für die Kriminalpolizei beim Bundeskriminalamt eingerichtet. Die einfachgesetzlichen Regelungen über die Tätigkeiten des Bundekriminalamts als Zentralstelle finden sich in § 2 BKAG.

Unter dem Dach des Bundeskriminalamts bieten sich auch am ehesten Möglichkeiten für eine noch weitergehende Zentralisierung der kriminalbehördlichen Informationsordnung. Das Bundeskriminalamt ist die „Informations- und Technikzentrale“[21] der Polizeien, bei der die Fäden der polizeilichen Informationsordnung zusammenlaufen. Um die Möglichkeiten für eine weitergehende Zentralisierung beim Bundeskriminalamt zu untersuchen, werden im Folgenden zunächst die verfassungsrechtlichen Grundlagen der Zentralstellenfunktion und ihre einfachgesetzliche Umsetzung betrachtet (1.). Diese Funktion und ihrer gesetzliche Regelung wurden seit der Gründung des Bundeskriminalamts[22] stetig erweitert. Außerdem stellt sich die Frage, ob es auf Grundlage von Art. 87 Abs. 1 Satz 2 GG möglich wäre, das Bundeskriminalamt mit weiteren Befugnissen auszustatten, um seine Stellung als zentrale informationsordnende Behörde zu stärken (2.).

1. Die Zentralstellenfunktion

Was der Begriff Zentralstelle in Art. 87 Abs. 1 Satz 2 GG im Einzelnen bedeutet und mit welchen Aufgaben und Befugnissen sich entsprechende Stellen ausstatten lassen,

[20] Siehe hierzu bereits oben Teil 1 C. I. 2.

[21] *Zöller*, S: 137; vgl. ähnlich *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (8); *von Dietel*, DVBl. 1982, 939; *Simon/Taeger*, JZ 1982, 140.

[22] Noch vor Gründung des Bundeskriminalamts lässt sich als historisches Vorbild aus der Zeit vor Erlass des Grundgesetzes das im Reichskriminalpolizeigesetz vom 21. Juli 1922 (RGBl. I, S. 593) vorgesehene zentrale Reichskriminalpolizeiamt mit seiner zentralen Nachrichtenstelle betrachten; vgl. *Riegel*, DVBl. 1982, 720 (721); zu den Bemühungen zur Schaffung zentraler kriminalpolizeilicher Einrichtungen nach dem Ersten Weltkrieg *Schweppe*, S. 12 f. Im Parlamentarischen Rat war umstritten, ob das Grundgesetz die Möglichkeit zur Schaffung eines Bundeskriminal(polizei)amtes vorsehen sollte, da zum Teil davon ausgegangen wurde, man könne gemeinsame Fragen der Kriminalitätsbekämpfung sowie auch des Informationswesens auch durch Vereinbarungen der Länder regeln; vgl. Stenografisches Protokoll der 6. Sitzung des Hauptausschusses am 19. November 1948, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 14/I, 2009, S. 169 (199); *Uhle*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 73 Rn. 19.

ist unklar und bedarf näherer Erörterung.[23] Die Unklarheiten hängen auch mit der Entstehungsgeschichte der Regelung zusammen, die erst spät auf Grundlage des „Polizeibriefs" der westalliierten Militärgouverneure an den Parlamentarischen Rat vom 14. April 1949[24] in das Grundgesetz eingefügt wurde. Der Behördentyp der Zentralstelle war vor dieser Regelung in den Entwürfen des Grundgesetzes unbekannt. Die Eigenart von Zentralstellen lässt sich kurz so zusammenfassen, dass sie zur Kompensation von Nachteilen dienen, die aus der föderalen Kompetenzordnung entstehen.[25] Ein solcher Nachteil ist, dass das Auskunfts- und Nachrichtenwesen der Polizei jedes Landes im föderalen Staat prinzipiell ein Eigenleben führt und es schwer ist, relevante Informationen zusammenzuführen bzw. an die richtige Stelle zu leiten.

Im Sinne der Kompensation von Nachteilen der föderalen Ordnung ist eine Zentralstelle nach der Rechtsprechung des Bundesverfassungsgerichts „im Wesentlichen auf die Wahrnehmung von Koordinationsaufgaben beschränkt"[26]. Diese Interpretation herrscht auch in der Literatur vor.[27] Besonders für die Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen ist die Erfassung, Auswertung und Weitergabe von Informationen ein wichtiger Aspekt der Koordinationsaufgabe.[28] Auch die zentrale Organisation der Informationsordnung und ihres Aufbaus ist für all diese Tätigkeiten relevant.[29] Der Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen kommt damit die Aufgabe zu, die Organisation des Informationsverbundes mit den Landespolizeien zu sichern. In diesem Sinne lässt sich dem Bundeskriminalamt schon verfassungsrechtlich die Aufgabe einer technischen Harmonisierung der polizeilichen Informationsordnung zuschreiben.

---

[23] *Bäcker*, GSZ 2018, 213 (214); *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BKAG Rn. 3; so auch schon *Ahlf*, Das Bundeskriminalamt, S. 1 ff.; *Becker*, DÖV 1978, 551; *Gusy*, DVBl. 1993, 1117 (1120).

[24] Memorandum der Militärgouverneure zur Regelung der Polizeigewalt vom 14. April 1949, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 8, 1995, S. 230 f.; vgl. näher dazu Stenografisches Protokoll der 5. Sitzung des Ausschusses für Zuständigkeitsabgrenzung am 29. September 1948, in: Werner, Der Parlamentarische Rat 1948–1949, Bd. 3, 1986, S. 173 (206); Stenografisches Protokoll der 54. Interfraktionellen Besprechung vom 5. Mai 1939, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 11, 1997, S. 269 (271 f.); zur Entstehung *Imle*, S. 126 ff. Die mit Art. 87 Abs. 1 Satz 2 GG korrespondierende Passage des Memorandums lautet: „Der Bundesregierung ist es gestattet, unverzüglich Bundesorgane zur Verfolgung von Gesetzesübertretung und Bundespolizeibehörden auf folgenden Gebieten zu errichten: [...] b) Sammlung und Verbreitung von polizeilichen Auskünften und Statistiken".

[25] Vgl. *Gärditz*, S. 370.

[26] BVerfGE 110, 33 (51).

[27] *Abbühl*, S. 91; *Ahlf*, Das Bundeskriminalamt, S. 52; *Becker*, DÖV 1978, 551 (553 f.); *Hermes*, in: Dreier, GG, 3. Aufl. 2018, Art. 87 Rn. 47; *Ibler*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 87 Rn. 117 ff.

[28] Vgl. *Abbühl*, S. 91.

[29] Vgl. zur Aufbauorganisation als Aspekt der Koordination *Becker*, DÖV 1978, 551 (554).

Einfachgesetzlich und tatsächlich hat die Funktion des Bundeskriminalamts als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen immer weiter an Bedeutung gewonnen.[30] Sie wurde besonders seit den 1970er-Jahren gesetzlich erweitert,[31] was auch in einem Zusammenhang mit technischen Entwicklungen steht. Die Computerisierung führte zu einem grundsätzlichen Wandel der Bedeutung des Bundeskriminalamts bei der Erfüllung dieser Aufgabe.

Das erste BKAG, mit dem das Amt 1951 eingerichtet wurde,[32] sprach noch nicht ausdrücklich von einer Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen. Es wies dem Bundeskriminalamt diese Aufgabe aber nach § 2 Nr. 1 BKAG 1951 tatsächlich schon zu.[33] Demnach hatte das Bundeskriminalamt „alle Nachrichten und Unterlagen für die kriminalpolizeiliche Verbrechensbekämpfung und die Verfolgung strafbarer Handlungen zu sammeln und auszuwerten, soweit die Nachrichten und Unterlagen nicht eine lediglich auf den Bereich eines Landes begrenzte Bedeutung haben." Diese Sammlung und Auswertung von Nachrichten und Unterlagen sollte unter anderem durch die Führung einer zentralen Fahndungskartei sowie die Anlage eines Fahndungsbuches und eines Steckbriefregisters erfolgen.[34] Die Aufgabe sollte „sowohl die vorbeugende [...] wie die verfolgende kriminalpolizeiliche Tätigkeit des Bundeskriminalamtes zum Ausdruck bringen."[35] Die Bündelung von Informationen war in dieser Zeit die Hauptaufgabe des Bundeskriminalamts.[36]

Das BKAG 1973[37] wies dem Bundeskriminalamt die Funktion als Zentralstelle dann erstmals ausdrücklich zu (§ 2 Abs. 1 Nr. 1 BKAG 1973) und erweiterte seine Aufgaben zugleich erheblich.[38] Mit § 2 Abs. 1 Nr. 1 Satz 2 BKAG 1973 wurde das Amt zur „Zentralstelle für den elektronischen Datenverbund zwischen Bund und Ländern". In diesem Rahmen sollte es auch den Ausbau von INPOL koordinieren.[39] Der Auftrag des Bundeskriminalamts zur Sammlung und Auswertung von Nachrichten und Un-

[30] *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 3.

[31] So wie auch die Aufgaben des Bundeskriminalamts insgesamt; vgl. *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (8).

[32] Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (Bundeskriminalamtes) vom 8. März 1951, BGBl. I, S. 165 f.

[33] Vgl. *Abbühl*, S. 108 f.; *Niggemeyer*, DÖV 1960, 97 (98).

[34] BT-Drs. I/1273, S. 6; vgl. ausführlich zum Begriff des Sammelns in diesem Zusammenhang *Ahlf*, Das Bundeskriminalamt, S. 310 ff.

[35] BT-Drs. I/1273, S. 7.

[36] *Abbühl*, S. 22, 109.

[37] Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes in der Fassung vom 29. Juni 1973, BGBl. I, S. 704 ff.

[38] Vgl. *Abbühl*, S. 130 f.

[39] *Simon/Taeger*, JZ 1982, 140.

terlagen wurde auch auf solche Informationen erweitert, die keine überregionale Bedeutung haben.[40] Diese Erweiterung des Auftrags sah der Gesetzgeber als notwendig an, um die Behörde in die Lage zu versetzen, seine Aufgabe als Zentralstelle für den elektronischen Datenverbund zu erfüllen.[41]

Das BKAG 1997 behielt die Aufgabenformulierung des Bundeskriminalamts als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen aus dem BKAG 1973 im Wesentlichen bei.[42] Die Regelung wurde allerdings entzerrt. § 2 Abs. 1 BKAG 1997 regelte die allgemeine Aufgabe als Zentralstelle in der noch heute geltenden Formulierung. Daraus, dass sich die Zentralstellenfunktion auf die Verhütung und Verfolgung von Straftaten bezieht, wird deutlich, dass sie den präventiven wie auch den repressiven Tätigkeitsbereich umfasst.

Auch der in § 2 Abs. 2 Nr. 1 BKAG 1997 formulierte Auftrag, „zur Wahrnehmung dieser Aufgabe [als Zentralstelle] alle hierfür erforderlichen Informationen zu sammeln und auszuwerten", wurde in den späteren Fassungen des Gesetzes übernommen. Unter dem Sammeln ist neben der Entgegennahme von dezentral erhobenen Informationen deren aktive Beschaffung durch das Bundeskriminalamt zu verstehen, sofern es gesetzlich hierzu befugt ist.[43] Unter der Auswertung ist die Sichtung von Informationen nach ihrer Relevanz zu verstehen.[44] § 2 Abs. 3 BKAG 1997 sah schließlich den Betrieb des polizeilichen Informationssystems nach dem BKAG vor.[45] Auch diese Formulierung wurde bis zum BKAG 2018 beibehalten – mit der einzigen Ausnahme, dass in § 2 Abs. 3 BKAG nun nicht mehr von einem Informationssystem, sondern von einem Informationsverbund die Rede ist. Der hier bezeichnete Informationsverbund ist die zweite Säule der neuen Informationsordnung des Bundeskriminalamts – das in § 29 BKAG näher geregelte Verbundsystem.[46]

---

[40] BT-Drs. 7/178, S. 7; *Abbühl*, S. 130 f.; *Kubica*, ÖVD 1982, 109; vgl. auch *Riegel*, DVBl. 1982, 720 (723), der die Änderung des Gesetzeswortlauts in dieser Hinsicht letztlich für unerheblich hält.

[41] BT-Drs. 7/178, S. 8.

[42] Das BKAG 1997 führte aber dadurch zu Veränderungen für die polizeiliche Informationsordnung, dass es erstmals Rechtsgrundlagen für die Speicherung von Daten in INPOL vorsah.

[43] *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BKAG Rn. 33; *Lersch*, in: FS Herold, S. 35 (40).

[44] *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BKAG Rn. 34.

[45] Ein Änderungsvorschlag des Bundesrates, wonach das Bundeskriminalamt das Informationssystem nach Art. 2 Abs. 3 BKAG 1997 „arbeitsteilig mit den Landeskriminalämtern" betreiben sollte, setzte sich nicht durch; vgl. BT-Drs. 13/1550, S. 41, 54.

[46] Vgl. BT-Drs. 18/11163, S. 84; siehe zu der Struktur des neuen „Datenhauses" im Einzelnen oben Teil 1 B. III. 3. b.

Die Funktion des Bundeskriminalamts als Zentralstelle wurde zuletzt mit dem BKAG 2018 durch die neuen Regelungen zur Informationsordnung gestärkt.[47] Aktuelle Tendenzen weisen in die Richtung einer weiteren Zentralisierung der Informationsordnung beim Bundeskriminalamt. So sollen im Rahmen des neuen polizeilichen Informationssystems für dessen einzelne Bestandteile anders als bisher einheitliche technische Verfahren zum Einsatz kommen, die das Bundeskriminalamt zur Verfügung stellt.[48] Der Grundsatz der Autonomie von Bundes- und Landessystemen in seiner bisherigen Form soll dadurch durchbrochen werden. Das Modell der Verbunddateien wird abgeschafft. Dieser grundsätzliche Neuansatz wird als notwendig angesehen, um einen einheitlichen Standard einzuführen, der in dem bestehenden System möglicherweise nachträglich nicht mehr praktisch umzusetzen wäre.[49] Diese Maßnahmen und die damit verbundene stärkere Zentralisierung des Systems sollen dazu dienen, Daten effizienter als bisher verschiedenen polizeilichen Stellen zur Verfügung zu stellen[50] und das System wirtschaftlicher zu gestalten.[51]

2. Befugnisse als Zentralstelle

Weiter fragt sich, ob und inwieweit Art. 87 Abs. 1 Satz 2 GG neben der Regelung der Aufgaben einer Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen auch die Regelung informationsordnender Befugnisse für diese Zentralstelle ermöglicht. Durch die Regelung entsprechender Befugnisse könnte die Stellung des Bundeskriminalamts als zentrale informationsordnende Behörde gestärkt werden.

Ob Art. 87 Abs. 1 Satz 2 GG die Schaffung außenwirksamer bzw. polizeilicher Befugnisse ermöglicht, ist umstritten.[52] Der Wortlaut der Vorschrift schließt dies ebenso wenig aus wie eine historische Lesart nach dem „Polizeibrief". In diesem Dokument findet sich ein Ausschluss von entsprechenden Befugnissen nur für eine Bundesverfassungsschutzbehörde.[53] Unter systematischen Gesichtspunkten lässt sich anführen, dass

[47] Vgl. *Rusteberg*, Föderale Sicherheitsarchitektur, S. 65.

[48] BMI, Polizei 2020, S. 9.

[49] So auch schon *Sehr*, Kriminalistik 1999, 532 im Bilde der Informationsordnung als Gebäude („man findet weit und breit keine Baufirma mehr, die das Gebäude stabilisieren, geschweige denn modernisieren kann.").

[50] BMI, Polizei 2020, S. 2.

[51] BMI, Polizei 2020, S. 9.

[52] Für eine solche Möglichkeit in begrenztem Rahmen *Abbühl*, S. 361; *Burgi*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 87 Rn. 147; *Gusy*, DVBl. 1993, 1117 (1122 f.); dagegen *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 7 f.

[53] „Der Bundesregierung wird es ebenfalls gestattet, eine Stelle zur Sammlung und Verbreitung von Auskünften über umstürzlerische, gegen die Bundesregierung gerichtete Tätigkeiten einzurichten. Diese Stelle soll keine Polizeibefugnis haben."

das Fehlen außenwirksamer Befugnisse ein Charakteristikum von Zentralstellen im Vergleich zu anderen Behörden ist.[54] Allerdings spricht vor allem die für Zentralstellen ebenfalls charakteristische Koordinierungsaufgabe dafür, dass der Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen nach Art. 87 Abs. 1 Satz 2 GG zumindest Befugnisse eingeräumt werden können, um „das Handeln der Landespolizeibehörden informationell zu verklammern, fachlich zu unterstützen und zu koordinieren."[55] Die Möglichkeit einer effektiven informationellen Verklammerung der Polizeien lässt sich insofern auch als notwendiges Gegengewicht zu der dezentralen Polizeistruktur in der Bundesrepublik begreifen.[56] Befugnisse zur Verklammerung und Koordinierung von informationellen Tätigkeiten sind ganz im Sinne des hier zugrunde gelegten verfassungsrechtlichen Verständnisses der Funktion von Zentralstellen. Sie widersprechen auch nicht der Polizeihoheit der Länder,[57] bei denen weiterhin die grundsätzliche Regelungskompetenz für polizeiliche Befugnisse verbleibt. Insofern erscheint die Regelung derartiger Befugnisse für das Bundeskriminalamt auf Grundlage von Art. 87 Abs. 1 Satz 2 GG möglich.

Für die Regelung von Befugnissen zur Koordinierung der polizeilichen Informationsordnung lässt sich aus Art. 87 Abs. 1 Satz 2 GG neben der Verwaltungskompetenz zur Einrichtung einer Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen eine ausschließliche Gesetzgebungskompetenz herauslesen.[58] Grundsätzlich regelt Art. 73 Abs. 1 Nr. 10 GG die (ausschließlichen) Gesetzgebungskompetenzen, die mit den Verwaltungskompetenzen in Art. 87 Abs. 1 Satz 2 GG korrespondieren.[59] Diese betreffen die Zusammenarbeit des Bundes und der Länder auf den Gebieten, die von der Zentralstellenkompetenz in Art. 87 Abs. 1 Satz 2 GG erfasst sind. Art. 73 Abs. 1 Nr. 10 GG ist jedoch insofern inkongruent zu Art. 87 Abs. 1 Satz 2 GG, als er keine Kompetenz für die Zusammenarbeit auf dem Bereich des polizeilichen Auskunfts- und Nachrichtenwesens enthält. Die Gründe für die Inkongruenz zwischen Art. 87 Abs. 1 Satz 2 GG und Art. 73 Abs. 1 Nr. 10 GG sind unklar. Aus den Akten und Protokollen

[54] *Gusy*, DVBl. 1993, 1117 (1123).

[55] *Bäcker*, GSZ 2018, 213 (215); vgl. auch *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2019, § 2 BKAG Rn. 7; anders *Hermes*, in: Dreier, GG, 3. Aufl. 2018, Art. 87 Rn. 49 (mit der Begründung, dass durch Weisungsrechte von Zentralstellen die grundgesetzlich vorgenommene Kompetenzverteilung unterlaufen werden könnte); *Gärditz*, S. 373; *Gusy*, DVBl. 1993, 1117 (1121).

[56] *Möstl*, Die Verwaltung 2008, 309 (323).

[57] Diesen Aspekt führt *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 7 gegen eine Kompetenz zur Regelung von Weisungsbefugnissen des BKA an.

[58] Vgl. für die Organisationsbefugnisse der Zentralstelle insgesamt *Ibler*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023 Art. 87 Rn. 9, 79; generell zur Herleitung von Gesetzgebungskompetenzen aus Art. 87 Abs. 1 Satz 2 GG *Ahlf*, Das Bundeskriminalamt, S. 76 ff.

[59] Vgl. zu dem unklaren Verhältnis der beiden Vorschriften BVerfGE 141, 220 (263 f.); *Ahlf*, Das Bundeskriminalamt, S. 59 ff.; *Gusy*, DVBl. 1993, 1117 (1118).

des Parlamentarischen Rates ergibt sich keine nähere Erklärung, die speziell den Zusatz „Zentralstellen für das polizeiliche Auskunfts- und Nachrichtenwesen" betrifft.[60] Es ist möglich, dass die Verfassungsgebenden das Auskunfts- und Nachrichtenwesen grundsätzlich nicht als regelungsbedürftig ansahen. Dieses Grundverständnis hat sich spätestens mit dem Volkszählungsurteil des Bundesverfassungsgerichts und der Verrechtlichung der polizeilichen Informationsordnung geändert.

Im Rahmen von Art. 73 Abs. 1 Nr. 10 GG ließe sich das polizeiliche Auskunfts- und Nachrichtenwesen auf Grundlage der ausschließlichen Gesetzgebungskompetenz des Bundes für die Regelung der Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei (lit. a) nur eingeschränkt regeln.[61] Der Begriff der Kriminalpolizei umfasst das polizeiliche Auskunfts- und Nachrichtenwesen. Dies ergibt sich aus einer historischen Betrachtung: Art. 73 Abs. 1 Nr. 10 GG ging aus einer ursprünglich für das Bundeskriminalwesen vorgesehen Kompetenz hervor, die nicht auf den Aspekt der Zusammenarbeit beschränkt gewesen war.[62] Zum Bundeskriminalwesen sollten besonders „Erkennungswesen und Nachrichtenwesen, Erkennungsdienst, Verfolgung"[63] gehören.[64] Der Begriff der Zusammenarbeit erfasst zudem neben anderen auf Dauer angelegten Formen der Kooperation zwischen Sicherheitsbehörden die Einrichtung und den Betrieb gemeinsamer Informationssysteme.[65] Dazu umfassen kriminalpolizeiliche Tätigkeiten präventives ebenso wie repressives Handeln. Allerdings kann der Begriff der Kriminalpolizei die polizeiliche Informationsordnung aus einem Grund nicht voll-

[60] Dieser wurde in der 58. Sitzung des Hauptausschusses ohne Begründung eingefügt; Stenografisches Protokoll der 58. Sitzung des Hauptausschusses am 6. Mai 1949, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 14/II, 2009, S. 1829 (1830).

[61] Vgl. *Gärditz*, S. 267.

[62] Vgl. dazu Stenografisches Protokoll der 8. Sitzung des Ausschusses für Zuständigkeitsabgrenzung am 6. Oktober 1948, in: Werner, Der Parlamentarische Rat 1948–1949, Bd. 3, 1986, S. 323 (345); *Uhle*, in: Dürig/Herzog/Scholz, GG, 100. EL November 2023, Art. 73 Rn. 10 ff. Diese Kompetenz war aufgrund der grundsätzlichen Zuständigkeit der Länder für das Polizeiwesen umstritten und setzte sich daher nicht durch; vgl. Stenografisches Protokoll der 10. Sitzung des Ausschusses für Zuständigkeitsabgrenzung am 8. Oktober 1948, in: Werner, Der Parlamentarische Rat 1948–1949, Bd. 3, 1986, S. 407 (410 f.); Stenografisches Protokoll der 6. Sitzung des Hauptausschusses am 19. November 1948, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 14/I, 2009, S. 169 (196 f.); Stenografisches Protokoll der 29. Sitzung des Hauptausschusses am 5. Januar 1949, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 14/II, 2009, S. 858 (878 ff.); Stenografisches Protokoll der 32. Sitzung des Hauptausschusses am 7. Januar 1949, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 14/II, 2009, S. 965 (969 f.); im Überblick auch *Uhle*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 73 Rn. 17 ff.

[63] Stenografisches Protokoll der 5. Sitzung des Ausschusses für Zuständigkeitsabgrenzung am 29. September 1948, in: Werner, Der Parlamentarische Rat 1948–1949, Bd. 3, 1986, S. 173 (206).

[64] Vgl. auch Stenografisches Protokoll der 49. Sitzung des Hauptausschusses am 9. Februar 1949, in: Feldkamp, Der Parlamentarische Rat 1948–1949, Bd. 14/II, 2009, S. 1541 (1563).

[65] BVerfGE 133, 277 (317 f.); *Uhle*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 73 Rn. 231.

ständig erfassen: Er ist auf polizeiliche Tätigkeiten beschränkt, die „bedeutsame Straftaten von Gewicht“[66] betreffen.[67] Das polizeiliche Auskunfts- und Nachrichtenwesen bezieht sich aber nicht nur auf solche Tätigkeiten, sondern auf das gesamte polizeiliche Aufgabenfeld. Dazu bezieht es sich auch auf Bereiche, die nicht unter die Zusammenarbeit von Bund und Ländern fallen.[68]

In Zusammenschau mit dem insofern unvollständigen Art. 73 Abs. 1 Nr. 10 GG ist aus Art. 87 Abs. 1 Satz 2 GG daher eine eingeschränkte ausschließliche Gesetzgebungskompetenz für Organisationsbefugnisse im Zusammenhang mit dem polizeilichen Auskunfts- und Nachrichtenwesen abzuleiten.[69] Andernfalls wären Einrichtung und Betrieb einer Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen unterhalb der Schwelle kriminalpolizeilicher Tätigkeiten nicht in Einklang mit dem Grundgesetz möglich. Das polizeiliche Auskunfts- und Nachrichtenwesen in diesem Sinne umfasst auch multifunktionale oder zweckoffene Informationsressourcen.[70]

Zusammengefasst bietet Art. 87 Abs. 1 Satz 2 GG also durchaus einen Spielraum, das Bundeskriminalamt mit weiteren informationsordnenden Befugnissen auszustatten. Die Kompetenz erlaubt zwar keine Regelung eigenständiger operativer Verfahren und außenwirksamer Eingriffsbefugnisse.[71] Für Befugnisse zur Verklammerung und Koordinierung des informationellen Handelns der Polizei durch die Zentralstelle bietet Art. 87 Abs. 1 Satz 2 GG aber Möglichkeiten.

III. Konkrete Regelungsansätze

Im Ergebnis wäre es auf Grundlage von Art. 87 Abs. 1 Satz 2 GG möglich, sowohl die Aufgaben des Bundeskriminalamtes als Zentralstelle für die polizeiliche Informationsordnung zu konkretisieren (1.) als auch seine Befugnisse zu erweitern (2.).

1. Konkretisierung und Erweiterung der Aufgaben

Die Aufgaben des Bundeskriminalamts als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen in § 2 BKAG könnten konkretisiert und erweitert werden.[72] Es

[66] BVerfGE 133, 277 (318).

[67] Vgl. auch *Brodowski*, S. 513; *Uhle*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 73 Rn. 239; *Heintzen*, in: v. Mangoldt/Klein/Starck, GG, 7. Aufl. 2018, Art. 73 Rn. 114.

[68] Vgl. *Abbühl*, S. 87 f.

[69] Vgl. *Hermes*, in: Dreier, GG, 3. Aufl. 2018, Art. 87 Rn. 34.

[70] Vgl. *Ahlf*, Polizeiliche Kriminalakten, S. 76; *Ibler*, in: Dürig/Herzog/Scholz, GG, 100. EL 2023, Art. 87 Rn. 129; *Möstl*, Stellungnahme BKAG 2018, S. 6.

[71] Vgl. *Bäcker*, GSZ 2018, 213 (215); *Graulich*, in: Schenke/Graulich/Ruthig, 2. Aufl. 2019, § 2 BKAG Rn. 1.

[72] Vgl. zur Möglichkeit von Zentralisierung von Aufgaben beim Bundeskriminalamt allgemein *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 3, 8; *Graulich*, GSZ 2019, 9 (16).

könnte die Aufgabe geregelt werden, die Kompatibilität bzw. Verknüpfbarkeit der bestehenden polizeilichen Informationsressourcen sicherzustellen. Konkret wäre dies in § 2 Abs. 5 BKAG möglich, der bereits eine Reihe von Tätigkeiten regelt, die das Bundeskriminalamt zur Unterstützung der Polizeien des Bundes und der Länder ergreifen kann. So sieht § 2 Abs. 5 Satz 1 Nr. 4 BKAG vor, dass das Bundeskriminalamt die Polizeien auf Ersuchen bei der Datenverarbeitung unterstützt. Diese Regelung ermöglicht es allerdings nur, dass das Bundeskriminalamt in Einzelfällen nach den Weisungen der Länder Daten verarbeitet.[73]

Außerdem wäre es möglich, dem Bundeskriminalamt ausdrücklich die Aufgabe zuzuweisen, die Qualität der im polizeilichen Informationsverbund gespeicherten Daten zu sichern. Dies wäre im Zusammenhang mit § 2 Abs. 3 BKAG möglich, wonach das Bundeskriminalamt einen einheitlichen polizeilichen Informationsverbund zu unterhalten hat. Was die Aufgabe des Unterhaltens eines solchen Informationsverbundes umfasst, könnte etwa durch Regelbeispiele konkretisiert werden. In diesem Kontext könnte die Entwicklung gemeinsamer Standards der Datenqualität für polizeiliche Informationssysteme als Aufgabe des Bundeskriminalamts geregelt werden. § 2 Abs. 6 Nr. 4 BKAG sieht bereits jetzt vor, dass das Bundeskriminalamt als Zentralstelle zur Unterstützung der Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten Verfahren zur Umsetzung von Datenschutzgrundsätzen entwickelt. Diese Regelung ermöglicht es, dass das BKA die Polizeien praktisch als Dienstleister bei technischen und organisatorischen Maßnahmen unterstützt.[74] Auch wenn die Datenqualität hier nicht ausdrücklich genannt ist, lässt sie sich im Sinne von Art. 4 Abs. 1 lit. d JI-Richtlinie als Datenschutzgrundsatz begreifen, dem das BKA zur Umsetzung verhilft. § 2 Abs. 6 Nr. 4 BKAG lässt sich also so verstehen, dass die Schaffung gemeinsamer Verfahren und Standards zur Sicherung der Datenqualität bereits vorgesehen, wenn auch noch nicht ausdrücklich als Aufgabe benannt ist.

2. Erweiterung der Befugnisse

Schließlich könnte das Bundeskriminalamt als Zentralstelle weitere Befugnisse erhalten, um den Aufbau der polizeilichen Informationsordnung zu organisieren. Dies entspräche der Koordinationsfunktion der Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen. Als solche muss das Bundeskriminalamt in der Lage sein, eine Informationsinfrastruktur zu schaffen und zu organisieren, die die informationelle Zusammenarbeit der verschiedenen Polizeibehörden ermöglicht.

---

[73] *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 71.
[74] *Barczak*, in: Barczak, BKAG, 2023, § 2 Rn. 85.

Das Bundeskriminalamt könnte zur Koordination der Informationsordnung konkret mit eingeschränkten Weisungsbefugnissen gegenüber den Landespolizeibehörden ausgestattet werden.[75] Vorstellbar wäre etwa eine Befugnis des Bundeskriminalamts, Polizeibehörden der Länder zur Mitteilung spezifischer Informationen – wie beispielsweise technischer Spezifika gestohlener Kraftfahrzeuge – zu verpflichten, wenn sie Daten in die Informationsordnung einspeisen. Ebenso könnten der Zentralstelle weitere Möglichkeiten eingeräumt werden, Polizeibehörden durch Richtlinien zur standardisierten Speicherung von Informationen zu verpflichten.[76] Nur wenn die die Daten erhebenden Polizeibeamten nach einer klaren Struktur vorgehen, kann eine Speicherung mit ausreichender Qualität gelingen.

Das Bundeskriminalamt könnte schließlich dazu ermächtigt werden, in koordinativer Rolle zentrale Auswertungen von Informationen vorzunehmen, die es von anderen Polizeibehörden erhält. Hierfür müsste eine neue Befugnis geschaffen werden, die die Möglichkeiten derartiger Auswertungen spezifisch bestimmt und prozedurale Schutzmaßnahmen vorsieht.

B. Umstrukturierung des Systems informationsordnender Befugnisse

Die Befugnisse zur Speicherung und Strukturierung von Informationen in kriminalbehördlichen Informationssystemen sind auf eine Vielzahl von Regelungen im Bundes- und Landesrecht verteilt. Im Wesentlichen sind diese Regelungen das Ergebnis der Vorgaben, die das Bundesverfassungsgericht vor rund vierzig Jahren in seinem Volkszählungsurteil für die Verarbeitung personenbezogener Daten durch den Staat machte.[77] Die Gesetzgeber in Bund und Ländern schufen auf Grundlage dieser Vorgaben unter anderem neue Befugnisse für die Verarbeitung personenbezogener Daten durch Polizeien und Staatsanwaltschaften. Was den Standort der Befugnisse in den jeweiligen (Po-

[75] *Aulehner*, S. 83; *Bäcker*, GSZ 2018, 213 (216 f.); *Schweppe*, S. 27; anders *Gusy*, DVBl. 1993, 1117 (1121); *Hermes*, in: Dreier, GG, 3. Aufl. 2018, Art. 87 Rn. 34 (mit Verweis auf Art. 73 Abs. 1 Nr. 10 GG).

[76] Vgl. zu einem ähnlichen Regelungsansatz in einem frühen Entwurf des BKAG *Schweppe*, S. 87.

[77] BVerfGE 65, 1; siehe oben Teil 1 C. III. 1. b.

lizei-)Gesetzen und ihre Systematik angeht, unterscheiden sich die Regelungen im Detail.[78] Eine besondere Würdigung informationsordnender Tätigkeiten nahm allerdings keiner der Gesetzgeber vor.[79]

Aufgrund der vielen unterschiedlichen gesetzlichen Normen auf Bundes- und Landesebene ist es nicht immer leicht, die für den konkreten Fall einschlägigen Regelungen zu identifizieren. Welche Norm zur Anwendung kommt, bestimmt sich danach, welche Behörde mit welcher Zielrichtung handelt. Für ein Handeln mit präventiver Zielrichtung gelten grundsätzlich die Polizeigesetze, für den repressiven Tätigkeitsbereich die Strafprozessordnung. Präventive und repressive Zielrichtungen lassen sich allerdings oftmals nicht sauber voneinander trennen. Bei der Speicherung von Daten lässt sich nur in der Theorie eindeutig festlegen, zu welchen Zwecken sie in Zukunft Verwendung finden werden.[80]

Hinzu kommt, dass von dem beschriebenen Grundsatz zur Bestimmung der anwendbaren Rechtsgrundlagen wichtige Ausnahmen gelten. Für Speicherungen von Daten zu Strafverfolgungszwecken in Systemen der Polizei, die sowohl präventiven als auch repressiven Zwecken dienen, finden nach § 483 Abs. 3 StPO die Polizeigesetze Anwendung. Dies gilt nach § 484 Abs. 4 StPO auch für die Speicherung von personenbezogenen Daten für Zwecke künftiger Strafverfahren durch die Polizei. Durch diese Regelungen hat der Bundesgesetzgeber die Bedeutung der Differenzierung zwischen präventivem und repressivem Tätigwerden für die polizeiliche Informationsordnung weitgehend eingeebnet, da viele polizeiliche Informationsressourcen zugleich präventiven und repressiven Zwecken dienen und die Speicherung von Daten oftmals für die Vorbereitung späterer Strafverfolgung erfolgt. Zum Teil wird kritisiert, dass der Bundesgesetzgeber sich durch diese Regelungstechnik seiner grundrechtlichen Regelungsverantwortung entzogen habe.[81]

Die Gründe für den Verzicht des Gesetzgebers der Strafprozessordnung auf eine eigenständige Regelung zu diesen praktisch wichtigen Bereichen liegen in einer Praxis, die die Polizei bereits etablierte, bevor die Verarbeitung personenbezogener Daten überhaupt als allgemein regelungsbedürftig angesehen wurde.[82] Die Polizei war schon

---

[78] *Möstl*, DVBl. 2007, 581 (582 f.). Teils waren die Gesetzgeber bemüht, bereits bestehende und neue informationelle Befugnisse in gemeinsamen Regelungsabschnitten zusammenzuführen. In der Regel wurden die neuen Regelungen aber von den bisherigen Befugnissen, die mit informationellen Eingriffen einhergingen, getrennt; vgl. dazu auch *Peitsch*, ZRP 1992, 127 (128).

[79] Vgl. zu den Datenerhebungsbefugnissen als Fremdkörpern in den Polizeigesetzen *Kral*, S. 165.

[80] Siehe oben Teil 1 A. III. 2.

[81] *Bäcker*, Kriminalpräventionsrecht, S. 498 sieht die Regelungen aus diesem Grund als verfassungswidrig an; kritisch auch *Albers*, Determination, S. 199.

[82] Vgl. *Weßlau*, in: SK-StPO, 4. Aufl. 2013, Vor § 483 Rn. 18; *Wolter*, GA 1988, 49 (55); *Zöller*, S. 217.

in frühen Zeiten der EDV-Nutzung Vorreiterin bei der Entwicklung und Verwendung von Informationssystemen und Datenbanken, während die Staatsanwaltschaften sich auf die Verwendung einzelner Systeme zur Vorgangsverwaltung beschränkten.[83] Gleichzeitig sitzt die Polizei, die in strafprozessualen Ermittlungen regelmäßig die Fäden in der Hand hält und als Erste vor Ort ist,[84] an der Quelle, indem sie zuerst Daten erhebt.[85] In der polizeilichen Informationsordnung entwickelten sich auch rasch die bis heute etablierten Mischdateien, die sowohl zu präventiven als auch zu repressiven Zwecken eingesetzt wurden.[86] Die Rolle der Polizei bei der Strafverfolgung ist – nicht nur auf dem Gebiet der Informationsordnung – infolge der technischen Entwicklung immer wichtiger geworden.[87] Dies führte auch zu Vorschlägen, der Polizei gegenüber den Staatsanwaltschaften in den rechtlichen Regelungen im Allgemeinen eine stärkere Rolle einzuräumen.[88] Diese Bemühungen führten bis zu einem von einer von den Konferenzen der Justiz- und Innenminister eingesetzten Gemeinsamen Kommission erarbeiteten Vorentwurf eines Gesetzes zum Verhältnis von Staatsanwaltschaft und Polizei vom 17. November 1978,[89] der allerdings nie umgesetzt wurde.[90]

Auch rechtlich reagierten die Gesetzgeber der Länder in ihren Polizeigesetzen mit Regelungen zur Informationsordnung schneller auf das Volkszählungsurteil des Bundesverfassungsgerichts als der Gesetzgeber der Strafprozessordnung. Dieser wurde damit faktisch und rechtlich vor vollendete Tatsachen gestellt: Die Polizeien betrieben Informationssysteme auf Grundlage der jeweiligen landesgesetzlichen Regeln. Der Bundesgesetzgeber stand damit vor der Wahl, das bestehende System der Polizeien durch eine abweichende Regelung in der Strafprozessordnung zu zerschlagen oder sich in dieses einzufügen.[91] Er entschied sich für Letzteres. Es hätte einen hohen administrativen, ökonomischen und technischen Aufwand bedeutet, in der Strafprozessordnung

[83] Siehe im Einzelnen oben Teil 1 B. III. 1. und IV.

[84] Vgl. in diesem Zusammenhang zu Forderungen eines eigenen polizeilichen Ermittlungsverfahrens *Häring*, Kriminalistik 1979, 269 (270).

[85] Vgl. Arbeitskreis AE, S. 119; *Herold*, Die Polizei 1972, 133 (134) („einzigartiges Erkenntnisprivileg"); *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, § 481 Rn. 1.

[86] Speziell auf die Speicherung von Daten in polizeiliche Mischdateien sowohl zu präventiven als auch zu repressiven Zwecken vorgehalten werden, ist § 483 Abs. 3 StPO ausgerichtet; BR-Drs. 433/18, S. 73; *Gieg*, in: KK-StPO, 9. Aufl. 2023, § 483 Rn. 5; *Singelnstein*, ZStW 120 (2008), 854 (874).

[87] *Kuhlmann*, DRiZ 1976, 265.

[88] Vgl. Gesamtbericht der von den Konferenzen der Justizminister/-senatoren und Innenminister/-senatoren eingesetzten „Gemeinsamen Kommission" über die Neugestaltung des Verhältnisses „Staatsanwalt – Polizei" vom 13. Mai 1975; abgedruckt bei *Schubert*, S. 489 ff.; kritisch hierzu nur *Gössel*, GA 1980, 325 ff.; *Häring*, Kriminalistik 1979, 269 (272).

[89] Abgedruckt bei *Schubert*, S. 506 ff.; vgl. dazu *Häring*, Kriminalistik 1979, 269 (272 ff.).

[90] Ein Grund hierfür könnte in der mangelnden Bereitschaft der Polizei liegen, der Staatsanwaltschaft Zugang zu ihren Informationssystemen zu gewähren; vgl. *Schaefer*, in: FS Hanack, S. 191 (192).

[91] *Weßlau*, in: SK-StPO, 4. Aufl. 2013, Vor § 483 Rn. 4.

ein eigenes Regelungsmodell für die Informationsordnung für Zwecke des Strafverfahrens zu etablieren und umzusetzen. So hat *Mark Zöller* die Auftrennung der Dateien in präventive und repressive Bestandteile als „fast schon utopische Hoffnung" bezeichnet.[92] Die weitgehende Überantwortung der Informationsordnung in das Polizeirecht diente dem Ziel, den weiteren Betrieb von Mischdateien zu ermöglichen und den Verwaltungsaufwand hierbei gering zu halten.[93] Die Regelungen in § 483 Abs. 3 StPO und § 484 Abs. 4 StPO sind damit zwar nicht als Aufgabe der rechtlichen Unterscheidung präventiven und repressiven polizeilichen Handelns zugunsten einer „operativen Dimension" anzusehen,[94] wohl aber als Zugeständnis an die Realität kriminalbehördlicher Datenverarbeitung.[95]

Mit der jüngsten Reform der Regelungen zur Informationsordnung in der Strafprozessordnung hat der Gesetzgeber teilweise mit dieser Logik gebrochen. § 483 Abs. 3 StPO gilt nicht für die Speicherung von Daten in dem neuen Informationssystem des polizeilichen „Datenhauses",[96] da die Norm nur auf die Speicherung in einem Dateisystem anwendbar ist.[97] Damit kommen die Regelungen der Strafprozessordnung zur Anwendung, wenn die Polizei Daten für Zwecke eines konkreten Verfahrens in ihrem neuen Informationsverbund speichert. Dieser ist nicht in Dateien organisiert.[98] Für die Speicherung personenbezogener Daten durch die Polizei für Zwecke künftiger Strafverfahren gelten allerdings auch bei einer Speicherung im neuen Informationssystem nach § 484 Abs. 4 StPO die Polizeigesetze.[99]

Das bestehende System informationsordnender Befugnisse ist historisch gewachsen. Es ist zu untersuchen, inwiefern Umstrukturierungen dazu beitragen könnten, den Ist-Zustand der kriminalbehördlichen Informationsordnung ihrem Soll-Zustand anzunähern (I.). Dabei werden als Umstrukturierungen gesetzgeberische Maßnahmen verstanden, um bestehende informationsordnende Befugnisse zusammenzuführen oder ihre Voraussetzungen zu vereinheitlichen. Um die Möglichkeiten zur Vornahme derartiger Maßnahmen einzugrenzen, sind verfassungsrechtliche Grenzen zu berücksichtigen, welche sich vor allem aus der Kompetenzordnung des Grundgesetzes ergeben und eine vollständige Harmonisierung des Informationsordnungsrechts verhindern (II.). Schließlich werden konkrete Möglichkeiten einer Zusammenführung und Vereinheitlichung von Regelungen betrachtet, namentlich die Schaffung einer eigenständigeren

[92] *Zöller*, S. 177.
[93] BT-Drs. 13/9718, S. 30; BT-Drs. 14/1484, S. 32; vgl. auch *Hilger*, NStZ 2001, 15 (17).
[94] So aber *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, § 481 Rn. 3.
[95] Vgl. *Singelnstein*, in: MüKo-StPO, 2019, § 483 Rn. 20.
[96] Siehe hierzu oben Teil 1 B. III. 3.
[97] BR-Drs. 433/18, S. 72.
[98] Siehe oben Teil 1 B. III. 3. b.
[99] Vgl. BR-Drs. 433/18, S. 73; BT-Drs. 19/4671, S. 66.

Regelung im Bundesrecht und eine „weiche" Harmonisierung, die ohne rechtliche Verbindlichkeit auf eine Vereinheitlichung im Polizeirecht hinwirken würde (III.).

I. Beitrag zur Lösung bestehender Herausforderungen

Eine Umstrukturierung des Systems informationsordnender Befugnisse könnte dessen Übersichtlichkeit verbessern und die Anwendung der Regelungen erleichtern. Letzteres könnte im Sinne der Anwender*innen der kriminalbehördlichen Informationsressourcen sein. Mehr Übersichtlichkeit der Regelungen und Klarheit bei der Bestimmung der anwendbaren Rechtsgrundlagen dürfte aber auch im Interesse jener Personen liegen, über die Daten im kriminalbehördlichen Informationsressourcen gespeichert sind.

Ungereimtheiten bei der Anwendung der Befugnisse können zunächst dadurch entstehen, dass sich präventive und repressive Zielrichtungen bei der Einrichtung von Informationssystemen ebenso wie bei der Speicherung von Daten darin oftmals nicht sauber voneinander trennen lassen. In der kriminalbehördlichen Praxis bereitet dieser Umstand allerdings nicht zwangsläufig Schwierigkeiten. Die im Rahmen dieser Untersuchung interviewten Anwender*innen polizeilicher Informationssysteme gaben an, dass die Rechtsgrundlagen für informationsordnende Tätigkeiten aus ihrer Sicht hinreichend klar seien (POL1, POL2). Dies erscheint angesichts der weitgehenden Wahlmöglichkeiten, die zwischen Befugnissen zu Gefahrenabwehr und Strafverfolgung in der Praxis bestehen, plausibel.[100] Wenn die Anwender*innen sowohl die präventive als auch die repressive Zielrichtung einer Maßnahme begründen können, ist eine beliebige Entscheidung für eine dieser Kategorien möglich. Im Rahmen des zur Verfügung stehenden Spielraums können die Polizeien interne Regelungen dazu treffen, wie mit den Befugnissen umzugehen ist.

Schwierigkeiten könnten sich aus der Struktur der kriminalbehördlichen Befugnisse zur Informationsordnung daher eher für die Personen ergeben, über die Daten in den Informationsressourcen gespeichert werden. Für diese erschwert die Unübersichtlichkeit der Regelungen die Bestimmung der angewandten Rechtsgrundlage und damit auch der rechtlichen Voraussetzungen der Datenspeicherung sowie der Möglichkeiten zum Rechtsschutz. Allerdings sind die Rechtsgrundlagen einer Speicherung den Betroffenen bei der Geltendmachung eines Auskunftsrechtes mitzuteilen.[101]

Problematisch könnte aus Sicht der Betroffenen auch die weitgehende Möglichkeit zur Wahl der Rechtsgrundlagen durch die kriminalbehördlichen Anwender*innen sein. Konkret kann bei einer Auswahl zwischen Befugnissen aus dem Polizeirecht und

[100] Siehe hierzu oben Teil 1 A. III. 1.
[101] Vgl. § 487 Abs. 2 StPO, § 57 Abs. 1 Satz 2 Nr. 3 BDSG.

Strafprozessrecht die Entscheidung für das Polizeirecht dazu führen, dass Schutzmechanismen des Strafprozessrechts umgangen werden. Oftmals bringen die strafprozessualen Befugnisse auch höhere Voraussetzungen für die Durchführung einer Maßnahme mit sich als jene im präventiven Bereich. Im Zusammenhang mit den Befugnissen zur kriminalbehördlichen Informationsordnung besteht allerdings nicht die Gefahr, dass spezifische Schutzmechanismen oder erhöhte Eingriffsschwellen der strafprozessrechtlichen Regelungen dadurch umgangen werden, dass die handelnden Akteure auf das Polizeirecht ausweichen. Die Voraussetzungen für Datenspeicherungen sind in beiden Bereichen sehr ähnlich. Spezifische Schutzvorkehrungen im Strafprozessrecht existieren nicht.

Zu beachten ist auch, dass Vorgänge der Datenverarbeitung der Kontrolle der Staatsanwaltschaften entzogen werden können, indem sich polizeiliche Anwender*innen im Zweifel für Rechtsgrundlagen aus dem Polizeirecht entscheiden. Allerdings geben §§ 483 Abs. 3, 484 Abs. 4 StPO für einen Großteil der relevanten Datenverarbeitungen ohnehin eine Geltung der Polizeigesetze vor. Im Ergebnis können den Staatsanwaltschaften im Zusammenhang mit Datenspeicherungen, die Strafverfolgungszwecke betreffen, in weiten Teilen ihre Kontrollmöglichkeiten genommen werden. Auch im Zusammenhang mit der Informationsordnung gehört es zu der Aufgabe der Staatsanwaltschaft, die Rechtmäßigkeit polizeilichen Handelns zu Strafverfolgungszwecken zu überprüfen.[102] Bereits im Zusammenhang mit dem lange fehlenden Zugriffsrecht der Staatsanwaltschaften auf das polizeiliche Informationssystem INPOL war immer wieder kritisiert worden, dass die Staatsanwaltschaft als rechtliche „Herrin des Ermittlungsverfahrens“ faktisch nicht „Herrin der Daten“ in der kriminalbehördlichen Informationsordnung sei.[103] Zweifelhaft ist praktisch gesehen aber, ob eine theoretische Kontrollmöglichkeit der Informationsordnung durch die Staatsanwaltschaften tatsächlich von Relevanz für die Betroffenen wäre. Während die Polizei die in der kriminalbehördlichen Informationsordnung gespeicherten Daten erhebt, sind die Staatsanwaltschaften naturgemäß weiter von diesen Vorgängen entfernt. Aus der geschichtlichen Entwicklung der kriminalbehördlichen Informationsordnung zeigt sich auch, dass Investitionen in diesen Bereich im Wesentlichen von den Polizeien getätigt wurden. Es erscheint tendenziell unwahrscheinlich, dass die Staatsanwaltschaften ein gesteigertes Interesse daran haben, informationsordnende Tätigkeiten der Polizeien näher zu kontrollieren und dadurch den Schutz der Informationssubjekte zu verbessern.

Weitere Ungereimtheiten bei der Anwendung informationsordnender Befugnisse können dadurch entstehen, dass die Voraussetzungen der Regelungen in den einzelnen

[102] *Gössel*, GA 1980, 325 (349).
[103] Siehe oben Teil 1 A. III. 2.

Gesetzen im Detail voneinander abweichen.[104] Auch hieraus entstehen jedoch nicht zwangsläufig Schwierigkeiten für einzelne Anwender*innen, solange die Voraussetzungen der jeweils angewandten Regelung für diese bestimmbar sind.

Im Ergebnis erscheinen eine Zusammenführung der Befugnisse zur Informationsordnung sowie die Vereinheitlichung ihrer Voraussetzungen nicht als überragend wichtiges Anliegen, um die Anforderungen kriminalbehördlicher Anwender*innen zu erfüllen oder die Interessen der von der Datenverarbeitung Betroffenen zu schützen. Sie könnte aber dazu beitragen, die Systematik der Befugnisse zu verbessern und diese von außen nachvollziehbarer zu machen.

II. Rechtliche Möglichkeiten und Grenzen

Die Möglichkeiten zur Veränderung der Struktur der informationsordnenden Befugnisse der Kriminalbehörden sind durch die Kompetenzordnung des Grundgesetzes stark eingeschränkt. Die Speicherung von Informationen zu Zwecken der Gefahrenabwehr und deren Vorbereitung ist nach Art. 70 Abs. 1 GG grundsätzlich im Landesrecht zu regeln, sofern nicht ausnahmsweise – wie etwa für die Abwehr von Gefahren des internationalen Terrorismus nach Art. 73 Abs. 1 Nr. 9a GG – eine Gesetzgebungskompetenz des Bundes besteht.

Ansonsten bleibt dem Bundesgesetzgeber die Möglichkeit, Befugnisse zur Informationsordnung auf Grundlage der konkurrierenden Gesetzgebungskompetenz des Bundes für das gerichtliche Verfahren nach Art. 74 Abs. 1 Nr. 1 GG zu regeln. Auf dieser Kompetenz beruhen die Regelungen des Strafprozessrechts einschließlich des strafprozessualen Ermittlungsverfahrens.[105] Die Einrichtung kriminalbehördlicher Informationsressourcen und die Speicherung von Daten hierin erfolgt jedoch regelmäßig unabhängig von konkreten Verfahren und bevor der Anfangsverdacht einer Tat vorliegt. Es war lange umstritten, ob sich für die hier relevante Phase der Vorbereitung der Verfolgung von Straftaten Regelungen auf Grundlage von Art. 74 Abs. 1 Nr. 1 GG treffen lassen.[106]

---

[104] Siehe zu den Abweichungen bei den Befugnissen zur Datenspeicherung in den Polizeigesetzen der Länder oben Teil 1 A. III. 1. a. aa).

[105] Siehe oben Teil 1 C. I. 1. a.

[106] Vgl. dazu nur *W. Schenke*, JR 1970, 48 (51); *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, Vor § 474 Rn. 19; *Zöller*, S. 88 ff. m.w.N.

Mit dem Bundesverfassungsgericht ist dies für den Umgang mit Daten anzunehmen, wenn dieser das Ziel hat, die Daten in ein späteres gerichtliches Verfahren einzuführen.[107] Es ist daher nicht zwingend, dass der Bezugspunkt einer Regelung eine bereits begangene Straftat ist, damit diese unter die Kompetenz aus Art. 74 Abs. 1 Nr. 1 GG fällt.[108] Auch ein Anfangsverdacht ist nicht Voraussetzung.[109] Demnach unterfällt eine Regelung polizeilicher Überwachungsmaßnahmen, die dazu dienen, im Hinblick auf noch nicht begangene, aber bevorstehende Straftaten Beweise zu sammeln und diese später in ein Strafverfahren einzubringen, der Gesetzgebungskompetenz für das gerichtliche Verfahren.[110] Die Länder dürften für diesen Aspekt der Vorbereitung auf die Strafverfolgung keine eigene Regelung treffen, sofern eine Reglung auf Bundesebene vorliegt oder die Regelungen des Bundesrechts als abschließend zu verstehen sind.

Diese Interpretation des Art. 74 Abs. 1 Nr. 1 GG ist angesichts der anerkannten Einbeziehung des strafprozessualen Ermittlungsverfahrens konsequent.[111] Dagegen wird zwar angeführt, dass der Wortlaut der Norm lediglich das gerichtliche Verfahren erfasse und das strafprozessuale Ermittlungsverfahren nur nach historischer Auslegung hierunter gefasst werden könne.[112] Bei der Auslegung der Kompetenz sind aber auch Entwicklungen in Betracht zu ziehen, die der Verfassungsgeber bei der Regelung der Kompetenzen noch nicht berücksichtigen konnte.[113] Hierzu zählen die technischen Entwicklungen in dem Bereich der elektronischen Datenverarbeitung, durch die die kriminalbehördliche Informationsordnung überhaupt erst zum relevanten Regelungsgegenstand wurde. Ähnlich wie das strafprozessuale Ermittlungsverfahren erscheint ihre Nutzung jedenfalls sinngemäß von Art. 74 Abs. 1 Nr. 1 GG abgedeckt. Weiter wird gegen die Interpretation des Bundesverfassungsgerichts vorgebracht, dass es sich nicht mit dem System des Strafprozessrechts vereinbaren ließe, Datenverarbeitungen zu repressiven Zwecken ohne das Erfordernis eines Anfangsverdachts vorzusehen.[114] Dieser Einwand vernachlässigt allerdings, dass eine Regelung von Datenverarbeitungen

[107] BVerfGE 113, 348 (369 f.); in diese Richtung bereits BVerfGE 30, 1 (29); BVerfGE 103, 21 (30); *Albers*, Determination, S. 271; *Soiné*, CR 1998, 257 (258); kritisch zu der Lösung des Bundesverfassungsgerichts *Kniesel*, Die Polizei 2018, 265 (269) („hat das Verhältnis von Gefahrenabwehr und Strafverfolgung verunklart"); *Kniesel*, Die Polizei 2017, 189 (195). Anders als Regelungen zur Strafverfolgungsvorsorge fallen nach dem Bundesverfassungsgericht allerdings solche zur Verhütung von Straftaten grundsätzlich nicht unter die Kompetenz aus Art. 74 Abs. 1 Nr. 1 GG.

[108] BVerfGE 113, 348 (370); vgl. auch BVerfGE 103, 21 (30).

[109] BVerfGE 113, 348 (370); anders *Gärditz*, S. 324 ff.

[110] BVerfGE 113, 348 (370).

[111] Vgl. *Soiné*, CR 1998, 257 (258).

[112] *Kniesel*, Die Polizei 2017, 189 (195).

[113] Vgl. *Siebrecht*, JZ 1996, 711 (714).

[114] *Kniesel*, Die Polizei 2017, 189 (195).

auf Grundlage von Art. 74 Abs. 1 Nr. 1 GG ihren Platz nicht zwangsläufig in der Strafprozessordnung finden müsste. Zudem regelt die Strafprozessordnung bereits eine Reihe von Maßnahmen, die unterhalb der Verdachtsschwelle ansetzen.[115]

Auf Grundlage dieser Auslegung des Art. 74 Abs. 1 Nr. 1 GG existieren Überlegungen zur Schaffung eines strafprozessualen Vorfeldrechts, die speziell Tätigkeiten im Blick haben, durch die die Polizei Informationen gewinnt.[116] So schlägt *Matthias Bäcker* die Regelung eines strafprozessualen Vorfeldrechts für jenen Handlungsbereich vor, in dem die „Polizei kriminelle Strukturen über den Einzelfall hinaus mit strategischen Überwachungen" ausleuchtet.[117] Konkret ist dies etwa bei der Organisierten Kriminalität und der Terrorismusbekämpfung[118] der Fall. Die Überlegungen zum strafprozessualen Vorfeldrecht stehen in einem Zusammenhang mit Ansätzen, strafprozessuale „Vorermittlungen" eigenständig zu behandeln und gesetzlich zu regeln.[119] Das Vorermittlungsverfahren ist als Verfahren zur Erforschung von Verdachtsmomenten aufgrund konkreter Anhaltspunkte zu verstehen. Es umfasst daher nicht die Speicherung von Daten zu von konkreten Verfahren unabhängigen Zwecken.[120]

III. Konkrete Regelungsansätze

Sowohl im präventiven als auch im repressiven Bereich ließen sich die Befugnisse zur Informationsordnung umstrukturieren und konsolidieren. Für das strafprozessuale Vorfeld könnte eine im Vergleich zu den §§ 483 ff. StPO stärker eigenständige Regelung außerhalb der Strafprozessordnung geschaffen werden (1.). Für die Gefahrenabwehr bzw. ihre Vorbereitung wäre eine „weiche" Harmonisierung ohne rechtliche Verbindlichkeit möglich, die etwa durch den Entwurf eines Musterpolizeigesetzes und die Abstimmung der Befugnisse im präventiven und repressiven Bereich erfolgen könnte (2.).

---

[115] *Rudolph*, S. 175 ff.

[116] *Bäcker,* Kriminalpräventionsrecht, S. 301 ff.; *Brodowski*, S. 556 ff.; vgl. allgemein auch *H.-J. Albrecht/Dorsch/Krüpe*, S. 466.

[117] *Bäcker*, Kriminalpräventionsrecht, S. 544. Die Regelung „gelegenheitsorientierter Präventionsmaßnahmen" sollte nach *Bäcker* hingegen weiterhin dem Polizeirecht überlassen bleiben. Vgl. kritisch *Kniesel*, Die Polizei 2018, 265 (266), der diesen Vorschlag rechtspolitisch als „Sandkastenspiel" bezeichnet; die Regelung eines strafprozessualen Vorfeldrechts „würde die funktionale Trennung zwischen beiden Rechtsgebieten aufheben und wäre ohne eine Verfassungsänderung nicht machbar." Eine nähere Begründung für die fehlende verfassungsrechtliche Machbarkeit bleibt *Kniesel* allerdings schuldig.

[118] Vgl. *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 3.

[119] Vgl. zu informationsordnenden Tätigkeiten als Vorermittlungen *Hilger*, in: FG Hilger, S. 11 (12); zur möglichen Regelung eines Vorermittlungsverfahrens *Lange*, S. 223 ff.; *Rudolph*, S. 192 ff.; *Wolter*, in: FS Rolinski, S. 273 (284).

[120] Vgl. *Lange*, S. 229; *Wolter*, in: EG Brauneck, S. 501 (511) (Vorermittlungen als „dritte Spur der Strafverfolgung" neben der Aufklärung von begangenen Straftaten und der Vorsorge für die Aufklärung bezeichnend).

1. Eigenständigere Regelung für das strafprozessuale Vorfeld

In einem strafprozessualen Vorfeldrecht könnten Regelungen über die Einrichtung von Informationsressourcen sowie die Speicherung und Ordnung von Daten hierin getroffen werden, sofern diese Tätigkeiten der Vorbereitung der Strafverfolgung dienen. Von den bereits vorhandenen Regelungen in §§ 483 ff. StPO könnten sich die Regelungen in einem strafprozessualen Vorfeldrecht dadurch unterscheiden, dass sie konkretere eigenständigere Vorgaben etwa für die notwendigen Anlässe enthielten. §§ 483 Abs. 3, 484 Abs. 4 StPO verweisen in praktisch relevanten Fällen der Datenspeicherung auf die einschlägigen Regelungen des Polizeirechts.

Die informationsordnenden Befugnisse müssten außerdem nicht notwendigerweise in der Strafprozessordnung geregelt werden oder sich in deren System einfügen.[121] Eine Regelung außerhalb der Strafprozessordnung erschiene sogar logischer und konsequenter. Der für Maßnahmen nach der Strafprozessordnung üblicherweise notwendige Anlass des Verdachts einer Straftat ergibt als Anlass für informationsordnende Maßnahmen wenig Sinn.[122] Anders als die in der Strafprozessordnung vorgesehenen Maßnahmen sind informationsordnende Tätigkeiten typischerweise nicht auf die Aufklärung einer konkreten Tat in einem konkreten Verfahren bezogen. Dementsprechend könnte in einer eigenständigen Regelung für informationsordnende Tätigkeiten zur Vorbereitung der Strafverfolgung eine sachgerechte Eingriffsschwelle gesetzlich festgelegt werden, deren mögliche Ausgestaltung im weiteren Verlauf der Arbeit näher untersucht wird.[123] Durch eine Ausgliederung der informationsordnenden Befugnisse könnte schließlich die Systematik und Kohärenz der Strafprozessordnung gestärkt werden. Der Vorbereitung künftiger Strafverfolgung dienende Regelungen wie § 81b Abs. 1 Var. 2, 481 und 483 StPO sind in diesem Gesetz eher Fremdkörper. Die vorsorgende Sammlung und Ordnung von Informationen passt nicht in die reaktive und retrospektive Logik des Strafverfahrensrechts, die auf die Auflösung in der Vergangenheit begründeter sozialer Konflikte ausgerichtet ist.[124]

Nicht entbehrlich machen würde die Regelung eines strafprozessualen Vorfeldrechts die Notwendigkeit einer Zuordnung von informationsordnenden Tätigkeiten zum präventiven oder repressiven Tätigkeitsbereich der Kriminalbehörden. Weiterhin müsste der künftige Verwendungszweck von Daten bei deren Speicherung geklärt werden. Um in den Anwendungsbereich des Vorfeldrechts zu fallen, müsste eine Tätigkeit

[121] Vgl. *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, Vor § 474 Rn. 21.
[122] Siehe dazu näher unten C. III. 1. a.
[123] Siehe unten C. III.
[124] *Gärditz*, S. 60; vgl. zum Strafrecht *Hassemer*, ZRP 1991, 121 (122); *Lüderssen*, S. 165.

der Vorbereitung auf die Strafverfolgung zugeordnet werden. Um einen gewissen harmonisierenden Effekt zu erzielen, ließe sich das strafprozessuale Vorfeldrecht allerdings so regeln, dass es dann zur Anwendung käme, wenn sich das Ziel einer Datenspeicherung nicht eindeutig feststellen ließe. Es hätte dann einen Auffangcharakter und würde auch für Tätigkeiten gelten, die nicht eindeutig dem präventiven oder repressiven Tätigkeitsbereich zuzuordnen sind.

Es ist Befugnissen im repressiven Bereich eigen, dass sie an strengere Voraussetzungen anknüpfen als vergleichbare Befugnisse im präventiven Bereich. Wenn der Schaden an einem Rechtsgut sich noch abwenden lässt, lässt die Rechtsordnung ein Handeln zu diesem Zweck tendenziell unter niedrigeren Voraussetzungen zu als wenn der Schaden bereits eingetreten ist. Lässt sich aber eine Handlungsrichtung nicht klar festlegen und ein repressiver Zweck sich nicht ausschließen, erscheint es sachgerecht, im Zweifel die strengeren Voraussetzungen eines repressiven Tätigwerdens anzulegen. Dies nimmt auch die Rechtsprechung an, wenn die Herkunft von Datensätzen nicht zweifelsfrei erkennbar ist.[125] Für den Bereich der Informationsordnung ist eine solche Zweifelsregel in besonderem Maße sinnvoll: Dass die präventive oder repressive Zweckrichtung von Datenspeicherungen nicht von vornherein feststeht, liegt gewissermaßen in der Natur der Sache.[126] Eine Regelung des Informationsordnungsrechts mit Auffangcharakter könnte schließlich Anreize dafür schaffen, bei der Speicherung von Informationen sauberer zwischen präventiven und repressiven Zwecke zu unterscheiden als bisher.

2. Weiche Harmonisierung

Neben den soeben untersuchten Möglichkeiten zur Regelung informationsordnender Befugnisse im Bundesrecht sind auch „weiche" Instrumente der Harmonisierung in Betracht zu ziehen. Diese entfalten keine verbindliche Wirkung im Sinne einer rechtlichen Verpflichtung, können aber dennoch auf eine Vereinheitlichung der Rechtslage hinwirken.[127] Naheliegend wäre die Schaffung von Regelungsvorschlägen zum Informationsordnungsrecht durch ein Musterpolizeigesetz, das von der ständigen Konferenz der Innenminister und -senatoren des Bundes und der Länder (IMK) entworfen würde.[128] Derartige Musterpolizeigesetze haben die Entwicklung des Polizeirechts,

[125] VG Hannover ZD 2016, 598; VG Hannover BeckRS 2015, 52476.

[126] Siehe oben Teil 1 A. III. 2.

[127] Vgl. zur weichen Harmonisierung *Bäcker*, GSZ 2018, 213 (217).

[128] Vgl. zu der Kritik, dass das Instrument des Musterpolizeigesetzes entgegen der Kompetenzordnung des Grundgesetzes faktisch zu einer Entwertung der Landesgesetzgebungskompetenz für das Polizeirecht führe *Kötter*, S. 113.

auch in seinen Bezügen zum Strafprozessrecht, im Laufe der Zeit immer wieder beeinflusst.[129]

Die ersten Entwürfe eines Musterpolizeigesetzes der IMK[130] entstanden in den Jahren 1975 bis 1977[131] aus einem Vereinheitlichungsdruck im Angesicht der terroristischen Bedrohungen in der Bundesrepublik zu dieser Zeit.[132] Der aus diesem Prozess resultierende Musterentwurf eines Polizeigesetzes aus dem Jahr 1977 (ME PolG 1977)[133] bezog sich im Wesentlichen auf die polizeilichen Standardbefugnisse[134] und enthielt keine Regelungen über Polizeiorganisation und Zuständigkeiten.[135] Ein besonderes Augenmerk legte der Entwurf auf das Verhältnis des Polizeirechts zur Strafprozessordnung,[136] zu deren Änderung er ebenfalls Vorschläge enthielt.[137]

Regelungen zur polizeilichen Informationsverarbeitung enthielt der ME PolG 1977 nicht.[138] Allerdings fanden sich solche Regelungen in einem von einem Arbeitskreis Polizeirecht erarbeiteten und im Januar 1979 vorgestellten Alternativentwurf einheitlicher Polizeigesetze des Bundes und der Länder (AE PolG).[139] Dessen Begründung er-

---

[129] *Thiel*, Die Verwaltung 2020, 1 (9 f.).

[130] Vgl. zu dem bereits 1953 erarbeiteten, aber erfolglosen Modell-Polizeigesetz *Peters*, DÖV 1953, 385 ff.; *Ule*, in: D. Merten, S. 27 (32 ff.); *Wacke*, DÖV 1953, 388 ff.

[131] Einen ersten Entwurf veröffentlichte die IMK im Jahr 1975 (abgedruckt bei *Schubert*, S. 533 ff.), überarbeitete ihn in der Folge und beschloss ihn auf ihrer Sitzung am 10. und 11. Juni 1976 in geänderter Form (abgedruckt bei *Schubert*, S. 571 ff.); vgl. zur Entstehung *Rasch*, DVBl. 1982, 126; *Ule*, in: D. Merten, S. 27 f.; kritisch zu dem Entwurf *Funk/Werkentin*, KJ 1976, 407 ff., *Seebode*, MDR 1976, 537 ff. Nach einer weiteren Überarbeitung und Harmonisierung mit den Regelungen der StPO beschloss die IMK am 25. November 1977 die letzte Fassung des Musterentwurfes.

[132] Vgl. *Kötter*, S. 113. Erstmals forderte die IMK einen gemeinsamen Musterentwurf für ein Polizeigesetz in ihrem Programm für die innere Sicherheit in der Bundesrepublik Deutschland im Jahr 1972 (Beilage zu GMBl. Nr. 31/1972, S. 20) das sie 1974 ergänzte (Beilage zu GMBl. Nr. 9/1974, S. 26).

[133] Abgedruckt bei *Heise/Riegel*, S. 5 ff.; kritisch hierzu *Hoffmann-Riem*, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 1117 ff.

[134] Vgl. §§ 8 ff. ME PolG 1977; kritisch zu den neuen Möglichkeiten zur Inanspruchnahme von Nichtstörern *Hoffmann-Riem*, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 1117 (1121 f.).

[135] Vgl. *Rasch*, DVBl. 1982, 126.

[136] Eine Arbeitsgruppe prüfte unter anderem, ob die Regelungen des Musterentwurfes die Abgrenzung von Strafverfolgung und Gefahrenabwehr wahrten und ob „die polizeirechtlichen Befugnisse unter verfassungsrechtlichen Aspekten in einem ausgewogenen Verhältnis zu den polizeilichen Befugnissen nach Strafprozeßrecht stehen"; *Riegel*, ZRP 1978, 14; vgl. dazu näher den Abschlussbericht der Arbeitsgruppe Harmonisierung vom 21. Oktober 1977; abgedruckt bei *Schubert*, S. 581 ff.

[137] Diese fanden in dem Gesetz zur Änderung der Strafprozessordnung vom 14. April 1978 (BGBl. I, S. 497 ff.) Berücksichtigung; vgl. BT-Drs. 8/996, S. 4 f., 9 f.; BT-Drs. 8/997, S. 1 f.; *Rasch*, DVBl. 1982, 126; *Riegel*, BayVBl. 1978, 589 ff.; kritisch zu dem Ansatz, die Strafprozessordnung ohne rechtliche Kompetenz hierzu „nachzubessern" *Busch/Funk/Kauß/Narr/Werkentin*, S. 197 f.

[138] Kritisch diesbezüglich *Riegel*, DÖV 1994, 814.

[139] §§ 37 ff. AE PolG; vgl. dazu Arbeitskreis Polizeirecht, S. XII ff., 113 ff.; *Kowalczyk*, S. 78 ff.; *Rasch*, DVBl. 1982, 126 (127); *Riegel*, DVBl. 1979, 709 (716).

wies sich als fortschrittlich und begriff die vorgeschlagenen Regelungen zur polizeilichen Informationsverarbeitung bereits vier Jahre vor dem Volkszählungsurteil des Bundesverfassungsgerichts als notwendige „Ermächtigungen zu Eingriffen in das grundgesetzlich geschützte informationelle Selbstbestimmungsrecht der Bürger“[140]. Die Vorschriften lehnten sich inhaltlich an das am 1. Januar 1978 in Kraft getretene erste Bundesdatenschutzgesetz[141] an.[142] § 37 AE PolG sollte eine Befugnis zur Speicherung sowie Veränderung von Informationen regeln und formulierte dabei in seinem Abs. 2[143] Anforderungen an die Datenqualität bei der Speicherung in polizeilichen Informationssystemen. § 45 AE PolG sah weitere Regelungen zur Transparenz der Systeme für Betroffene und zur zeitlichen Begrenzung der Speicherung von Informationen vor.

Der harmonisierende Erfolg des ME PolG 1977 wird unterschiedlich beurteilt.[144] Eine Gesetzesinitiative, um den ME PolG 1977 im Bund (im Rahmen des kompetenzrechtlich Zulässigen) umzusetzen, scheiterte.[145] Viele Länder reformierten ihre Polizeigesetze aber auf Grundlage des Musterentwurfes.[146] Der AE PolG hatte indes maßgeblichen Einfluss auf das Bremische Polizeigesetz vom 16. März 1983,[147] das als erstes deutsches Polizeigesetz eine umfassende Regelung polizeilicher Informationsbefugnisse enthielt.[148]

Aktualität erlangte das Thema eines Musterpolizeigesetzes in der Folge wieder nach dem Volkszählungsurteil im Jahr 1983. Dieses gab einen wesentlichen Impuls für die Arbeiten an einem neuen Vorentwurf für den Musterentwurf eines Polizeigesetzes (VE MPolG 1986), der am 12. März 1986 veröffentlicht wurde.[149] Ein Kernstück des Vorentwurfes waren seine Regelungen zur Datenverarbeitung. Als Generalklausel für die Datenspeicherung, -veränderung und -nutzung sah § 10a VE MPolG 1986 vor, dass

---

[140] Arbeitskreis Polizeirecht, S. 114.

[141] BGBl. I 1977, S. 201 ff.

[142] Vgl. Arbeitskreis Polizeirecht, S. 115.

[143] „Werden Bewertungen über Betroffene in einem polizeilichen Informationssystem gespeichert, muß erkennbar sein, wer die Bewertung vorgenommen hat und wo die Erkenntnisse gespeichert sind, die der Bewertung zugrunde liegen. Erfolgt die Speicherung dieser Erkenntnisse nicht in dem polizeilichen Informationssystem, müssen die schriftlichen Unterlagen bis zum Löschungszeitpunkt aufbewahrt werden.“

[144] Mit negativem Urteil *F. Sydow*, ZRP 1977, 199 (120 f.); *Walter*, Kriminalistik 2019, 243 (244 ff.); wohlwollender hingegen *Busch/Funk/Kauß/Narr/Werkentin*, S. 198 ff.; *Götz*, DVBl. 1975, 876 (878).

[145] BT-Drs. 8/997.

[146] *Aden/Fährmann*, S 12 m.w.N.; vgl. auch *Rasch*, DVBl. 1982, 126 (127 ff.); *Schupp*, RiA 1979, 66.

[147] BremGBl., S. 141.

[148] Vgl. *Alberts*, NVwZ 1983, 585 ff.; *Scholz/Pitschas*, S. 162.

[149] *Kniesel/Vahle*, S. V f.; vgl. zu dem Anfang 1985 vom Ausschuss „Recht der Polizei“ des Arbeitskreises II der Innenministerkonferenz vorgelegten Vorentwurf (abgedruckt in Bürgerrechte & Polizei/CILIP 21 (2/1985), 44 ff.), der diesem zugrunde lag *Kniesel/Vahle*, DÖV 1987, 953 (954).

diese zulässig ist, sofern sie zur Erfüllung polizeilicher Aufgaben erforderlich ist.[150] Damit lieferte diese Regelung das Vorbild für die meisten bis heute geltenden Befugnisse zur Speicherung von personenbezogenen Informationen durch die Polizei. Der VE ME PolG 1986 hatte in seinen datenschutzrechtlichen Regelungen auch erheblichen Einfluss auf die 1997[151] abgeschlossene grundlegende Reform des BKAG[152] zur Umsetzung der Vorgaben aus dem Volkszählungsurteil.[153] In §§ 7 ff. BKAG 1997 wurden erstmals Rechtsgrundlagen für die Informationsordnung des Bundeskriminalamts geschaffen.[154]

Ein vielfach kritisch betrachteter Aspekt des VE ME PolG 1986 war seine Regelung zur vorbeugenden Verbrechensbekämpfung.[155] § 1 Abs. 1 Satz 2 VE ME PolG sah es ausdrücklich als polizeiliche Aufgaben vor, „für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (vorbeugende Bekämpfung von Straftaten) sowie Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können (Vorbereitung auf die Gefahrenabwehr).“[156] Diese Erweiterung der polizeilichen Aufgaben erfuhr im Schrifttum heftige Kritik.[157] Die vorbeugende Bekämpfung von Straftaten wurde weitgehend mit der Sammlung von Daten gleichgesetzt. Die Aufgabe der vorbeugenden Bekämpfung von Straftaten ist zwar nicht vollständig mit informationellen Tätigkeiten

[150] Vgl. dazu *Kniesel/Vahle*, DÖV 1987, 953 (958 f.).

[151] Der erfolgreichen Reform des BKAG waren seit den 1980er-Jahren mehrere gescheiterte Versuche vorangegangen; vgl. *Aden*, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6 (8).

[152] Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten vom 7. Juli 2997; BGBl. I, S. 1650 ff.; vgl. zu den Inhalten der Reform *Lersch*, in: FS Herold, S. 35 (40 ff.); *W. Schreiber*, NJW 1997, 2137 ff.

[153] BT-Drs. 13/1550, S. 19. Dabei erkannte die Begründung des BKAG 1997 allerdings auch die Unterschiede zwischen den Aufgaben und Funktionen der Landespolizeien und dem BKAG – insbesondere als Zentralstelle für das polizeiliche Informationswesen – an, die dazu führen, dass nicht sämtliche Konzepte und Vorschriften aus dem VE ME PolG übernommen werden konnten.

[154] Die für die Speicherung von Daten im Rahmen der Funktion als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen zentralen Regelungen fanden sich dabei in §§ 8, 9 BKAG 1997. Den Betrieb von INPOL regelten §§ 11-13 BKAG 1997. Zuvor war das System lediglich auf Grundlage von Beschlüssen der Innenministerkonferenz betrieben worden; vgl. *Abbühl*, S. 149; *Zöller*, S. 140.

[155] Dies war schon bei den Musterentwürfen der 1970er-Jahre diskutiert; aber nicht realisiert worden; *F. Sydow*, ZRP 1977, 119 (124 f.).

[156] Abgedruckt bei *Kniesel/Vahle*, S. 1.

[157] Vgl. *Schoreit*, DRiZ 1986, 54 f.; *Schoreit*, CR 1986, 224 (227); *Schwan*, in: Hohmann, S. 276 (284 f.); *Kniesel*, in: Bull, S. 105 (114), („Einfallstor für polizeiliche Omnipräsenz und Omnipotenz durch Datenverfügungsmacht über jedermann“); anders hingegen *Kowalczyk*, S. 98, die in § 1 Abs. 1 Satz 2 VE ME PolG keine Erweiterung der Aufgaben der Polizei sah.

gleichzusetzen.[158] Der Tätigkeitsbereich der Vorbereitung auf bzw. Vorsorge[159] zur Strafverfolgung und Gefahrenabwehr[160] deckt sich allerdings weitgehend mit solchen.[161] Die Datensammlung zu Zwecken der vorbeugenden Verbrechensbekämpfung sei „nichts anderes als Datenvorratswirtschaft zu ‚noch nicht bestimmbaren Zwecken'."[162] Dazu sah man in dem Begriff der „vorbeugenden Bekämpfung von Straftaten" eine Verwischung der Grenzen zwischen Prävention und Repression.[163] Dadurch, dass das Bundesverfassungsgericht in seinem Volkszählungsurteil jede staatliche Verarbeitung personenbezogener Daten angesichts der neuen technologisch bedingten Risiken unter Gesetzesvorbehalt stellte,[164] stellte sich erstmals die Frage nach der Gesetzgebungskompetenz für Regelungen über entsprechende Datenverarbeitungen.[165] § 1 Abs. 1 Satz 2 VE ME PolG und die darin festgehaltene Annahme, dass die vorbeugende Verbrechensbekämpfung vollständig der Gefahrenabwehr zuzuordnen sei,[166] lassen sich als Reaktion auf diese Entwicklung verstehen.

---

[158] So aber *Möstl*, DVBl. 2007, 581 (585); vgl. in diese Richtung auch *Siebrecht*, JZ 1996, 711 (712). Es existieren auch eine Reihe von nicht spezifisch informationsbezogenen Tätigkeiten, die der vorbeugenden Bekämpfung von Straftaten dienen. Darunter können Streifengänge ebenso fallen wie Beratungsgespräche mit Bürger*innen oder Aufenthaltsverbote; vgl. *Albers*, Determination, S. 125; *Baldus*, Die Verwaltung 2014, 1 (20); *Bull*, in: Bull, S. 15 (27 f.). In § 10 Abs. 1 Nr. 2 ME PolG 1976 bezog sich der Begriff der vorbeugenden Verbrechensbekämpfung auf erkennungsdienstliche Maßnahmen; vgl. *F. Sydow*, ZRP 1977, 119 f.

[159] Die Begriffe Vorsorge und Vorbereitung werden in diesem Zusammenhang großteils synonym verwendet. *Knemeyer*, in: FS Rudolf, S. 483 (488) gibt dem Begriff der Vorbereitung den Vorzug, da dieser stärker als der Begriff der Vorsorge deutlich mache, dass es bei dieser Tätigkeit nicht darum gehe, „den Eintritt von Gefahren zu verhindern oder Straftaten zu verhüten oder ihnen vorzubeugen", sondern allgemein auf die Situation der Gefahrenabwehr und Strafverfolgung im konkreten Fall vorbereitet zu sein; vgl. auch *Albers*, Determination, S. 126; zu dem weitgehend deckungsgleichen Begriff der antizipierten Strafverfolgung *Rudolph*, S. 6 ff.

[160] Ein dritter Aspekt der vorbeugenden Verbrechensbekämpfung ist die Verbrechensverhinderung bzw. Verhütung von Straftaten, die Maßnahmen erfasst, „die drohende Rechtsgutverletzungen von vornherein und in einem Stadium verhindern sollen, in dem es noch nicht zu strafwürdigem Unrecht gekommen ist" und dem präventiven Bereich zuzuordnen ist; BVerfGE 113, 348 (369); vgl. auch BVerfGE 141, 220 (263); *Knemeyer*, in: FS Rudolf, S. 483 (490); *Siebrecht*, JZ 1996, 711 (712).

[161] Vgl. *Graulich*, NVwZ 2014, 685; *Knemeyer*, in: FS Rudolf, S. 483 (495 f.); *Möstl*, S. 31, 212 f.; *Park*, S. 229 f.

[162] *Schwan*, in: Hohmann, S. 276 (297).

[163] Deutscher Richterbund, DRiZ 1986, 110; *Ernesti*, ZRP 1986, 57; *Rachor*, S. 33 ff.; vgl. auch *Behrendes*, Die Polizei 1988, 220 (224).

[164] BVerfGE 65, 1 ff. Dass jede Speicherung personenbezogener Informationen einen Grundrechtseingriff bedeutet hatte bis dahin nur eine Literaturmeinung so gesehen; so etwa *Schwan*, VerwArch 66 (1975), 120 (128); *Seidel*, NJW 1970, 181 (183); *Schlink*, S. 192 ff.; vgl. auch *Hoffmann-Riem*, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 1117 (1120 f.).

[165] Vgl. *Stephan*, VBlBW 2005, 410.

[166] Dies ergab sich aus § 1 Abs. 1 Satz 1 VE ME PolG. Die Regelung in Satz 2 der Vorschrift sollte demgegenüber klarstellenden Charakter haben; vgl. Amtliche Begründung zum VE ME PolG, abgedruckt bei *Kniesel/Vahle*, S. 50.

Die Zuordnung der Aufgabe der vorbeugenden Verbrechensbekämpfung blieb in der Folge umstritten. Stimmen in der Literatur vertraten neben der vollständigen Einordnung in den präventiven[167] oder repressiven[168] Bereich auch differenzierende Auffassungen[169]. Die wohl herrschende Meinung sowie die Rechtsprechung[170] neigten wie der VE ME PolG einer Einordnung in den präventiven Bereich zu.[171] Ein wesentliches Argument war hierbei, dass ein repressives Tätigwerden bzw. das Tätigwerden im Hinblick auf ein gerichtliches Verfahren eine bereits begangene Tat voraussetze. Teilweise wurde und wird die Vorbereitung auf Gefahrenabwehr und Strafverfolgung dabei auch als neben Gefahrenabwehr und Strafverfolgung eigenständige polizeiliche Aufgabe eingeordnet.[172] Nach der Entscheidung des Bundesverfassungsgerichts zur vorbeugenden Telekommunikationsüberwachung aus dem Jahr 2005[173] hat sich eine differenziertere Betrachtungsweise durchgesetzt: Je nachdem, ob die Vorbereitung der Strafverfolgung oder Gefahrenabwehr dient, ist sie dem präventiven oder repressiven Tätigkeitsbereich der Polizei zuzuordnen.[174]

Zwar betonte der Musterentwurf von 1986 in seiner Begründung auch die Notwendigkeit, das Verhältnis des Polizeirechts zum Strafprozessrechts zu berücksichtigen,[175] allerdings erfolgten um diesen Aspekt deutlich weniger Bemühungen als noch beim ME PolG 1977. Der Erfolg des VE ME PolG 1986 wird ähnlich wie jener seines Vorgängers tendenziell kritisch beurteilt.[176] Jedenfalls hatte er erheblichen Einfluss auf die

---

[167] So etwa *K.-H. Braun*, Die Polizei 1989, 213 (217); *Kowalczyk*, S. 102 f.; *Scholz/Pitschas*, S. 164 f.; *Ahlf,* KritV 1988, 136 (147 ff.); *Paeffgen* JZ 1991, 437 (441 ff.).

[168] So etwa *Lilie*, ZStW 106 (1994), 625 (634 ff.); *K. Merten*, NStZ 1987, 10 (13); *Schoreit*, KritV 1988, 157 (166 ff.); *Wolter*, StV 1989, 358 (366); *Schweckendieck*, ZRP 1989, 125 ff.

[169] *Denninger,* CR 1988, 51 (54); *O. Müller*, StV 1995, 602 (604); *Wolter*, in: FS Rolinski, S. 273 (277).

[170] Vgl. nur BVerwG NJW 1990, 2765 (2766 f.); BVerwG NJW 1990, 2768 (2769); BayVerfGH, NVwZ 1996, 166 (167); OVG Berlin NJW 1986, 2004; MVVerfG LKV 2000, 345 (347); SächsVerfGH LKV 1996, 273 (275).

[171] Vgl. mit einem Überblick zum Streitstand vor der Entscheidung des BVerfG *Lepsius*, JURA 2006, 929 (933).

[172] *Albers*, Determination, S. 254, 347; *Gusy*, StV 1993, 269 (270); *F. Sydow*, ZRP 1977, 119 (125); *Weßlau,* S. 158 f.; ähnlich *Knemeyer*, in: FS Rudolf, S. 483 (490); *Pitschas*, DÖV 2002, 221; anders hingegen *Möstl*, DVBl. 2007, 581 (585).

[173] BVerfGE 113, 348.

[174] Dass sich die Gesetzgeber der Länder seinerzeit deutlich für eine präventive Zuordnung positionierten und die Gesetzgebungskompetenz für Fragen der kriminalbehördlichen Informationsordnung damit für sich beanspruchten, hat aber heute noch Folgen. Es wirkte sich auf die Gesetzgebung des Bundes aus. Bei der Reform der Strafprozessordnung durch das StVÄG 1999 nutzte der Bundesgesetzgeber seine Regelungskompetenz für die polizeiliche Informationsordnung im Hinblick auf die Vorbereitung für die Verfolgung von Straftaten als Teilbereich der vorbeugenden Verbrechensbekämpfung nicht.

[175] *Kniesel/Vahle*, S. 45.

[176] Vgl. *Albers*, Determination, S. 180; *Walter*, Kriminalistik 2019, 243 (245).

Entwicklung der informationsordnenden Befugnisse im Polizeirecht sowie die Einführung der zweifelhaften Aufgabe der vorbeugenden Verbrechensbekämpfung in den Polizeigesetzen.[177]

Derzeit existieren Bestrebungen zur Schaffung eines neuen Entwurfes für ein Musterpolizeigesetz.[178] Im Juni 2017 erteilte die IMK ihrem Arbeitskreis II (Innere Sicherheit) den Auftrag zur Erarbeitung eines Entwurfes durch eine länderoffene Arbeitsgruppe unter Beteiligung des BMI (AG-MPG).[179] Auch der Koalitionsvertrag für die 19. Legislaturperiode vom 12. März 2018 sieht die Schaffung eines Musterpolizeigesetzes vor.[180] Ein Anstoß für diese Bemühungen waren die Defizite in der polizeilichen Kooperation bei der Aufklärung der NSU-Mordserie und im Fall *Anis Amri*.[181] Wann ein entsprechender Entwurf fertiggestellt wird, lässt sich derzeit noch nicht absehen.[182] Der neue Musterentwurf ist als „Vollgesetz" mit Regelungsvorschlägen zum gesamten Polizeirecht geplant, wobei eine Erwartung der tatsächlichen Vereinheitlichung der Landespolizeigesetze nicht besteht und der Entwurf eher als „Werkzeugkasten" verstanden werden soll.[183]

Das Projekt eines Musterpolizeigesetzes steht in einer gewissen Konkurrenz zu der bereits abgeschlossenen Gesetzgebung auf Bundes- und Landesebene. Zum Teil wird dem BKAG 2018 faktisch die Rolle eines Musterpolizeigesetzes zugeschrieben, da es einen aktuellen Katalog polizeilicher Befugnisse enthält und grundlegende Entwicklungen der jüngeren Verfassungsrechtsprechung berücksichtigt.[184] Es erscheint aber unpassend, dem BKAG einen Modellcharakter für die Landesgesetzgebung zuzuschreiben, da dem Bundeskriminalamt im Vergleich zu den Landespolizeien grundlegend andere

[177] Vgl. zur Umsetzung des VE ME PolG 1986 insgesamt *Rachor*, S. 3 f.

[178] *Thiel*, Die Verwaltung 2020, 1 (10 ff.).

[179] IMK, Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 206. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder, S. 43.

[180] CDU, CSU und SPD, Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land, 2018, S. 126, Zeile 5922 ff.

[181] *Walter*, Kriminalistik 2019, 243.

[182] Auf eine Kleine Anfrage zum Stand des Verfahrens antwortete das BMI Ende August 2018, mit Ergebnissen sei nicht vor dem Jahr 2020 zu rechnen; BT-Drs. 19/4075, S. 19. Auf eine weitere Kleine Anfrage Ende 2020 gab die Bundesregierung an, mit einem Abschluss des Verfahrens sei nicht vor 2021 zu rechnen; BT-Drs. 19/23914, S. 4; zum Sachstand im Jahr 2021 IMK, Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 214. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder, S. 14.

[183] *Thiel*, Die Verwaltung 2020, 1 (11).

[184] *Graulich*, KriPoZ 2017, 278; vgl. auch *Walter*, Kriminalistik 2019, 243 (245).

Aufgaben zukommen.[185] Auch jüngst reformierten Landespolizeigesetzen wird teilweise eine Mustergültigkeit zugeschrieben – so etwa dem als besonders „progressiv"[186] geltenden und verhältnismäßig früh reformierten Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (BayPAG). Welche Rolle das BKAG 2018 oder reformierte Landesgesetze allerdings für die Arbeiten der IMK an einem neuen Musterentwurf tatsächlich spielen, ist unklar.[187] Es ist wahrscheinlich, dass die großteils bereits abgeschlossenen und teilweise noch laufenden Reformen der Polizeigesetze in den Bundesländern das Vorhaben zur Schaffung eines Musterentwurfes beeinflussen könnten. Gegen mehrere reformierte Polizeigesetze wurden bereits Beschwerden vor dem Bundesverfassungsgericht sowie Verfassungsgerichten der Länder erhoben.[188] Hierauf könnten Entscheidungen ergehen, die eine Relevanz für die möglichen und sinnvollen Regelungsgehalte eines Musterpolizeigesetzes haben.[189] Aus praktischer Sicht dürfte es daher sinnvoll sein, die entsprechenden Entscheidungen abzuwarten, bevor ein finale Musterentwurf vorgelegt wird, um diesen nicht sogleich wieder überarbeiten zu müssen.

Der neue Musterentwurf eines Polizeigesetzes würde sich in besonderem Maße anbieten, um ein einheitliches Modell für informationsverarbeitende Befugnisse der Polizei vorzuschlagen. Die traditionellen Aufgaben und Standardbefugnisse der Polizei sind bereits aufgrund der früheren Musterentwürfe weitgehend harmonisiert.[190] Der rechtspolitische Diskussions- und Harmonisierungsbedarf ist im Zusammenhang mit der polizeilichen Datenverarbeitung sowie dem Einsatz technologischer Hilfsmittel weitaus höher. Dies zeigt sich unter anderem darin, dass einzelne Bundesländer die polizeiliche Datenverarbeitung bereits in eigenen Gesetzen neben den allgemeinen Polizeigesetzen regeln.[191]

In diesem Sinne könnte auch der Komplex der Informationsordnung eine Rolle in einem neuen Musterentwurf spielen. Trotz der fehlenden Verbindlichkeit könnte damit ein wichtiger Schritt zur Stärkung und Vereinheitlichung des Informationsordnungsrechts getan werden. Auch Anforderungen an die Datenqualität könnten ein

---

[185] Ähnlich und mit weiterer Kritik *Thiel*, Die Verwaltung 2020, 1 (13 f.); zum BKA als multifunktionaler Sonderpolizeibehörde *Barczak*, in: Barczak, BKAG, 2023, § 1 Rn. 10 ff.

[186] *Walter*, Kriminalistik 2019, 243 (245).

[187] Vgl. *Walter*, Kriminalistik 2019, 243 (247).

[188] Vgl. etwa die von der Gesellschaft für Freiheitsrechte koordinierten Verfassungsbeschwerden gegen die Polizeigesetze von Baden-Württemberg, Bayern, Hessen und Sachsen; abrufbar unter https://freiheitsrechte.org/polizeigesetze/.

[189] Vgl. BT-Drs. 19/6074, S. 2; *Walter*, Kriminalistik 2019, 243 (245).

[190] Vgl. *Aden/Fährmann*, S. 8.

[191] Vgl. das hamburgische Gesetz über die Datenverarbeitung der Polizei vom 12. Dezember 2019 (HmbGVBl. 2019, S. 485) sowie das saarländische Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei vom 6. Oktober 2020 (Amtsblatt I 220, S: 1133).

wichtiger Anker für den Einsatz polizeilicher Informationssysteme sein.[192] Überlegungen in diese Richtung bestanden schon im AE PolG aus dem Jahre 1979, wurden aber von der IMK seinerzeit nicht aufgegriffen.

C. Konkretisierung der Anlässe zur Speicherung von Daten

Die im Polizei- und Strafprozessrecht geregelten Befugnisse zur Speicherung von Daten in kriminalbehördlichen Informationssystemen sind sich recht ähnlich. Die geregelten Voraussetzungen sind weit gefasst.[193] Sie unterscheiden sich kaum von den Anforderungen, die die Gesetze an andere Formen der Weiterverarbeitung von Daten nach ihrer erstmaligen Erhebung stellen.

Im Folgenden werden Möglichkeiten untersucht, die Anlässe für informationsordnende Tätigkeiten spezifischer zu fassen. Ein besonderes Augenmerk liegt dabei darauf, ob und inwiefern eine konkretere Regelung der Eingriffsschwellen dazu beitragen könnte, bestehende Probleme in der kriminalbehördlichen Informationsordnung zu lösen und ihren Ist-Zustand ihrem Soll-Zustand anzunähern (I.). Auf dieser Grundlage wird der gesetzgeberische Spielraum zur Regelung der Eingriffsschwellen für informationsordnende Tätigkeiten untersucht (II.). Schließlich wird beleuchtet, wie eine Regelung der Voraussetzungen für informationsordnende Tätigkeiten konkret aussehen könnte (III.).

I. Beitrag zur Lösung bestehender Herausforderungen

Konkreter gefasste rechtliche Regelungen über die Speicherung von Daten könnten dazu beitragen, das Wachstum kriminalbehördlicher Informationsbestände zu begrenzen. Dies zeigt sich beispielsweise an dem oben ausgeführten Fall der Datei „Gewalttäter Sport“. Hier hat die Zahl der erfassten Personen aufgrund einer Anpassung der Kriterien zur Speicherung in den letzten Jahren abgenommen.[194] Die Anpassung erfolgte zwar nicht auf gesetzlicher Ebene, sondern in der Errichtungsanordnung der Datei. Allerdings könnten derartige Spezifizierungen auch auf gesetzlicher Ebene erfolgen. Dies würde im Gegensatz zu einer Festlegung durch Exekutivakte auch dazu führen, dass die

[192] Ähnlich *Aden/Fährmann*, S. 34; siehe näher zu Regelungen bezüglich der Datenqualität oben Teil 2 C. III.

[193] Siehe oben Teil 2 A. III. 1. a.

[194] Siehe oben Teil 2 D. I. 1.

kriminalbehördlichen Informationsressourcen und ihre Handhabung für Bürger*innen transparenter würden als bisher.

Eine nähere Festlegung der notwendigen Anlässe für die Speicherung von Informationen durch den Gesetzgeber könnte auch Rechtsanwender*innen zumindest partiell entlasten. Sie könnte die Prüfung der Befugnisse vereinfachen und die damit verbundene Rechtsunsicherheit abmildern. Aus Sicht der Betroffenen, über die Daten in der kriminalbehördlichen Informationsordnung gespeichert sind, könnten konkretere Regelungen Risiken wie jene der Stigmatisierung und Kriminalisierung berücksichtigen und diesen damit besser gerecht werden als die bisher geltenden Regelungen.

II. Rechtliche Möglichkeiten und Grenzen

Eine Konkretisierung der Voraussetzungen für staatliches Eingriffshandeln, zu dem auch die Speicherung von personenbezogenen Daten gehört, ist aus rechtsstaatlicher Sicht prinzipiell begrüßenswert. Im Folgenden werden die unions- und verfassungsrechtlichen Rahmenbedingungen für die Regelung von Befugnissen zur Speicherung von Daten durch Kriminalbehörden betrachtet. Ein besonderes Augenmerk liegt dabei auf den Eingriffsschwellen dieser Befugnisse.

Wenig Vorgaben dafür, wann eine Speicherung personenbezogener Daten durch Kriminalbehörden zulässig ist, ergeben sich zunächst aus der JI-Richtlinie, die das Datenschutzrecht für kriminalbehördliche Datenverarbeitungen auf unionsrechtlicher Ebene harmonisiert.[195] Aus Art. 8 Abs. 1 JI-Richtlinie ergibt sich lediglich, dass die Speicherung von Daten für die Erfüllung polizeilicher bzw. staatsanwaltschaftlicher Aufgaben erforderlich und hierfür eine Rechtsgrundlage vorhanden sein muss. Nach Art. 8 Abs. 2 JI-Richtlinie müssen im Recht der Mitgliedstaaten „zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben“ werden.

Ähnliche Anforderungen ergeben sich nach dem deutschen Verfassungsrecht aus dem Vorbehalt des Gesetzes sowie den rechtsstaatlichen Grundsätzen der Verhältnismäßigkeit und Bestimmtheit.[196] Da die Speicherung personenbezogener Daten durch eine staatliche Stelle ein Eingriff in das Recht auf informationelle Selbstbestimmung ist, bedarf es hierfür einer gesetzlichen Befugnis. Der Grundsatz der Verhältnismäßig-

[195] Siehe hierzu bereits oben Teil 1 C. III. 1. b.

[196] Zu deren Bedeutung für die Prüfung und Entwicklung von Eingriffsbefugnissen im Sicherheitsrecht insgesamt vgl. BVerfGE 110, 33 (55), BVerfGE 113, 348 (375 ff.); BVerfGE 120, 274 (317 f.); *Gärditz*, GSZ 2017, 1 (3); *Poscher*, in: Vesting/Korioth, S. 245 (261); *R. Schenke*, in: FS Würtenberger, S. 1079 (1088 ff.); *Trute*, Die Verwaltung 2009, 85 (88 ff., 96 ff.); *Zöller*, in: GS Weßlau, S. 551 sowie speziell zu Informationsbefugnissen *Möstl*, in: Spiecker gen. Döhmann/Collin, S. 239 (248 f.).

keit begrenzt die zulässige Weite einer derartigen Befugnis, ist aber auch bei ihrer Anwendung zu beachten.[197] Bezüglich der Schaffung neuer Befugnisse zur Datenverarbeitung ist namentlich das Gebot der Zweckbindung relevant, welches aus der Verhältnismäßigkeit folgt. In den geltenden Befugnissen zur Informationsordnung findet der Grundsatz der Verhältnismäßigkeit vor allem Ausdruck in der Voraussetzung der Erforderlichkeit und (daran anknüpfenden) zeitlichen Begrenzungen der Speicherung von Daten.[198]

Auch aus dem rechtsstaatlichen Grundsatz der Bestimmtheit ergeben sich Anforderungen an die Ausgestaltung von Befugnisnormen. So hat das Bestimmtheitsgebot im Zusammenhang mit Befugnissen zur Datenverarbeitung die „spezifische Funktion, eine hinreichend präzise Umgrenzung des Verwendungszwecks der [von einer Datenverarbeitung] betroffenen Informationen sicherzustellen."[199] Dadurch, dass das Bestimmtheitsgebot dem Gesetzgeber vorgibt, die Zwecke der Verarbeitung von Daten einzugrenzen, hängt es mit dem datenschutzrechtlichen Gebot der Zweckbindung zusammen und verstärkt dieses.[200] Da die Befugnisse zur Informationsordnung als Regelungen zur Vorsorge zu begreifen sind, gelten besondere Voraussetzungen für ihre Bestimmtheit. Das Bestimmtheitsgebot lässt eine gewisse Flexibilität von Eingriffsnormen zu, um insbesondere deren Offenheit für technische und gesellschaftliche Entwicklungen zu wahren.[201]

Insgesamt hängen die Maßstäbe der Verhältnismäßigkeit und der Bestimmtheit eng miteinander zusammen. Mit den Worten des Bundesverfassungsgerichts beeinträchtigen „Mängel hinreichender Normenbestimmtheit und -klarheit [...] die Beachtung des verfassungsrechtlichen Übermaßverbots"[202]. Weit gefasste rechtliche Befugnisse können leichter an den Anforderungen der Erforderlichkeit und Angemessenheit scheitern als engere Regelungen. Hinzu kommt, dass die durch das Bestimmtheitsgebot vorgegebene Notwendigkeit, in einer Befugnis zur Datenverarbeitung ihren Zweck festzulegen,

---

[197] Bei der Anwendung der Befugnisse ermöglicht es der Grundsatz der Verhältnismäßigkeit, flexibel auf informationstechnische Entwicklungen zu reagieren. So kann etwa die Eingriffsintensität einer Maßnahme dadurch steigen, dass sie mit neuen technischen Hilfsmitteln durchgeführt wird, die bei der Schaffung der entsprechenden Befugnis noch nicht zur Verfügung standen. Auch die Bedeutung der Speicherung und Auswertung von Daten haben sich infolge technischer Entwicklungen verändert. Die Prüfung der Verhältnismäßigkeit kann hier dazu dienen, den Anwendungsbereich der Befugnisse zu begrenzen; vgl. zu der wachsenden Bedeutung des Verhältnismäßigkeitsgrundsatzes für informationelle Befugnisse angesichts technologischer Entwicklungen *Singelnstein/Putzer*, GA 2015, 564 (566 f.).

[198] Siehe näher zu Letzteren unten D. III. 1.

[199] BVerfGE 120, 351 (366).

[200] BVerfGE 120, 351 (366); vgl. auch BVerfGE 118, 168 (187 f.).

[201] Vgl. BVerfGE 49, 89 (135).

[202] BVerfGE 110, 33 (55).

ebenso als Ausgangspunkt für die Prüfung der Verhältnismäßigkeit dient. Normenklarheit und Bestimmtheit lassen sich damit als Voraussetzungen der Operationalisierung des Grundsatzes der Verhältnismäßigkeit verstehen.[203]

Aus den rechtsstaatlichen Grundsätzen der Verhältnismäßigkeit und Bestimmtheit ergeben sich für kriminalbehördliche Befugnisse zur Speicherung von personenbezogenen Daten als Grundvoraussetzungen, dass die Speicherung einem festgelegten Zweck dienen und die Speicherung von Daten zu dessen Erfüllung erforderlich sein müssen. Insofern stimmen diese Vorgaben weitgehend mit jenen aus Art. 8 JI-Richtlinie überein. Im Folgenden werden zunächst die Aspekte der Zweckfestlegung (1.) und der Erforderlichkeit (2.) näher betrachtet. Darüber hinaus wird untersucht, ob und inwieweit sich aus dem vom Bundesverfassungsgericht formulierten Grundsatz der hypothetischen Datenneuerhebung Voraussetzungen für die Regelungen von Befugnissen zur Speicherung von Daten in kriminalbehördlichen Informationssystemen ergeben (3.).

1. Die Zweckfestlegung als Ausgangspunkt der rechtlichen Bewertung

Die Speicherung personenbezogener Daten in einer kriminalbehördlichen Informationsressource kann nur zulässig sein, wenn sie einem legitimen Zweck dient. Der verfolgte Zweck erweist sich damit als notwendiger Ausgangspunkt der rechtlichen Betrachtung.[204]

Sowohl das Bundesverfassungsgericht als auch der Europäische Gerichtshof sehen die anlasslose Bevorratung von personenbezogenen Daten zu unbestimmten Zwecken als grundsätzlich unzulässig an. Das Bundesverfassungsgericht folgert dies aus dem datenschutzrechtlichen Gebot der Zweckbindung, das wiederum auf dem Grundsatz der Verhältnismäßigkeit beruht. Das Gericht führte in seinem Volkszählungsurteil aus, dass „die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" zumindest bei einem Zwang zur Angabe personenbezogener Daten nicht mit der Pflicht des Gesetzgebers vereinbar wäre, den Verwendungszweck der Daten „bereichsspezifisch und präzise" zu bestimmen.[205] Dieser Linie führte das Gericht in mehreren Entscheidungen fort.[206]

In seiner Entscheidung zur Vorratsspeicherung von Telekommunikationsverkehrsdaten[207] positionierte sich das Bundesverfassungsgericht genauer. Zwar griff das Gericht auch hier das grundsätzliche Verbot einer Speicherung von Daten auf Vorrat auf und betonte, dass es unzulässig sei, unabhängig von konkreten Zweckbestimmungen

[203] *Trute*, Die Verwaltung 2009, 85 (96).
[204] *Möstl*, in: Spiecker gen. Döhmann/Collin, S. 239 (247).
[205] BVerfGE 65, 1 (46).
[206] BVerfGE 100, 313 (360); BVerfGE 115, 320 (350); BVerfGE 118, 168 (187).
[207] Vgl. zu der Geschichte der Vorratsdatenspeicherung in Deutschland *Szuba*, S. 116 ff.

„einen Datenpool auf Vorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt."[208] Allerdings formulierte es auch einen möglichen Spielraum für die Regelung einer Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten. Die „sechsmonatige anlasslose Speicherung von Telekommunikationsverkehrsdaten für qualifizierte Verwendungen im Rahmen der Strafverfolgung, der Gefahrenabwehr und der Aufgaben der Nachrichtendienste" unterfalle „nicht schon als solche dem strikten Verbot einer Speicherung von Daten auf Vorrat".[209] Eine vorsorgliche anlasslose Datensammlung sei ausnahmsweise zulässig und unterliege „sowohl hinsichtlich ihrer Begründung als auch hinsichtlich ihrer Ausgestaltung, insbesondere auch in Bezug auf die vorgesehenen Verwendungszwecke, besonders strengen Anforderungen."[210] Das Gericht betonte das besondere Eingriffsgewicht dieser Form der Speicherung von Daten.[211]

Diese Position hat das Bundesverfassungsgericht in einer Entscheidung zur Verpflichtung von Telekommunikationsanbietern zur Speicherung von vergebenen Telekommunikationsnummern und personenbezogenen Daten der Anschlussinhaber nach § 111 TKG weiterentwickelt. Eine vorsorgliche und anlasslose Speicherung dieser Daten sei nicht generell verboten, sondern bringe nur besondere Begründungsanforderungen mit sich.[212] Vorsorgliche Datensammlungen könnten ausnahmsweise „als Grundlagen vielfältiger staatlicher Aufgabenwahrnehmung ihre Berechtigung haben"[213]. Eine unzulässige Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken läge nicht vor, sondern lediglich eine „Vorhaltung bestimmter, begrenzter und in ihrem Informationsgehalt genau umschriebener Daten für die in den §§ 112, 113 TKG eingehend definierten Verwendungszwecke".[214] Aufgrund der Eingrenzung der betroffenen Daten und ihrer begrenzten Aussagekraft sah das Gericht in diesem Fall auch trotz der großen Streubreite des

[208] BVerfGE 125, 260 (345).

[209] BVerfGE 125, 260 (316). In diesem Zusammenhang handelte sich das Gericht die Kritik ein, das Verbot einer anlasslosen Speicherung personenbezogener Daten auf Vorrat aufzuweichen; *Meinicke*, HRRS 2011, 398 (400).

[210] BVerfGE 125, 260 (317). Diese Anforderungen an die Rechtfertigung führte das Gericht in seiner Entscheidung im Hinblick auf die die Speicherung von Telekommunikationsverkehrsdaten näher aus. „Maßgeblich für die Rechtfertigungsfähigkeit einer solchen Speicherung" sei „insbesondere, dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Diensteanbieter grundsätzlich untersagt ist."; BVerfGE 125, 260 (324).

[211] BVerfGE 125, 260 (324).

[212] BVerfGE 130, 151 (187).

[213] BVerfGE 130, 151 (189).

[214] BVerfGE 130, 151 (187).

Eingriffs bzw. der Vielzahl der betroffenen Personen keinen besonders gewichtigen Eingriff gegeben.[215]

Ähnliche Anforderungen formulierte der Europäische Gerichtshof in seinen Entscheidungen zur Vorratsdatenspeicherung in den Jahren 2014 und 2016 (Digital Rights und Tele 2).[216] Er rügte Regelungen, die die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten und Standortdaten zur Regel machten und „keine Differenzierung, Einschränkung oder Ausnahme in Abhängigkeit von dem verfolgten Ziel" vorsahen.[217] Eine weitreichende Speicherung derartiger Daten bedeute einen besonders schwerwiegenden Eingriff in Art. 7 und Art. 8 GRCh.[218] Mit Blick auf die darin gewährleisteten Rechte sei besonders eine Regelung zur Vorratsdatenspeicherung problematisch, die sich „weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung von Straftaten beitragen könnten"[219] beschränke. Möglich sei hingegen eine Regelung „die zur Bekämpfung schwerer Straftaten vorbeugend die gezielte Vorratsspeicherung von Verkehrs- und Standortdaten ermöglicht, sofern die Vorratsdatenspeicherung hinsichtlich Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsspeicherung auf das absolut Notwendige beschränkt ist."[220]

In seiner jüngeren Rechtsprechung zur Vorratsdatenspeicherung hat der Europäische Gerichtshof die Grundsätze aus den Entscheidungen Digital Rights und Tele 2 beibehalten, sich aber genauer mit den Ausnahmen hierzu befasst. So betrachtete das Gericht eine allgemeine und unterschiedslose Vorratsdatenspeicherung unter engen

[215] BVerfGE 130, 151 (189).

[216] In beiden Fällen ging es um die Zulässigkeit der Speicherung von Telekommunikationsverkehrsdaten und Standortdaten. In seiner Entscheidung Digital Rights erklärte der Gerichtshof die Richtlinie 2006/24/EG mit Art. 7, 8 und 11 GRCh für unvereinbar. In der Entscheidung Tele 2 erklärte der Gerichtshof Regelungen zur Vorratsdatenspeicherung in Schweden und Großbritannien für mit Art. 15 Abs. 1 Richtlinie 2002/58/EG im Lichte von Art. 7, 8 und 11 GRCh unvereinbar.

[217] EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 – Tele 2, Rn. 104 f.; ähnlich EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights, Rn. 57.

[218] EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights, Rn. 37; EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 – Tele 2, Rn. 100.

[219] EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 – Tele 2, Rn. 106; ähnlich EuGH, Urteil vom 8. April 2014, Rs. C-293/12 und C-594/12 – Digital Rights, Rn. 59.

[220] EuGH, Urteil vom 21. Dezember 2016, Rs. C-203/15 und C-698/15 – Tele 2, Rn. 108.

Voraussetzungen bei „einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit" als möglich.[221] Eine solche Maßnahme müsste aber auf das absolut notwendige Maß beschränkt sein und einer wirksamen Kontrolle unterliegen.[222] Die Ausführungen des Europäischen Gerichtshofs zur (Un-)Zulässigkeit der Vorratsdatenspeicherung ähneln in vielerlei Hinsicht jenen des Bundesverfassungsgerichts. Mit seinen jüngeren Entscheidungen hat der Europäische Gerichtshof einen weiteren Spielraum als bisher für die ausnahmsweise Zulässigkeit einer Vorratsdatenspeicherung angenommen, formuliert hierfür aber insgesamt strengere Anforderungen als das Bundesverfassungsgericht.

Das vom Bundesverfassungsgericht und dem Europäischen Gerichtshof angenommene grundsätzliche Verbot der Bevorratung personenbezogener Daten zu unbestimmten Zwecken ist grundsätzlich auch für die kriminalbehördliche Informationsordnung und andere Instrumente zur Bevorratung von Informationen zu Sicherheitszwecken relevant.[223] So erweist sich etwa eine allgemeine längerfristige Speicherung von Fluggastdaten ohne besonderen Anlass als grundrechtlich ähnlich problematisch wie die Speicherung von Telekommunikationsdaten auf Vorrat.[224] In der kriminalbehördlichen Informationsordnung dürfte es allerdings kaum zu vergleichbaren Konstellationen einer anlasslosen Datenspeicherung kommen. Dass Kriminalbehörden oder andere staatliche Stellen Daten speichern, ganz ohne hierfür einen Zweck oder Anlass angeben zu können, wird praktisch nur in seltenen Ausnahmefällen vorkommen.[225]

Wichtiger erscheint im Kontext der kriminalbehördlichen Informationsordnung die Frage, in welcher Weite die Zwecke der Datenspeicherung durch den Gesetzgeber festgelegt werden dürfen.[226] Nach der Rechtsprechung des Bundesverfassungsgerichts kann die Zweckbestimmung staatlich gespeicherter Daten im Wesentlichen durch die Definition der Anforderungen an ihre spätere Nutzung geschehen.[227] Die zulässigen Zwecke der Weiterverarbeitung werden dann zugleich als Zwecke der Datensammlung

[221] EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net, Rn. 137; EuGH, Urteil vom 5. April 2022, Rs. C-140/20 – Commissioner of the Garda Síochána, Rn. 58; EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – SpaceNet und Telekom Deutschland, Rn. 72; vgl. näher zu den vom EuGH anerkannten Ausnahmen *M. Müller/Schwabenbauer*, NJW 2021, 2079 (2081 f.); *Roßnagel*, ZD 2022, 650 (653).

[222] EuGH, Urteil vom 6. Oktober 2020, Rs. C-511/18, C-512/18 und C-520/18 – La Quadrature du Net, Rn. 138; EuGH, Urteil vom 5. April 2022, Rs. C-140/20 – Commissioner of the Garda Síochána, Rn. 58; EuGH, Urteil vom 20. September 2022, Rs. C-793/19 und C-794/19 – SpaceNet und Telekom Deutschland, Rn. 72.

[223] *Boehm/Cole*, MMR 2014, 569 (570).

[224] Vgl. EuGH, Urteil vom 21. Juni 2022, Rs. C-817/19 – Ligue des droits humains, Rn. 261.

[225] *Ladeur*, DuD 2000, 12 (14).

[226] Vgl. für die Steuerung des polizeilichen Umgangs mit Informationen und Daten insgesamt *Albers*, Determination, S. 277.

[227] BVerfGE 155, 119 (180).

angesehen. Die Verfassungsmäßigkeit einer Speicherung kann demnach nicht isoliert betrachtet werden, sondern ist von den Regeln über die weitere Datenverwendung abhängig.[228] Dennoch spricht unabhängig von den einschlägigen Verwendungsregelungen die in dieser Untersuchung festgestellte eigenständige Relevanz des Schrittes der Datenspeicherung dafür, dass deren Voraussetzungen eigenständig gesetzlich spezifiziert werden sollten.

Die geltenden Befugnisse zur Informationsordnung in Strafprozessordnung und Polizeigesetzen sind in ihrer Zweckfestlegung weit gefasst. Neben Zwecken der Dokumentation und Vorgangsverwaltung sind Speicherungen zur Erfüllung polizeilicher Aufgaben, für Zwecke konkreter Strafverfahren sowie für Zwecke künftiger Strafverfahren zulässig. Gerade der pauschale Verweis auf Zwecke künftiger Strafverfahren in § 484 Abs. 1 StPO erscheint problematisch weit.[229] Stellte man als Bezugspunkt für die Speicherung von Informationen allgemein auf die Vorsorge für unbestimmte zukünftige Verfahren ab, ließe sich praktisch das Vorhalten jeglicher Informationen als erforderlich begründen – besonders, wenn es um schwerwiegende Bedrohungen ginge.[230] Dies wird der grundrechtlichen Regelungsverantwortung für den Schritt der Datenspeicherung nicht gerecht. Wie eine konkretere Regelung aussehen könnte, wird sogleich untersucht.[231]

2. Zweckdienlichkeit der Datenspeicherung

Neben der Notwendigkeit einer Zweckbestimmung lässt sich aus der höchstrichterlichen Rechtsprechung als Mindestvoraussetzung für die Speicherung von personenbezogenen Daten in kriminalbehördlichen Datensammlungen herleiten, dass diese geeignet sein müssen, zu der Erfüllung des Zweckes der jeweiligen Datensammlung beizutragen.[232]

Dies erfordert mit der Rechtsprechung des Bundesverfassungsgerichts „eine auf die Eignung der Daten für den Sammlungszweck bezogene Prognoseentscheidung der speichernden Behörde zum Zeitpunkt der Datenspeicherung.“[233] Die Prognoseentscheidung ist auf objektiven Grundlagen durch eine Wertung zu treffen.[234] Als tatsächliche Grundlage für eine Prognose können unter Umständen bereits vage Erkenntnisse

[228] BVerfGE 155, 119 (180); BVerfGE 125, 260 (327 f.).
[229] So auch *Weßlau/Puschke*, in: SK-StPO, 5. Aufl. 2020, Vor § 474 Rn. 55.
[230] *Poscher*, in: Vesting/Korioth, S. 245 (253).
[231] Siehe unten III. 2.
[232] BVerfGE 120, 351 (367).
[233] BVerfGE 120, 351 (367).
[234] Vgl. zur Prognose als „gedankliche[r] Verknüpfung von Informationen über Tatsachen mit Erwartungen über künftige Ereignisse“ *Darnstädt*, DVBl. 2017, 88.

ausreichen,[235] welche über bloße Vermutungen oder ein „Bauchgefühl" hinaus gehen.[236] So kommen als mögliche Grundlagen etwa Erkenntnisse über die Begehung einer Straftat oder Ankündigungen, eine solche zu begehen in Betracht. Auch kriminalbehördliches Erfahrungswissen ist als Teil der Tatsachengrundlage zu berücksichtigen.[237]

Auf der Tatsachengrundlage muss eine individuelle Einschätzung erfolgen, dass die Speicherung von Daten dem verfolgten Zweck dienlich ist. Dies erfordert eine individuelle Bewertung des Einzelfalles.[238] Schließlich gebietet es der Grundsatz der Verhältnismäßigkeit, im Rahmen der Prüfung der Erforderlichkeit von Datenspeicherungen eine Interessenabwägung durchzuführen, bei der die einer Speicherung entgegenstehenden Interessen der betroffenen Person zu berücksichtigen sind.[239] Bei dieser sind das Recht auf informationelle Selbstbestimmung bzw. Datenschutz, aber auch der Schutz vor Diskriminierung und die Unschuldsvermutung – zumindest wertungsmäßig – zu berücksichtigen.

Konkret bedeutet dies für die Anforderungen an die Prognose im Zusammenhang mit der Speicherung von Daten zu Zwecken der (Vorbereitung der) Strafverfolgung: Werden Daten im Zusammenhang mit einem bestimmten Verfahren gespeichert oder strukturiert, muss sich die Prognose auf deren Nutzen in diesem Verfahren beziehen. So ist die Befugnis in § 483 Abs. 1 Satz 1 StPO für die Speicherung von Daten für Zwecke eines Strafverfahrens streng auf den in dem Verfahren verfolgten Ermittlungszweck begrenzt.[240] Relevant sind dabei in erster Linie Daten, die tatsächliche Anhaltspunkte für verfolgbare Straftaten im Sinne von § 152 Abs. 2 StPO enthalten.[241] Aufgrund des konkreten Verfahrensbezugs wird sich die Prognose regelmäßig an jener eines Tatverdachts orientieren können.

Weniger klar ist der Maßstab der Prognose, wenn die Speicherung von Daten für die Vorbereitung künftiger Strafverfolgung dienen soll. Die in diesem Zusammenhang einschlägigen Befugnisse in § 484 Abs. 1 StPO, § 81b Abs. 1 Var. 2 StPO und § 81g StPO brechen aus dem System der strafprozessualen Datenverarbeitungsbefugnisse aus, die sich grundsätzlich an einem konkreten Ermittlungszweck orientieren. Sie setzen jedoch voraus, dass Ausgangspunkt der Speicherung ein konkretes Strafverfahren ist,

---

[235] Vgl. ähnlich zu dem Merkmal „Anhaltspunkte" als gesetzlich am weitesten gefasster Prognosegrundlage *Albers*, Determination, S. 286.

[236] *Rachor/Graulich*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. E Rn. 149; vgl. auch *Kral*, S. 110 f.

[237] Vgl. VGH Mannheim NVwZ-RR 2000, 287 (288); VGH Mannheim ZD 2015, 542 (544); OVG Saarlouis BeckRS 2012, 58861; kritisch hierzu *Kral*, S. 40 f.

[238] Vgl. BVerfG BeckRS 2009, 35816.

[239] Vgl. OLG Dresden MMR 2003, 592 (593); OLG Frankfurt a.M. NStZ-RR 2008, 183 (184); OLG Frankfurt a.M. NStZ-RR 2010, 350 (351); OLG Hamburg NStZ 2009, 707 (708).

[240] Vgl. BVerfGE 113, 29 (52).

[241] *Singelnstein*, in: MüKo-StPO, 2019, § 483 Rn. 10.

aus dem die Daten hervorgehen.[242] Die genaueren Anforderungen an die Prognose in diesem Zusammenhang werden sogleich untersucht.[243]

3. Der Grundsatz der hypothetischen Datenneuerhebung

Es stellt sich schließlich die Frage, ob bei der Regelung von Befugnissen zur Datenspeicherung auch der verfassungsrechtliche Grundsatz der hypothetischen Datenneuerhebung zu berücksichtigen ist. Zuletzt haben das BKAG und mehrere Landespolizeigesetze die Kriterien des vom Bundesverfassungsgericht formulierten Grundsatzes der hypothetischen Datenerhebung zur Voraussetzung für die Speicherung von Informationen in der polizeilichen Informationsordnung gemacht. Im Folgenden wird dieser Grundsatz näher untersucht (a.). Auf dieser Grundlage wird betrachtet, ob er für die Speicherung von Daten in kriminalbehördlichen Informationsressourcen notwendigerweise Anwendung findet (b.).

a. Der verfassungsrechtliche Grundsatz

Der Grundsatz der hypothetischen Datenneuerhebung konkretisiert die verfassungsrechtlichen Anforderungen an die Zweckbindung bei der Verarbeitung personenbezogener Daten. Das Bundesverfassungsgericht hat ihn in seinem Urteil zum BKAG aus dem Grundsatz der Verhältnismäßigkeit entwickelt. Das Gericht differenzierte zwischen drei Arten der Nutzung von Daten, an die demnach unterschiedliche Anforderungen zu stellen sind. Die erste Kategorie der Nutzung von Daten zu ihrem ursprünglichen Zweck in dem Verfahren, in dem sie erhoben wurden („zweckrealisierende Nutzung“[244]), setzt das Bundesverfassungsgericht in seinen Ausführungen voraus. Für die Folgenutzung von Daten unterschied es zwei weitere Kategorien, für die es abgestufte Voraussetzungen formulierte: Die weitere Nutzung (aa)) und die darüber hinaus gehende zweckändernde Nutzung (bb)).

aa) Die weitere Nutzung von Daten

Die weitere Nutzung erfasst die Nutzung von Daten innerhalb der ursprünglichen Zwecksetzung „über das für die Datenerhebung maßgebende Verfahren hinaus“[245]. Eine solche weitere Nutzung kommt in Betracht, wenn die Datenverarbeitung „seitens

---

[242] BVerwG NJW 1983, 772 (773); *Rudolph*, S. 175 (jeweils zu § 81b Abs. 1 Var. 2 StPO); BT-Drs. 14/1484, S. 18 (zu §§ 483 ff. StPO).

[243] Siehe unten III.

[244] *Schwabenbauer*, in: Lisken/Denninger, 7. Aufl. 2021, G Rn. 32.

[245] BVerfGE 141, 220 (324).

derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter“[246] wie bei der Datenerhebung erfolgt. Das Bundesverfassungsgericht etablierte diese Kategorie durch sein Urteil zum BKAG neu. Vieles spricht dafür, dass die „weitere Nutzung“ von Daten nach der vorherigen Rechtsprechung des Bundesverfassungsgerichts sowie nach herrschender Auffassung der Literatur als ein Teil der zweckändernden Verarbeitung anzusehen war.[247] Die neue Kategorie lässt sich auch als Annäherung an die unionsrechtliche Kategorie einer zweckkompatiblen Nutzung verstehen, die weniger strengen Anforderungen unterliegt als eine zweckändernde Nutzung.[248]

Das Bundesverfassungsgericht gestattet in seinem Urteil insbesondere die weitere Nutzung von Daten als „Spurenansatz“, wenn dabei dieselbe behördliche Aufgabe wahrgenommen wird wie bei der Datenerhebung und dieselben Rechtsgüter geschützt werden.[249] Damit will das Bundesverfassungsgericht ausdrücklich einem sicherheitsbehördlichen Interesse an der „Generierung von Wissen“[250] Rechnung tragen. Was das Kriterium des Spurenansatzes in diesem Zusammenhang erfordert, ist aber im Einzelnen unklar. Der strafprozessuale Begriff des Spurenansatzes gibt für die Bestimmung des Anlasses kaum etwas her, weil er sich auf die Verwendung von Daten zu Ermittlungszwecken bezieht, deren Verwendung zu Beweiszwecken eingeschränkt ist und nicht mit bestimmten Anforderungen verknüpft ist.[251]

Offen ist auch, welche Art von Rechtsgrundlage für eine weitere Nutzung notwendig ist. Vorstellbar wäre entweder eine Weiterverarbeitung auf derselben Grundlage, nach der die ursprüngliche Erhebung durchgeführt wurde, oder eine gesonderte Rechtsgrundlage.[252] Einfachgesetzlich hat die Kategorie der weiteren Nutzung in § 12 Abs. 1 BKAG und vergleichbaren Normen der Landespolizeigesetze Niederschlag gefunden, wonach das Bundeskriminalamt personenbezogene Daten, die es selbst erhoben hat, zur Erfüllung derselben Aufgabe und zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten weiterverarbeiten kann.

bb) Die zweckändernde Nutzung von Daten

Eine zweckändernde Nutzung ist die Weiterverarbeitung personenbezogener Daten für eine andere als die bei der ursprünglichen Erhebung vorgesehene Zweckrichtung. An

[246] BVerfGE 141, 220 (325).
[247] *Müllmann*, NVwZ 2016, 1692 (1693).
[248] *Wolff*, in: Schantz/Wolff, Rn. 399.
[249] BVerfGE 141, 220 (325 f.).
[250] BVerfGE 141, 220 (325 f.).
[251] Vgl. *Singelnstein*, in: MüKo-StPO, 2019, § 477 Rn. 33 ff.
[252] Vgl. *Schwabenbauer*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 32.

eine zweckändernde Nutzung sind nicht die gleichen strengen Voraussetzungen zu stellen wie an die ursprüngliche Erhebung der Daten. Auch diese bedarf jedoch „eines eigenen, hinreichend spezifischen Anlasses."[253] Das Bundesverfassungsgericht fordert, „dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt."[254] Der Gesetzgeber könne „eine Zweckänderung von Daten grundsätzlich dann erlauben, wenn es sich um Informationen handele, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist."[255] Was ein konkreter Ermittlungsansatz ist und wie er sich von anderen Anlassschwellen unterscheidet, lässt das Bundesverfassungsgericht weitgehend offen.[256] Gerade der Vergleich zum Kriterium des Spurenansatzes legt aber nahe, dass zumindest ein einzelfallbezogener tatsächlicher Anlass vorliegen muss.[257]

In der Terminologie des Bundesverfassungsgerichts zur hypothetischen Datenneuerhebung ist die Speicherung personenbezogener Daten in der polizeilichen Informationsordnung regelmäßig eine zweckändernde Nutzung, die im Anwendungsbereich des BKAG an dessen § 12 Abs. 2 zu messen ist. Die Voraussetzungen für eine „weitere Nutzung" im Sinne von § 12 Abs. 1 BKAG, dass die Speicherung seitens derselben Behörde im Rahmen derselben Aufgabe und für den Schutz derselben Rechtsgüter erfolgt, wird praktisch aber kaum zu erfüllen sein. Aufgrund der Multipolarität der Informationsordnung wird es nach dem aktuellen Konzept der Informationsordnung jedenfalls an den Voraussetzungen der Erfüllung derselben Aufgabe scheitern.

Die Beantwortung der Frage, wann dieselbe Aufgabe im Sinne der Vorschrift vorliegt, lässt einen gewissen Interpretationsspielraum.[258] Es fragt sich, inwieweit hinsichtlich der polizeilichen Aufgaben zwischen sämtlichen in den Polizeigesetzen geregelten Aspekten zu trennen ist – also der Gefahrenabwehr im engeren Sinne, der Verhütung von Straftaten, der vorbeugenden Bekämpfung von Straftaten und der Vorbereitung der Gefahrenabwehr. Für eine solch kleinteilige Unterscheidung der Aufgaben im einfachgesetzlichen Zusammenhang des Grundsatzes der hypothetischen Datenneuerhebung sprechen § 12 Abs. 2 BKAG und die entsprechenden Regelungen der Landespolizeigesetze. Diese unterscheiden zwischen den Aufgaben der Verhütung, Aufdeckung

[253] BVerfGE 141, 220 (328).
[254] BVerfGE 141, 220 (329).
[255] BVerfGE 141, 220 (329).
[256] Vgl. *Bäcker*, Stellungnahme BKAG 2018, S. 7; *Zöller* StV 2019, 419 (425).
[257] *Bäcker*, Stellungnahme BKAG 2018, S. 7.
[258] Vgl. *Löffelmann*, GSZ 2019, 16 (17).

und Verfolgung von Straftaten (§ 12 Abs. 2 Nr. 1 lit. a BKAG) und dem Schutz von Rechtsgütern (§ 12 Abs. 2 Nr. 1 lit. b BKAG). Auch das Bundesverfassungsgericht nimmt an, dass bei einer weiteren Verwendung von zu repressiven Zwecken gespeicherten Daten zu präventiven Zwecken und andersherum von einer Zweckänderung auszugehen ist. Nach dieser Wertung bedeutet auch jede Datenspeicherung für gemischt präventiv-repressive Zwecke eine Zweckänderung. Im Rahmen der polizeilichen Informationsordnung ist es allerdings typisch, dass Daten zu gemischt präventiv-repressiven Zwecken gespeichert werden.[259] Dies könnte dafür sprechen, die weitere Speicherung als Annex zu der bei der Erhebung verfolgten Aufgabe zu verstehen, solange noch kein weiterer Zweck der Verwendung feststeht. Zudem erfüllt das Bundeskriminalamt in seiner Funktion als Zentralstelle für die Informationsordnung eine gemischt präventiv-repressive Aufgabe.[260] Diese Argumente schlagen jedoch zumindest gegenüber der einfachgesetzlichen Ausgestaltung des Grundsatzes nicht durch, die ein differenziertes System der verfolgten Zwecke vorsieht und keine Privilegierung der Speicherung für gemischte Zwecke kennt.

Somit sind für die Speicherung von Informationen in der Informationsordnung regelmäßig die in § 12 Abs. 2 BKAG und den entsprechenden Vorschriften der Landespolizeigesetze geregelten Voraussetzungen der zweckändernden Verarbeitung zu erfüllen.

Nach § 12 Abs. 2 BKAG kann das Bundeskriminalamt zur Erfüllung seiner Aufgaben personenbezogene Daten zu anderen Zwecken, als denjenigen, zu denen sie erhoben worden sind, weiterverarbeiten, wenn mindestens vergleichbar schwerwiegende Straftaten verhütet, aufgedeckt oder verfolgt oder vergleichbar bedeutsame Rechtsgüter geschützt werden sollen und sich im Einzelfall konkrete Ermittlungsansätze zur Verhütung, Aufdeckung oder Verfolgung solcher Straftaten ergeben oder zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.[261]

b. Die Bedeutung des Grundsatzes für die Informationsordnung

Die Gesetzgeber der Polizeigesetze haben den Grundsatz der hypothetischen Datenneuerhebung wie vom Bundesverfassungsgericht formuliert teilweise als Anforderung für die Speicherung von Daten in der kriminalbehördlichen Informationsordnung um-

[259] Siehe oben Teil 1 A. III. 2.

[260] Vgl. zu dem daraus entstehenden Konflikt mit der Logik der Lehre von der Zweckbindung und dem Grundsatz der hypothetischen Datenneuerhebung *Möstl*, Stellungnahme BKAG 2018, S. 6 f.

[261] Zu den Voraussetzungen im Einzelnen *Schulenberg*, in: Barczak, BKAG, 2023, § 12 Rn. 115 ff.

gesetzt. Erstmals geschah dies in § 12 BKAG, der Bedingungen für sämtliche Weiterverarbeitungen[262] von Daten nach ihrer erstmaligen Erhebung im Anwendungsbereich des BKAG enthält.[263] Einige Länder nahmen sich diese Regelung zum Vorbild und trafen vergleichbare Regelungen in ihren Polizeigesetzen.[264] Ähnliche Regelungen finden sich auch in weiteren Sicherheitsgesetzen.[265]

Bei der Reform der Strafprozessordnung wurde die Entscheidung des Bundesverfassungsgerichts zum BKAG – anders als im Zusammenhang mit den Polizeigesetzen – nicht so interpretiert, dass die Voraussetzungen der hypothetischen Datenneuerhebung auf die Speicherung jeglicher Daten in polizeilichen Informationssystemen zu übertragen sind.[266] Würde man hier die Voraussetzungen für die Datenverarbeitung ebenso interpretieren wie im Zusammenhang mit dem BKAG, müssten die Anforderungen an die Speicherung von Daten in Dateien nach § 484 StPO erhöht werden.[267]

So stellt sich insgesamt die Frage, ob der Grundsatz der hypothetischen Datenneuerhebung notwendigerweise auf die Speicherung von Daten in kriminalbehördlichen Informationsressourcen angewendet werden sollte und muss. Unter dem Gesichtspunkt des Sollens ist die Anwendung des Grundsatzes der hypothetischen Datenneuerhebung problematisch, weil dieser unpraktikabel enge Voraussetzungen für informationsordnende Tätigkeiten begründet und nicht ausreichend zwischen informationsordnenden Tätigkeiten und weiteren Formen der Weiterverarbeitung differenziert. Neben der verfassungsrechtlichen Notwendigkeit der Berücksichtigung des Grundsatzes ist schließlich auch die technische Realisierbarkeit seiner Vorgaben zweifelhaft.

Unpraktikabel hohe Anforderungen für das Speichern und Ordnen von Daten begründet die Voraussetzung eines konkreten Ermittlungsansatzes, weil die kriminalbehördliche Informationsordnung zu erheblichen Teilen darauf ausgelegt ist, Informationen vorsorgend zu bevorraten, ohne dass bereits Ansätze für konkrete Ermittlungen

---

[262] Unter diesen weiten Begriff fällt die Speicherung von Daten ebenso wie ihre Auswertung und weitere Nutzungsschritte nach der erstmaligen Erhebung; vgl. BR-Drs. 109/17, S. 104.

[263] Die Geltung von § 12 BKAG als allgemeiner Grundsatz ergibt sich schon aus seiner systematischen Stellung zu Beginn von Abschnitt 2 Unterabschnitt 2 („Weiterverarbeitung von Daten") BKAG. Dies entspricht auch dem Willen des Gesetzgebers; vgl. BT-Drs. 18/11163, S. 92. Für die Weiterverarbeitung von Daten im Informationssystem des BKAG ergibt sich die Geltung von § 12 BKAG auch direkt aus § 16 Abs. 1 BKAG („nach Maßgabe des § 12").

[264] § 15 BWPolG; § 20 HSOG; § 36 SOG MV; § 23 PolG NRW; § 51 POG RP; § 13b SOG LSA.

[265] Vgl. *Löffelmann*, GSZ 2019, 16 f.

[266] Vgl. BR-Drs. 433/18, S. 46.

[267] Vgl. für eine Erhöhung der Voraussetzungen bereits *Zöller*, S. 104 ff.

bestehen.[268] Trotzdem ist § 12 BKAG als einfachgesetzliche Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung auf Grundlage von Wortlaut,[269] Systematik[270] und Begründung[271] des BKAG auf die Speicherung und Ordnung von Daten im neuen Informationssystem anzuwenden, wenngleich §§ 18, 19 BKAG ebenfalls Voraussetzungen für die Speicherung personenbezogener Daten im Informationssystem des Bundeskriminalamts regeln.

Dieses Resultat deutet auch darauf hin, dass der Gesetzgeber des BKAG nicht ausreichend zwischen unterschiedlichen Formen der Weiterverarbeitung von Daten differenziert hat.[272] Der Grundsatz der hypothetischen Datenneuerhebung in unterschiedsloser Anwendung lässt jede weitere Verwendung von personenbezogenen Daten im Rahmen der Informationsordnung als eine Art Echo ihrer ursprünglichen Erhebung erscheinen. Die Umstände der erstmaligen Erhebung sind maßgeblich für jede weitere Verwendung, obwohl diese gänzlich anderen Zwecken dienen kann und die mit der ursprünglichen Erhebung einhergehenden Eingriffe längst abgeschlossen sind.[273] Während es für gezielte Auswertungen von Daten Sinn ergeben mag, diese an dem ursprünglichen Ziel der Erhebung zu messen,[274] ist dies in der Phase der Informationsordnung weniger plausibel, weil die Informationen hier unvollendet sind und einer neuen konkreten Verwendung harren.

Für die beschriebene Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung bestand keine verfassungsrechtliche Notwendigkeit. Der Grundsatz nach der Entscheidung des Bundesverfassungsgerichts zum BKAG ist nicht auf die kriminalbehördliche Informationsordnung im Ganzen anwendbar. Das Gericht formulierte ihn ausdrücklich „für Daten aus eingriffsintensiven Überwachungs- und Ermittlungsmaßnahmen“[275]. Für andere Daten erscheint die Anwendung des Grundsatzes zumindest nicht in der in dem Urteil entwickelten Form zwingend oder geboten.[276] Daher erscheint es in der Gesamtbetrachtung verfehlt, dass die Polizeigesetzgeber den Grundsatz

[268] *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 35.
[269] Vgl. § 16 Abs. 1 BKAG.
[270] Vgl. die Verortung von § 12 BKAG am Beginn des zweiten Unterabschnitt des zweiten Abschnitts des BKAG.
[271] BT-Drs. 18/11163, S. 92 („allgemeiner Grundsatz“).
[272] So auch *Bäcker*, Stellungnahme BKAG 2018, S. 9.
[273] *Rusteberg*, KritV 2017, 24 (32).
[274] Vgl. dazu BVerfG, Beschluss vom 10. November 2020, 1 BvR 3214/15 – Antiterrordateigesetz II, Rn. 97 ff.
[275] BVerfGE 141, 220 (327).
[276] So auch BR-Drs. 109/17 (B), S. 4.

der hypothetischen Datenneuerhebung nach dem Bundesverfassungsgericht zum Herzstück der neuen polizeilichen Informationsordnung insgesamt gemacht haben.[277]

Die Begründung zu § 12 BKAG und der Neuordnung der polizeilichen Informationsordnung, die Einführung dieser Regelung und die technische Umstellung seien unter anderem aufgrund des Urteils des Bundesverfassungsgerichts zum BKAG notwendig geworden, wirkt fadenscheinig. Auffällig ist, dass die Konzeption des neuen „Datenhauses" der Polizei viele Ähnlichkeiten zu der ursprünglichen Konzeption von INPOL-neu aufweist.[278] Angesichts dessen überrascht es nicht, dass im Gesetzgebungsprozess zum BKAG die Vermutung aufkam, die Entscheidung des Bundesverfassungsgerichts sei gar nicht Auslöser der Neuordnung der polizeilichen Informationsordnung gewesen, sondern entsprechende Pläne hätten bereits unabhängig davon bestanden.[279]

Schließlich wirft die technische Realisierbarkeit der Anforderungen aus § 12 BKAG Zweifel auf, die unabhängig davon bestehen, ob das geschilderte System auf einer theoretischen juristischen Ebene saubere Abgrenzungen ermöglicht. Um die Anforderungen einer zweckändernden Nutzung zu prüfen, sind nach § 12 Abs. 5 BKAG organisatorische und technische Vorkehrungen notwendig. Technisch zu konkretisieren sein werden in dem Abrufsystem unter anderem, wann eine Weiterverarbeitung im Sinne von § 12 Abs. 1 BKAG „zur Erfüllung derselben Aufgabe" und „zum Schutz derselben Rechtsgüter oder zur Verfolgung oder Verhütung derselben Straftaten" dient.

Die Anforderungen von § 12 Abs. 5 BKAG sind dazu in den Verpflichtungen zur Kennzeichnung von Daten in § 14 BKAG sowie der Regelung von Zugriffsberechtigungen in § 15 BKAG näher spezifiziert.[280] Eine lückenlose Umsetzung dieser Anforderungen ab Geltung der einschlägigen Regelungen ist dabei vom Gesetzgeber allerdings nicht vorgesehen. Zu treffen sind für eine unbestimmte Übergangszeit lediglich „geeignete Maßnahmen, die ein hohes Maß an Beachtung des Grundsatzes der hypothetischen Neuerhebung gewährleisten"[281].

Besonders die Kennzeichnungspflicht aus § 14 BKAG bringt erhebliche technische und organisatorische Herausforderungen mit sich. § 14 Abs. 1 BKAG erfordert für die Speicherung von Daten umfangreiche Angaben zu Mitteln der Erhebung, der betroffenen Personengruppe, der geschützten Rechtsgüter bzw. verfolgten Straftaten sowie der erhebenden Stelle. Die Regelung verlangt es dabei nicht eindeutig, festzuhalten, ob die

[277] *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 35; *Graulich*, KriPoZ 2017, 278 (279); *Möstl*, Stellungnahme BKAG 2018, S. 5.

[278] Siehe ausführlich zu INPOL-neu oben Teil 1 B. III. 2.

[279] Vgl. DAV, Stellungnahme BKA 2018, S. 9.

[280] BT-Drs. 18/11163, S. 95.

[281] BT-Drs. 18/11163, S. 95.

ursprüngliche Datenerhebung zu präventiven oder zu repressiven Zwecken erfolgte.[282] Die Angabe der Rechtsgrundlage der Erhebung ist nach § 14 Abs. 1 Satz 2 BKAG nicht zwingend („kann"). Eine fehlerhafte oder unvollständige Kennzeichnung begründet im Übrigen aber ein Verbot der Weiterverarbeitung (§ 14 Abs. 2 BKAG). Eine zusätzliche Herausforderung besteht darin, dass die Kennzeichnungspflicht auch eine Bedingung für die rechtmäßige Verarbeitung von „Altdaten" ist, die bereits vor Geltung der Regelung erhoben wurden und nun im Rahmen des neuen Informationssystems weiterverarbeitet werden sollen.[283]

III. Konkrete Regelungsansätze

Im Ergebnis besteht ein weiter Spielraum bei der Regelung der Voraussetzungen für die Speicherung von personenbezogenen Daten in kriminalbehördlichen Systemen. Im Folgenden wird näher untersucht, welche konkreten Regelungsansätze für derartige Befugnisse dazu beitragen könnten, den Ist-Zustand der kriminalbehördlichen Informationsordnung ihrem Soll-Zustand anzunähern. Dafür wird zunächst kurz betrachtet, inwiefern die Eingriffsvoraussetzungen in diesem Bereich von anderen Bereichen abzugrenzen sind (1.), um anschließend eigene Voraussetzungen zu entwickeln (2.). Letzteres geschieht vor allem mit Blick auf den Zweck der Vorbereitung künftiger Strafverfolgung.

1. Abgrenzung von Eingriffsvoraussetzungen aus anderen Bereichen

Für die Speicherung von Daten in kriminalbehördlichen Systemen erweisen sich weder die Anlasskategorien von Gefahr und Verdacht aus dem Polizei- und Strafprozessrecht (a.) noch die Vorsorgekategorien des Risikoverwaltungsrechts (b.) als geeignet.

a. Gefahr und Verdacht

Die Anlasskategorien von Gefahr und Verdacht sind für die Speicherung von Daten deswegen nicht geeignet, weil die Speicherung weitestgehend dem Bereich der Vorsorge zuzuordnen ist und außerhalb konkreter Verfahren stattfindet.[284] Durch Vorbereitungshandlungen im Rahmen der Informationsordnung sollen erst die Bedingungen geschaffen werden, um in Zukunft Gefahren abwehren oder Straftaten verfolgen zu

[282] Vgl. *Möstl*, Stellungnahme BKAG 2018, S. 7. Die Vorgabe in § 14 Abs. 1 Satz 1 Nr. 3 BKAG, die „Rechtsgüter, deren Schutz die Erhebung dient oder Straftaten, deren Verfolgung oder Verhütung die Erhebung dient" anzugeben, ist bei doppelfunktionalen Erhebungen nicht eindeutig.

[283] Vgl. BT-Drs. 18/11163, S. 95.

[284] Vgl. BVerfGE 110, 33 (55); BVerfGE 113, 348 (377 f.); *Möstl*, DVBl. 2010, 808 (810); *Schulze-Fielitz*, in: FS Schmitt Glaeser, S. 407 (413); siehe auch schon oben Teil 1 B. II.

können. Während die Gefahr bei der Ermittlung akut relevanter Sachverhalte als Anlassschwelle operabel ist, löst sich das Informationsordnungsrecht von dieser Situationsgebundenheit. Der Anfangsverdacht ist schon deshalb als Anlasskategorie ungeeignet, weil es bei der Speicherung von Daten in kriminalbehördlichen Systemen in der Regel nicht um die retrospektive Bewältigung sozialer Konflikte geht, sondern darum, Vorkehrungen hierfür zu treffen. Gemeinsam mit strafprozessualen Maßnahmen, die einen Tatverdacht erfordern, hat es die Speicherung von Daten zu Vorsorgezwecken, dass auch sie zumindest das Fernziel hat, zur Verwirklichung materiellen Strafrechts zu dienen.[285]

Dass es nicht sachgerecht und notwendig ist, informationsordnende Befugnisse an den Kategorien von Gefahr und Verdacht auszurichten, ergibt sich zudem aus dem Eingriff in das Recht auf informationelle Selbstbestimmung, den diese rechtfertigen sollen.[286] Kennzeichnend für das Datenschutzrecht insgesamt und das Recht auf informationelle Selbstbestimmung ist, dass es einen Vorfeldschutz entfaltet.[287] Mit dem Bundesverfassungsgericht „flankiert und erweitert [es] den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit, indem es ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen lässt."[288] Eine Gefährdung des informationellen Selbstbestimmungsrechts könne „bereits im Vorfeld konkreter Bedrohungen benennbarer Rechtsgüter entstehen, insbesondere wenn personenbezogene Informationen in einer Art und Weise genutzt und verknüpft werden können, die der Betroffene weder überschauen noch verhindern kann."[289] Aus der Formulierung des Bundesverfassungsgerichts wird deutlich, dass das Datenschutzrecht nicht stets, wenn es zur Anwendung kommt, die Funktion eines Vorfeldschutzes erfüllt. Im Bereich der Informationsordnung dürfte der Vorfeldschutz aber die primär maßgebliche Funktion sein. Dies korrespondiert mit dem unvollendeten Charakter von Informationen im Stadium der Informationsordnung.[290]

Dass für die Speicherung von Informationen in Datenbanken der Vorfeldschutz greift, wirkt sich auf die Anforderungen zur Rechtfertigung des Eingriffs aus.[291] Zwar wird der Betroffene bei einer Speicherung von Informationen in einer großen Informationsressource nicht etwa „faktisch anonym", weil er in der Informationsmasse untergeht. Eine Speicherung von personenbezogenen Daten in großer Menge mindert deren

[285] Vgl. *Gärditz*, S. 52 ff.; allgemein zur dienenden Funktion des Verfahrens *Ossenbühl*, NVwZ 1982, 465 f.
[286] *Möstl*, DVBl. 2007, 581 (585).
[287] *Bull*, NJW 2006, 1617 (1623); *von Lewinski*, S. 78 ff.; siehe auch schon oben Teil 1 C. III. 1. a.
[288] BVerfGE 120, 274 (312).
[289] BVerfGE 120, 274 (312).
[290] Siehe dazu oben Teil 1 A. I. 1.
[291] Vgl. *Möstl*, DVBl. 2007, 581 (585).

Eingriffsintensität nicht,[292] sondern erhöht sie aufgrund der daraus folgenden Kombinationsmöglichkeiten eher. Moderne technische Hilfsmittel ermöglichen es, Individuen auch aus großen Datenbeständen heraus verlässlich zu identifizieren und nachzuverfolgen. Auch die Risiken der Stigmatisierung und Kriminalisierung von Betroffenen nehmen bei großen verknüpfbaren Datenbeständen tendenziell zu.[293] Dennoch lässt sich aus dem Gedanken des Vorfeldschutzes spiegelbildlich folgern, dass die Speicherung von Informationen, die für die Betroffenen nicht spürbar ist, weniger konkret umrissenen Zwecken und Interessen dienen muss als die spätere Verwendung in einem konkreten Kontext, die für den Betroffenen spürbar wird.[294]

Dies darf aber nicht zur Folge haben, dass Datenspeicherungen unter niedrigen Voraussetzungen Tür und Tor für eingriffsintensive Auswertungen auf dieser Basis öffnen. Die Konsequenz möglicherweise folgenreicher Eingriffe nach der Speicherung der Informationen ist bereits bei dieser mitzudenken und das Kompensationsverhältnis der Voraussetzungen für Datenspeicherung und Datenauswertung zu beachten.[295] Zudem ist in der kriminalbehördlichen Informationsordnung zu berücksichtigen, dass noch eine Anbindung an das (Fern-)Ziel der Verwendung von Informationen in Strafverfahren oder zur Gefahrenabwehr besteht. Zumindest insofern kann eine gewisse Orientierung der Anlässe des Eingriffs an die Kategorien von Tatverdacht und Gefahr Sinn ergeben.[296]

b. Vorsorgekategorien des Risikoverwaltungsrechts

Die Nähe des modernen Polizei- und Sicherheitsrechts zum Risikoverwaltungsrecht und besonders zum Technikrecht wird immer wieder betont und zumindest ansatzweise untersucht.[297] Vorsorgekategorien aus dem Risikoverwaltungsrecht lassen sich zur Bestimmung der Anlässe im Informationsordnungsrecht allerdings nur eingeschränkt heranziehen.

Das Informationsordnungsrecht lässt sich von zwei Seiten des Risikorechts betrachten. Erstens soll es den Risiken begegnen, die durch den Betrieb von kriminalbehördlichen Informationssystemen und Datenbanken für Bürger*innen entstehen. Zweitens

---

[292] So aber *Ladeur*, DÖV 2009, 45 (53) sowie die abweichende Meinung der Richterin Haas zum Beschluss des Ersten Senats vom 4. April 2006 – 1 BvR 518/02, BVerfGE 115, 320 (373 f.).

[293] Siehe oben Teil 2 B. II.

[294] Ähnlich *Horn*, in: FS Schmitt Glaeser, S. 435 (460).

[295] Siehe oben Teil 1 A. II.

[296] Vgl. *Park*, S. 219.

[297] Vgl. zu der Nähe des Sicherheitsrechts zum Risikoverwaltungsrecht insgesamt nur *Darnstädt*, S. 121 ff., 205 ff.; *S. Meyer*, JZ 2017, 429 ff.; *Möstl*, S. 199 ff.; *Park*, S. 208 ff. sowie *Pitschas*, DÖV 2002, 221 (224), der eine Umorientierung der bestehenden Regelungen des Polizeirechts „von der Gefahrenabwehr zur kriminalpräventiven Risikovorsorge" feststellt.

soll eben dieser Betrieb von Informationsressourcen Risiken begegnen, die von anderer Seite ausgehen. Meistens geht es hierbei um die Disposition von Individuen, sich gefährlich oder riskant zu verhalten. Die Befugnisse zur Informationsordnung haben damit eine doppelte Ausrichtung zur Vorsorge. Beide Vorsorgegedanken sind Grund dafür, die Anlässe zur Speicherung von Informationen zu begrenzen.

Der erste Vorsorgegedanke, der auf die Risiken der Informationsressourcen bezogen ist, kommt in der datenschutzrechtlichen Prägung der informationsordnenden Befugnisse zum Ausdruck. Das Datenschutzrecht ist ein besonderer Teil des Risikoverwaltungsrechts mit ausdifferenzierten Regelungen zur Einhegung der Risiken der elektronischen Datenverarbeitung für Persönlichkeitsrechte.[298] Es ist insofern nicht notwendig, den Betrieb von kriminalbehördlichen Informationssystemen und Datenbanken mit jenem von Atomkraftwerken oder umweltschädlicher Anlagen zu vergleichen,[299] da für die ihm eigenen schwer beherrschbaren Risiken bereits ein risikoverwaltungsrechtliches Instrumentarium bereitsteht. Es lässt sich gleichwohl kritisieren, dass sich die Risiken im Bereich der kriminalbehördlichen Informationsordnung durch die traditionellen datenschutzrechtlichen Konzepte, auf denen die geltenden Regelungen beruhen, nur unbefriedigend bewältigen lassen.

Der zweite, eingriffsseitige Vorsorgegedanke bezieht sich auf Risiken, die von den Informationssubjekten ausgehen, die zum Gegenstand der Informationsordnung gemacht werden. Hier lässt sich die Disposition eines Individuums, beispielsweise einen terroristischen Anschlag zu verüben, als schwer kalkulierbares Risiko betrachten.[300] Auf dieser Grundlage erscheint es aber nicht sachgerecht, etwa die technikrechtliche Anlassschwelle des Besorgnispotentials[301] auf die Speicherung von personenbezogenen Daten zu übertragen.[302]

Erstens ließe sich ein solches grundlegendes Besorgnispotential für beliebige Menschen annehmen, die in der Lage sind, mit gewissen Hilfsmitteln schwere Schäden zu verursachen. Dies wäre praktisch jeder Mensch im Vollbesitz seiner körperlichen Kräfte. Anders als einer Technologie erscheint es verfassungsrechtlich nicht statthaft, Menschen rechtlich ein „Basisrisiko“[303] zuzuschreiben. Die inneren und äußeren Faktoren, die dazu führen, dass Menschen Terroranschläge oder andere Straftaten bege-

[298] Siehe oben Teil 1 C. III. 1. c.

[299] Vgl. zu dem Gedanken, den „Betrieb von Anlagen zur elektronischen Verarbeitung personenbezogener Daten einem Genehmigungsverfahren nach Vorbild entsprechender Regelungen im BImschG“ zu unterwerfen *Scholz/Pitschas*, S. 63.

[300] Vgl. *S. Meyer*, JZ 2017, 429 (434).

[301] Vgl. BVerwG NVwZ 1986, 208 (212) (zum Vorsorgebegriff im AtomG).

[302] In diese Richtung allerdings *S. Meyer*, JZ 2017, 429 (434 ff.).

[303] Vgl. im Zusammenhang mit gentechnisch veränderten Organismen BVerfGE 128, 1 (39).

hen, mögen in einem gewissen Maße sozialwissenschaftlicher und psychologischer Ergründung zugänglich sein. Die hierbei verbleibenden Unsicherheiten lassen sich aber nicht mit den naturwissenschaftlichen Unsicherheiten vergleichen, die etwa beim Betrieb eines Kernkraftwerks bestehen.

Zweitens hat die Übertragung von Anlassschwellen aus dem technischen Risikoverwaltungsrecht den Makel, dass sie die Risiken für die Informationssubjekte nicht ausreichend berücksichtigt. Zwar bringen auch aufgrund eines Besorgnispotentials im technischen Sicherheitsrecht getroffene Maßnahmen Eingriffe in Grundrechte (wie die Eigentums- oder Berufsfreiheit) mit sich, allerdings sind sie in ihrer individuellen Intensität nicht mit jenen Eingriffen vergleichbar, die durch die Speicherung in kriminalbehördlichen Datenbanken erfolgen.[304] Die Anwendung einer Anlassschwelle aus dem technischen Risikoverwaltungsrecht wäre konsequenterweise nur dann möglich, wenn sie gemeinsam mit einem Schutz von Persönlichkeitsrechten verankert würde. In den aktuellen Regelungen des Informationsordnungsrechts tritt diese doppelte Implikation der Anlassschwelle nicht klar hervor. Das zentrale Kriterium der Erforderlichkeit einer Datenverarbeitung zur Erfüllung bestimmter Aufgaben wurde vor allem zum Schutz von Persönlichkeitsrechten gesetzlich geregelt. Es knüpft zwar an die Erfüllung kriminalbehördlicher Aufgaben an, erfordert aber auch eine Abwägung unter Berücksichtigung der Interessen des betroffenen Informationssubjekts.

Schließlich dient die kriminalbehördliche Informationsordnung einer Reihe von Zwecken, die nicht mit der Bewältigung von Großrisiken im Umwelt- und Technikrecht vergleichbar sind. Während der Vergleich der*des potentiellen Terrorist*in mit einem Kernreaktor zumindest hinsichtlich der drohenden Schäden noch passen mag, finden sich in polizeilichen Informationsressourcen auch Daten zur künftigen Verfolgung von Fahrraddieb*innen oder gelegentlichen Konsument*innen verbotener Betäubungsmittel. Allenfalls für die gezielte Vorsorge der Abwehr von Gefährdungen hochrangiger Rechtsgüter oder Verfolgung schwerwiegender Straftaten ließe sich eine Schwelle wie jene des Besorgnispotentials komplementär zur einer persönlichkeitsschützenden Einhegung einsetzen.

Im Ergebnis sind für das von einer doppelten Vorsorgedimension geprägte Informationsordnungsrecht eigenständige Anlassschwellen zu entwickeln. Auch wenn sich die Vorsorge bis zu einem gewissen Grad als allgemeines Rechtsprinzip begreifen lässt, ist die Bestimmung eines konkreten Vorsorgeanlasses ohnehin von dem konkret betrachteten Bereich abhängig.[305] Damit ist allerdings nicht jeder Übernahme von Gedanken aus dem technischen Risikoverwaltungsrechts für das Informationsrecht als As-

[304] Ähnlich *Papier*, DVBl. 2010, 801 (805); anders *S. Meyer*, JZ 2017, 429 (435).
[305] Vgl. *Albers*, Determination, S. 123; *Ossenbühl*, NVwZ 1986, 161 (164).

pekt des technisierten Sicherheitsrechts eine Absage zu erteilen. Besonders eine verstärkte Bezugnahme auf verobjektivierte wissenschaftliche und statistische Erkenntnisse erscheint diskutabel.

2. Voraussetzungen für die Speicherung von Daten für die Strafverfolgungsvorsorge

Wie sich Befugnisse zur Vornahme informationsordnender Handlungen sinnvoll eingrenzen lassen, um sie besser anwendbar zu machen und die Risiken für die Informationssubjekte abzumildern, wird im Folgenden untersucht. Dabei konzentriert sich die Betrachtung auf die Voraussetzungen für eine Speicherung von Daten zu Zwecken der Vorbereitung der Strafverfolgung. Wie die Elemente der Zweckfestlegung (a.) und Zweckdienlichkeit (b.) der Datenverarbeitung gesetzlich konkreter festgelegt werden könnten, wird anhand dieses Aspektes näher beleuchtet. Aus den gewonnenen Erkenntnissen wird der Wortlaut einer möglichen Befugnis zur Speicherung von Daten zur Vorbereitung der Strafverfolgung formuliert (c.).

a. Zweckfestlegung

Eine Befugnis für die Speicherung von Daten allgemein „für Zwecke künftiger Strafverfahren" – so die Formulierung von § 484 Abs. 1 StPO – vorzusehen, erscheint problematisch weit.[306] Durch eine genauere Differenzierung der Zwecke von Datenspeicherungen ließen sich die Weichen für eine genauere Festlegung ihrer Voraussetzungen stellen.

Bezüglich der von einer Speicherung betroffenen Personen lässt sich grundsätzlich unterscheiden zwischen Personen, gegen die in Zukunft Strafverfahren erwartet werden und anderen Personen, deren Daten in Strafverfahren gegen Dritte relevant werden können.

Diese Differenzierung ist in §§ 18, 19 BKAG angelegt, welche zwischen der Weiterverarbeitung von Daten zu Verurteilten, Beschuldigten, Tatverdächtigen und sonstigen Anlasspersonen (§ 18 BKAG) sowie anderen Personen (§ 19 BKAG) unterscheiden.[307] Die Speicherung von personenbezogenen Daten für künftige Strafverfahren bedarf in erhöhtem Maße einer Begründung, wenn die Verfahren nicht gegen die betroffene Person erwartet werden. Für Personen, die nicht durch ein eigenes Verhalten Anlass zu der Prognose gegeben haben, dass von ihnen Schädigungen ausgehen könn-

[306] Siehe oben II. 2.
[307] Siehe bereits oben Teil 2 A. III. 1. a. aa).

ten, ist der Eingriff in ihre Rechte durch die Speicherung ihrer Daten in kriminalbehördlichen Ressourcen als besonders intensiv zu werden.[308] Es erscheint daher konsequent, ihn wie in § 19 Abs. 1 Satz 3 BKAG grundsätzlich von einer Einwilligung der Betroffenen abhängig zu machen und nicht auf Grundlage einer gesetzlichen Befugnis zuzulassen. Dies betrifft insbesondere die möglichen Opfer und Zeug*innen künftiger Taten. Anders verhält es sich im Zusammenhang mit Personen, gegen die selbst keine Strafverfahren erwartet werden, die aber in Kontakt zu Dritten stehen, bei denen dies der Fall ist.

Auch im Übrigen lässt sich der Zweck (der Vorbereitung) künftiger Strafverfahren spezifizieren. Gespeicherte Daten können dazu dienen, einen Überblick über bestimmte Kriminalitätsphänomene zu gewinnen, das ermittlungstaktische Vorgehen der Kriminalbehörden vorzubereiten oder Maßnahmen zum eigenen Schutz zu treffen.[309] Sie können aber auch dazu dienen, um unbekannte Tatverdächtige zu identifizieren oder neue Verdachtsmomente zu generieren.[310] Dabei sind die Betroffenen etwa durch das Generieren von Verdachtsmomenten deutlich größeren Risiken ausgesetzt als durch das Festhalten allgemeiner Erkenntnisse zur Kriminalitätsbekämpfung. Diese Risiken können auch dadurch eingegrenzt werden, dass strengere Anforderungen für den nachfolgenden Verarbeitungsschritt der Auswertung der Daten aufgestellt werden.

b. Zweckdienlichkeit

Wie bereits erörtert,[311] setzt sich eine für die Entscheidung über die Speicherung von Daten durchzuführende Prognose aus einer Tatsachengrundlage (aa)) und einer hierauf beruhenden einzelfallbezogenen Einschätzung (bb)) zusammen. Diese Aspekte ließen sich in der gesetzlichen Regelung konkretisieren.

aa) Tatsächliche Grundlagen (Prognosebasis)

Dass es einer Tatsachengrundlage für die Annahme bedarf, dass eine Speicherung von Daten für die Durchführung künftiger Strafverfahren nützlich sein kann, ist zumindest im Rahmen von § 484 Abs. 2 StPO anerkannt.[312] Ausdrücklich erwähnt wird diese Voraussetzung im Gesetzestext allerdings nicht. Im Rahmen von § 484 Abs. 1 StPO, der Befugnis zur Speicherung gewisser Basisdaten über einen bestimmten Beschuldigten

[308] Vgl. zur Veranlassung der Datenverarbeitung durch den Betroffenen als Kriterium der Eingriffsintensität BVerfGE 115, 320 (347); BVerfGE 100, 313 (376); BVerfGE 107, 299 (318 ff.).

[309] Vgl. Runderlass des Innenministeriums NRW zur Führung von Kriminalakten vom 21. Februar 2002 – 42.2 – 6422, MBl. NRW.2002 S. 324.

[310] Vgl. *Arzt*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 1217.

[311] Siehe oben II. 2.

[312] *Soiné*, StPO, 142. EL 2023, § 484 Rn. 8.

für künftige Strafprozesse, wird das Vorliegen einer Tatsachengrundlage nicht in der gleichen Form gefordert wie bei Abs. 2 der Vorschrift.[313] Allerdings ergibt sich eine entsprechende Voraussetzung daraus, dass nur Daten zu einer Person gespeichert werden dürfen, die Beschuldigter in einem Strafverfahren ist. In diesem Verfahren musste eine Tatsachengrundlage zumindest für die Annahme eines Tatverdachts bestehen. Auf dieser Grundlage sind jedoch keine weitreichenden Schlüsse über die Nützlichkeit der Daten in möglichen künftigen Strafverfahren möglich.

Die Voraussetzung einer Tatsachengrundlage sollte in informationsordnenden Befugnissen jedenfalls zur Klarstellung grundsätzlich gesetzlich festgehalten werden. Hierfür könnte sich der Gesetzgeber am Wortlaut mehrerer Polizeigesetze orientieren. Diese verwenden hierfür Begriffe wie „Anhaltspunkte“[314] oder „tatsächliche Anhaltspunkte“[315]. Auch wenn dies dem Wortlaut nach auf unterschiedliche Bedeutungsgehalte und damit unterschiedliche materielle Voraussetzungen hindeutet,[316] ergibt sich aus der Systematik und der Regelungshistorie der Polizeigesetze kein Hinweis darauf, dass die Gesetzgeber unterschiedliche Eingriffsschwellen vorsehen wollten.[317] Insgesamt wäre es im Sinne der Rechtsklarheit wünschenswert, wenn sämtliche informationsordnende Befugnisse in einer einheitlichen Terminologie ausdrücklich das Vorliegen von tatsächlichen Anhaltspunkten für die Datenspeicherung fordern würden.

bb) Einzelfallbezogene Einschätzung

Auf der Tatsachengrundlage hat die Kriminalbehörde eine einzelfallbezogene Einschätzung zu treffen, ob und inwiefern die Speicherung der betroffenen Daten für künftige Strafverfahren nützlich ist. Aus dem Wortlaut von § 484 Abs. 1 StPO geht diese Anforderung nicht ausdrücklich hervor, wird aber in die Regelung hineingelesen.[318] In Abs. 2 der Vorschrift ergibt sie sich aus dem Merkmal „erforderlich“.

Eine pauschale Annahme, dass bestimmte Arten von Daten grundsätzlich für die Vorbereitung der Strafverfolgung erforderlich seien, reicht zur Begründung nicht aus.[319] In diese Richtung geht aber die Formulierung in § 484 Abs. 1 StPO, welcher unter anderem die Verarbeitung der Personendaten des Beschuldigten und der Daten

[313] Vgl. *Ritscher/Klinge*, in: SSW-StPO, 5. Aufl. 2023, § 484 Rn. 5.

[314] § 23 Abs. 2 Satz 1 Nr. 2 PolG NRW.

[315] § 75 Abs. 3 BWPolG.

[316] Vgl. mit einer differenzierten Auseinandersetzung mit verschiedenen Schwellen *Albers*, Determination, S. 286 f.

[317] Vgl. *Kral*, S.120; *Rachor/Graulich*, in: Lisken/Denninger, 6. Aufl. 2018, Kap. E Rn. 141.

[318] *Wittig*, in: BeckOK-StPO, 47. Ed. 2023, § 484 Rn. 1; *Weßlau/Deiters*, in: SK-StPO, 5. Aufl. 2020, § 484 Rn. 10.

[319] Vgl. aber für den präventiven Bereich im Zusammenhang mit dem ME PolG 1986 *Riegel*, DVBl. 1987, 325 (329).

über die ihm vorgeworfenen Straftaten zulässt, ohne dafür ausdrücklich zu verlangen, dass dies für künftige Strafverfahren erforderlich sein muss. Dies lässt sich als eine Art „Nützlichkeitsvermutung“[320] bzgl. der aufgezählten Daten verstehen, die aber entkräftet werden kann. Solange die Zwecke der Speicherung nicht näher beschrieben sind als mit den Zwecken künftiger Strafverfahren, ist dieses Regelungskonstrukt mit Blick auf die vielen Verwendungsmöglichkeiten der Daten allerdings problematisch. Die Annahme, dass eine Speicherung von Daten im Zweifelsfall als erforderlich anzusehen sei, wenn eine Prognose nicht zu einem eindeutigen Ergebnis gelangt, erscheint prinzipiell als unzulässig.[321]

Die Einschätzung erfordert die Anwendung einer Prognosemethode.[322] Die Methode liefert die Begründung dafür, weshalb aus bereits vorliegenden Tatsachen eine Wahrscheinlichkeit für den Eintritt künftiger Ereignisse gefolgert wird.[323] Prinzipiell ist die Erforderlichkeit einer Datenspeicherung vollständig gerichtlich überprüfbar. Die Rechtsprechung will allerdings das Wahrscheinlichkeitsurteil der Anwender*innen darüber, ob eine Person in Zukunft einer Straftat verdächtigt werden könnte, im Sinne eines Prognosespielraums von der Überprüfbarkeit ausnehmen.[324] Zwar handelt es sich bei den entsprechenden gesetzlichen Voraussetzungen der Erforderlichkeit und Notwendigkeit um unbestimmte Rechtsbegriffe, für diese ist aber kein Beurteilungsspielraum der speichernden Stelle anzunehmen. Ein solcher ist weder vom Wortlaut der Befugnisse noch von deren Begründungen intendiert. Es dürfte nicht in jedem Fall praktisch möglich sein, die Gründe für eine Datenspeicherung lückenlos nachzuvollziehen. Gerade auf eine einzelne Person bezogene Entscheidungen, in die Erfahrungswissen der Anwender*innen einfließt, haben auch ein intuitives Element.[325] Bei den Prognosen über das künftige strafrechtlich relevante Verhalten einer Person bestehen allerdings keine Wissensprobleme, die etwa mit solchen im Bereich des technischen Risikorechts vergleichbar sind.[326] Daher sprechen die besseren Gründe für eine grundsätzlich volle rechtliche Überprüfbarkeit der für die Datenspeicherungen zur Vorbereitung der Strafverfolgung durchzuführenden Prognosen.

---

[320] So *Bäcker*, Kriminalpräventionsrecht, S. 508 f. zu § 8 Abs. 1 BKAG aF.

[321] Vgl. zu einer entsprechenden polizeilichen Praxis *Wellbrock*, CR 1986, 149 (157); *Rachor*, S. 97 ff.

[322] Zu der Prognosemethode als Bestandteil der Prognose *Schwabenbauer/Kling*, VerwArch 2010, 231 (233).

[323] *Schwabenbauer/Kling*, VerwArch 2010, 231 (233).

[324] OVG Bautzen BeckRS 2015, 51246; VGH Mannheim BeckRS 2016, 45327; VG Mainz BeckRS 2018, 37558 (jeweils zu § 81b Abs. 1 Var. 2 StPO); VGH Mannheim ZD 2015, 542 (543); VG Karlsruhe BeckRS 2019, 5082 Rn. 27 f. (jeweils zu § 38 Abs. 3 BWPolG aF).

[325] *Schwabenbauer/Kling*, VerwArch 2010, 231 (242 f.).

[326] Vgl. *Bäcker*, Kriminalpräventionsrecht, S. 203 f.

Im Fall der Vorsorge für die Strafverfolgung gegen die von der Datenspeicherung betroffene Person ist vor allem eine Prognose darüber vorzunehmen, ob das Informationssubjekt in Zukunft als Verdächtiger einer Straftat in Betracht kommen wird.[327] Dabei ist zu beachten, dass die Annahme, eine Person werde in Zukunft als Straftäter*in in Erscheinung treten, besondere Risiken für die Betroffenen mit sich bringt. Sie kann dazu führen, dass Personen immer wieder in das Visier der Strafverfolgung geraten und Ziel von Ermittlungsmaßnahmen werden.[328] Eine Prognose, die zu einem entsprechenden Ergebnis kommt, bedeutet für die Betroffenen daher einen schwerwiegenden Eingriff. In der Praxis zeigt sich, dass eine derartige Einschätzung von Personen mitunter schwer nachvollziehbar sein kann und nicht immer gut begründet ist. So berichtete ein*e interviewte*r Mitarbeiter*in der Datenschutzaufsicht:

> „Es war das Ergebnis vieler Prüfungen [...], dass die Wiederholungsgefahr nirgends dokumentiert wurde. Es gab ein Menü in diesem elektronischen System mit kurzen Vorschlägen, mit Schlagworten, zur Wiederholungsgefahr, und oft wurde die Prüfung nur so pro forma gemacht. Es gibt einen Fall, der mir noch in Erinnerung ist. Ein junger Mann hatte irgendwo angegeben, er habe sexuelle Kontakte mit einer Dreizehnjährigen gehabt. Das führte dazu, dass man bei ihm eine Hausdurchsuchung gemacht hat. Man hat den Computer beschlagnahmt. Es stellte sich dann heraus, dass da überhaupt nichts dran war. Die Staatsanwaltschaft hat das eingestellt und dann wurde als Wiederholungsgefahr angegeben ‚Sexualstraftäter'." (DSA1)

Die Rechtsprechung nimmt die Prognose über die zukünftige Relevanz von Daten, die aus der Strafverfolgung stammen, derart vor, dass sie auf Grundlage eines „Restverdachts" eine „Wiederholungsgefahr" prüft. Der Begriff des Restverdachts bezieht sich darauf, dass der Verdacht der Begehung einer Straftat gegen einen Beschuldigten in einem Strafverfahren nicht ausgeräumt wurde.[329] Auch wenn ein Strafverfahren nicht mit einer Verurteilung endete, kann weiterhin eine Tatsachengrundlage bestehen, nach der anzunehmen ist, dass das Informationssubjekt sich der ihm vorgeworfenen Straftat

[327] Vgl. VGH Mannheim NJW 1987, 2762; VGH Mannheim NVwZ-RR 2000, 287; *Bäcker*, Kriminalpräventionsrecht, S. 511 f.; *Gaede*, in: FS Merkel, S. 1283 (1288 f.).

[328] *Arzt*, in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 1217.

[329] Der Begriff Verdacht ist in diesem Zusammenhang nicht ganz passend, da der „Restverdacht" die ursprüngliche Funktion des strafprozessualen Tatverdachts als Verurteilungsprognose nicht mehr erfüllen kann; vgl. *Stuckenberg*, in: FG Hilger, S. 25 (35).

schuldig gemacht hat.[330] Das Informationssubjekt muss dafür aufgrund der vorliegenden Beweismittel noch ernsthaft als Täter*in in Betracht kommen. Die nur theoretische Möglichkeit seiner Schuld ist nicht ausreichend.[331]

Das Bundesverfassungsgericht[332] und die Verwaltungsgerichte[333] sehen es dabei als mit der Unschuldsvermutung vereinbar an, den in einem früheren Verfahren festgestellten Tatverdacht zur Grundlage der Prognose zu machen, auch wenn das Verfahren eingestellt wurde oder ein Freispruch ergangen ist. Es bedürfe in diesem Fall aber einer „Überprüfung, ob noch Verdachtsmomente gegen den Betroffenen bestehen, die eine Fortdauer der Speicherung" rechtfertigen.[334] Während dies im Zusammenhang mit der Verfahrenseinstellung nachvollziehbar erscheint, ist es mit Art. 6 Abs. 2 EMRK unvereinbar, den „Restverdacht" nach Freispruch zur Grundlage einer Prognose strafbaren Verhaltens zu machen.[335]

Für sich genommen wäre ein „Restverdacht" nur ausreichend, um eine Speicherung der Daten für Zwecke des Verfahrens zu rechtfertigen, das sich auf den konkreten Vorwurf bezieht. Der (Rest-)Verdacht einer einzelnen Straftat kann nicht die allgemeine Annahme begründen, eine Person werde auch künftig strafrechtlich in Erscheinung treten. Sogar wenn feststeht, dass eine Person in der Vergangenheit eine Straftat begangen hat, kann daraus nicht ohne eine Einzelfallbewertung geschlossen werden, dass die gleiche Person wahrscheinlich wieder in den Verdacht einer entsprechenden Tat geraten wird. Vor diesem Hintergrund ist § 75 Abs. 3 Satz 1 BWPolG problematisch, der die Speicherung von personenbezogenen Daten zur Vorbereitung der Gefahrenabwehr[336] für eine Dauer von bis zu zwei Jahren für erforderlich erklärt, wenn der Verdacht einer Straftat besteht. Die Regelung ist unverhältnismäßig und verfassungswidrig, da der Verdacht einer in der Vergangenheit liegenden beliebigen Straftat ungeeignet ist, die Erforderlichkeit einer Speicherung von personenbezogenen Daten zu präventiven Zwecken zu rechtfertigen.[337] Aufgrund seines eindeutigen Wortlauts lässt sich § 75 Abs. 3 Satz 1 BWPolG auch nicht verfassungskonform auslegen.

---

[330] Vgl. OVG Saarlouis ZD 2018, 233 (234); VGH Kassel BeckRS 2017, 103690; VGH München BeckRS 2015, 43079.

[331] OVG Greifswald BeckRS 2016, 42877; OVG Lüneburg BeckRS 2014, 58848.

[332] BVerfG NJW 2002, 3231 f.; vgl. auch BVerfG BeckRS 2009, 35816.

[333] BVerwG DÖV 1973, 752 f.; VGH München BeckRS 2013, 52269; OVG Saarlouis BeckRS 2012, 58861.

[334] BVerfG NJW 2002, 3231 (3232) (bezogen auf den präventiven Bereich der Verbrechensbekämpfung).

[335] Dazu im Einzelnen oben Teil 2 A. III 1. b) bb).

[336] In der problematischen Terminologie der vorbeugenden Bekämpfung von Straftaten.

[337] Mit Bedenken auch *Kahlert/Sander*, in: Belz/Mussmann/Kahlert/Sander, BWPolG, 8. Aufl. 2015, § 38 Rn. 16; anders VG Freiburg BeckRS 2018, 19277 (jeweils zu § 38 Abs. 2 Satz 1 BWPolG aF).

Eine ähnliche Problematik besteht im Zusammenhang mit § 18 Abs. 1 BKAG. Nach dessen Nr. 1 und Nr. 2 kann das Bundeskriminalamt zur Erfüllung seiner Aufgaben Daten von Verurteilten und Beschuldigten grundsätzlich ohne weitere Voraussetzungen weiterverarbeiten. Bei Tatverdächtigen (Nr. 3) fordert die Vorschrift hingegen, dass 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. Bei sonstigen Anlasspersonen (Nr. 4) ist notwendig, dass tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden. Der Umstand, dass eine Person verurteilt oder angeklagt wurde, macht die Speicherung ihrer Daten aber nicht zwangsläufig über das jeweilige Verfahren hinaus erforderlich. Auch hier muss in die Befugnis zumindest als zusätzliche Voraussetzung hineingelesen werden, dass die Speicherung für die Erfüllung der Aufgaben des Bundeskriminalamts erforderlich ist. Aus Gründen der Rechtsklarheit vorzugswürdig wäre es, in § 18 Abs. 1 Nr. 1 und Nr. 2 BKAG ähnlich wie in Nr. 3 der Vorschrift die Voraussetzung zu verankern, dass eine Einschätzung vorliegt, die jeweilige Person werde erneut in einer für Gefahrenabwehr oder Strafverfolgung relevanten Weise in Erscheinung treten.

Im Ergebnis können sowohl der „Restverdacht" als auch eine in der Vergangenheit liegende Verurteilung Grundlage einer Prognose über die künftige Begehung von Straftaten sein, die anhand des Einzelfalles erfolgen und relevante Umstände umfassend berücksichtigen muss.[338] Diese Art von Prüfung nimmt die Rechtsprechung unter dem Begriff der „Wiederholungsgefahr" vor.[339] Der Begriff der Wiederholung ist in diesem Zusammenhang unglücklich, weil es suggeriert, das Informationssubjekt könne eine Straftat wiederholen, die ihm trotz eines Restverdachts gerade nicht nachgewiesen ist.[340] Auch der Begriff der Gefahr ist irreführend, da die Anforderungen an das Wahrscheinlichkeitsurteil nicht jenen des polizeirechtlichen Gefahrenbegriffs gleichen. Sinnvoller erscheint es daher, statt von einer Wiederholungsgefahr von Anhaltspunkten für die künftige Begehung von Straftaten zu sprechen.

Diese Anhaltspunkte sind aus einer Gesamtschau von Umständen betreffend der dem Informationssubjekt ursprünglich vorgeworfenen Tat (auf die sich der Restverdacht bezieht), betreffend anderer ihm vorgeworfener Taten und betreffend der Biographie und Persönlichkeit des Informationssubjekts zu ermitteln. Hinsichtlich nicht ausgeräumter (oder sogar durch eine Verurteilung bestätigter) Tatvorwürfe sind Art,

[338] So auch BVerfG BeckRS 2009, 35816.

[339] Vgl. nur OVG Saarlouis BeckRS 2012, 58861; OVG Greifswald BeckRS 2016, 42877; OVG Lüneburg BeckRS 2014, 58848; OVG Münster BeckRS 2010, 49130.

[340] Der Begriff der Wiederholungsgefahr ließe sich allerdings auch so verstehen, dass lediglich die Annahme besteht, das Informationssubjekt werde erneut als Verdächtiger in Erscheinung treten.

Schwere und Begehungsweise der Taten zu berücksichtigen.[341] Liegt keine Verurteilung vor, spielt hierbei auch der Grad des Tatverdachts eine Rolle – nur geringe Verdachtsmomente bedürfen umso stärkerer Anhaltspunkte für eine mögliche Tatbegehung in der Zukunft. Auch § 484 Abs. 2 StPO formuliert ausdrücklich Kriterien, nach denen zu bestimmen ist, ob „weitere Strafverfahren gegen den Beschuldigten zu führen sind". Zu berücksichtigen sind demnach Art der Tat, Ausführung der Tat, Persönlichkeit des Beschuldigten oder Tatbeteiligten und sonstige Erkenntnisse.

Die Art der Tat kann ein gewisses Indiz für die Möglichkeit einer späteren Begehung ähnlicher Taten sein. Allerdings entlastet dies die speichernden Stellen auch bei Taten, bei denen oftmals von einer Begehung aufgrund von Abhängigkeiten (Betäubungsmitteldelikte) oder persönlichen Neigungen (Sexualstraftaten) ausgegangen wird, nicht davon, die Annahme, jemand könne in Zukunft im Zusammenhang mit einer solchen Tat in Erscheinung treten, im Einzelfall zu begründen.[342] Die pauschale Annahme einer Notwendigkeit der Speicherung von Daten zur Strafverfolgungsvorsorge beim Verdacht von bestimmten Straftaten oder bei einer entsprechenden Verurteilung wäre aufgrund der damit verbundenen Beeinträchtigung des Informationssubjekts nicht verhältnismäßig. Die pauschale Annahme einer Perseveranz ist auch kriminalistisch nicht begründbar.[343]

Die Schwere und Begehungsweise einer vorgeworfenen Tat wirken sich auf die Anforderungen aus, die an den Wahrscheinlichkeitsgrad eines künftigen strafrechtlich relevanten Auftretens zu stellen sind. Dieser muss höher sein, je geringer der Vorwurf gegen den Betroffenen ausfällt.[344] Hinsichtlich der Begehungsweise können Indizien für eine mögliche Wiederholung ein im konkreten Fall bereits wiederholtes, ein besonders planmäßiges bzw. „professionelles" oder auch ein gewerbliches Vorgehen sein.[345]

Im Rahmen der Berücksichtigung der Biographie und Persönlichkeit des Informationssubjekts ist besonders zu berücksichtigen, ob es für einem längeren Zeitraum nicht strafrechtlich in Erscheinung getreten ist.[346] Mit wachsendem Zeitabstand sinkt in der

---

[341] Vgl. BVerwG NJW 1983, 772 (773); BVerwG NJW 1983, 1338 (1339); BVerwG NJW 1990, 2768 (2770); OVG Saarlouis BeckRS 2012, 58861; OVG Lüneburg BeckRS 2014, 58848; OVG Münster BeckRS 2010, 49130; *Gaede*, in: FS Merkel, S. 1283 (1290); *Stuckenberg*, in: FG Hilger, S. 25 (33). Diese Kriterien nennen auch die Polizeigesetze für die Datenspeicherung zu präventiven Zwecken aufgrund einer „Wiederholungsgefahr"; vgl. § 75 Abs. 3 Satz 4 BWPolG; § 36b Abs. 5 Satz 1 BremPolG; § 36 Abs. 2 Satz 6 HmbPolDVG; § 37 Abs. 1 SOG MV; § 39 Abs. 2 Satz 3 NPOG.

[342] Vgl. OVG Greifswald BeckRS 2016, 42877 (im Zusammenhang mit Sexualstraftaten).

[343] Vgl. *Eisenberg*, in: FS Meyer-Goßner, S. 193 (297).

[344] OVG Saarlouis ZD 2018, 233 (234).

[345] *Gaede*, in: FS Merkel, S. 1283 (1290).

[346] BVerwG NJW 1983, 772 (773); BVerwG NJW 1983, 1338 (1339); BVerwG NJW 1990, 2768 (2770); OVG Saarlouis BeckRS 2012, 58861; OVG Münster BeckRS 2010, 49130; vgl. auch *Eisenberg*, in: FS Meyer-Goßner, S. 193 (296 f.).

Regel auch die Wahrscheinlichkeit einer künftigen Tatbegehung. Im Übrigen sind das Verhalten einer Person im Zusammenhang mit in der Vergangenheit nachweislich begangenen Taten, ggf. Bewährungsverhalten sowie die aktuellen Lebensumstände heranzuziehen.[347] Bezüglich einer dem Informationssubjekt zuvor vorgeworfenen Tat ist besonders das Verhältnis zum Opfer zu betrachten.[348]

Bei der Speicherung von Daten über Personen, die in Kontakt zu anderen stehen, die als Verdächtige einer Straftat in Betracht kommen, unterscheidet sich der Bezugspunkt der Prognose. In diesem Fall ist ein Wahrscheinlichkeitsurteil darüber zu fällen, ob diese Personen Kenntnisse haben könnten, die für die künftige Verfolgung bestimmter Taten, die durch andere begangen werden, relevant sind. Gleichwohl sind bei der Speicherung von Daten über Personen, die nicht selbst als zukünftige Tatverdächtige wahrscheinlich erscheinen, erhöhte Anforderungen zu stellen. Konsequent erscheint es, wie in § 19 Abs. 1 BKAG festgelegt, die Speicherung nur für künftige Verfahren wegen Straftaten von erheblicher Bedeutung zuzulassen. Unter solchen Straftaten sind nach einer einzelfallbezogenen Betrachtung besonders gefährliche kriminelle Verhaltensweisen zu verstehen, die den Rechtsfrieden empfindlich zu stören geeignet sind.[349] Die erhebliche Bedeutung einer Straftat ergibt sich nicht aus dem gesetzlich vorgesehenen Strafrahmen, allerdings kann dieser eine gewisse Orientierung bieten.[350]

Die in § 484 Abs. 2 StPO genannten Kriterien zur Prüfung der Erforderlichkeit könnten auf der Grundlage der vorliegenden Ausführungen spezifiziert werden. Auch wenn es nicht möglich und auch nicht notwendig sein wird, sämtliche Kriterien der Beurteilungsgrundlage gesetzlich abschließend aufzuführen,[351] könnte der bestehende Katalog um einige Eckpunkte erweitert werden.

c. Möglicher Normtext einer Befugnis zur Datenspeicherung

Eine Befugnis zur Speicherung von Daten für Zwecke künftiger Strafverfahren könnte auf Grundlage der vorangegangenen Untersuchung wie folgt lauten:

(1) Soweit tatsächliche Anhaltspunkte dafür bestehen, dass in der Zukunft ein Strafverfahren gegen eine Person zu führen sein wird, dürfen die Strafverfolgungsbehörden die zu diesem Zweck erforderlichen Daten über diese Person speichern. Anhaltspunkte für ein zukünftiges Strafverfahren können sich in einer einzelfallbezogenen Würdigung insbesondere aus der Art oder Ausführung einer dem Betroffenen nachgewiesenen

[347] *Gaede*, in: FS Merkel, S. 1283 (1290) m.w.N.

[348] *Eisenberg*, in: FS Meyer-Goßner, S. 193 (297).

[349] Vgl. zu dem entsprechenden Kriterium in § 81g StPO BT-Drs. 13/10791, S. 5; *Goers*, in: BeckOK-StPO, 47. Ed. 2023, § 81g Rn. 3; *Hadamitzky*, in: KK-StPO, 9. Aufl. 2023, § 81g Rn. 5 m.w.N.

[350] *Goers*, in: BeckOK-StPO, 47. Ed. 2023, § 81g Rn. 3.

[351] Vgl. *Bäcker*, Kriminalpräventionsrecht, S. 208.

oder vorgeworfenen Tat oder im Zusammenhang mit einem straftatbezogenen Vorverhalten aus seiner Persönlichkeit und seinen Lebensumständen ergeben.

(2) Wird ein Beschuldigter rechtskräftig freigesprochen, so ist die Speicherung von Daten über ihn aus dem betreffenden Strafverfahren unzulässig. Wird die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, so ist die Speicherung unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, dass der Beschuldigte die Tat nicht oder nicht rechtswidrig begangen hat.

(3) Die Strafverfolgungsbehörden dürfen auch Daten über Personen speichern, die mit Personen im Sinne von Abs. 1 in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung von Straftaten gewonnen werden können, weil tatsächliche Anhaltspunkte dafür bestehen, dass die Personen von der Planung oder der Vorbereitung von Straftaten von erheblicher Bedeutung Kenntnis haben oder daran mitwirken.

D. Regelungen über Datenstrukturen, Verfahren und Organisation

Neben den Regelungen über die behördliche Organisation und die Befugnisse für informationsordnende Handlungen könnten auch Regelungen über die Datenstrukturen sowie Verfahren und Organisation der Datenverarbeitung dazu beitragen, den Ist-Zustand der kriminalbehördlichen Informationsordnung ihrem Soll-Zustand anzunähern.

Regelungen über Datenstrukturen beziehen sich nicht auf einzelne Schritte der Datenverarbeitung, sondern vor allem auf die Errichtung und Einrichtung von Systemen. Während die Errichtung die Schaffung einer Informationsressource an sich betrifft, meint die Einrichtung ihre nähere Ausgestaltung.[352] Errichtung und Einrichtung entscheiden über den möglichen Inhalt und die möglichen Funktionen von Informationsressourcen.

Die Regelungen über Datenstrukturen lassen sich als Teil der Regelungen über die Organisation der Datenverarbeitung begreifen. Dazu betreffen die verfahrens- und organisationsrechtliche Aspekte der Informationsordnung unter anderem die Art und Weise, wie Daten gespeichert werden, ihre Überprüfung und die technischen Möglichkeiten des Zugriffs.

---

[352] Siehe oben Teil 1 A. I. 2.; vgl. zu diesen Begriffen *von Lewinski*, in: Seckelmann, S. 107 (115); *von Lewinski*, in: Hill/Schliesky, S. 177, (181 ff.).

Die rechtliche Bedeutung der objektiven bzw. systemischen Aspekte des Datenschutzes, welche Organisation und Verfahren betreffen, hat in den letzten Jahren zugenommen.[353] Das Bundesverfassungsgericht betonte diese bereits in seinem Volkszählungsurteil.[354] Zuletzt hat die objektiv-institutionelle Ebene des Datenschutzes in der Rechtsprechung des Bundesverfassungsgerichts[355] ebenso verstärkt Beachtung gefunden wie in der Rechtsprechung des Europäischen Gerichtshofs und des Europäischen Gerichtshofs für Menschenrechte.[356]

Unter anderem begründen additive Grundrechtseingriffe[357] und die vom Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung geforderte „Überwachungsgesamtrechnung“[358] die Notwendigkeit, Verfahren und organisatorische Vorkehrungen vorzusehen, um die Gesamtheit der Eingriffe überblicken zu können. Stellen, die durch informationsgewinnende oder informationsordnende Maßnahmen in Grundrechte des Betroffenen eingreifen, müssen über ähnliche Handlungen durch andere Stellen informiert sein, um die Gesamtbelastung für die Betroffenen einschätzen zu können.[359] Dies kann es erforderlich machen, dass Gesetzgeber Verfahren sowie organisatorische Vorkehrungen entwickeln, um die „Überwachungsdichte“[360] bzw. im Fall der Informationsordnung die Gesamtheit der Datenaggregationen zu ermitteln.

In der Praxis der Informationsordnung betonen die Konzepte zur Neuordnung der Systeme von Bundeskriminalamt und Europol zunehmend einen systemischen bzw. strukturellen Datenschutz. Das Bundeskriminalamt will die organisatorische Gewährleistung des Datenschutzes durch die Speicherung von Informationen in verschiedene

[353] Vgl. *Ladeur*, DuD 2000, 12 (15 ff.); *Schöndorf-Haubold*, S. 170; *Würtenberger*, in: GS Kopp, S. 428 (436) sowie zum Systemschutz als technisch-organisatorischer Gestaltung der Kommunikationsinfrastruktur *Hoffmann-Riem*, in: Hoffmann-Riem, Offene Rechtswissenschaft, S. 499 (520).

[354] BVerfGE 65, 1 (44 ff.); vgl. auch *Scholz/Pitschas*, S. 43; *Vogelgesang*, S. 79 ff., 183 ff.

[355] So formulierte das Bundesverfassungsgericht in seiner Entscheidung zur Vorratsdatenspeicherung im Rahmen der Verhältnismäßigkeit unter anderem besondere verfassungsrechtliche Anforderungen an die Datensicherheit, den Umfang der Datenverwendung und die Transparenz der Datenverwendung (BVerfGE 125, 260 (326 ff.)); vgl. dazu *Britz*, JA 2011, 81 (82 ff.); *Westphal*, EuZW 2010, 494 (499).

[356] Vgl. *Marsch*, S. 115 m.w.N.

[357] BVerfGE 112, 304 (319 f.).

[358] BVerfGE 125, 260 (324); Begriff von *Roßnagel*, NJW 2010, 1238; siehe dazu bereits oben Teil 1 A. II.

[359] Vgl. *Knierim*, ZD 2011, 17 (21); *Moser-Knierim*, S. 243.

[360] *Knierim*, ZD 2011, 17 (21).

Dateien durch ein abgestuftes System von Zugriffsrechten ersetzen, welches als horizontales Datenschutzkonzept bezeichnet wird.[361] Die Planungen zu der Informationsordnung von Europol auf Grundlage der Europol-VO gehen in eine ähnliche Richtung.[362]

Die Regelungen über Datenstrukturen, Verfahren und Organisation sind in einem engen Zusammenhang mit den Befugnissen zur Durchführung der einzelnen Verarbeitungsschritte zu betrachten. Welche Möglichkeiten die Struktur eines Systems zur Datenverarbeitung eröffnet, wirkt sich darauf aus, wie weit die Befugnisse für den Umgang mit ihm geregelt werden können.[363] Sind die möglichen Inhalte eines Informationssystems bereits stark begrenzt, kann dies es rechtfertigen, die Anlässe zur Speicherung und Verwendung der Daten weiter zu fassen als im Zusammenhang mit Systemen, die die Speicherung von Daten in einem offenerem Rahmen ermöglichen. Auch andere verfahrens- und organisationsrechtliche Vorgaben eignen sich, um informationsordnende Tätigkeiten gerade angesichts ihrer schwer bestimmbaren Eingriffsschwellen einzuhegen.[364]

I. Beitrag zur Lösung bestehender Herausforderungen

Neue Regelungen zu Datenstrukturen, Verfahren und Organisation könnten in mehrerlei Hinsicht zur Bewältigung bestehender Herausforderungen beitragen. Sie könnten dabei helfen, die Datenqualität zu verbessern. Vorgaben für die Ausgestaltung der Umgebungen, in die Daten eingepflegt werden, könnten der inhaltlichen Richtigkeit und Genauigkeit der Angaben ebenso förderlich sein wie prozedurale Vorgaben. Pflichten für die Überprüfung von Datenbeständen könnten ihre Aktualität sicherstellen.

Die Strukturen der Datenbestände spielen auch für die Möglichkeit ihrer Verknüpfung und Auswertung eine große Rolle. Nach einheitlichen Vorgaben erfasste, aktuelle und inhaltlich richtige Daten sind eine notwendige Basis, um durch automatisierte Verarbeitungen Schlüsse aus Ihnen ziehen zu können.[365]

Schließlich können verfahrens- und organisationsrechtliche Vorgaben zur Wahrung der Interessen der Betroffenen bei Abruf und Verknüpfung der Daten dienen.

---

[361] BT-Drs. 18/11163, S. 76; siehe näher oben Teil 1 B. III. 3. c.

[362] Siehe oben Teil 1 B. VI.

[363] Vgl. *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung, S. 34.

[364] Vgl. *Kugelmann*, DÖV 2003, 781 (787); *Möstl*, S. 240; *Trute*, in: GS Jeand'Heur, S. 403 (419 ff.); *Trute*, Die Verwaltung 2009, 85 (90); im Zusammenhang mit der verdeckten Informationserhebung *Neumann*, S. 180 ff.

[365] Siehe oben Teil 2 C. I.

Dies leisten neben den bereits erwähnten Vorgaben zur Datenqualität auch Regelungen, die die Transparenz zugunsten der Betroffenen verbessern.

II. Rechtliche Möglichkeiten und Grenzen

Es existieren nur wenige grundsätzliche rechtliche Vorgaben, die Datenstrukturen sowie Verfahren und Organisation der Datenverarbeitung betreffen.

Die Errichtung kriminalbehördlicher Informationsressourcen steht nicht unter einem allgemeinen Gesetzesvorbehalt und ist per Exekutivakt möglich.[366] Allerdings kann sich unter Umständen aus besonderen rechtlichen Gründen die Notwendigkeit einer gesetzlichen Regelung für die Errichtung einer Informationsressource ergeben.[367] Dies gilt etwa für Dateien, die Informationsbestände in besonders eingriffsintensiver Weise zusammenführen – so etwa die Antiterrordatei, an der unter anderem das Bundeskriminalamt, die Bundespolizei, das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst, der Militärischer Abschirmdienst, das Zollkriminalamt, die Landeskriminalämter sowie die Landesämter für Verfassungsschutz beteiligt sind.[368] Das Bundesverfassungsgericht stellte in seiner ersten Entscheidung zum Antiterrordateigesetz allerdings keine allzu hohen Anforderungen an die Bestimmtheit von einfachgesetzlichen Grundlagen zur Errichtung von Dateien. Das Gericht verlangte vor allem eine Spezifizierung auf der Ebene der Exekutive. Die Verwaltung habe die Anwendung von Dateien als Ausgleich zu der unbestimmten gesetzlichen Regelung zu konkretisieren sowie dies zu dokumentieren und zu veröffentlichen.[369] Dies solle einer „uferlosen oder missbräuchlichen" Verwendung der Dateien entgegenwirken und ihre Kontrolle durch den Betroffenen sowie die Datenschutzbeauftragten ermöglichen.[370]

Für die Einrichtung von kriminalbehördlichen Informationsressourcen lassen sich genauere normative Vorgaben herleiten als für ihre Errichtung. Während die konkrete Ausgestaltung der Ressourcen größtenteils ebenso der Exekutive überlassen ist wie ihre Errichtung, ergeben sich aus verfassungsrechtlichen und einfachgesetzlichen Vorgaben zumindest Leitlinien, anhand derer Exekutivakte wie Errichtungsanordnungen überprüft werden können.

Objektiv-rechtlichen Vorgaben für die Strukturierung von Informationsressourcen sowie Organisation und Verfahren der Datenverarbeitung ergeben sich vor allem aus

---

[366] Vgl. *Creemers*, in: Grutzpalk, S. 101 (116).

[367] *Von Lewinski*, in: Seckelmann, S. 107 (113).

[368] Deren Errichtung findet ihre rechtliche Grundlage in § 1 Abs. 1 Satz 1 ATDG i. V. m. § 1 Abs. 3 Nr. 1 lit. d) BPolZV.

[369] BVerfGE 133, 277 (357 f.).

[370] BVerfGE 133, 277 (358).

den Grundsätzen des Datenschutzrechts, die für den kriminalbehördlichen Handlungsbereich in Art. 4 JI-Richtlinie und Vorschriften zu dessen Umsetzung[371] geregelt sind und ihre Wurzel in Art. 8 GRCh finden.[372] Als strukturellen Vorgaben für die Datenverarbeitung sind die Grundsätze der Zweckfestlegung und Zweckbindung (Art. 4 Abs. 1 lit. b und lit. c JI-Richtlinie), der Richtigkeit und Aktualität (Art. 4 Abs. 1 lit. d JI-Richtlinie), der Speicherbegrenzung (Art. 4 Abs. 1 lit. e JI-Richtlinie), der Datensicherheit (Art. 4 Abs. 1 lit. f JI-Richtlinie) sowie der in Art. 4 JI-Richtlinie nicht explizit formulierte Grundsatz der Transparenz von besonderem Interesse.

Nach dem hergebrachten deutschen verfassungsrechtlichen Verständnis der Zweckbindung bedarf die Verwendung von Daten zu einem anderem Zweck als jenem ihrer ursprünglichen Erhebung einer neuen Rechtfertigung. Das Unionsrecht stellt nuanciert anders nicht auf die Andersartigkeit des Zwecks ab, sondern verbietet grundsätzlich die Verarbeitung zu einem mit dem ursprünglichen Verarbeitungszweck unvereinbaren Zweck.[373] Das unionsrechtliche Prinzip der Zweckkompatibilität ist damit im Ergebnis weniger streng als das deutsche Zweckbindungsprinzip.[374] Während nach deutschem Recht beispielsweise eine Weiterverarbeitung von Daten zu repressiven Zwecken, die zu präventiven Zwecken erhoben wurden, stets eine Zweckänderung darstellt, erscheint es unionsrechtlich im Einzelfall möglich zu argumentieren, dass die Weiterverarbeitung mit dem ursprünglichen Erhebungszweck noch kompatibel ist. Dies hängt auch mit dem integrierten Verständnis des präventiven und repressiven Rechtsgüterschutzes im Unionsrecht zusammen.[375]

Als Begrenzungen der Datenverarbeitung im Sinne der Verhältnismäßigkeit mit der Zweckbindung verwandt sind die Prinzipien der Datenminimierung[376] und Speicherbegrenzung[377]. Während das Prinzip der Datenminimierung die Beschränkung von Datenverarbeitungen auf das für die Erfüllung des Zwecks geringstmögliche Maß gebietet,[378] stellt das Prinzip der Speicherbegrenzung eine zeitliche Grenze für die Speicherung auf und verlangt die Löschung von Daten, die für die verfolgten Zwecke nicht mehr benötigt werden.[379] Diese Grundsätze ähneln insofern den bisher im deutschen

[371] Z.B. § 47 BDSG.
[372] Vgl. *Johannes/Weinhold*, § 1 Rn. 123.
[373] Vgl. Art. 4 Abs. 1 lit. b und lit. c JI-Richtlinie.
[374] *Kühling/Martini*, EuZW 2016, 448 (451).
[375] Siehe oben Teil 1 C. I. 1. b.
[376] Art. 4 Abs. 1 lit. c JI-Richtlinie.
[377] Art. 4 Abs. 1 lit. e JI-Richtlinie; vgl. zum Zusammenhang von Speicherbegrenzung und Zweckbindung *F. Braun*, in: Gola/Heckmann, 3. Aufl. 2022, § 47 BDSG Rn. 16 ff.
[378] Vgl. zum Verhältnis der Datenminimierung zu den Grundsätzen der Verhältnismäßigkeit sowie der Zweckbestimmung und Zweckbindung *Wolff*, in: Schantz/Wolff Rn. 420.
[379] *Wolff*, in: Schantz/Wolff, Rn. 444.

Recht bekannten Grundsätzen der Datenvermeidung und Datensparsamkeit.[380] Als Ausprägung des Grundsatzes der Speicherbegrenzung regelt Art. 5 Satz 1 JI-Richtlinie, dass die Mitgliedstaaten vorsehen, „dass für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen sind."[381] Die Einhaltung dieser Fristen ist gemäß Satz 2 der Vorschrift durch verfahrensrechtliche Vorkehrungen sicherzustellen.

III. Konkrete Regelungsansätze

Im Folgenden werden vier Bereiche betrachtet, in denen Regelungen über Datenstrukturen, Verfahren und Organisation konkretisiert werden könnten, um den Ist-Zustand der kriminalbehördlichen Informationsordnung ihrem Soll-Zustand anzunähern: Die Einspeisung und Validierung von Informationen (1.), die zeitliche Begrenzung von Datenspeicherungen (2.), die Begrenzung von Zugriffsmöglichkeiten (3.) sowie Vorkehrungen zur Sicherstellung der Transparenz und Kontrollierbarkeit von Informationsressourcen (4.).

1. Regelungen über die Einspeisung und Validierung von Informationen

Zunächst wären konkretere Verfahrensregelungen denkbar, die dazu beitragen, dass Daten bei ihrer Einspeisung in kriminalbehördliche Informationsressourcen (a.) und auch in der Folge in gewissen Zeitabständen (b.) auf ihre Richtigkeit und Aktualität überprüft werden.

a. Die Einspeisung von Informationen

Schon bei der erstmaligen Einspeisung von Informationen in kriminalbehördliche Systeme ist sicherzustellen, dass diese vollständig und präzise sind. Ein bei der erstmaligen Speicherung erzeugtes Defizit in der Datenqualität ist nachträglich nur schwer zu beheben. Die Anforderungen an die Qualität bei der Einspeisung von Informationen gelten entsprechend, wenn durch die Nutzung der Informationsordnung – etwa im Rahmen automatisierter Datenauswertungen – Informationen erzeugt werden, durch die bereits zuvor vorhandene Informationen in einen neuen Kontext gerückt werden.

Für die Sicherung der Qualität bei der erstmaligen Einspeisung von Daten bedarf es technischer und organisatorischer Vorkehrungen. Organisatorisch ist sicherzustellen, dass die Herkunft von Informationen dokumentiert ist und Datensätze entsprechend

[380] Vgl. *Johannes/Weinhold*, § 1 Rn. 132; *Wolff*, in: Schantz/Wolff Rn. 427.
[381] Vgl. *M. Müller/Schwabenbauer,* in: Lisken/Denninger, 7. Aufl. 2021, Kap. G Rn. 497.

gekennzeichnet sind.[382] Die Durchführung dieser organisatorischen Maßnahmen ließe sich durch die Schaffung entsprechender rechtlicher Verpflichtungen absichern.

Technisch ist sicherzustellen, dass Informationsressourcen Daten mit ausreichender Präzision aufnehmen können. Zum Teil sind in kriminalbehördlichen Informationssystemen Defizite bei der Datenqualität „vorprogrammiert", etwa wenn sie mit Namen aus anderen Kulturkreisen arbeiten oder Schriften transkribiert werden müssen. So lässt sich beispielsweise die traditionelle fünfteilige Struktur arabischer Namen in polizeilichen Informationssystemen nicht durch das systemisch vorgegebene Schema von Vor- und Nachname erfassen. Wie *Fall 3* zeigt, kann dies unter anderem zu Verwechslungen führen. Die Festlegung technischer Standards, um eine genaue Datenerfassung zu ermöglichen, könnte auch auf untergesetzlicher Ebene erfolgen.

b. Die weitere Überprüfung von Daten

Nach der erstmaligen Speicherung sind weitere Maßnahmen zur Sicherung der Datenqualität notwendig. In diesem Sinne sieht Art. 7 Abs. 2 Satz 2 JI-Richtlinie vor, dass Daten vor ihrer Übermittlung und Bereitstellung zu kontrollieren sind. Eine routinemäßige Überprüfung von Daten auf ihre Aktualität und Richtigkeit ist vor ihrer Verwendung für weiterführende Maßnahmen generell sinnvoll. Sie ist für Daten, die sensible Informationen enthalten oder deren Speicherung lange zurückliegt, in besonderem Maße geboten.

Regelungen auf nationaler Ebene, die ihre unionsrechtliche Grundlage in Art. 5 JI-Richtlinie finden, verpflichten die Kriminalbehörden, die Erforderlichkeit der Speicherung von Daten in regelmäßigen Abständen zu überprüfen. Allerdings handelt es sich hierbei nicht um Verpflichtungen zur Sicherung der Datenqualität im engeren Sinne, sondern um Regelungen zur Speicherbegrenzung, auf die sogleich näher eingegangen wird.[383] Sie dienen nicht dazu, die Richtigkeit und Aktualität der Datenbestände sicherzustellen, sondern sollen vor allem dafür sorgen, dass nicht mehr erforderliche Daten ausgesondert werden. Die regelmäßigen Löschfristen sind aber bei der Regelung von Maßnahmen zur Sicherung der Datenqualität zu bedenken. So könnten Überprüfungen der Erforderlichkeit einer weiteren Speicherung und der Qualität der Daten auch praktisch miteinander verbunden werden.

Die genauen Anforderungen an die Validierung und Kontrolle von Daten sind auch von der Tragweite der Maßnahmen abhängig, die auf Grundlage der Daten getroffen werden. So sollte beispielsweise vor der Zusammenführung von Datensätzen oder der Veränderung von Namensdaten eine besonders strenge Kontrolle erfolgen, da derartige

[382] *Rusteberg*, in: Münkler, S. 233 (257).
[383] Siehe unten 2.

Schritte weitreichende Konsequenzen für Folgemaßnahmen haben können. Um die Standards an die Datenqualität praktisch gewährleisten zu können, sind die Nutzer*innen der kriminalbehördlichen Informationsordnung zudem gezielt auszubilden und für Risiken zu sensibilisieren.[384]

Spezielle Anforderungen an die Überprüfung der Aktualität und Richtigkeit von Daten ergeben sich schließlich aus der Unschuldsvermutung. Das Bundesverfassungsgericht leitet aus der Unschuldsvermutung eine besondere Anforderung an die Datenqualität ab, wenn ein Freispruch oder eine Verfahrenseinstellung erfolgt. Die speichernde Stelle trifft dann eine Pflicht, die Daten darauf zu überprüfen, „ob noch Verdachtsmomente gegen den Betroffenen bestehen, die eine Fortdauer der Speicherung zur präventiv-polizeilichen Verbrechensbekämpfung rechtfertigen."[385]. Nach den Berichten der Datenschutzaufsicht wird dies in der polizeilichen Praxis allerdings nicht immer befolgt.[386]

Dass Verfahrenseinstellungen und Freisprüche bei der Speicherung von Daten in Informationssystemen praktisch häufig nicht ausreichend Berücksichtigung finden, hat mehrere mögliche Ursachen. Eine davon ist die Mitteilung dieser Informationen, die sich nach den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) richtet. Aus der obligatorischen Mitteilung an den Beschuldigten nach Nr. 88 RiStBV ergeben sich die Gründe einer Verfahrenseinstellung nicht zwangsläufig.[387] Die Pflicht der Staatsanwaltschaft zur Benachrichtigung der Polizei über den Ausgang des Verfahrens nach § 482 Abs. 2 Satz 1 StPO betrifft nur die Entscheidungsformel, die entscheidende Stelle sowie das Datum und die Art der Entscheidung, nicht aber die näheren Gründe hierfür. Zwar wird aus § 482 Abs. 2 Satz 1 StPO teilweise eine Pflicht der Polizei hergeleitet, zu prüfen, ob die Daten aus dem betroffenen Verfahren weiter gespeichert werden dürfen,[388] diese steht allerdings auf unsicheren Füßen.

Um sicherzustellen, dass nach Einstellungen und Freisprüchen keine veralteten oder fehlerhaften Datensätze gespeichert bleiben, sollte eine ausdrückliche Pflicht der speichernden Stelle geregelt werden, nach Kenntnis von einer Einstellung oder einem Freispruch eine Überprüfung der weiteren Notwendigkeit der Datenspeicherung durchzuführen und diese bei positivem Ergebnis zu begründen. Dabei ist davon auszugehen,

---

[384] Vgl. *Creemers*, in: Grutzpalk, S. 101 (120); vgl. dazu im Zusammenhang mit dem Erfordernis effektiven Wissensmanagements *Augsberg*, S. 72.

[385] BVerfG NJW 2002, 3231 (3232); BVerfG BeckRS 2009, 35816.

[386] LfD Bayern, 27. Tätigkeitsbericht 2015/2016, S. 59 ff.; LfDI Hamburg, 26. Tätigkeitsbericht 2016/2017, S. 26.

[387] Vgl. BVerwG NJW 2011, 405 (406 f.).

[388] *Singelnstein*, in: MüKo-StPO, 2019, § 482 Rn. 4.

dass Daten über Freigesprochene zu Zwecken der Strafverfolgungsvorsorge grundsätzlich nicht gespeichert werden dürfen.[389]

2. Die zeitliche Begrenzung von Speicherungen

Weiter ließen sich die Regelungen konkretisieren, die die Speicherung von Daten in kriminalbehördlichen Informationssystemen zeitlich begrenzen. Sie fußen vor allem auf dem datenschutzrechtlichen Prinzip der Speicherbegrenzung. Aus diesem Prinzip lässt sich das Erfordernis ableiten, dass für die Speicherung von Daten in kriminalbehördlichen Informationsressourcen Fristen vorzusehen und diese technisch abzusichern sind.[390]

Aktuell sehen die Regelungen zur kriminalbehördlichen Informationsordnung grundsätzlich keine absoluten Höchstfristen für Datenspeicherungen vor.[391] Sie sehen aber auf Grundlage von Art. 5 JI-Richtlinie vor, dass die Erforderlichkeit der Speicherung innerhalb gewisser Fristen zu überprüfen ist. Zum Teil werden Regelfristen hierfür direkt in den Gesetzen festgelegt,[392] zum Teil wird die Festlegung der Prüfungstermine der speichernden Stelle überlassen.[393] Bei Daten, die nach § 484 StPO für Zwecke künftiger Strafverfahren gespeichert wurden, beträgt die Frist zur Überprüfung gemäß § 489 Abs. 3 StPO grundsätzlich zehn Jahre, bei Jugendlichen fünf Jahre, in Fällen des rechtskräftigen Freispruchs, der unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens und der nicht nur vorläufigen Verfahrenseinstellung drei Jahre und bei nicht Strafmündigen schließlich zwei Jahre. Nach § 489 Abs. 5 StPO beginnen die Fristen mit dem Tag, an dem das letzte Ereignis eingetreten ist, das zur Speicherung der Daten geführt hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung.

Die in § 489 Abs. 3 StPO, aber auch in den Polizeigesetzen im Wesentlichen ähnlich geregelten, Aussonderungsprüffristen erscheinen recht großzügig bemessen, wenn man bedenkt, dass die grundsätzliche Zehnjahresfrist auch für die Vorbereitung der Verfolgung vergleichsweise geringfügiger Delikte gilt, bei einem Freispruch oder einer Einstel-

[389] Siehe oben Teil 1 A. III. 1. b. bb).

[390] Ähnlich *Stubenrauch*, S. 136.

[391] Solche sind nur in Ausnahmefällen vorgesehen, so etwa in Art. 33 Abs. 8 BayPAG für offene Bild- und Tonaufnahmen.

[392] Vgl. etwa § 76 Abs. 2 BWPolG; Art. 53 Abs. 5 Satz 2, Art. 54 Abs. 2 Satz 3 BayPAG; § 35 Abs. 2 HmbPolDVG; § 45a SOG MV; § 43 Abs. 3 und 4 SächsPolG.

[393] Vgl. etwa § 49 Abs. 3 Satz 2 ASOG Bln; § 37 Satz 2 BbgPolG; § 22 Abs. 2 PolG NRW.

lung die Unschuldsvermutung eher eine sofortige Überprüfung bzw. Löschung der Daten gebietet und Strafunmündige nicht einmal als Beschuldigte in Betracht kommen.[394] Zwar ist nach § 489 Abs. 4 StPO eine Festlegung kürzerer Prüffristen in Errichtungsanordnungen möglich und auch im Übrigen die Möglichkeit außerordentlichen Prüfung rechtlich nicht versperrt, allerdings setzen die in § 489 Abs. 3 StPO vorgesehenen Fristen einen wichtigen Anker für die Prüfungspraxis.

Da die gesetzlichen Regelungen lediglich zu einer Prüfung verpflichten, kann es auch nach Ablauf der Fristen zu einer Fortsetzung der Speicherung kommen. Nach der Grundkonzeption des Datenschutzrechts ist das Speichern personenbezogener Daten allerdings naturgemäß ein zeitlich begrenzt zulässiger Vorgang. Welche Speicherdauer angemessen ist, wird sich nur im Einzelfall präzise beantworten lassen. Auch eine längere Speicherdauer als zehn Jahre kann zu Zwecken der Strafverfolgungsvorsorge im Einzelfall erforderlich und angemessen sein, wenn es etwa um schwere Delikte oder besonders auffällige Persönlichkeiten geht. In Fällen von Delikten von geringer Tragweite, bei denen die Tatverdächtigen keinen besonders gefährlichen Neigungen oder Verstrickungen in kriminelle Organisationen aufweisen, erscheint allerdings eine kürzere Speicherdauer angebracht. Auch der Grad des Tatverdachts sollte bei der Bestimmung der angemessenen Speicherdauer Berücksichtigung finden.

Schon die Speicherung von Daten über den Verdacht von Straftaten von vergleichsweise geringem Gewicht kann sich negativ auf das Informationssubjekt auswirken und dessen Ansehen schaden. Dies verdeutlicht etwa der Fall Khelili, in dem eine Frau in einer Polizeidatenbank aufgrund eines bloßen Verdachts 18 Jahre lang als Prostituierte gekennzeichnet wurde.[395] Sie zog aufgrund dessen bis vor den Europäischen Gerichtshof für Menschenrechte, der diese Datenspeicherung im Lichte der Unschuldsvermutung als rechtswidrig betrachtete.[396] Auch die im Rahmen dieser Untersuchung interviewten Mitarbeiter*innen der Datenschutzaufsicht schilderten die langfristige Speicherung personenbezogener Daten in polizeilichen Ressourcen aufgrund des Vorwurfs von Bagatelldelikten als praktisches Problem. So berichtete etwa ein*e Interviewpartner*in:

> „Wir hatten eine Petentin, eine Greenpeace-Aktivistin, die immer wieder bei Demonstrationen dabei war und immer wieder wegen Nötigung, weil man sie wegtragen musste, oder Sachbeschädigung [...] gespeichert wurde – und das über zwanzig oder mehr Jahre. [...] Es gab eine Demonstration bei Lidl auf dem Parkplatz. Da ging es um die Hühnerhaltung, es wurden mit Sprühkreide Eier auf den Parkplatz gesprüht. Dann kam die Polizei und hat alle durchsucht. Bei

[394] *Hilger*, NStZ 2001, 15 (19); *Singelnstein*, in: MüKo-StPO, 2019, § 489 Rn. 20.
[395] Siehe oben Teil 1 C. III. 2. b.
[396] EGMR (2. Sektion), Urteil vom 18. Oktober 2011, Khelili gegen Schweiz, No. 16188/07.

> dieser Dame hat man dann Deckel von Sprühflaschen entdeckt und sie gleich wieder wegen Sachbeschädigung für fünf Jahren gespeichert, obwohl der Schaden nur bei 20 oder 30 Euro lag." (DSA1)

In Anbetracht der Tatsache, dass die Mehrzahl der polizeilich gespeicherten Daten nicht der Vorbereitung auf die Verfolgung schwerwiegender Straftaten oder der Aufdeckung komplexer kriminelle Organisationen dienen, erschiene daher eine kürzere Speicherfrist geboten, bei deren Ablauf des zur automatischen Löschung der Daten kommt, wenn nicht die Notwendigkeit einer weiteren Speicherung nach einer Überprüfung ausdrücklich bejaht und dieses Ergebnis dokumentiert wird. Um dem datenschutzrechtlichen Prinzip der Speicherbegrenzung gerecht zu werden, sollte damit die Löschung der Daten nach Fristablauf zum Regelfall werden.

Wenn es – wie in dem soeben geschilderten Fall der Demonstration bei Lidl – zu jahrzehntelangen Speicherungen wegen Bagatelldelikten kommt, dann liegt dem oftmals ein „Mitzieheffekt" bzgl. der gespeicherten Daten zugrunde. Einige Polizeigesetze sehen im Zusammenhang mit den Aussonderprüffristen vor, dass bei der Speicherung von mehreren Datensätzen über dieselbe Person die Prüffrist für alle Daten mit der letztmöglichen Frist endet.[397] Eine ähnliche Regelung war auch in § 489 Abs. 6 Satz 1 StPO aF vorgesehen gewesen. Von Seiten der Gesetzgeber und Anwender*innen werden diese Regelungen mit dem Interesse daran begründet, ein möglichst vollständiges Bild über eine Person und ihren „kriminellen Werdegang" zu erhalten.[398] Derartige Regelungen verhindern allerdings eine Gewährleistung der Verhältnismäßigkeit einer Datenspeicherung dadurch, dass die Prüfung ihrer Erforderlichkeit unter Umständen über Jahrzehnte hinausgezögert werden kann.[399] Das Hinzukommen neuer Daten macht eine Überprüfung des bereits vorhandenen Datensatzes zur Sicherung seiner Gesamtqualität eher notwendig, als dass es davon entbinden kann. Regelungen zu einer derartigen „Mitziehautomatik" sollten daher ersatzlos aus den Polizeigesetzen gestrichen werden, so wie es in der StPO bereits geschehen ist.

3. Die Begrenzung von Zugriffsmöglichkeiten

Dass die Möglichkeiten des Zugriffs auf kriminalbehördliche Datenbestände Beschränkungen unterliegen müssen, lässt sich aus den Prinzipien der Zweckbindung und der Datensicherheit herleiten. Derartige Beschränkungen lassen sich in Regelungen zu Verfahren und Organisation festlegen. Da das „neue Datenhaus" der Polizei nach einem

---

[397] § 76 Abs. 3 Satz BWPolG; Art. 54 Abs. 2 Satz 6 BayPAG; § 35 Abs. 3 Satz 2 HmbPolDVG; § 45a Abs. 2 Satz 3 SOG MV.

[398] *von der Grün*, in: BeckOK-BWPolG, 29. Ed. 2023, § 76 Rn. 13.

[399] BfDI, Stellungnahme StPO 2019, S. 9 f.

abgestuften System von Zugriffsrechten erschlossen werden soll,[400] nimmt die Bedeutung von Zugriffsregelungen aktuell zu.

Die Zweckbindung erfordert organisatorisch nicht nur eine frühzeitige und präzise Zweckbestimmung, sondern auch Verfahrensregelungen, die eine Bindung an die festgelegten Zwecke bei der Weiterverarbeitung von Daten sicherstellen.[401] Dazu gehört eine Festlegung von Zugriffsrechten. In einem engen Zusammenhang mit der Zweckbindung als organisatorischem Prinzip für die Sammlung von Informationen steht die „informationelle Gewaltenteilung". Nach den Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil bezeichnet der Begriff eine von mehreren möglichen organisatorischen Vorkehrungen zur Wahrung der Zweckbindung.[402] Informationelle Gewaltenteilung besagt, dass jede Stelle „nur diejenigen Informationen erhalten und verarbeiten [darf], die zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich sind."[403] Sie soll dadurch Bürger*innen vor der übermäßigen Konzentration von Informationsmacht schützen.[404] Losgelöst von ihrer datenschutzrechtlichen Einordnung lässt sich informationelle Gewaltenteilung als „Folge der dezentralen Behördenorganisation und der damit einhergehenden Zuständigkeitsverteilung sowie der notwendigen Arbeitsteilung innerhalb der Verwaltung"[405] verstehen.[406] Sie lässt sich daher auch auf die Ebene einzelner Sachbearbeiter*innen beziehen.

Auch aus dem Prinzip der Datensicherheit[407] ergeben sich Anforderungen an Zugriffsschranken. Datensicherheit erfordert neben der Integrität und Verfügbarkeit auch die Vertraulichkeit von Daten. Unter dem Aspekt der Vertraulichkeit müssen Zugriffsrechte auf Daten in kriminalbehördlichen Informationssystemen auf den Kreis jener Personen beschränkt bleiben, die zur Erfüllung ihrer Aufgaben auf sie angewiesen sind.[408] Die Anforderungen an die Datensicherheit hängen insofern mit jenen der

---

[400] Siehe oben Teil 1 B. III. 3. c.

[401] Vgl. BVerfGE 125, 260 (333).

[402] BVerfGE 65, 1 (69); vgl. auch *Riegel*, DVBl. 1988, 121 f.; *Stubenrauch*, S. 131. Im Einzelnen ist der Zusammenhang der „informationellen Gewaltenteilung" mit der Zweckbindung allerdings unklar.

[403] *Bull*, iur 1986, 287 (292); vgl. auch *Forgó/Krügel/Rapp*, S. 16 („systematische Aufsplitterung der Verwaltung und der von ihr verarbeiteten Informationen in kleine Zellen zum Zwecke ihrer Abschottung gegeneinander").

[404] *Bull*, iur 1986, 287 (292); vgl. zu dem Verhältnis zum Recht der Amtshilfe *Bull*, DÖV 1979, 689 (692 ff.).

[405] *Forgó/Krügel/Rapp*, S. 49.

[406] Als Fortsetzung der klassischen Gewaltenteilung erscheint die informationelle Gewaltenteilung hingegen nicht. Aus der Verfassung lässt sich zwar eine vertikale Teilung der Verwaltung von Bund, Ländern und Kommunen (Art. 20, 28 und 30 GG), aber keine konkrete horizontale Gewaltenteilung innerhalb der Verwaltung ableiten; vgl. *Forgó/Krügel/Rapp*, S. 50; *Schlink*, S. 31.

[407] Art. 4 Abs. 1 lit. f JI-Richtlinie.

[408] *Kipker*, S. 62 f.

Zweckbindung zusammen, da der verfolgte Zweck die Grenzen der Notwendigkeit bestimmt.[409]

Durch welche Maßnahmen die Datensicherheit konkret sichergestellt wird, obliegt in hohem Maße den verantwortlichen Stellen. Auch dem Gesetzgeber steht bei Vorgaben zur Datensicherheit ein weiter Spielraum zu.[410] Da die Wahrung von Standards zur Datensicherheit stark von einer technischen Dynamik abhängt, wird es hier kaum erlässlich sein, auf außerrechtliche Wertungen zurückzugreifen – etwa durch einen Verweis auf den Stand der Technik.[411] Bei Systemen, die eine zentrale Datenbevorratung vorsehen, sind aufgrund der damit verbundenen Missbrauchsmöglichkeiten tendenziell höhere Anforderungen an die Datensicherheit zu stellen als bei dezentralen Systemen.[412] Die Anforderungen steigen zudem mit Umfang und potentieller Aussagekraft der betroffenen Datenbestände.[413]

Eine Regelung über Beschränkungen des Zugriffs auf Datenbestände im Sinne der Grundsätze der Zweckbindung und Datensicherheit könnte vorsehen, dass die verantwortlichen Stellen den Zugriff auf Informationssysteme und ihre einzelnen Bereiche auf diejenigen Einheiten und Personen beschränken müssen, die diese Informationen zur Erfüllung ihrer Aufgaben benötigen. Eine solche Verpflichtung könnte dadurch begleitet werden, dass die erteilten Zugriffsrechte begründet und dokumentiert werden müssen.

4. Transparenz und Kontrolle

Schließlich könnten die Regelungen erweitert und konkretisiert werden, die dazu dienen, die informationsordnenden Handlungen der Kriminalbehörden für die Betroffenen nachvollziehbar und kontrollierbar zu machen. Gerade von großen Datensammlungen kann eine diffuse Bedrohlichkeit für die Betroffenen ausgehen, die durch Transparenzregeln aufgefangen werden kann.[414] Anforderungen an die Transparenz der Datenverarbeitung ergeben sich verfassungsrechtlich aus Rechtsstaatsprinzip und Rechtsschutzgarantie[415] sowie unionsrechtlich aus dem Regelungskontext der JI-Richtlinie.[416]

---

[409] Vgl. *Kipker*, S. 63.
[410] Vgl. zu der Vorratsspeicherung von Telekommunikationsdaten *Britz*, JA 2011, 81 (82).
[411] Vgl. BVerfGE 125, 260 (326).
[412] Vgl. *Kühling*, NVwZ 2014, 681 (684).
[413] Vgl. zu der Vorratsspeicherung von Telekommunikationsdaten BVerfGE 125, 260 (325).
[414] BVerfGE 125, 260 (335).
[415] BVerfGE 118, 168 (207 f.); BVerfGE 133, 277 (366 f.); *Britz*, JA 2011, 81 (85).
[416] Der Grundsatz der Transparenz ist in Art. 4 JI-Richtlinie nicht explizit formuliert, da der Richtliniengeber dies offenbar im Widerspruch zu der Möglichkeit verdeckter Ermittlungen sah; vgl. *F. Braun*, in: Gola/Heckmann, 3. Aufl. 2022, § 47 BDSG Rn. 6; *Schwichtenberg*, in: Kühling/Buchner, § 47 BDSG

Dabei sind Transparenzanforderungen sowohl für einzelne Informationsressourcen als auch auf der übergeordneten Ebene zu stellen. Jedes einzelne System muss Vorkehrungen zur Transparenz vorsehen. Darüber hinaus sollte strukturell die Gesamtheit der kriminalbehördlichen Ressourcen, in denen Daten gespeichert werden, erkennbar sein.

Um Informationsverarbeitungen transparent zu machen, spielen Betroffenenrechte zur Auskunft und Benachrichtigungspflichten der Datenverarbeiter eine wichtige Rolle.[417] Aufgrund der zunehmenden Komplexität der Informationsordnung und dem Expertenwissen, das notwendig ist, um die dahinter liegenden Strukturen zu begreifen und Betroffenenrechte effektiv geltend zu machen, sind Transparenzlösungen über Betroffenenrechte aber nicht vollends befriedigend. Perspektivisch eher sinnvoll erscheint es, vermittelnde Instanzen zu schaffen, die die Transparenz für Betroffene herstellen und über mehr Wissen über die Informationsordnung und mehr rechtliche Mittel hierfür verfügen.[418]

Ob die Datenschutzbeauftragten von Bund und Ländern diese Aufgabe erfüllen können, erscheint zunächst aufgrund ihrer knappen personellen Ressourcen zweifelhaft. Speziell zur Kontrolle des polizeilichen Bereichs stehen den Behörden nur wenige Mitarbeiter*innen zur Verfügung. So berichteten auch die im Rahmen dieser Untersuchung interviewten Mitarbeiter*innen der Datenschutzaufsicht von Problemen bei der Überprüfung von polizeilichen Informationssystemen und Dateien aufgrund mangelnder personeller Ressourcen und Kapazitäten. Insbesondere sei es schwer, die gesetzlich für bestimmte Dateien[419] vorgesehenen Prüfungen durchzuführen und daneben eigeninitiativ tätig zu werden.

Auch die technische Komplexität der Systeme und die teils geringe Kooperationsbereitschaft der Polizei würden die Kontrolle der Informationsordnung erschweren. Auf die Frage, welche besonderen Herausforderungen bei der Kontrolle polizeilicher Datenbanken bestünden, antworte ein*e Mitarbeiter*in der Datenschutzaufsicht:

> „Zum einen sind die Polizeidatenbanken sehr komplex, auch technisch. Es gibt komplexe Rechte- und Rollenkonzepte in dem Bereich, die wir teilweise nur schwer durchschauen. Dafür sind natürlich die Experten von der Polizei vor Ort, die uns diese dann darstellen. Und das machen die auch recht gut. Man merkt aber, dass sie immer nur so weit etwas mitteilen, wie wir fragen. [...] Sobald unsere Fragen kritisch werden, wird dort das Verhalten sehr defensiv

Rn. 3. Dennoch enthält die JI-Richtlinie diverse transparenzwahrende Vorschriften; vgl. insbesondere Art. 12 ff. JI-Richtlinie.

[417] *Stubenrauch*, S. 139.

[418] Vgl. *Kipker*, S. 59.

[419] Wie die Rechtsextremismus-Datei (§ 11 Abs. 2 RED-G) und die Antiterrordatei (§ 10 Abs. 2 ATDG).

> und dann wird man auch sehr schmallippig. Die Herausforderung ist eine Mischung aus technischer Komplexität der Systeme und dem nur bedingten Willen, uns das alles zu offenbaren. Natürlich, ich habe so gut wie nicht erlebt, dass jemand sagt: Ich sage Ihnen das jetzt nicht. Aber man muss es teilweise den Leuten dort aus der Nase ziehen. Das ist unangenehm, das erlebe ich bei anderen Stellen anders." (DSA2)

In den Interviews gaben die Mitarbeiter*innen der Datenschutzaufsicht auch an, dass die Landschaft der vorhandenen polizeilichen Informationsressourcen aktuell faktisch kaum zu überschauen und daher nur schwer kontrollierbar sei. So berichtete exemplarisch ein*e Mitarbeiter*in einer Behörde über die Kontrolle von polizeilichen Informationsressourcen:

> „Natürlich besorgt man sich vorher Unterlagen und Regelungen und, und, und. Und kann die ja durcharbeiten und daraus Schlüsse ziehen. Aber es ist natürlich erstmal nur Theorie. Und wenn man in die Prüfsituation geht, dann wird man mit der Praxis konfrontiert. Und dann ist es eben häufig schwierig, erstmal überhaupt in der ganzen Bandbreite zu verstehen, was da abläuft. Das ist manchmal sogar für diejenigen, die da drin arbeiten, nicht immer ganz klar. Und häufig kennen selbst die Leute, die davor sitzen, immer nur ihren kleinen Bereich, mit dem sie arbeiten. Da können sie was dazu sagen. Aber sobald man nach rechts oder links fragt, dann wird auf einen Techniker verwiesen. Oder Support-Leute, oder den Hersteller. Weil sie das selber nicht verstehen oder wissen, wie das abläuft. Und das macht solche Prüfungen natürlich sehr aufwändig." (DSA4)

Die Datenschutzaufsichtsbehörden haben schließlich gegenüber der Polizei teilweise nur eingeschränkte Befugnisse. In mehreren Bundesländern sind sie nicht, oder nur bei erheblichen Verstößen befugt, verbindlich auf die Datenverarbeitungen der Polizei einzuwirken und Missbräuche effektiv abzustellen.[420]

Die Transparenz der Nutzung der Informationsordnung ließe sich neben der Datenschutzaufsicht möglicherweise auch durch eine Instanz sicherstellen, die allgemein mit der Kontrolle der Polizei befasst ist. Unabhängige Stellen zur Aufsicht über die Polizei existieren bereits in vielen europäischen Staaten;[421] die Schaffung derartiger Stellen

---

[420] Dies widerspricht der unionsrechtlichen Vorgabe aus Art. 47 Abs. 2 JI-Richtlinie, wonach die Datenschutzaufsicht mit wirksamen Abhilfebefugnissen auszustatten ist. Eine verbesserte Ausstattung der Datenschutzaufsicht mit Ressourcen und Befugnissen zur Kontrolle der polizeilichen Datenverarbeitung ist daher nicht nur wünschenswert, sondern auch rechtlich zwingend geboten; vgl. zu dieser Problematik *Golla*, KriPoZ 2019, 238 (242 ff.).

[421] Das britische Independent Office for Police Conduct setzt sich beispielsweise systematisch mit dem Missbrauch polizeilicher Datenbanken auseinander und kategorisiert diesen als eigene Form polizeilichen Fehlverhaltens.

schreitet auch in Deutschland voran.[422] Mit Fragen der Datenverarbeitung sind Polizeibeauftragte bisher nur wenig befasst. Ihre Befassung damit hätte gegenüber der Datenschutzaufsicht den Vorzug, dass eine solche Stelle mit den Strukturen der Polizei besser vertraut ist. Zudem könnte sie Risiken und Probleme der Informationsordnung betrachten, die durch das Datenschutzrecht nicht abgedeckt sind. Allerdings wäre kaum zu erwarten, dass eine solche Stelle die technisch komplexe Informationsordnung der Kriminalbehörden von vornherein leichter durchschauen könnte als die Datenschutzaufsicht.

In jedem Fall sollte die Datenschutzaufsicht nach derzeitigem Stand durchweg mit Befugnissen ausgestattet werden, um auf kriminalbehördliche Datenverarbeitungen einzuwirken. Um diese Datenverarbeitungen transparenter zu machen, könnten zusätzliche proaktive Informationspflichten der Kriminalbehörden bzw. Mitwirkungspflichten der Aufsicht geregelt werden, wenn neue Informationsressourcen eingerichtet oder bestehende Ressourcen erheblich verändert werden.

Zwischenergebnis

Es sind zahlreiche Änderungen im Strafprozessrecht, im Polizeirecht und in den begleitenden Regelungen zum Datenschutz möglich, die dazu beitragen könnten, den Ist-Zustand der kriminalbehördlichen Informationsordnung ihrem Soll-Zustand anzunähern.

Auf Grundlage von Art. 87 Abs. 1 Satz 2 GG könnten die Aufgaben des Bundeskriminalamtes als Zentralstelle für die polizeiliche Informationsordnung konkretisiert werden. So könnten ihm ausdrücklich die Aufgaben zugewiesen werden, die Kompatibilität bzw. Verknüpfbarkeit der bestehenden polizeilichen Informationsressourcen sicherzustellen und die Qualität der im polizeilichen Informationsverbund gespeicherten Daten zu sichern. Auf diese Weise könnte das Bundeskriminalamt einen stärkeren Beitrag als bisher dazu leisten, dass die Systeme die Anforderungen ihrer Anwender*innen erfüllen. Der Behörde könnten außerdem weitergehende Befugnisse als bisher eingeräumt werden, um das informationelle Handeln der Polizei zu koordinieren. Dafür kämen eingeschränkte Weisungsbefugnisse gegenüber den Landespolizeibehörden etwa zur Mitteilung spezifischer Informationen oder zur Festlegung von Richtlinien zur standardisierten Speicherung in Betracht.

Bestehende Befugnisse für informationsordnende Handlungen der Kriminalbehörden könnten zusammengeführt und in ihren Voraussetzungen vereinheitlicht werden.

---

[422] *Piening/Kühne/Töpfer*, Bürgerrechte & Polizei/CILIP 130 (4/2022), 17 ff.

Hierdurch könnte ihre Anwendbarkeit erleichtert werden. Die Möglichkeiten zur Umstrukturierung der informationsordnenden Befugnisse sind durch die Kompetenzordnung des Grundgesetzes stark eingeschränkt. Auf Grundlage der konkurrierenden Gesetzgebungskompetenz des Bundes für das gerichtliche Verfahren nach Art. 74 Abs. 1 Nr. 1 GG könnte jedoch zumindest für das strafprozessuale Vorfeld eine weitergehende und eigenständigere Regelung geschaffen werden als in den §§ 483, 484 StPO, die für die Voraussetzungen der Datenverarbeitung in mehreren wichtigen Fällen auf das Polizeirecht verweisen. Daneben kommt auch eine „weiche" Harmonisierung der informationsordnenden Befugnisse in Betracht, die ohne rechtliche Verbindlichkeit auf eine Vereinheitlichung im Polizeirecht hinwirken würde. So könnte der neue Musterentwurf eines Polizeigesetzes ein einheitliches Modell für informationsverarbeitende Befugnisse der Polizei vorsehen.

Die notwendigen Anlässe für informationsordnende Handlungen könnten spezifischer gefasst werden. Hierdurch könnte für die Anwender*innen mehr Rechtsklarheit geschaffen und das Vorgehen für die Betroffenen vorhersehbarer gemacht werden. Bezogen auf die Speicherung von Daten könnten sowohl deren Zwecke als auch die Anforderungen an die Prognose, inwiefern die Speicherung zur Erfüllung des jeweiligen Zweckes dienlich ist, gesetzlich geschärft werden. Namentlich § 484 StPO macht die Grundlagen der Prognose, auf deren Grundlage Daten zu Zwecken der Strafverfolgungsvorsorge gespeichert werden dürfen, nicht hinreichend deutlich.

Schließlich könnten die bislang wenig ausgeprägten Regelungen über die Datenstrukturen sowie Verfahren und Organisation der Datenverarbeitung geschärft werden. Hier bieten sich insbesondere Möglichkeiten, die Qualität der Daten strukturell zu verbessern, ihre Verknüpfung zu erleichtern und die Transparenz der Vorgänge für die Betroffenen zu erhöhen. Durch nähere Regelungen zu Verfahren und Organisation könnten auch Schwierigkeiten bei der Festlegung von Anlässen für informationsordnende Tätigkeiten ein Stück weit zu kompensiert werden. Näher geregelt werden könnten konkret die prozeduralen Anforderungen an die Einspeisung und Validierung von Informationen, die Fristen für die Überprüfung von Daten, die Möglichkeiten zur Einräumung von Zugriffsrechten sowie Aspekte der Transparenz und Kontrollierbarkeit von Informationsressourcen insbesondere durch die Datenschutzaufsicht.

Zusammenfassung und Gesamtergebnis

I.

Informationsordnende Tätigkeiten wie das Speichern von Daten und das Errichten von Systemen hierfür sind seit eh und je von großer Bedeutung für die Polizei und die Staatsanwaltschaften. Sie bilden die Grundlage für Ermittlungen und operative Maßnahmen. Welche Daten auf welche Art und Weise gespeichert und strukturiert werden, kann diese Maßnahmen erheblich beeinflussen. Die Informationsressourcen der Kriminalbehörden sind außerdem ein wichtiger Bestandteil der nationalen und europäischen Sicherheitsarchitektur. Dies gilt besonders für die im Vergleich zu jenen der Staatsanwaltschaften weiter entwickelten Systeme der Polizei.

Die Bedeutung informationsordnender Tätigkeiten hat mit der technischen Entwicklung der hierfür zur Verfügung stehenden Möglichkeiten zugenommen. Einen tiefen Einschnitt bedeutete in dieser Hinsicht die Einführung der elektronischen Datenverarbeitung in der öffentlichen Verwaltung, die die informationsordnenden Tätigkeiten der Polizei seit Ende der 1960er-Jahre stark geprägt hat. Mit dem technischen Wandel haben sich auch die Anforderungen der Anwender*innen an die kriminalbehördliche Informationsordnung sowie ihre rechtlichen Rahmenbedingungen verändert. So gehört die schnelle und mobile Abrufbarkeit aktueller Daten aus polizeilichen Informationssystemen heute zu den selbstverständlichen Erwartungen an die Informationsordnung.

Aktuell entwickeln sich vor allem die Bedürfnisse zur Auswertung und Verknüpfung von Daten aufgrund neuer technischer Möglichkeiten weiter. Sie bilden einen Schwerpunkt bei aktuellen Erneuerungen der Informationsordnung, etwa im Rahmen des Programmes Polizei 20/20. Diese Ansätze lassen sich auch im Kontext einer allgemeinen Tendenz zur Vernetzung im Sicherheitsbereich betrachten. Für die Betroffenen, über die Informationen in kriminalbehördlichen Ressourcen gespeichert sind, haben mit den neuen technischen Möglichkeiten die Risiken zugenommen, dass sie in der freien Entfaltung ihrer Persönlichkeit beeinträchtigt werden. Die leichte Verfügbarkeit von Daten erhöht die Wahrscheinlichkeit, durch informationelle Tätigkeiten stigmatisiert und kriminalisiert werden. Die neuen Bestrebungen zur Verknüpfung von Datenbeständen verschärfen diese Problematik.

II.

Im Verhältnis zu ihrer tatsächlichen Bedeutung und angesichts ihrer Risiken sind die rechtlichen Anforderungen an die informationsordnenden Tätigkeiten der Kriminalbehörden nicht sonderlich ausgeprägt. Die Funktionen der Informationssysteme und die Anforderungen an sie sind kaum normiert. Erst infolge der durch die elektronische Datenverarbeitung bedingten Risiken für die Betroffenen wurden die Befugnisse für informationsordnende Tätigkeiten der Kriminalbehörden überhaupt geregelt. Mit der verfassungsrechtlichen Anerkennung des Rechts auf informationelle Selbstbestimmung wurden Verarbeitungen personenbezogener Daten durch staatliche Stellen unter einen allgemeinen Gesetzesvorbehalt gestellt. Die auf dieser Grundlage im Strafprozess- und Polizeirecht geschaffenen Befugnisse stellen sich als notwendige Ergänzungen dar, um informationsordnende Tätigkeiten in rechtsstaatlichen Bahnen zu halten. Die informationsordnenden Befugnisse lassen sich nur eingeschränkt mit herkömmlichen kriminalbehördlichen Befugnissen vergleichen und bedürfen einer eigenständigen Betrachtung.

Allerdings wurden diese Befugnisse seit ihrer Einführung in Folge des Volkszählungsurteils des Bundesverfassungsgerichts kaum verändert. Auch die JI-Richtlinie der Europäischen Union hat insofern nicht zu beachtenswerten neuen Anforderungen geführt. Die Befugnisse weisen einige Schwächen auf, die sowohl zulasten ihrer Anwendbarkeit als auch zulasten des Schutzes der Informationssubjekte gehen. Sie sind uneinheitlich, weit gefasst und regeln die erforderlichen Anhaltspunkte und die Maßstäbe der Prognose für eine Speicherung von personenbezogenen Daten nicht oder nur teilweise. In dieser Hinsicht sollte besonders § 484 StPO nachgeschärft werden. Allerdings wäre auch eine Anpassung und Harmonisierung der auf Bundes- und Landesgesetze verteilten Befugnisse zur Informationsordnung im Polizeirecht wünschenswert. Eine solche könnte im Rahmen eines neuen Musterpolizeigesetzes und dessen Umsetzung geschehen.

Einer verbindlichen Harmonisierung auf Bundesebene ist das Recht der kriminalbehördlichen Informationsordnung aufgrund der getrennten Kompetenzen für Gefahrenabwehr und Strafverfolgung nur sehr eingeschränkt zugänglich, obwohl sich diese beiden Bereiche bei informationsordnenden Tätigkeiten kaum sauber voneinander abgrenzen lassen. Auf Grundlage der konkurrierenden Gesetzgebungskompetenz des Bundes für das gerichtliche Verfahren nach Art. 74 Abs. 1 Nr. 1 GG könnte allenfalls eine eigenständigere Regelung informationsordnender Befugnisse für das strafprozessuale Vorfeld geschaffen werden.

Weiter sind die Regelungen über die Speicherung von Daten nach einem Freispruch problematisch. Da ein Freispruch als Bestätigung der Unschuldsvermutung zu verstehen ist, erscheint eine Speicherung von Daten aus einem Strafverfahren nach einem solchen als grundsätzlich unzulässig. Neben den Befugnissen zur Datenverarbeitung sollten außerdem die begleitenden Regelungen zu den Speicherfristen von Daten hierin, der Sicherung der Datenqualität, den Zugriffsmöglichkeiten auf Informationsressourcen und ihre Kontrolle geschärft werden. Der empirische Teil dieser Untersuchung hat gezeigt, dass gerade bezüglich der Sicherung der Datenqualität und der Kontrolle der Informationsordnung in der Praxis erhebliche Schwierigkeiten bestehen. Die Datenqualität wird zudem im Vergleich zu den Anforderungen der Verfügbarkeit und Verknüpfbarkeit von Daten zumindest dem äußeren Anschein nach mit geringerer Priorität behandelt. Dies ist schon deshalb problematisch, weil eine hohe Datenqualität nicht nur im Sinne der Informationssubjekte, sondern auch unabdingbar für eine sinnvolle Verknüpfung und Auswertung von Daten ist. Die Datenqualität könnte konkret etwa dadurch gestärkt werden, dass für die Einspeisung von Daten in Informationssysteme und ihre fortlaufende Kontrolle explizit gesetzliche Standards geregelt werden.

III.

Aus praktischer Sicht bereiten schließlich das stetige Wachstum der Menge vorhandener Informationen und die Inkompatibilität der verschiedenen Systeme Herausforderungen bei der Nutzung der kriminalbehördlichen Informationsordnung. Diese Faktoren beeinträchtigen besonders die Verfügbarkeit und Verknüpfbarkeit von Informationen. Zwar werden sich die kriminalbehördliche Informationsordnung – als organisch gewachsenes Gefüge von Systemen – und ihre Inhalte nicht innerhalb von kurzer Zeit harmonisieren und „entschlacken“ lassen. Allerdings könnten gezielte Maßnahmen unter Federführung des Bundeskriminalamtes als Zentralstelle für die polizeiliche Informationsordnung zumindest im polizeilichen Bereich dazu beitragen, die Anforderungen besser zu erfüllen. Hierfür könnten der Aufgabenbereich des Bundeskriminalamts konkretisiert und seine Befugnisse – etwa in Form von Weisungsrechten gegenüber den speichernden Behörden – auf Grundlage von Art. 87 Abs. 1 Satz 2 GG gezielt erweitert werden.

IV.

Vor allem die polizeiliche Informationsordnung steht aktuell auf nationaler wie auf internationaler Ebene vor einem Umbruch. Das Projekt des neuen „Datenhauses“ beim Bundeskriminalamt und des „Data Lake“ bei Europol unterstreichen die Bedeutung von vernetzten Informationssystemen für die Kriminalitätsbekämpfung der Zukunft. So wichtig derartige Systeme für die Arbeit von Polizei und Staatsanwaltschaften sind, so undurchsichtig ist ihr Wirken für die Öffentlichkeit und die Betroffenen. Diese Arbeit hat die Anforderungen an die Informationsordnung und ihre Risiken betrachtet sowie Möglichkeiten zu ihrer rechtlichen Handhabe aufgezeigt. Das Thema wird aus rechts- und sozialwissenschaftlicher Sicht allerdings Anlass für weitere Untersuchungen geben. Empirisch sind die Handhabe und die Risiken derartiger Systeme bisher nur ansatzweise erforscht. Die rechtswissenschaftliche Forschung kann hieran anknüpfen, um die normativen Anforderungen für den Einsatz der Systeme weiterzuentwickeln. Gerade ihre Intransparenz gibt Anlass, die kriminalbehördliche Informationsordnung aus wissenschaftlicher Sicht weiter kritisch zu begleiten.

Literaturverzeichnis

Abbühl, Anicee: Der Aufgabenwandel des Bundeskriminalamts, Von der Zentralstelle zur multifunktionalen Intelligence-Behörde des Bundes, Stuttgart 2010.

Aden, Hartmut: Das Bundeskriminalamt, Intelligence-Zentrale oder Schaltstelle des bundesdeutschen Polizeisystems?, Bürgerrechte & Polizei/CILIP 62 (1/1999), 6-17.

Aden, Hartmut: Koordination und Koordinationsprobleme im ambivalenten Nebeneinander: Der polizeiliche Informationsaustausch im EU-Mehrebenensystem, dms 2014, 55-73.

Aden, Hartmut: Besserer Datenschutz – auch für Polizei und Strafjustiz?, vorgänge 2018, 93-102.

Aden, Hartmut; *Fährmann*, Jan: Polizeirecht vereinheitlichen? Kriterien für Muster-Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive, Berlin 2018.

Aden, Hartmut; *Fährmann*, Jan; *Bosch*, Alexander: Technologieentwicklung und Polizei: intensivere Grundrechtseingriffe auch ohne Gesetzesänderung, KrimJ 2020, 135-148.

Ahlf, Ernst-Heinrich: Der Begriff des "Eingriffes" insbesondere bei kriminalpolizeilicher Tätigkeit und die sog. "Schwellentheorie" zu § 163 Abs. 1 StPO, Die Polizei 1983, 41-53.

Ahlf, Ernst-Heinrich: Das Bundeskriminalamt als Zentralstelle, Wiesbaden 1985 (zitiert: *Ahlf*, Das Bundeskriminalamt).

Ahlf, Ernst-Heinrich: Polizeiliche Kriminalakten (KpS), Wiesbaden 1988 (zitiert: *Ahlf*, Polizeiliche Kriminalakten).

Ahlf, Ernst-Heinrich: Rechtsprobleme der polizeilichen Kriminalaktenführung, KritV 1988, 136-156.

Albers, Marion: Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001 (zitiert: *Albers*, Determination).

Albers, Marion: Information als Dimension im Recht, Rechtstheorie 33 (2002), 51-89.

Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden 2005 (zitiert: *Albers*, Informationelle Selbstbestimmung).

Albers, Marion: Die Komplexität verfassungsrechtlicher Vorgaben für das Wissen der Verwaltung, Zugleich ein Beitrag zur Systembildung im Informationsrecht, in: Spiecker gen. Döhmann, Indra; Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, 50-69.

Albers, Marion: Sicherheitsbehördliche Vernetzung und Datenschutz, in: Seckelmann, Margrit (Hrsg.): Digitalisierte Verwaltung, Vernetztes E-Government, 2. Aufl., Berlin 2019, 509-534.

Alberts, Hans-Werner: Das neue Bremische Polizeigesetz, NVwZ 1983, 585-588.

Albrecht, Hans-Jörg; *Dorsch*, Claudia; *Krüpe*, Christiane: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg im Breisgau 2003.

Albrecht, Horst: Im Dienst der Inneren Sicherheit, Die Geschichte des Bundeskriminalamtes, Wiesbaden 1988.

Amelung, Knut: Probleme des Rechtsschutzes gegen strafprozessuale Grundrechtseingriffe, NJW 1979, 1687-1692.

Arbeitskreis Polizeirecht: Alternativentwurf einheitlicher Polizeigesetze des Bundes und der Länder, Neuwied 1979.

Arbeitskreis deutscher, österreichischer und schweizerischer Strafrechtslehrer, Alternativ-Entwurf Reform des Ermittlungsverfahrens (AE-EV), München 2001 (zitiert: Arbeitskreis AE).

Ariel, Barak: Advocate, Technology in Policing, in: Weisburd, David; Braga, Antony A. (Hrsg.), Police Innovation, Contrasting Perspectives, 2. Aufl., Cambridge 2019, 485-516.

Von Arnauld, Andreas: Die Europäisierung des Rechts der inneren Sicherheit, JA 2008, 327-335.

Arzt, Clemens: Verbunddateien des Bundeskriminalamts – Zeitgerechte Flurbereinigung, NJW 2011, 352-354.

Arzt, Clemens; *Eier*, Jana: Zur Rechtmäßigkeit der Speicherung personenbezogener Daten in "Gewalttäter"-Verbunddateien des Bundeskriminalamts, DVBl. 2010, 816-824.

Arzt, Clemens: Umsetzung des europäischen Datenschutzrechts für die Polizei, SächsPVDG und SächsDSUG – eine kritische Bestandsaufnahme, SächsVBl. 2019, 345-352.

Augsberg, Ino: Informationsverwaltungsrecht, Zur kognitiven Dimension der rechtlichen Steuerung von Verwaltungsentscheidungen, Tübingen 2014.

Aulehner, Josef: Polizeiliche Gefahren- und Informationsvorsorge, Grundlagen, Rechts- und Vollzugsstrukturen, dargestellt auch im Hinblick auf die deutsche Beteiligung an einem Europäischen Polizeiamt (EUROPOL), Berlin 1998.

Bäcker, Matthias: Das G 10 und die Kompetenzordnung, DÖV 2011, 840-848.

Bäcker, Matthias: Kriminalpräventives Strafrecht und polizeiliche Kriminalprävention, in: Baumeister, Peter; Roth, Wolfgang; Ruthig, Josef (Hrsg.), Staat, Verwaltung und Rechtsschutz, Festschrift für Wolf-Rüdiger Schenke zum 70. Geburtstag, Berlin 2011, 331-354 (zitiert: *Bäcker*, in: FS Schenke).

Bäcker, Matthias: Kriminalpräventionsrecht, Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, Tübingen 2015 (zitiert: *Bäcker*, Kriminalpräventionsrecht).

Bäcker, Matthias: Stellungnahme zu dem Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes vom 16. März 2017, Ausschussdrucksache 18(4)806 D (zitiert: *Bäcker*, Stellungnahme BKAG 2018).

Bäcker, Matthias: *Der Umsturz kommt zu früh: Anmerkungen zur polizeilichen Informationsordnung nach dem neuen BKA-Gesetz, Verfassungsblog vom 8. Juni 2017*, abrufbar unter https://verfassungsblog.de/der-umsturz-kommt-zu-frueh-anmerkungen-zur-polizeilichen-informationsordnung-nach-dem-neuen-bka-gesetz/.

Bäcker, Matthias: Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in: Hill, Hermann/Kugelmann, Dieter/Martini, Mario (Hrsg.), Perspektiven der digitalen Lebenswelt, Baden-Baden 2017, 63-88.

Bäcker, Matthias: Sicherheitsarchitektur und Terrorismusbekämpfung, Stellungnahme für die Anhörung des 1. Untersuchungsausschusses der 19. Wahlperiode des Deutschen Bundestages am 17. Mai 2018, Ausschussdrucksache 19(25)249 (zitiert: *Bäcker*, Sicherheitsarchitektur und Terrorismusbekämpfung).

Bäcker, Matthias: Weitere Zentralisierung der Terrorismusbekämpfung?, GSZ 2018, 213-219.

Bäcker, Matthias: Von der Gefahr zum „Gefährder", in: Kulick, Andreas; Goldhammer, Michael (Hrsg.), Der Terrorist als Feind?, Tübingen 2020, 147-165.

Baldus, Manfred: Entgrenzungen des Sicherheitsrechts – Neue Polizeirechtsdogmatik?, Die Verwaltung 2014, 1-23.

Balzacq, Thierry: The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies, JCMS 2008, 75-100.

Bateson, Gregory: Ökologie des Geistes, Anthropologische, psychologische, biologische und epistemologische Perspektiven, Berlin 1985.

Barczak, Tristan: BKAG, Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, Baden-Baden, 2023.

Baumann, Karsten: Vernetzte Terrorismusbekämpfung oder Trennungsgebot?, DVBl. 2005, 798-805.

Becker, Bernd: Zentralstellen gemäß Art. 87 Abs. 1 GG, Analyse eines vielseitig verwendbaren Behördentyps, DÖV 1978, 551-555.

Beck'scher Online-Kommentar Datenschutzrecht, herausgegeben von Wolff, Heinrich Amadeus; Brink, Stefan, 44. Edition, München 2023 (zitiert: *Bearbeiter*, in: BeckOK-Datenschutzrecht).

Beck'scher Online-Kommentar StGB, herausgegeben von von Heintschel-Heinegg, Bernd, 57. Edition, München 2023 (zitiert: *Bearbeiter*, in: BeckOK-StGB).

Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, herausgegeben von Graf, Jürgen, 47. Edition, München 2023 (zitiert: *Bearbeiter*, in: BeckOK-StPO).

Beck'scher Online-Kommentar Grundgesetz, herausgegeben von Epping, Volker; Hillgruber, Christian, 55. Edition, München 2023 (zitiert: *Bearbeiter*, in: BeckOK-GG).

Beck'scher Online-Kommentar Polizeirecht Baden-Württemberg, herausgegeben von Möstl, Markus; Trurnit, Christoph, 29. Edition, München 2023 (zitiert: *Bearbeiter*, in: BeckOK-BWPolG).

Bedner, Mark; *Ackermann*, Tobias: Schutzziele der IT-Sicherheit, DuD 2010, 323-328.

Behrendes, Udo: Von der Eilzuständigkeit zur Allzuständigkeit?, Die Polizei 1988, 220-228.

Benda, Ernst: Das Recht auf informationelle Selbstbestimmung und die Rechtsprechung des Bundesverfassungsgerichts zum Datenschutz, DuD 1984, 86-90.

Belz/Mussmann/Kahlert/Sander: Polizeigesetz für Baden-Württemberg, herausgegeben von Kahlert, Henning; Sander, Gerald G., 8. Aufl., Stuttgart 2015.

Berg, Wilfried: Vom Wettlauf zwischen Recht und Technik, Am Beispiel neuer Regelungsversuche im Bereich der Informationstechnologie, JZ 1985, 401-407.

Bergemann, Nils: Die Freiheit im Kopf? – Neue Befugnisse für die Nachrichtendienste, Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, NVwZ 2015, 1705-1710.

Bergien, Rüdiger: „Big Data" als Vision, Computereinführung und Organisationswandel in BKA und Staatssicherheit (1967–1989), Zeithistorische Forschungen, 2017, 258-285.

Bethge, Herbert: Staatszwecke im Verfassungsstaat, 40 Jahre Grundgesetz, DVBl. 1989, 841-850.

Beyer, Lothar: Informationsmanagement und öffentliche Verwaltung, Perspektiven und Grenzen, Wiesbaden 1992.

Bizer, Johann: Vom Eros der Fragestellung: Die Rechtsinformatik auf der Suche nach ihrem Gegenstand, in: Taeger, Jürgen; Wiebe, Andreas (Hrsg.), Informatik – Wirtschaft – Recht, Regulierung in der Wissensgesellschaft, Festschrift für Wolfgang Kilian, Baden-Baden 2004, 39-58 (zitiert: *Bizer*, in: FS Kilian).

Boehm, Franziska; *Cole*, Mark D.: Vorratsdatenspeicherung und (k)ein Ende?, MMR 2014, 569-570.

Boehme-Neßler, Volker: Unscharfes Recht. Rechtstheoretische Überlegungen zur Vermessung des virtuellen Raums, in: Hill, Hermann; Schliesky, Utz (Hrsg.), Die Vermessung des virtuellen Raums, E-Volution des Rechts- und Verwaltungssystems III, Baden-Baden 2012, 237-264.

Boge, Heinrich: Thesen zur Funktion und Bedeutung der Datenverarbeitung bei der Polizei, 10 Jahre INPOL-Fahndungssystem, Kriminalistik 1982, 619-623.

Böse, Martin: Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, Göttingen 2007.

Böse, Martin: Europäisches Strafrecht, mit polizeilicher Zusammenarbeit, in: Enzyklopädie Europarecht, herausgegeben von Hatje, Armin; Müller-Graff, Peter-Christian, Band 9, Baden-Baden 2013.

Braun, Frank; *Albrecht*, Florian: Der Freiheit eine Gasse? Anmerkungen zur „Überwachungsgesamtrechnung" des Bundesverfassungsgerichts, VR 2017, 151-155.

Braun, Karl-Heinz: Die vorbeugende Bekämpfung von Straftaten als polizeiliche Aufgabe im Zusammenhang mit der Problematik der polizeilichen Kriminalakten und erkennungsdienstlichen Unterlagen, Die Polizei 1989, 213-222.

Brinkhoff, Sven: Big Data Mining by the Dutch Police: Criteria for a Future Method of Investigation, Eur J Secur Res 2017 (2), 57-69.

Britz, Gabriele: Schutz informationeller Selbstbestimmung gegen schwerwiegende Grundrechtseingriffe – Entwicklungen im Lichte des Vorratsdatenspeicherungsurteils, JA 2011, 81-86.

Britz, Gabriele: Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, Tübingen 2010, 561-596 (*Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft).

Britz, Gabriele: Freie Entfaltung durch Selbstdarstellung, Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, Tübingen 2007.

Britz, Gabriele: Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1-11.

Brodersen, Kilian: Das Strafverfahrensänderungsgesetz 1999, NJW 2000, 2536-2542.

Brodowski, Dominik: Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht, Zur rechtsstaatlichen und rechtspraktischen Notwendigkeit eines einheitlichen operativen Ermittlungsrechts, Tübingen 2016.

Broemel, Roland; *Trute*, Hans-Heinrich: Alles nur Datenschutz? Zur rechtlichen Regulierung algorithmenbasierter Wissensgenerierung, Berliner Debatte Initial 27 (2016), 50–65.

Bull, Hans Peter: Datenschutz contra Amtshilfe, Von der „Einheit der Staatsgewalt" zur „informationellen Gewaltenteilung", DÖV 1979, 689-696.

Bull, Hans Peter: Die Grundprobleme des Informationsrechts, Antrittsvorlesung als Cobbenhagen-Professor für Recht der Informationsbeziehungen und vergleichendes Staats- und Verwaltungsrecht an der katholischen Universität Tilburg, Zwolle 1985.

Bull, Hans Peter: Was ist Informationsrecht?, iur 1986, 287-293.

Bull, Hans Peter: Die „Sicherheitsgesetze" im Kontext von Polizei- und Sicherheitspolitik, in: Bull, Hans Peter (Hrsg.), Sicherheit durch Gesetze?, Baden-Baden 1987, 15-43.

Bull, Hans Peter: Zweifelsfragen um die informationelle Selbstbestimmung – Datenschutz als Datenaskese?, NJW 2006, 1617-1624.

Bull, Hans Peter: Über die rechtliche Einbindung der Technik, Juristische Antworten auf Fragen der Technikentwicklung, Der Staat 58 (2019), 57–100.

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes vom 10. März 2017, Ausschussdrucksache 18(4)806 A (zitiert: BfDI, Stellungnahme BKAG 2018).

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 14. Februar 2019 (zitiert: BfDI, Stellungnahme StPO 2019).

Bundesministerium des Inneren, Polizei 2020, White Paper, Berlin 2016 (zitiert: BMI, Polizei 2020).

Bund-Länder-Arbeitsgruppe Überprüfung und Anpassung der beim Bundeskriminalamt geführten Datei „Gewalttäter Sport“, Abschlussbericht, 2016, abrufbar unter https://cdn.netzpolitik.org/wp-upload/2017/01/blag-gewaelttaeter-sport-abschlussbericht.pdf.

Burczyk, Dirk: Von der Kartei zum „Datenhaus“, Eine kleine Geschichte polizeilicher Datenverarbeitung, Bürgerrechte & Polizei/CILIP 121 (4/2020), 16-25.

Burkert, Herbert: Informationsrecht als Methode, in: Garstka, Hansjürgen/Coy, Wolfgang (Hrsg.), Wovon – für wen – wozu, Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis, Berlin 2014, 177-193 (zitiert: *Burkert*, in: GS Steinmüller).

Busch, Heiner: INPOL-neu, Informatisierung des polizeilichen Alltags, Bürgerrechte & Polizei/CILIP 76 (3/2003), 12-19.

Busch, Heiner; *Funk*, Albrecht; *Kauß*, Udo; *Narr*, Wolf-Dieter; *Werkentin*, Falco: Die Polizei in der Bundesrepublik, Frankfurt am Main 1985.

Byrne, James; *Marx*, Gary: Technological Innovations in Crime Prevention and Policing, A Review of the Research on Implementation and Impact, Cahiers Politiestudies 3/2011, 17-40.

Chan, Janet; *Moses*, Lyria Bennett: Is Big Data challenging criminology?, Theoretical Criminology 20 (2016), 21-39.

Cobler, Sebastian: Herold gegen alle – Gespräch mit dem Präsidenten des Bundeskriminalamts, Transatlantik 11/1980, 29-40.

Collin, Peter; *Spiecker gen. Döhmann*, Indra: Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts – ein Problemaufriss –, in: Spiecker gen. Döhmann, Indra; Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, 3-25.

Coudert, Fanny: The Europol Regulation and Purpose Limitation: From the ‚Silo-Based Approach‘ to... What Exactly?, European Data Protection Law Review 2017, 313-324.

Creemers, Niklas; *Guagnin*, Daniel; Datenbanken in der Polizeipraxis: Zur computergestützten Konstruktion von Verdacht, KrimJ 2014, 134-148.

Creemers, Niklas: Über Datenbanken und Datenanalysetools, in: Grutzpalk, Jonas (Hrsg.), Polizeiliches Wissen, Formen, Austausch, Hierarchien, Frankfurt am Main 2016, 101-129.

Danne, Marius: Prävention und Repression im Sicherheitsrecht, Grenzen juristischer Begriffsbildung, Berlin 2022.

Darnstädt, Thomas: Gefahrenabwehr und Gefahrenvorsorge, Frankfurt am Main 1983.

Darnstädt, Thomas: Ein personenbezogener Gefahrbegriff – Analyse der Bedingungen des Bundesverfassungsgerichts an Vorfeld-Ermächtigungen im BKA-Gesetz, DVBl. 2017, 88-96.

Deleuze, Gilles: Postskriptum über die Kontrollgesellschaften, in: Deleuze, Gilles: Unterhandlungen – 1972-1990, Frankfurt am Main 1993, 254-262.

Denninger, Erhard: Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf inforationelle Selbstbestimmung, ZRP 1981, 231-235.

Denninger, Erhard: Das Recht auf informationelle Selbstbestimmung, Folgerungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts, in: Hohmann, Harald (Hrsg.), Freiheitssicherung durch Datenschutz, Frankfurt am Main 1987, 127-172.

Denninger, Erhard: Der Präventions-Staat, KJ 1988, 1-15.

Denninger, Erhard: Verfassungsrechtliche Grenzen polizeilicher Datenverarbeitung insbesondere durch das Bundeskriminalamt, CR 1988, 51-60.

Derin, Benjamin; *Meyer,* Christian; *Wegner*, Friederike: Der Blick nach vorn im Daten-Dschungel, Datafizierung und Prävention, Bürgerrechte & Polizei/CILIP 121 (4/2020), 3-15.

Deutscher Richterbund, Presseerklärung vom 7. Februar 1986, DRiZ 1986, 110.

Dickopf, Paul; *Holle*, Rolf: Das Bundeskriminalamt, Bonn 1971.

Von Dietel, Rainer: Zur Zentralstellenkompetenz des Bundeskriminalamts, DVBl. 1982, 939-940.

Dietlein, Johannes: Die Lehre von den grundrechtlichen Schutzpflichten, Berlin 1992.

Disco, Cornells; *van der Meulen*, Barend: Introduction, in: Disco, Cornells; van der Meulen, Barend (Hrsg.), Getting New Technologies Together, Studies in Making Sociotechnical Order, Berlin 1998, 1-13.

Dix, Alexander: Rechtsfragen der Polizeilichen Datenverarbeitung, JURA 1993, 571-578.

Di Fabio, Udo: Risikoentscheidungen im Rechtsstaat, Zum Wandel der Dogmatik im öffentlichen Recht, insbesondere am Beispiel der Arzneimittelüberwachung, Tübingen 1994.

Dolata, Ulrich; *Werle*, Raymund: „Bringing technology back in": Technik als Einflussfaktor sozioökonomischen und institutionellen Wandels, in: Dolata, Ulrich; Werle, Raymund (Hrsg.), Gesellschaft und die Macht der Technik, Sozioökonomischer und institutioneller Wandel durch Technisierung, Frankfurt am Main 2007, 15-43.

Drackert, Stefan: Die Risiken der Verarbeitung personenbezogener Daten, Eine Untersuchung zu den Grundlagen des Datenschutzrechts, Berlin 2014.

Dreier, Horst: Erkennungsdienstliche Maßnahmen im Spannungsfeld von Gefahrenabwehr und Strafverfolgung, JZ 1987, 1009-1017.

Dreier, Horst: Grundgesetz, Kommentar, 3. Aufl., Tübingen 2013 ff.

Dumortier, Jos: Hat das Fachgebiet „Recht und Informatik" noch Zukunft?, in: Taeger, Jürgen; Wiebe, Andreas (Hrsg.), Informatik – Wirtschaft – Recht, Regulierung in der Wissensgesellschaft, Festschrift für Wolfgang Kilian, Baden-Baden 2004, 59-70 (zitiert: *Dumortier*, in: FS Kilian).

Eisenberg, Ulrich; *Kölbel*, Ralf: Kriminologie, 7. Aufl., Tübingen 2017.

Eisenberg, Ulrich: Informationelle Selbstbestimmung und gesetzgeberische Unbestimmtheiten in § 81g Abs. 1 StPO, in: Eser, Albin; Goydke, Jürgen; Maatz, Kurt Rüdiger; Meurer, Dieter (Hrsg.), Strafverfahrensrecht in Theorie und Praxis, Festschrift für Lutz Meyer-Goßner zum 65. Geburtstag, München 2001, 293.305 (zitiert: *Eisenberg*, in: FS Meyer-Goßner).

Eisenberg, Ulrich; *Singelnstein*, Tobias: Speicherung von DNA-Identifizierungsmustern als erkennungsdienstliche Maßnahme zur „Strafverfolgungsvorsorge" trotz Nichtverurteilung?, GA 2006, 169-182.

Emmerig, Ernst: Die Doppelfunktion der Polizei, DVBl. 1958, 338-344.

Ericson, Richard V.; *Haggerty*, Kevin D.: Policing the Risk Society, Toronto und Buffalo 1997.

Ernesti, Günter: Informationsverbund Justiz – Polizei, NStZ 1983, 57-63.

Ernesti, Günter: Staatsanwaltschaft, Polizei und die Zusammenarbeit mit den Nachrichtendiensten, ZRP 1986, 57-60.

Ernst, Marcus A.: Verarbeitung und Zweckbindung von Informationen im Strafprozess, Berlin 1993.

Europol, Europol Programming Document 2019 – 2021, 2019, abrufbar unter https://www.europol.europa.eu/publications-documents/europol-programming-document.

Europol, 2018 Consolidated Annual Activity Report, 2019, abrufbar unter https://www.europol.europa.eu/publications-documents/consolidated-annual-activity-report-caar-2018.

Fehling, Michael: Mittelbare Diskriminierung und Art. 3 (Abs. 3) GG: Vom europäischen Recht lernen!?, in: Heckmann, Dirk; Schenke, Ralf P.; Sydow, Gernot (Hrsg.), Verfassungsstaatlichkeit im Wandel, Festschrift für Thomas Würtenberger zum 70. Geburtstag, Berlin 2013, 669-688 (zitiert: *Fehling*, in: FS Würtenberger).

Feldkamp, Michael F.: Der Parlamentarische Rat 1948-1949, Akten und Protokolle, Band 8: Die Beziehungen des Parlamentarischen Rates zu den Militärregierungen, München 2009.

Feldkamp, Michael F.: Der Parlamentarische Rat 1948-1949, Akten und Protokolle, Band 11: Interfraktionelle Besprechungen, München 1997.

Feldkamp, Michael F.: Der Parlamentarische Rat 1948-1949, Akten und Protokolle, Band 14: Hauptausschuß, München 2009.

Felgenhauer, Harald: Grundlagen der institutionalisierten Polizeizusammenarbeit in der Europäischen Union – Entwicklung und Zukunft des Europäischen Polizeiamtes Europol, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Rieß, Peter; Zöller, Mark Alexander (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg 2003, 75-90 (zitiert: *Felgenhauer*, in: FG Hilger).

Ferguson, Andrew Guthrie: Big Data and Predictive Reasonable Suspicion, University of Pennsylvania Law Review 163 (2015), 327-410.

Ferguson, Andrew Guthrie: Policing Predictive Policing, Washington University Law Review 94 (2017), 1115-1194.

Fiedler, Herbert: Rechenautomaten in Recht und Verwaltung, JZ 1966, 689-696.

Fiedler, Herbert: Automatisierung im Recht und juristische Informatik, 1. Teil. Grundbegriffe der elektronischen Informationsverarbeitung und ihrer juristischen Anwendung, JuS 1970, 432-436.

Fiedler, Herbert: Automatisierung im Recht und juristische Informatik, 3. Teil. Elektronische Rechtsdokumentation und juristische Informationssysteme, JuS 1970, 603-607.

Forgó, Nikolaus*; Hawellek*, Christian; *Knok*e, Friederike; *Stoklas*, Jonathan: The Collection of Electronic Evidence in Germany: A Spotlight on Recent Legal Developments and Court Rulings, in: Corrales, Marcelo; Fenwick, Mark; Forgó, Nikolaus (Hrsg.), New Technology, Big Data and the Law, Singapur 2018, 251-279.

Forgó, Nikolaus/*Krügel*, Tina/*Rapp*, Stefan: Zwecksetzung und informationelle Gewaltenteilung, Ein Beitrag zu einem datenschutzgerechten E-Government, Baden-Baden 2006.

Forsthoff, Ernst: Der Staat der Industrie-Gesellschaft, Dargestellt am Beispiel der Bundesrepublik Deutschland, 2. Aufl., München 1971.

Franko Aas, Katja: From narrative to database, Technological change and penal culture, Punishment & Society 2004, 379-393.

Franzius, Claudio: Das Recht auf informationelle Selbstbestimmung, ZJS 2015, 259-270.

Frisch, Wolfgang: Voraussetzungen und Grenzen staatlichen Strafens, NStZ 2016, 16-25.

Fuchs, Peter: Organisatorische Grundzüge der elektronischen Datenverarbeitung im Bereich der Polizei, Versuch einer Zwischenbilanz nach einem halben Jahrhundert, Kriminalistik 2018, 707-710.

Fuchs, Eckhard: Führungsrelevante Auswirkungen der IuK-Technik auf das Verwaltungshandeln, in: Reinermann, Heinrich (Hrsg.), Führung und Information, Chancen der Informationstechnik für die Führung in Politik und Verwaltung, Heidelberg 1991, 125-143.

Funk, Albrecht; *Werkentin*, Falco: Der Musterentwurf für ein einheitliches Polizeigesetz – ein Muster exekutiven Rechtsstaatsverständnisses, KJ 1976, 407-422.

Fuß, Ernst-Werner: Rechtsfragen des polizeilichen Erkennungsdienstes, in: Vogel, Klaus; Tipke, Klaus (Hrsg.), Verfassung, Verwaltung, Finanzen, Festschrift für Gerhard Wacke zum 70. Geburtstag, Köln 1972, 305-326 (zitiert: *Fuß*, in: FS Wacke).

Gadorosi, Holger: INPOL-neu, Überführung in den Wirkbetrieb ab Mitte August 2003, Kriminalistik 2003, 402-409.

Gaede, Karsten: § 81g StPO – Musterbeispiel für die schöne neue Welt der Strafverfolgungsvorsorge?, in: Bublitz, Jan Christoph; Bung, Jochen; Grünewald, Anette; Magnus, Dorothea; Putze, Holm; Scheinfeld, Jörg (Hrsg.), Recht – Philosophie – Literatur, Festschrift für Reinhard Merkel zum 70. Geburtstag, Berlin 2020, 1283-1299 (zitiert: *Gaede*, in: FS Merkel).

Gärditz, Klaus Ferdinand: Strafprozeß und Prävention, Entwurf einer verfassungsrechtlichen Zuständigkeits- und Funktionenordnung, Tübingen 2003.

Gärditz, Klaus Ferdinand: Prävention und Repression als Kategorien im Recht der Europäischen Union, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Hilger, Hans; Ruthig, Josef; Zöller, Mark A. (Hrsg.), Alternativentwurf Europol und europäischer Datenschutz, Heidelberg 2008, 192-232 (zitiert: *Gärditz*, in: AE Europol).

Gärditz, Klaus Ferdinand: Der digitalisierte Raum des Netzes als emergente Ordnung und die repräsentativ-demokratische Herrschaftsform, Der Staat 54 (2015), 113-139.

Gärditz, Klaus Ferdinand: Sicherheitsrecht als Perspektive, GSZ 2017, 1-6.

Gärditz, Klaus Ferdinand: Zentralisierung von Verfassungsschutzaufgaben und bundesstaatliche Kompetenzarchitektur, AöR 144 (2019), 81-132.

Garland, David: Kultur der Kontrolle, Verbrechensbekämpfung und soziale Ordnung in der Gegenwart, Frankfurt am Main 2008.

Gasser, Urs; *Burkert*, Herbert; *Thouvenin*, Florent; *Nolan*, Caroline: ICANN: Observations from an Information Law Perspective, in: Sethe, Rolf; Heinemann, Andreas; Hilty, Reto M.; Nobel, Peter; Zäch, Roger (Hrsg.), Kommunikation, Festschrift für Rolf H. Weber zum 60. Geburtstag, Bern 2011, 469-497 (zitiert: *Gasser/Burkert/Thouvenin/Nolan*, in: FS Weber).

Gless, Sabine: Predictive policing und operative Verbrechensbekämpfung, in: Herzog, Felix; Schlothauer, Reinhold; Wohlers, Wolfgang; Wolter, Jürgen (Hrsg.), Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächtnisschrift für Edda Weßlau, Berlin 2016, 165-180 (zitiert: *Gless*, in: GS Weßlau).

Goffman, Erwing: Stigma, Über Techniken der Bewältigung beschädigter Identität, Frankfurt am Main 1967.

Gola, Peter; *Heckmann*, Dirk: Datenschutz-Grundverordnung –Bundesdatenschutzgesetz, 3. Auflage, München 2022.

Golla, Sebastian: Risiken der polizeilichen Informationsordnung, in: Blatt, Henning; Dix, Alexander; Kelber, Ulrich; Kloepfer, Michael; Kugelmann, Dieter; Schaar, Peter; Schoch, Friederich (Hrsg.), Informationsfreiheit und Informationsrecht, Jahrbuch 2019, Berlin 2020, 199-216 (zitiert: *Golla*, JB InfoR 2019).

Golla, Sebastian: Datenschutzrechtliche Schattengewächse in den Ländern, Herausforderungen bei der Umsetzung der JI-Richtlinie für die Polizei, KriPoZ 2019, 238-244.

Golla, Sebastian: Lernfähige Systeme, lernfähiges Polizeirecht, Regulierung von künstlicher Intelligenz am Beispiel von Videoüberwachung und Datenabgleich, KrimJ 2020, 149-161.

Golla, Sebastian; *Michel*, Anna: Unklares Datenschutzrecht und Verantwortungsdiffusion bei polizeilichen Informationssystemen, in Thüne, Martin; Klaas, Kathrin; Feltes, Thomas (Hrsg.), Digitale Polizei, Frankfurt am Main 2022, 330-340.

Gössel, Karl Heinz: Überlegungen über die Stellung der Staatsanwaltschaft im rechtsstaatlichen Strafverfahren und über ihr Verhältnis zur Polizei, GA 1980, 325-354.

Götz, Volkmar: Polizei- und Ordnungsrecht heute, Zugleich Besprechung von Drews/Wacke/Vogel, Gefahrenabwehr, 8. Auflage, Bd. 1, 1975, DVBl. 1975, 876-879.

Götz, Volkmar: Die Entwicklung des allgemeinen Polizei- und Ordnungsrechts (1984 bis 1986), NVwZ 1987, 858-865.

Götz, Volkmar: Die Entwicklung des allgemeinen Polizei- und Ordnungsrechts (1987 bis 1989), NVwZ 1990, 725-733.

Götz, Volkmar: Die Entwicklung des allgemeinen Polizei- und Ordnungsrechts (1994-1997), NVwZ 1998, 679-688.

Grabitz/Hilf/Nettesheim: Das Recht der Europäischen Union: EUV/AEUV, herausgegeben von Nettesheim, Martin, 78. Aufl., München 2023.

Graulich, Kurt: Strafverfolgungsvorsorge, Gegenstand und rechtliche Verortung, NVwZ 2014, 685-691.

Graulich, Kurt: Aufgaben und Befugnisse des Bundeskriminalamts im digitalen Rechtsraum – Das Gesetz zur Neugestaltung des BKAG im Jahr 2017, KriPoZ 2017, 278-287.

Graulich, Kurt: Brauchen wir einen [sic] Musterpolizeigesetz? Überlegungen zur Standardisierung und Differenzierung im Sicherheitsrecht, GSZ 2019, 9-16.

Greve, Holger: Das neue Bundesdatenschutzgesetz, NVwZ 2017, 737-744.

Grimm, Dieter: Verfassungsrechtliche Anmerkungen zum Thema Prävention, KritV 1986, 38 ff.

Grimm, Dieter: Das Grundgesetz nach vierzig Jahren, NJW 1989, 1305-1312.

Groß, Karl-Friedrich: SISY – Geschichte, Ziele und Standort im Prozeßrecht, JurPC 1996, 24-25.

Grutzpalk, Jonas: Einleitung zum Sammelband: Polizeiliches Wissen, in: Grutzpalk, Jonas (Hrsg.), Polizeiliches Wissen, Formen, Austausch, Hierarchien, Frankfurt am Main 2016, 8-13.

Grutzpalk, Jonas: Die Erforschung des Wissensmanagements in Sicherheitsbehörden mit Hilfe der Akteurs-Netzwerk-Theorie: Polizeiliches Wissen, in: Grutzpalk, Jonas (Hrsg.), Polizeiliches Wissen, Formen, Austausch, Hierarchien, Frankfurt am Main 2016, 15-48.

Gurlit, Elke: Konturen eines Informationsverwaltungsrechts, DVBl. 2003, 1119-1134.

Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035-1041.

Gusy, Christoph: Anmerkung zu BGH, Urteil vom 14.05.1991 – 1 StR 699/90, StV 1991, 499-500.

Gusy, Christoph: Polizeiarbeit zwischen Gefahrenabwehr und Strafverfolgung, StV 1993, 269-277.

Gusy, Christoph: Die Zentralstellenkompetenz des Bundes, DVBl. 1993, 1117-1128.

Gusy, Christoph: Rechtsgüterschutz als Staatsaufgabe, Verfassungsfragen der "Staatsaufgabe Sicherheit", DÖV 1996, 573-583.

Gusy, Christoph: Polizeiliche Datenerhebung und -verwendung nach der EMRK, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Rieß, Peter; Zöller, Mark Alexander (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg 2003, 117-133 (zitiert: *Gusy*, in: FG Hilger).

Gusy, Christoph: Die Vernetzung innerer und äußerer Sicherheitsinstitutionen in der Bundesrepublik Deutschland, in: Weidenfeld, Werner (Hrsg.), Herausforderung Terrorismus, Die Zukunft der Sicherheit, Wiesbaden 2004, 197-221.

Gusy, Christoph: Vom neuen Sicherheitsbegriff zur neuen Sicherheitsarchitektur, VerwArch 101 (2010), 309-333.

Gusy, Christoph: Reform der Sicherheitsbehörden, ZRP 2012, 230-233.

Gusy, Christoph/*Eichenhofer*, Johannes: Polizei- und Ordnungsrecht, 11. Aufl., Tübingen 2023.

Häberle, Peter: Entstehungsgeschichte der Artikel des Grundgesetzes, Neuausgabe des Jahrbuch des öffentlichen Rechts der Gegenwart, Band 1, 2. Aufl., Tübingen 2010.

Hacker, Philipp: Teaching Fairness to Artificial Intelligence, Existing and Novel Strategies against Algorithmic Discrimination under EU Law, Common Market Law Review 2018, 1143-1186.

Haefner, Klaus: Der „Große Bruder", Chancen und Gefahren für eine informierte Gesellschaft, Düsseldorf 1980.

Haggerty, Kevin D.; *Ericson*, Richard V., The surveillant assemblage, British Journal of Sociology 51 (2000), 605-622.

Halfmann, Jost: Technikrecht aus Sicht der Soziologie, in: Schulde, Martin; Schröder, Rainer (Hrsg.), Handbuch des Technikrechts, 2. Aufl. 2011, Heidelberg/Dordrecht/London/New York 2010.

Hanschmann, Felix: „Gefährder" – eine neue alte Figur im Öffentlichen Recht, KJ 2017, 434-447.

Häring, Hermann: Zukünftige rechtliche Ausgestaltung des Verhältnisses Staatsanwaltschaft – Polizei – aus Sicht der Polizei, Kriminalistik 1979, 269-274.

Harnischmacher, Robert; *Semerak*, Arved: Deutsche Polizeigeschichte, Eine allgemeine Einführung in die Grundlagen, Stuttgart 1986.

Hassemer, Winfried: Die „Funktionstüchtigkeit der Strafrechtspflege" – ein neuer Rechtsbegriff?, StV 1982, 275-280.

Hassemer, Winfried: Telefonüberwachung und Gefahrenabwehr, ZRP 1991, 121-125.

Hassemer, Winfried: Strafverfahren ohne Datenschutz?, in: Institut für Kriminalwissenschaften Frankfurt a. M. (Hrsg.), Vom unmöglichen Zustand des Strafrechts, Frankfurt am Main 1995, 101-121.

Hauck, Pierre: Heimliche Strafverfolgung und Schutz der Privatheit, Eine vergleichende und interdisziplinäre Analyse des deutschen und englischen Rechts unter Berücksichtigung der Strafverfolgung in der Europäischen Union und im Völkerstrafrecht, Tübingen 2014.

Hebeler, Timo: Die Gefährderansprache, NVwZ 2011, 1364-1366.

Heinrich, Stephan: Innere Sicherheit und neue Informations- und Kommunikationstechnologien, Veränderungen des Politikfeldes zwischen institutionellen Faktoren, Akteursorientierungen und technologischen Entwicklungen, Münster 2007.

Heise, Gerd/*Riegel*, Reinhard: Musterentwurf eines einheitlichen Polizeigesetzes, mit Begründung und Anmerkungen, Stuttgart, 2. Aufl. 1978.

Henseler, Maren: Die Datei „Gewalttäter Sport" nach der Entscheidung BVerwGE 137, 113, NWVBl. 2015, 53-62.

Herold, Horst: Organisatorische Grundzüge der elektronischen Datenverarbeitung im Bereich der Polizei, Versuch eines Zukunftsmodells, in: Taschenbuch für Kriminalisten, Band XVIII, Hilden 1968, 240-259.

Herold, Horst: Neue Wege kriminalpolizeilicher Verbrechensbekämpfung (Kurzfassung des Referats), in: Göppinger, Hans; Witter, Hermann (Hrsg.), Kriminologische Gegenwartsfragen, Vorträge bei der XV. Tagung der Gesellschaft für die gesamte Kriminologie vom 2. bis 5. Oktober 1969 in Saarbrücken, Stuttgart 1970, 208-234.

Herold, Horst: Gesellschaftlicher Wandel – Chance der Polizei?, Die Polizei 1972, 133-137.

Herold, Horst: Rationalisierung und Automation in der Verbrechensbekämpfung, Universitas 1976, 63-74.

Herold, Horst: Polizei und Justiz im Informationsverbund, in: Bundeskriminalamt, Polizei und Justiz, Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 12. bis 15. Oktober 1976, Wiesbaden 1977, 79-87 (zitiert: *Herold*, in: BKA, Polizei und Justiz).

Heymann, Matthias; *Wengenroth*, Ulrich: Die Bedeutung von „tacit knowledge" bei der Gestaltung von Technik, in: Beck, Ulrich; Bonß, Wolfgang (Hrsg.), Die Modernisierung der Moderne, Frankfurt am Main 2001, 106-121.

High-level expert group on information systems and interoperability, Final Report, Brüssel 2017, abrufbar unter https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1.

Hilgendorf, Eric: Informationsrecht als eigenständige Disziplin? Kritische Anmerkungen zu einigen Grundlagenfragen von Rechtsinformatik und Informationsrecht, in: Taeger, Jürgen/Vassilaki, Irini (Hrsg.), Rechtsinformatik und Informationsrecht im Spannungsfeld von Recht, Informatik und Ökonomie, 1. Wissenschaftliches Forum für Recht & Informatik, 2009, 1-12.

Hilger, Hans: Zum Strafverfahrensrechtsänderungsgesetz 1999 (StVÄG 1999) - 1. Teil, NStZ 2000, 561-565.

Hilger, Hans: Zum Strafverfahrensrechtsänderungsgesetz 1999 (StVÄG 1999) - 2. Teil, NStZ 2001, 15-19.

Hilger, Hans: in: Eser, Albin; Goydke, Jürgen; Maatz, Kurt Rüdiger; Meurer, Dieter (Hrsg.), Strafverfahrensrecht in Theorie und Praxis, Festschrift für Lutz Meyer-Goßner zum 65. Geburtstag, München 2001, 755-770 (zitiert: *Hilger*, in: FS Meyer-Goßner).

Hilger, Hans: Vor(feld)ermittlungen / Datenübermittlungen, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Rieß, Peter; Zöller, Mark Alexander (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg 2003, 11-24 (zitiert: *Hilger*, in: FG Hilger).

Hoeren, Thomas: Zur Einführung: Informationsrecht, JuS 2002, 947-953.

Hoeren, Thomas: Big Data und Datenqualität – ein Blick auf die DS-GVO, ZD 2016, 459-463.

Hoeren, Thomas: Internetrecht, Ein Grundriss, 3. Aufl., Berlin 2018.

Hoeren, Thomas: Von Judge Jury zum Beck-Blog: Die Rechtswissenschaft der Berliner Republik im medialen Wandel, in: Duve, Thomas; Ruppert, Stefan (Hrsg.), Rechtswissenschaft in der Berliner Republik, Berlin 2018, 212-237.

Hoffmann, Friedrich: Staatsanwaltschaftliches Informationssystem, ZRP 1990, 55-59.

Hoffmann-Riem, Wolfgang: Informationelle Selbstbestimmung in der Informationsgesellschaft, Auf dem Wege zu einem neuen Konzept des Datenschutzes, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, Tübingen 2010, 499-523 (zitiert: *Hoffmann-Riem*, in: Hoffmann-Riem, Offene Rechtswissenschaft).

Hoffmann-Riem, Wolfgang: Abbau von Rechtsstaatlichkeit durch Neubau des Polizeirechts? Kritik am Musterentwurf eines einheitlichen Polizeigesetzes, dargestellt an den Normen über die Personalienfeststellung, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, Tübingen 2010, 1117-1130 (zitiert: *Hoffmann-Riem*, in: Hoffmann-Riem, Offene Rechtswissenschaft).

Hoffmann-Riem, Wolfgang; *Schmidt-Aßmann*, Eberhard; *Voßkuhle*, Andreas: Grundlagen des Verwaltungsrechts, Band I, 2. Aufl., München 2012.

Hoffmann-Riem, Wolfgang; *Schmidt-Aßmann*, Eberhard; *Voßkuhle*, Andreas: Grundlagen des Verwaltungsrechts, Band II, 2. Aufl., München 2012.

Hoffmann-Riem, Wolfgang: Innovation und Recht – Recht und Innovation, Recht im Ensemble seiner Kontexte, 2016.

Hofmann, Henning: Predictive Policing, Methodologie, Systematisierung und rechtliche Würdigung der algorithmusbasierten Kriminalitätsprognose durch die Polizeibehörden, Berlin 2020.

Honnacker, Heinz: Rechtsgrundlagen für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS), Erwiderung auf Schoreit in Computer und Recht, CR 1986, 287-291.

Hoppe, Rolf-Peter; *Grutzpalk*, Jonas: Polizeiliches Handlungswissen, Eine mehrstufige Untersuchung des Wissensbedarfs und Wissenstransfers in Kreispolizeibehörden, Polizei & Wissenschaft 4/2018, 13-22.

Horn, Hans-Detlef: Sicherheit und Freiheit durch vorbeugende Verbrechensbekämpfung – Der Rechtsstaat auf der Suche nach dem rechten Maß, in: Horn, Hans-Detlef (Hrsg.), Recht im Pluralismus, Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, Berlin 2003, 435-463 (zitiert: *Horn*, in: FS Schmitt Glaeser).

Hornung, Gerrit; *Schindler*, Stephan: Zivile Sicherheit als Gegenstand und Ziel der Informations- und Kommunikationsverarbeitung, in: Gusy, Christoph; Kugelmann, Dieter; Würtenberger, Thomas (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin/Heidelberg 2017, 247-271.

Hornung, Gerrit; *Schindler*, Stephan; *Schneider*, Jana: Die Europäisierung des strafverfahrensrechtlichen Datenschutzes, Zum Anwendungsbereich der neuen Datenschutz-Richtlinie für Polizei und Justiz, ZIS 2018, 566-574.

Hornung, Gerrit; *Schnabel*, Christoph: Verfassungsrechtlich nicht schlechthin verboten, Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung, DVBl. 2010, 824-833.

Hu, Margaret: Big Data Blacklisting, Florida Law Review 67 (2016), 1735-1809.

Huber, Hans: Das Recht im technischen Zeitalter, Rektoratsrede 1959, Bern 1960.

Imle, Walter: Zwischen Vorbehalt und Erfordernis, Eine historische Studie zur Entstehung des nachrichtendienstlichen Verfassungsschutzes nach 1945, München 1984.

Isensee, Josef: Das Grundrecht auf Sicherheit, Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, Berlin 1983.

Isensee, Josef; *Kirchhof*, Paul: Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band IV: Aufgaben des Staates, 3. Aufl., Heidelberg 2006.

Jacobs, James B.: The Eternal Criminal Record, Cambridge 2015.

Janovsky, Thomas: Der EDV-Arbeitsplatz des Staatsanwalts in der "SIJUS-Welt", JurPC 1996, 30-35.

Jasch, Michael: Neue Sanktionspraktiken im präventiven Sicherheitsrecht, KJ 2014, 237-248.

Joerges, Bernward: Die Brücken des Robert Moses: Stille Post in der Stadt- und Techniksoziologie, Leviathan 27 (1999), 43-63.

Johannes, Paul C.; *Weinhold*, Robert: Das neue Datenschutzrecht bei Polizei und Justiz, Europäisches Datenschutzrecht und deutsche Datenschutzgesetze, Baden-Baden 2018.

Jones, Richard: Digital Rule, Punishment, Control and Technology, Punishment & Society 2000, 5-22.

Karlsruher Kommentar zur Strafprozessordung: herausgegeben von Barthe, Christoph; Gericke, Jan, 4. Aufl. München 2023 (zitiert: *Bearbeiter*, in: KK-StPO).

Kaufmann, Franz-Xaver: Diskurse über Staatsaufgaben, in: Grimm, Dieter (Hrsg.), Staatsaufgaben, Baden-Baden 1994, 15-41.

Kaufmann, Stefan: Das Themenfeld „Zivile Sicherheit“, in: Gusy, Christoph; Kugelmann, Dieter; Würtenberger, Thomas (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin/Heidelberg 2017, 3-22.

Kehr, Thomas: Datei Gewalttäter Sport, Eine Untersuchung der Rechtsgrundlagen des BKAGs unter besonderer Berücksichtigung datenschutzrechtlicher und verfassungsrechtlicher Aspekte, Baden-Baden 2015.

Kelsen, Hans: Reine Rechtslehre, 2. Aufl. 2006, Nachdruck, Wien 2000.

Kennhöfer, Ulrich: Hat die Kripo resigniert? Die Fortentwicklung des INPOL-Systems stockt, Kriminalistik 1987, 182-185.

Kestel, Oliver: §§ 474 ff. StPO – eine unbekannte Größe, StV 1997, 266-269.

Kießling, Andrea: Die dogmatische Einordnung der polizeilichen Gefährderansprache in das allgemeine Polizeirecht, Überlegungen zu einer neuen "Standardmaßnahme", DVBl. 2012, 1210-1217.

Kilian, Wolfgang: Idee und Wirklichkeit der Rechtsinformatik in Deutschland, CR 2017, 202-212.

Kipker, Dennis-Kenji: Informationelle Freiheit und staatliche Sicherheit, Tübingen 2016.

Kitschelt, Herbert: Technologiepolitik als Lernprozeß, in: Grimm, Staatsaufgaben, Baden-Baden 1994, 391-425.

Klein, Eckart: Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633-1640.

Klein, Oliver: Das Untermaßverbot – Über die Justiziabilität grundrechtlicher Schutzpflichterfüllung, JuS 2006, 960-964.

Klink, Manfred: Hat die „RAF" die Republik verändert? 30 Jahre Terrorismus und Terrorismusbekämpfung in Deutschland, in: Bundeskriminalamt (Hrsg.), Festschrift für Horst Herold zum 75. Geburtstag, Das Bundeskriminalamt am Ausgang des 20. Jahrhunderts, Wiesbaden 1998, 65-99 (zitiert: *Klink*, in: FS Herold).

Kloepfer, Michael: Der Vorbehalt des Gesetzes im Wandel, JZ 1984, 685-695.

Kloepfer, Michael: Informationsrecht, München 2002.

Knackstedt, Ralf; Eggert, Mathias; *Gräwe*, Lena; *Spittka*, Jan: Forschungsportal für Rechtsinformatik und Informationsrecht – Weg zu einer disziplinenübergreifenden Forschungsübersicht Forschungsportal für Rechtsinformatik und Informationsrecht, MMR 2010, 528-533.

Knemeyer, Franz-Ludwig: Datenerhebung, Datenverarbeitung und Datennutzung als Kernaufgaben polizeilicher Vorbereitung auf die Gefahrenabwehr und Straftatenverfolgung (Informationsvorsorge), in: Arndt, Hans-Wolfgang; Knemeyer, Franz-Ludwig; Kugelmann, Dieter; Meng, Werner; Schweitzer, Michael (Hrsg.), Völkerrecht und deutsches Recht: Festschrift für Walter Rudolf zum 70. Geburtstag, München 2001, 483-496 (zitiert: *Knemeyer*, in: FS Rudolf).

Knierim, Antonie: Kumulation von Datensammlungen auf Vorrat - Vorratsspeicherung von TK- und Fluggastdaten und das Verbot umfassender Überwachung, ZD 2011, 17-23.

Kniesel, Michael: Zur Eingriffsqualität sicherheitsbehördlicher Datenerhebung, Die Polizei 1983, 374-385.

Kniesel, Michael: Neue Polizeigesetze contra StPO? Zum Regelungsstandort der vorbeugenden Bekämpfung von Straftaten und zur Verfassungsmäßigkeit polizeilicher Vorfeldaktivität, ZRP 1987, 377-383.

Kniesel, Michael; *Vahle*, Jürgen: Fortentwicklung des materiellen Polizeirechts, Zum Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder (VE ME PolG), DÖV 1987, 953-960.

Kniesel, Michael; *Vahle*, Jürgen: VE ME PolG, Musterentwurf eines einheitlichen Polizeigesetzes in der Fassung des Vorentwurfs zur Änderung des ME PolG, Heidelberg 1990.

Kniesel, Michael: Neuzuschnitt der Polizeigesetze zum Nachteil der Strafverfolgung?, in: Bull, Hans Peter (Hrsg.), Sicherheit durch Gesetze?, Baden-Baden 1987, 105-121.

Kniesel, Michael: Polizeiliche Gefahrenvorsorge im Spannungsfeld von Freiheit und Sicherheit, Die Polizei 1991, 185-190.

Kniesel, Michael: Kriminalitätsbekämpfung – Gefahrenabwehr oder Strafverfolgung?, Die Polizei 2017, 189-203.

Kniesel, Michael: Sicherheitsrecht – Anmerkungen zu einem Rechtsgebiet in der Findungsphase, Die Polizei 2018, 265-274.

Koch, Katharina; *Nguyen*, Alexander: Schutz vor mittelbarer Diskriminierung – Gleiches Recht für alle?, Das Verbot der mittelbaren Diskriminierung in der höchstrichterlichen Rechtsprechung, EuR 2010, 364-378.

Koper, Christopher S.; *Lum*, Cynthia: Critic, The Limits of Police Technology, in: Weisburd, David; Braga, Antony A. (Hrsg.), Police Innovation, Contrasting Perspectives, 2. Aufl., Cambridge 2019, 517-543.

König, Stefan; *Voigt*, Lea: Datenverarbeitung im Strafverfahren in Zeiten der „E-Akte", in: Herzog, Felix; Schlothauer, Reinhold; Wohlers, Wolfgang; Wolter, Jürgen (Hrsg.), Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächtnisschrift für Edda Weßlau, Berlin 2016, 181-192 (zitiert: *König/Voigt*, in: GS Weßlau).

Körffer, Barbara: Auswertung personenbezogener Daten für Strafverfolgung und Gefahrenabwehr, DANA 2014, 146-150.

Kötter, Matthias: Pfade des Sicherheitsrechts, Begriffe von Sicherheit und Autonomie im Spiegel der sicherheitsrechtlichen Debatte der Bundesrepublik Deutschland, Baden-Baden 2008.

Koselleck, Reinhart: Preußen zwischen Reform und Revolution, Allgemeines Landrecht, Verwaltung und soziale Bewegung von 1791 bis 1848, Stuttgart 1967.

Kowalczyk, Anneliese: Datenschutz im Polizeirecht, Reaktionen der Gesetzgeber auf das Volkszählungsurteil des Bundesverfassungsgerichts, Köln 1989.

Kral, Sebastian: Die polizeilichen Vorfeldbefugnisse als Herausforderung für Dogmatik und Gesetzgebung des Polizeirechts, Begriff, Tatbestandsmerkmale und Rechtsfolgen, Berlin 2012.

Kreuter-Kirchhof, Charlotte: Die polizeiliche Gefährderansprache, AöR 139 (2014), 257-286.

Kube, Edwin: Rechtsgrundlagen polizeilicher Datenverarbeitung, in: Bundeskriminalamt (Hrsg.), Polizeiliche Datenverarbeitung, Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 2. bis 5. November 1982, Wiesbaden 1983, 99-120 (zitiert: *Kube*, in: BKA, Polizeiliche Datenverarbeitung).

Kubica, Johann: § 1 BKA-Gesetz und die Zentralstellenbefugnisse des Bundeskriminalamtes, ÖVD 1982, 109-111.

Kubica, Johann; *Leineweber*, Heinz: Grundfragen zu den Zentralstellenaufgaben des Bundeskriminalamtes, NJW 1984, 2068-2072.

Kühl, Kristian: Unschuldsvermutung, Freispruch und Einstellung, Köln 1983.

Kühling, Jürgen: Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht, NVwZ 2014, 681-685.

Kühling, Jürgen; *Martini*, Mario: Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448-454.

Kühling, Jürgen; *Buchner*, Benedikt: Datenschutz-Grundverordnung, BDSG, 3. Aufl., München 2020.

Kühne, Hans-Heiner: Die Definition des Verdachts als Voraussetzung strafprozessualer Zwangsmaßnahmen, NJW 1979, 617-622.

Kuhlmann, Goetz-Joachim: Gedanken zum Bericht über das Verhältnis „Staatsanwaltschaft und Polizei", DRiZ 1976, 265-269.

Kugelmann, Dieter: Der polizeiliche Gefahrenbegriff in Gefahr? Anforderungen an die Voraussetzungen polizeilicher Eingriffsbefugnisse, DÖV 2003, 781-789.

Kugelmann, Dieter: Entwicklungslinien eines grundrechtsgeprägten Sicherheitsverwaltungsrechts, Die Verwaltung 2014, 25-55.

Kunz, Karl-Ludwig; *Singelnstein*, Tobias: Kriminologie, Eine Grundlegung, 7. Aufl., Bern 2016.

Küster, Dieter: Informationstechnologie, Entwicklung und Auswirkungen auf die Polizei, in: Zachert, Hans-Ludwig (Hrsg.), 40 Jahre Bundeskriminalamt, Stuttgart 1991, 107-12 (zitiert: *Küster*, in: FS BKA).

Lackner/Kühl/Heger, StGB, bearbeitet von Heger, Martin, 30. Aufl., München 2023.

Ladeur, Karl-Heinz: Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, Zur „objektiv-rechtlichen Dimension" des Datenschutzes, DuD 2000, 12-19.

Ladeur, Karl-Heinz: Das Recht auf informationelle Selbstbestimmung: Eine juristische Fehlkonstruktion?, DÖV 2009, 45-55.

Ladeur, Karl-Heinz: Die Gesellschaft der Netzwerke und ihre Wissensordnung, in: Süssenguth, Florian (Hrsg.), Die Gesellschaft der Daten: Über die digitale Transformation der sozialen Ordnung, Bielefeld 2015, 225-252.

Lageson, Sarah E.: Digital Punishment, Privacy, Stigma, and the Harms of Data-Driven Criminal Justice, New York 2020.

Lageson, Sarah E.; *Maruna*, Shadd: Digital degradation: Stigma management in the internet age, Punishment & Society 2018, 113-133.

Lange, Nicole: Vorermittlungen, Die Behandlung des staatsanwaltschaftlichen Vorermittlungsverfahrens unter besonderer Berücksichtigung von Abgeordneten, Politikern und Prominenten, Frankfurt am Main 1999.

Legnaro, Aldo: Kennzeichen des Gefährdens, Skizzen einer Ethnomethodologie des Sich-verdächtig-Machens, KrimJ 2018, 123-138.

Lemke, Michael: Länderübergreifendes staatsanwaltschaftliches Verfahrensregister, NStZ 1995, 484-486.

Lepsius, Oliver: Dritter Beratungsgegenstand: Risikosteuerung durch Verwaltungsrecht: Ermöglichung oder Begrenzung von Innovationen?, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Hamburg vom 1. bis 4. Oktober 2003, Berlin 2004, 264-308.

Lepsius, Oliver: Die Grenzen der präventivpolizeilichen Telefonüberwachung, JURA 2006, 929-937.

Lersch, Roland: Die Entwicklung des BKA-Gesetzes zu einem modernen Polizeigesetz, in: Bundeskriminalamt (Hrsg.), Festschrift für Horst Herold zum 75. Geburtstag, Das Bundeskriminalamt am Ausgang des 20. Jahrhunderts, Wiesbaden 1998, S. 35-64 (zitiert: *Lersch*, in: FS Herold).

Von Lewinski, Kai: Rechte und Rechtspositionen an und in virtuellen Räumen – Recht der Adress- und Namensräume, in: Hill, Hermann; Schliesky, Utz (Hrsg.), Die Vermessung des virtuellen Raums, E-Volution des Rechts- und Verwaltungssystems III, Baden-Baden 2012, 177-192.

Von Lewinski, Kai: Die Matrix des Datenschutzes, Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014.

Von Lewinski, Kai: Datenbanken sowie Ordnungs- und Personenkennzeichen, in: Seckelmann, Margrit (Hrsg.): Digitalisierte Verwaltung, Vernetztes E-Government, 2. Aufl., Berlin 2019, 107-126.

Liborius, Alexander: INPOL-neu: Anmerkungen zum Entwicklungsstand, Kriminalistik 1999, 686.

Lilie, Hans: Das Verhältnis von Polizei und Staatsanwaltschaft im Ermittlungsverfahren, ZStW 106 (1994), 625-643.

Linzbach, Karoline Maria: Beobachtung von Einzelpersonen durch das Bundesamt für Verfassungsschutz, GSZ 2022, 7-14.

Lisken/Denninger: Handbuch des Polizeirechts, Gefahrenabwehr – Strafverfolgung – Rechtsschutz, herausgegeben von Bäcker, Matthias; Denninger, Erhard; Graulich, Kurt, 6. Aufl., München 2018.

Lisken/Denninger: Handbuch des Polizeirechts, Gefahrenabwehr – Strafverfolgung – Rechtsschutz, herausgegeben von Bäcker, Matthias; Denninger, Erhard; Graulich, Kurt, 7. Aufl., München 2021.

Lodde, Rüdiger: Datenfernverarbeitung, in: Bundeskriminalamt (Hrsg.), Datenverarbeitung, Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 13. März bis 17. März 1972, Wiesbaden 1972, 25-35 (*Lodde*, in: BKA, Datenverarbeitung).

Löffelmann, Markus: Die Zukunft der deutschen Sicherheitsarchitektur – Vorbild Bayern?, GSZ 2018, 85-91.

Löffelmann, Markus: Die Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung – Schema oder Struktur?, GSZ 2019, 16-22.

Lüderssen, Klaus: Abschaffen des Strafens?, Frankfurt am Main 1995.

Luhmann, Niklas: Soziale Systeme, Grundriß einer allgemeinen Theorie, Frankfurt am Main 1987 (zitiert: *Luhmann*, Soziale Systeme).

Luhmann, Niklas: Das Recht der Gesellschaft, Frankfurt am Main 1995 (zitiert: *Luhmann*, Das Recht der Gesellschaft).

Lum, Cynthia; *Koper*, Christopher S.; *Willis*, James: Understanding the Limits of Technology's Impact on Police Effectiveness, Police Quarterly 20 (2017), 135-163.

Lyon, David: Surveillance as social sorting, Computer codes and mobile bodies, in: Lyon, David (Hrsg.), Surveillance as Social Sorting, Privacy, risk and digital discrimination, London und New York 2003, 13-30.

Mangold, Hannes: Fahndung nach dem Raster, Informationsverarbeitung bei der bundesdeutschen Kriminalpolizei, 1965-1984, Zürich 2017.

Von Mangoldt/Klein/Starck: Grundgesetz, Kommentar, herausgegeben von Huber, Peter M.; Voßkuhle, Andreas, 8. Aufl., München 2018.

Manning, Peter K.: Information Technologies and the Police, Crime and Justice 15 (1992), 349-398.

Manning, Peter K.: The Technology of Policing, Crime Mapping, Information Technology and the Rationality of Crime Control, New York und London 2008.

Manovich, Lev: The Language of New Media, Cambridge und London 2001.

Marsch, Nikolaus: Das europäische Datenschutzgrundrecht, Grundlagen – Dimensionen – Verflechtungen, Tübingen 2018.

Marscholleck, Dietmar: Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes, NJW 2015, 3611-3616.

Martínez Soria, José: Grenzen vorbeugender Kriminalitätsbekämpfung im Polizeirecht: Die automatisierte Kfz-Kennzeichenerkennung, DÖV 2007, 779-785.

Masing, Johannes: Gesetz und Gesetzesvorbehalt – zur Spannung von Theorie und Dogmatik am Beispiel des Datenschutzrechts, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, Tübingen 2010, 467-496 (zitiert: *Masing*, in: Hoffmann-Riem, Offene Rechtswissenschaft).

Matheis, Frank: Strafverfahrensänderungsgesetz 1999, Die Neuregelung der §§ 474 ff. StPO, Baden-Baden 2007.

Matzner, Tobias: Beyond data as representation: The performativity of Big Data in surveillance, Surveillance & Society 2016, 197-210.

Dürig/Herzog/Scholz: Grundgesetz, Kommentar, herausgegeben von Herdegen, Matthias; Herzog, Roman; Klein, Hans H.; Scholz, Rupert, 100. EL, München 2023.

Mayer-Schönberger, Viktor*; Cukier*, Kenneth: Big Data, Die Revolution, die unser Leben verändern wird, München 2013.

Mayring, Philipp: Qualitative Inhaltsanalyse, 12. Aufl., Weinheim 2015.

Mehde, Veith: Terrorismusbekämpfung durch Organisationsrecht, JZ 2005, 815-822.

Meinicke, Dirk: Aktuelle strafprozessuale Folgefragen des "Vorratsdatenurteils" des BVerfG, HRRS 2011, 398-404.

Merten, Karlheinz: Das Abrufrecht der Staatsanwaltschaft aus polizeilichen Dateien, NStZ 1987, 10-15.

Meyer, Frank: Der Grundsatz der Verfügbarkeit, NStZ 2008, 188-194.

Meyer, Frank: Entwicklungen und Herausforderungen bei Informationssammlung und -austausch in der strafrechtlichen Zusammenarbeit, in: Kugelmann, Dieter; Rackow, Peter (Hrsg.), Prävention und Repression im Raum der Freiheit, der Sicherheit und des Rechts, Belastbarkeit der Konzepte von Strafe und Gefahrenabwehr zwischen Staat und EU, Baden-Baden 2014, 41-59.

Meyer, Stephan: Kriminalwissenschaftliche Prognoseinstrumente im Tatbestand polizeilicher Vorfeldbefugnisse, JZ 2017, 429-439.

Meyer-Goßner, Lutz; *Schmitt*, Bertram: Strafprozessordnung, Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 65. Aufl., München 2022.

Meyer-Ladewig, Jens; *Nettesheim*, Martin; *von Raumer*, Stefan: EMRK, Handkommentar, 5. Aufl., Baden-Baden 2023.

Middel, Stefan: Innere Sicherheit und präventive Terrorismusbekämpfung, Baden-Baden 2007.

Möllers, Christoph: Netzwerk als Kategorie des Organisationsrechts, Zur juristischen Beschreibung dezentraler Steuerung, in: Oebbecke, Janbernd (Hrsg.), Nicht-normative Steuerung in dezentralen Systemen, Stuttgart 2005, 285-302.

Molnar, Adam: Technology, Law, and the Formation of (Il)Liberal Democracy?, Surveillance & Society 2017, 381-388.

Momsen, Carsten; *Rennert*, Cäcilia: Big Data-Based Predictive Policing and the Changing Nature of Criminal Justice, Consequences of the extended Use of Big Data, Algorithms and AI in the Area of Criminal Law Enforcement, KriPoZ 2020, 160-172.

Monroy, Matthias: 220 Abfragen pro Sekunde, Das Schengener Informationssystem wächst dynamisch, Bürgerrechte & Polizei/CILIP 121 (4/2020), 67-74.

Morgenstern, Christine: Der ewige Makel – Straftheorie, Grundrechte und das Strafregister, ZStW 131 (2019), 625–665.

Moser-Knierim, Antonie: Vorratsdatenspeicherung, Zwischen Überwachungsstaat und Terrorabwehr, Wiesbaden 2014.

Möstl, Markus: Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, Tübingen 2002.

Möstl, Markus: Die neue dogmatische Gestalt des Polizeirechts – Thesen zur Integration eines modernen informationellen Vorfeldrechts in das klassische rechtsstaatliche Gefahrenabwehrrecht, DVBl. 2007, 581-589.

Möstl, Markus: Eingriffsschwellen im polizeilichen Informationsrecht, in: Spiecker gen. Döhmann, Indra; Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, Tübingen 2008, 239-258.

Möstl, Markus: Polizeiliche Sicherheitsgewährleistung in Mehrebenensystem, Die Verwaltung 2008, 309-343.

Möstl, Markus: Rechtsgrundlagen und Rechtsbestand der Europäischen Sicherheitspolitik, EuR 2009, Beiheft 3, 33-51.

Möstl, Markus: Datenverfügbarkeit als Voraussetzung für innere Sicherheit. Ein Bericht aus Deutschland, SIAK-Journal 2/2010, 61-69.

Möstl, Markus: Das Bundesverfassungsgericht und das Polizeirecht, Eine Zwischenbilanz aus Anlass des Urteils zur Vorratsdatenspeicherung, DVBl. 2010, 808-816.

Möstl, Markus: Stellungnahme im Rahmen der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages zum Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes (BT-Drs. 18/11163 und 11326) am 20. März 2017, Ausschussdrucksache 18(4)806 B (zitiert: *Möstl*, Stellungnahme BKAG 2018).

Müller, Henning Ernst: Labeling von „Intensivtätern"? Karriere eines kriminologischen Theorieansatzes und seine heutige Relevanz, in: Strafverteidigertag (Hrsg.), Wehe dem, der beschuldigt wird..., 34. Strafverteidigertag Hamburg, 26.-28.2.2010, Berlin 2011, 169-189.

Müller, Michael W.; *Schwabenbauer*, Thomas: Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden, NJW 2021, 2079-2085.

Müller, Oswin: Der Abschied von der konkreten Gefahr als polizeirechtliche Eingriffsbefugnis, StV 1995, 602-606.

Müller, Wolfgang; *Römer*, Sebastian: Legendierte Kontrollen, Die gezielte Suche nach dem Zufallsfund, NStZ 2012, 543-547.

Müller-Wille, Björn: The Effect of International Terrorism on EU Intelligence Co-operation, JCMS 2008, 49-73.

Müllmann, Dirk: Zweckkonforme und zweckändernde Weiternutzung, Die Konsolidierung der Rechtsprechung des BVerfG zur Weiterverwendung zweckgebunden erhobener Daten im Urteil zum BKA-Gesetz vom 20.4.2016, NVwZ 2016, 1692-1696.

Münch, Holger: Kriminalitätsbekämpfung weiterdenken, Phänomene – Herausforderungen – Handlungsoptionen im Zeitalter von Big Data, Algorithmen und autonomen Systemen, Kriminalistik 2019, 11-16.

von Münch/Kunig: Grundgesetz-Kommentar, herausgegeben von Kämmerer, Axel; Kotzur, Markus, 7. Aufl. 2021, München 2021.

Münchener Kommentar zur Strafprozessordung: herausgegeben von Knauer, Christoph; Kudlich, Hans; Schneider, Hartmut, München 2014 ff. (zitiert: *Bearbeiter*, in: MüKo-StPO).

Murswiek, Dietrich: Zweiter Beratungsgegenstand: Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Hannover vom 4. bis 7. Oktober 1989, Berlin 1990, 207-234.

Narr, Wolf-Dieter: Die Technologisierung der Polizei, ...und ihre dringliche Politisierung, Bürgerrechte & Polizei/CILIP 76 (3/2003), 6-11.

National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report, New York City 2004.

Nehm, Kay: Das nachrichtendienstrechtliche Trennungsgebot und die neue Sicherheitsarchitektur, NJW 2004, 3289-3295.

Neubacher, Frank: Kriminologie, 4. Aufl., Baden-Baden 2020.

Neumann, Dieter: Vorsorge und Verhältnismäßigkeit, Die kriminalpräventive Informationserhebung im Polizeirecht, Berlin 1994.

Nicklisch, Fritz: Das Recht im Umgang mit dem Ungewissen in Wissenschaft und Technik, NJW 1986, 2287-2291.

Nietzsche, Friedrich: Menschliches, Allzumenschliches, Ein Buch für freie Geister, Band 1, Leipzig 1886.

Niggemeyer, Bernhard: Die Stellung des Bundeskriminalamtes im Rahmen der kriminalpolizeilichen Verbrechensbekämpfung, DÖV 1960, 97-102.

Nogala, Detlef: Polizei, avancierte Technik und soziale Kontrolle, Funktion und Ideologie technikbesetzter Kontrollstrategien im Prozeß der Rationalisierung von Herrschaft, Pfaffenweiler 1989.

Nogala, Detlef: Polizei, avancierte Technik und soziale Kontrolle – wie geht's dem Frosch heute?, vorgänge 2019, 21-32.

Ogorek, Markus: Alte Daten, neue Verdächtigungen? Eine Kritik am polizeilichen Informationssystem INPOL, ZRP 2023, 86-89.

Ossenbühl, Fritz: Verwaltungsverfahren zwischen Verwaltungseffizienz und Rechtsschutzauftrag, NVwZ 1982, 465-472.

Ossenbühl, Fritz: Vorsorge als Rechtsprinzip im Gesundheits-, Arbeits- und Umweltschutz, NVwZ 1986, 161-171.

Ostendorf, Heribert: Rechtliche Grundlagen und kriminalpolitische Aspekte der Kriminalprävention in Deutschland, in: Samson, Erich; Dencker, Friedrich; Frisch, Peter; Frister, Helmut; Reiß, Wolfram (Hrsg.), Festschrift für Gerald Grünwald zum siebzigsten Geburtstag, Baden-Baden 1999, 419-431 (zitiert: *Ostendorf*, in: FS Grünwald).

Pache, Eckhard: Zweiter Beratungsgegenstand: Verantwortung und Effizienz in der Mehrebenenverwaltung, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Rostock vom 4. bis 7. Oktober 2006, Berlin 2007, 106-151.

Paeffgen, Hans-Ullrich: Art. 30, 70, 101 I GG — vernachlässigbare Normen? — Revisibilität von Landesrecht durch das BVerwG und „vorbeugende Verbrechensbekämpfung", JZ 1991, 437-446.

Paeffgen, Hans-Ullrich: Problemskizze bei der Aufgabenbeschreibung von Europol, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Hilger, Hans; Ruthig, Josef; Zöller, Mark A. (Hrsg.), Alternativentwurf Europol und europäischer Datenschutz, Heidelberg 2008, 173-191 (zitiert: *Paeffgen*, in: AE Europol).

Papier, Hans-Jürgen Papier: Rechtsstaat im Risiko, DVBl. 2010, 801-807.

Park, Byungwoog: Wandel des klassischen Polizeirechts zum neuen Sicherheitsrecht, Eine Untersuchung am Beispiel der Entscheidung über sogenannte Online-Durchsuchungen, Berlin 2013.

Peitsch, Dietmar: Vom Polizeirecht zum Informationsrecht, Begriffe und Inhalte bereichsspezifischer Regelungen der polizeilichen Datenerhebung und Datenverarbeitung, Die Polizei 1991, 305-308.

Peitsch, Dietmar: Die Informationsbeschaffung im neuen Polizeirecht, ZRP 1992, 127-130.

Peters, Hans: Ein Modell-Polizeigesetz, DÖV 1953, 385-387.

Piening, Marie-Theres; *Kühne*, Marius, *Töpfer*, Eric: Parlamentarische Polizeibeauftragte, Vermittlungsstatt Ermittlungsstellen, Bürgerrechte & Polizei/CILIP 130 (4/2022), 17-28.

Pietrzak, Alexandra: Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte, JuS 1994, 748-753.

Pinch, Trevor J.; *Bijker*, Wiebe E.: The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other, in: Bijker, Wiebe E.;

Hughes, Thomas P.; Pinch, Trevor J. (Hrsg.), The Social Construction of Technological Systems, New Directions in the Sociology and History of Technology, Cambridge und London 1987, 17-50.

Pitschas, Rainer; *Aulehner*, Josef: Informationelle Sicherheit oder "Sicherheitsstaat"?, NJW 1989, 2353-2359.

Pitschas, Rainer: Fortentwicklung des Polizeirechts und Legitimität des Staates, in: Schriftenreihe der Polizei-Führungsakademie 4/1991, Polizeirecht heute, Beiträge zu rechtspolitischen Zielsetzungen, gesetzgeberischen Entscheidungen, praktischen Auswirkungen, Lübeck 1991, 7-31.

Pitschas, Rainer: Europäisches Polizeirecht als Informationsrecht, ZRP 1993, 174-177.

Pitschas, Rainer: Innere Sicherheit und internationale Verbrechensbekämpfung als Verantwortung des demokratischen Verfassungsstaates, JZ 1993, 858-866.

Pitschas, Rainer: Polizeirecht im kooperativen Staat, Innere Sicherheit zwischen Gefahrenabwehr und kriminalpräventiver Risikovorsorge, DÖV 2002, 221-231.

Pohle, Jörg: Datenschutz und Technikgestaltung, Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, Berlin 2017, abrufbar unter https://edoc.hu-berlin.de/handle/18452/19886.

Pollähne, Helmut: Strafverfolgungsvorsorge-Register (§ 484 StPO), GA 2006, 807-824.

Ponsaers, Paul: Reading about "community (oriented) policing" and police models, in: Policing: An International Journal of Police Strategies & Management, 2001, 470-497.

Popitz, Heinrich: Phänomene der Macht, 2. Aufl., Tübingen 1992.

Poscher, Ralf: Gefahrenabwehr, Eine dogmatische Rekonstruktion, Berlin 1999.

Poscher, Ralf: Eingriffsschwellen im Recht der inneren Sicherheit, Ihr System im Licht der neueren Verfassungsrechtsprechung, Die Verwaltung 2008, 345-373.

Poscher, Ralf: Sicherheitsverfassungsrecht im Wandel, in: Vesting, Thomas; Korioth, Stefan (Hrsg.), Der Eigenwert des Verfassungsrechts, Tübingen 2011, 245-262.

Poscher, Ralf: Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander, Hans-Helmuth; Perron, Walter; Poscher, Ralf; Riescher, Gisela; Würtenberger, Thomas (Hrsg.): Resilienz in der offenen Gesellschaft, Symposium des Centre for Security and Society, Baden-Baden 2012, 167-190.

Poscher, Ralf; *Kilchling*, Michael; *Landerer*, Lukas: Ein Überwachungsbarometer für Deutschland, Entwicklung eines Konzeptes zur periodischen Erfassung staatlicher Überwachungsmaßnahmen, GSZ 2021, 225-232.

Poster, Mark: The second media age, Cambridge 1995.

Preu, Peter: Polizeibegriff und Staatszwecklehre, Die Entwicklung des Polizeibegriffs durch die Rechts- und Staatswissenschaften des 18. Jahrhunderts, Göttingen 1983.

Preuß, Ulrich K.: Risikovorsorge als Staatsaufgabe, in: Grimm, Staatsaufgaben, Baden-Baden 1994, 523-551.

Priebe, Reinhard: Europol – neue Regeln für die Zusammenarbeit auf dem Gebiet der Strafverfolgung, EuZW 2016, 894-896.

Prügel, Jan-Willem: Entscheidungsanmerkung zu BVerfG, Urt. v. 24.4.2013 – 1 BvR 1215/07 – Zur Verfassungsmäßigkeit des Anti-Terror-Datei-Gesetzes, ZIS 2013, 529-534.

Puschke, Jens: Die kumulative Anordnung von Informationsbeschaffungsmaßnahmen im Rahmen der Strafverfolgung, Eine Untersuchung unter rechtlichen, rechtstatsächlichen und kriminologischen Aspekten, Berlin 2006.

Puschke, Jens: Sicherheitsgesetzgebung ohne Zweck, Die Vorratsdatenspeicherung von Verkehrsdaten der Telekommunikation als Prototyp einer verfehlten neuartigen Sicherheitsarchitektur, in: Goeckenjan, Ingke; Puschke, Jens; Singelnstein, Tobias (Hrsg.), Für die Sache – Kriminalwissenschaften aus unabhängiger Perspektive Festschrift für Ulrich Eisenberg zum 80. Geburtstag, Berlin 2019, 695-716 (zitiert: *Puschke*, in: FS Eisenberg).

Rachor, Frederik: Vorbeugende Straftatenbekämpfung und Kriminalakten, Zur Aufbewahrung und Verwendung von Informationen aus Strafverfahren durch die Polizei, Baden-Baden 1989.

Rademacher, Timo: Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?, JZ 2019, 702-710.

Rademacher, Timo: Predictive Policing im deutschen Polizeirecht, AöR 142 (2017), 366-416.

Rammert, Werner: Technik – Handeln – Wissen, Zu einer pragmatistischen Technik- und Sozialtheorie, 2. Aufl., Wiesbaden 2016.

Rasch, Ernst: Der Musterentwurf eines einheitlichen Polizeigesetzes und seine Verwirklichung, DVBl. 1982, 126-130.

Rebmann, Kurt; *Schoreit*, Armin: Elektronische Datenverarbeitung (EDV) in Strafverfolgungsangelegenheiten und Datenschutz, NStZ 1984, 1-7.

Rebmann, Kurt: Der Einsatz verdeckt ermittelnder Polizeibeamter im Bereich der Strafverfolgung, NJW 1985, 1-6.

Reinhardt, Jörn: Konturen des europäischen Datenschutzgrundrechts, Zu Gehalt und horizontaler Wirkung von Art. 8 GRCh, AöR 142 (2017) 528-565.

Riegel, Reinhard: Neueste Entwicklungstendenzen im Polizei- und Strafverfahrensrecht, ZRP 1978, 14-24.

Riegel, Reinhard: Die neuen Grundlagen der polizeilichen Personenkontrolle und Durchsuchung von Wohnungen im Strafverfahrensrecht, BayVBl. 1978, 589-597.

Riegel, Reinhard: Musterentwurf und Alternativentwurf für ein einheitliches Polizeigesetz: Ein Vergleich zweier Konzeptionen, DVBl. 1979, 709-717.

Riegel, Reinhard: Stellung und Aufgaben des Bundeskriminalamtes: Überblick und Probleme, DVBl. 1982, 720-727.

Riegel, Reinhard: Grundfragen zu den Zentralstellenaufgaben des Bundeskriminalamtes, NJW 1983, 656-661.

Riegel, Reinhard: Der unbescholtene Bürger als Objekt sicherheitsbehördlicher Informationsverarbeitung?, Ein Beitrag zu Entwicklungstendenzen im Sicherheitsrecht, DVBl. 1987, 325-333.

Riegel, Reinhard: Grenzen informationeller Zusammenarbeit zwischen Polizei und Verfassungsschutz, DVBl. 1988, 121-129.

Riegel, Reinhard: Stand und Entwicklungstendenzen bei den Befugnissen für informationelle Tätigkeit der Polizei, Zugleich ein Beitrag zu den Grenzen der Gesetzgebungskunst, Die Polizei 1991, 1-9.

Riegel, Reinhard: Zu Stand und Entwicklungstendenzen des informationellen Befugnisrechts zur polizeilichen Aufgabenerfüllung: Licht, Schatten und Hoffnung, DÖV 1994, 814-821.

Ringwald, Gerhard: INPOL und StA, Zum Abrufrecht der Staatsanwaltschaften aus polizeilichen Datenspeichern, München 1984.

Ringwald, Gerhard: Gegenpol zu INPOL? Computer bei der Justiz, ZRP 1988, 178-183.

Robbers, Gerhard: Sicherheit als Menschenrecht, Aspekte der Geschichte, Begründung und Wirkung einer Grundrechtsfunktion, Baden-Baden 1987.

Roewer, Helmut: Trennung von Polizei und Verfassungsschutzbehörden, DVBl. 1986, 205-208.

Rogall, Klaus: Informationseingriff und Gesetzesvorbehalt im Strafprozessrecht, Tübingen 1992.

Roggan, Fredrik; *Bergemann*, Nils: Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland – Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz, NJW 2007, 876-881.

Roggan, Fredrik: Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, NJW 2009, 257-262.

Roggan, Frederik: Zur Doppelfunktionalität von heimlichen Ermittlungsmaßnahmen am Beispiel der Online-Durchsuchungen, Zugleich eine Besprechung von BGH, 2 StR 247/16 („legendierte Kontrollen"), GSZ 2018, 52-56.

Ronellenfitsch, Michael: Die Bewältigung der wissenschaftlichen und technischen Entwicklung durch das Verwaltungsrecht, DVBl. 1989, 851-866.

Roßnagel, Alexander; *Wedde*, Peter; *Hammer*, Volker; *Pordesch*, Ulrich: Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen 1990.

Roßnagel, Alexander: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238-1242.

Roßnagel, Alexander: Vorratsdatenspeicherung – was geht noch und was nicht mehr?, ZD 2022, 650-655.

Rouvroy, Antoinette; *Poullet*, Yves: The Right to Informational Self-Determination and the Value of Self-Development; Reassessing the Importance of Privacy for Democracy, in: Gutwirth, Serge; Poullet, Yves; De Hert, Paul; de Terwangne, Cécile; Nouwt, Sjaak (Hrsg.), Reinventing Data Protection?, Dordrecht 2009, 45-76.

Rublack, Susanne: INPOL-neu aus datenschutzrechtlicher Sicht, DuD 1999, 437-441.

Ruch, Andreas; *Feltes*, Thomas: Gewalttäterdateien, Rechtliche Probleme und kriminologische Risiken, NK 2016, 62-77.

Rudolph, Bernd: Antizipierte Strafverfolgung, Köln 2005.

Rückert, Christian: Zwischen Online-Streife und Online-(Raster-)Fahndung – Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, ZStW 129 (2017), 302-333

Rusteberg, Benjamin: Die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz – Eine Zwischenbilanz des allgemeinen Sicherheitsrechts, KritV 2017, 24-35.

Rusteberg, Benjamin: Zivile Sicherheit in der Sicherheitsarchitektur des deutschen Bundesstaates, in: Gusy, Christoph; Kugelmann, Dieter; Würtenberger, Thomas (Hrsg.), Rechtshandbuch Zivile Sicherheit, Berlin/Heidelberg 2017, 113-136.

Rusteberg, Benjamin: Stellungnahme zu dem Thema „Föderale Sicherheitsarchitektur" zur Vorbereitung der öffentlichen Anhörung des 1. Untersuchungsausschusses des Deutschen Bundestages der 19. Wahlperiode am 17. Mai 2018, Ausschussdrucksache 19(25)239 (zitiert: *Rusteberg*, Föderale Sicherheitsarchitektur).

Rusteberg, Benjamin: Wissensgenerierung in der personenbezogenen Prävention, Zwischen kriminalistischer Erfahrung und erkenntnistheoretischer Rationalität, in: Münkler, Laura (Hrsg.), Dimensionen des Wissens im Recht, Tübingen 2019, 233-264.

Rusteberg, Benjamin: Auf der Suche nach dem verlorenen Normalzustand, in: Brings-Wiesen, Tobias; Ferreau, Frederik (Hrsg.), 40 Jahre "Deutscher Herbst", Neue Überlegungen zu Sicherheit und Recht, Baden-Baden 2019, 191-206.

Sachs, Michael: Grundgesetz, Kommentar, 9. Aufl., München 2021.

Sack, Fritz: Selektion und Kriminalität, Kritische Justiz 1971, 384-400.

Samour, Nahed: Politisches Freund-Feind-Denken im Zeitalter des Terrorismus, in: Kulick, Andreas; Goldhammer, Michael (Hrsg.), Der Terrorist als Feind?, Tübingen 2020, 49-66.

Satzger, Helmut; *Schluckebier*, Wilhelm; *Widmaier*, Gunter: StPO, 5. Aufl., Köln 2023 (zitiert: *Bearbeiter*, in: SSW-StPO).

Saurer, Johannes: Die Ausweitung sicherheitsrechtlicher Regelungsansprüche im Kontext der Terrorismusbekämpfung, NVwZ 2005, 275-282.

Schaefer, Hans Christoph: Die Panne – Zum Nebeneinander polizeilicher und justizieller Informationssysteme, NJW 1998, 3178.

Schaefer, Hans Christoph: Zur Entwicklung des Verhältnisses Staatsanwaltschaft-Polizei, in: Ebert, Udo; Rieß, Peter; Roxin, Claus; Wahle, Eberhard (Hrsg.), Festschrift für Ernst-Walter Hanack zum 70. Geburtstag am 30. August 1999, Berlin 1999, 191-205 (zitiert: *Schaefer*, in: FS Hanack).

Schantz, Peter; *Wolff*, Heinrich Amadeus: Das neue Datenschutzrecht, Datenschutz-Grundverodnung und Bundesdatenschutzgesetz in der Praxis, München 2017.

Schenke, Ralf P.: Konstitutionalisierung: Vorbild für die Europäisierung des Sicherheitsrechts?, in: Heckmann, Dirk; Schenke, Ralf P.; Sydow, Gernot (Hrsg.), Verfassungsstaatlichkeit im Wandel, Festschrift für Thomas Würtenberger zum 70. Geburtstag, Berlin 2013, 1079-1100 (zitiert: *R. Schenke*, in: FS Würtenberger).

Schenke, Wolf-Rüdiger: Kompetenz des Landesgesetzgebers zur Regelung polizeilicher Befugnisse auf dem Gebiet der Strafverfolgung?, JR 1970, 48-52.

Schenke, Wolf-Rüdiger: Probleme der Übermittlung und Verwendung strafprozessual erhobener Daten für präventivpolizeiliche Zwecke, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Rieß, Peter; Zöller, Mark Alexander (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg 2003, 225-245 (zitiert: *Schenke*, in: FG Hilger).

Schenke, Wolf-Rüdiger; *Graulich*, Kurt; *Ruthig*, Josef: Sicherheitsrecht des Bundes, 2. Auflage, München 2019.

Scherr, Albert: Soziologische Diskriminierungsforschung, in: Scherr, Albert; El-Mafaalani, Aladin; Yüksel, Gökçen (Hrsg.), Handbuch Diskriminierung, Wiesbaden 2017, 39-58.

Schily, Ottto: Eröffnung und Festvortrag, Netzwerke des Terrors – Netzwerke gegen den Terror, in: Bundeskriminalamt, Netzwerke des Terrors – Netzwerke gegen den Terror, BKA-Herbsttagung 2004, München 2005, 5-14 (zitiert: *Schily*, in: BKA, Netzwerke).

Schlink, Bernhard: Die Amtshilfe, Ein Beitrag zu einer Lehre von der Gewaltenteilung in der Verwaltung, Berlin 1982.

Schmidt, Magdalena: Der Grundsatz der Verfügbarkeit, Ziel, Rechtsstand und Perspektiven des strafrechtlichen Informationsaustauschs in der Europäischen Union, Wiesbaden 2018.

Schneider, Jens-Peter: Informationssysteme als Bausteine des Europäischen Verwaltungsverbunds, NVwZ 2012, 65-70.

Schneider, Stefan: Länderübergreifendes staatsanwaltschaftliches Verfahrensregister – zugleich ein Instrument zur Bekämpfung der Massenkriminalität?, NJW 1996, 302-304.

Schoch, Friedrich: Zweiter Beratungsgegenstand: Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Osnabrück vom 1. bis 4. Oktober 1997, Berlin 1998, 158-215.

Schoch, Friedrich: Abschied vom Polizeirecht des liberalen Rechtsstaats? -- Vom Kreuzberg-Urteil des Preussischen Oberverwaltungsgerichts zu den Terrorismusbekämpfungsgesetzen unserer Tage, Der Staat 43 (2004), 347-369.

Scholz, Rupert; *Pitschas*, Rainer: Informationelle Selbstbestimmung und staatliche Informationsverwaltung, Berlin 1984.

Schöndorf-Haubold, Bettina: Netzwerke in der deutschen und europäischen Sicherheitsarchitektur, in: Boysen, Sigrid; Bühring, Ferry; Franzius, Claudio; Herbst, Tobias; Kötter, Matthias; Kreutz, Anita; von Lewinski, Kai; Meinel, Florian; Nolte, Jakob; Schönrock, Sabrina (Hrsg.): Netzwerke, 47. Assistententagung Öffentliches Recht, Baden-Baden 2007, 149-171 (zitiert: *Schöndorf-Haubold*, in: 47. ATÖR).

Schöndorf-Haubold, Bettina: Europäisches Sicherheitsverwaltungsrecht, Baden-Baden 2010.

Schoreit, Armin: Verwaltungsstreit um Kriminalakten: Eine zweifelhafte Entscheidung zur präventivpolizeilichen Verbrechensbekämpfung, NJW 1985, 169-172.

Schoreit, Armin: Weiterer Ausbau der zentralistischen polizeilichen EDV-Systeme zum Nachteil der Justiz, DRiZ 1986, 54-56.

Schoreit, Armin: Keine Rechtsgrundlagen der zentralen Datenverarbeitung des Bundeskriminalamts, Eine ausweglose Situation, CR 1986, 224-231.

Schoreit, Armin: Polizeiliche Kriminalakten als Grundlagen der Informationsverarbeitung, KritV 1988, 157-177.

Schramm, Horst: Zielvorstellungen des Bundeskriminalamtes zur Einführung der Datenverarbeitung, in: Bundeskriminalamt (Hrsg.), Datenverarbeitung, Arbeitstagung des Bundeskriminalamtes Wiesbaden vom 13. März bis 17. März 1972, Wiesbaden 1972, 13-24 (zitiert: *Schramm*, in: BKA, Datenverarbeitung).

Schreiber, Manfred: Elektronische Datenverarbeitung – wohin?, Die Polizei 1967, 71-72.

Schreiber, Wolfgang: Das Bundeskriminalamtgesetz vom 7. 7. 1997 – ein "überfälliges" Gesetz, NJW 1997, 2137-2145.

Schröder, Christian: Stigmatisierung in Polizeidatenbanken durch „personengebundene Hinweise", in: Müller-Heidelberg, Till; Steven, Elke; Pelzer, Marei; Heiming, Martin; Fechner, Heiner; Gössner, Rolf; Niehaus, Holger; Stößel, Martin (Hrsg.), Grundrechte-Report 2015, Zur Lage der Bürger- und Menschenrechte in Deutschland, Frankfurt am Main 2015, 38-42.

Schubert, Werner: Staatsanwaltschaftsrecht (1934-1982), Quellen zu den Reformprojekten (Organisation – Innerer Dienstbetrieb – Ermittlungsverfahren – Verhältnis der Staatsanwaltschaft zur Polizei) und zur Anordnung über Organisation und Dienstbetrieb der Staatsanwaltschaft (OrgStA), Frankfurt am Main 2013.

Schuhr, Jan C.: Recht, Technik, Roboter, Rechtstheorie 2015, 225-261.

Schulze-Fielitz, Helmut: Nach dem 11. September, An den Leistungsgrenzen eines verfassungsstaatlichen Polizeirechts?, in: Horn, Hans-Detlef (Hrsg.), Recht im Pluralismus, Festschrift für Walter Schmitt Glaeser zum 70. Geburtstag, Berlin 2003, S. 407-434 (zitiert: *Schulze-Fielitz*, in: FS Schmitt Glaeser).

Schünemann, Bernd: Polizei und Staatsanwaltschaft – Teil 1, Die deutsche Polizei als Gehilfe der Staatsanwaltschaft: Struktur, Organisation und Tätigkeiten, Kriminalistik 1999, 74-79.

Schupp, Günther: Bringt uns der Musterentwurf eines einheitlichen Polizeigesetzes (ME) dem Polizeistaat näher?, RiA 1979, 66-70.

Schwabenbauer, Thomas; *Kling*, Michael: Gerichtliche Kontrolle administrativer Prognoseentscheidungen am Merkmal der „Zuverlässigkeit", VerwArch 2010, 231-256

Schwabenbauer, Thomas: Heimliche Grundrechtseingriffe, Tübingen 2013.

Schwan, Eggert: Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, VerwArch 66 (1975), 120-150.

Schwan, Eggert: Auf dem Weg zum Überwachungsstaat? Plädoyer für eine rechtsstaatliche Datenverarbeitung der Polizei, in: Hohmann, Harald (Hrsg.), Freiheitssicherung durch Datenschutz, Frankfurt am Main 1987, 276-312.

Schweckendieck, Helmut: Dateien zur „vorbeugenden Verbrechensbekämpfung" im Lichte der Rechtsprechung zu § 81b Alt. 2 StPO, ZRP 1989, 125-127.

Schweinoch, Joachim: Das INPOL-Fortentwicklungskonzept 1981, Synthese zwischen Sicherheitspolitik und Datenschutz, Die Polizei 1984, 292-294.

Schweppe, Reinhard: FBI und BKA, Ein Vergleich von Organisation und Kompetenzen, Stuttgart 1974.

Schwinghammer, Torsten: BKA-Präsident Horst Herold, KrimJ 1980, 241-255.

Seebode, Manfred: Strafverfolgung nach Polizeirecht? Kritische Bemerkungen zum Musterentwurf einheitlicher Polizeigesetze, MDR 1976, 537-540.

Sehr, Peter: INPOL-neu: System mit Merkmalen eines extremen Wandels, Zum Entwicklungsstand des Informationssystems der Polizei, Kriminalistik 1999, 532-536.

Seidel, Ulrich: Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, NJW 1970, 1581-1583.

Sieber, Ulrich: Informationsrecht und Recht der Informationstechnik – Die Konstituierung eines Rechtsgebietes in Gegenstand, Grundfragen und Zielen, NJW 1989, 2569-2580.

Siebrasse, Pamela: Strafregistrierung und Grundgesetz, Frankfurt am Main 2002.

Siebrecht, Michael: Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozeßrecht, JZ 1996, 711-714.

Siemen, Birte: Datenschutz als europäisches Grundrecht, Berlin 2006.

Sikora, Judith: Die schwierige Lage des Rechts im Raum der Freiheit, der Sicherheit und des Rechts, in: Brings-Wiesen, Tobias; Ferreau, Frederik (Hrsg.), 40 Jahre "Deutscher Herbst", Neue Überlegungen zu Sicherheit und Recht, Baden-Baden 2019, 59-72.

Simitis, Spiros: Informationskrise des Rechts und Datenverarbeitung, Karlsruhe 1970.

Simitis, Spiros; *Hornung*, Gerrit; *Spiecker gen. Döhmann*, Indra: Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019.

Simon, Jürgen; *Taeger*, Jürgen: Grenzen kriminalpolizeilicher Rasterfahndung, JZ 1982, 140-145.

Singelnstein, Tobias: Strafprozessuale Verwendungsregelungen zwischen Zweckbindungsgrundsatz und Verwertungsverboten: Voraussetzungen der Verwertung von Zufallsfunden und sonstiger zweckentfremdender Nutzung personenbezogener Daten im Strafverfahren seit dem 1. Januar 2008, ZStW 120 (2008), 854-893.

Singelnstein, Tobias: Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, 593-606.

Singelnstein, Tobias: Logik der Prävention, Eine kriminologische Perspektive auf das Strafrecht und andere Formen sozialer Kontrolle, in: Brunhöber, Beatrice (Hrsg.), Strafrecht im Präventionsstaat, Stuttgart 2014, 41-57.

Singelnstein, Tobias: Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NStZ 2018, 1-9.

Singelnstein, Tobias: Big Data und Strafverfolgung, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data – Regulative Herausforderungen, Baden-Baden 2018, 175-181 (zitiert: *Singelnstein*, in: Hoffmann-Riem, Big Data).

Singelnstein, Tobias: Digitalisierung, Big Data und das Strafverfahren, in: Stein, Ulrich; Greco, Luís; Jäger, Christian; Wolter, Jürgen (Hrsg.), Systematik in Strafrechtswissenschaft und Gesetzgebung, Festschrift für Klaus Rogall zum 70. Geburtstag, Berlin 2018, 725-738 (zitiert: *Singelnstein*, in: FS Rogall).

Singelnstein, Tobias; *Putzer*, Max: Rechtliche Grenzen strafprozessualer Ermittlungsmaßnahmen – Aktuelle Bestandsaufnahme und neue Herausforderungen, GA 2015, 564-578.

Singelnstein, Tobias: Folgen des neuen Datenschutzrechts für die Praxis des Strafverfahrens und die Beweisverbotslehre, NStZ 2020, 639-644.

Singelnstein, Tobias; *Stolle*, Peer: Die Sicherheitsgesellschaft, Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., Wiesbaden 2012.

Soiné, Michael: Datenverarbeitung für Zwecke künftiger Strafverfahren, CR 1998, 257-264.

Soiné, Michael: Strafprozessordnung, Kommentar für Polizeibeamte im Ermittlungsdienst, 142. EL, Heidelberg 2023.

Son, Jae-Young: Heimliche polizeiliche Eingriffe in das informationelle Selbstbestimmungsrecht, Berlin 2006.

Spatscheck, Rainer; *Dovas*, Maria-Urania; *Feldle*, Jochen: Die Löschung elektronischer Akten und Aktenkopien im Strafverfahren NStZ 2022, 705-711.

Spiecker gen. Döhmann, Indra: Teil-Verfassungsordnung Datenschutz, in: Vesting, Thomas; Korioth, Stefan (Hrsg.), Der Eigenwert des Verfassungsrechts, Tübingen 2011, 263-287.

Spiecker gen. Döhmann, Indra: Rechtliche Begleitung der Technikentwicklung im Bereich moderner Infrastrukturen und Informationstechnologien, in: Hill, Hermann; Schliesky, Utz (Hrsg.), Die Vermessung des virtuellen Raums, E-Volution des Rechts- und Verwaltungssystems III, Baden-Baden 2012, 137-161.

Spiecker gen. Döhmann, Indra: Die technischen Grenzen des Rechts: Recht durch Technik und Technik durch Recht, in: Funke, Andreas; Lachmayer, Konrad (Hrsg.), Formate der Rechtswissenschaft, Weilerswist 2017, 181-207.

Spiecker gen. Döhmann, Indra; *Kehr*, Thomas: Die Entscheidung des Bundesverwaltungsgerichts vom 09.06.2010 - Datei Gewalttäter Sport, DVBl. 2011, 930-936.

Stegmaier, Peter; *Feltes*, Thomas: ‚Vernetzung' als neuer Effektivitätsmythos für die ‚innere Sicherheit', APuZ 12/2007, 18-25.

Steinat, Björn: Die Speicherung personenbezogener Daten gewalttätiger Fußballfans, zur Datei „Gewalttäter Sport", Hamburg 2012.

Stephan, Ulrich: Zur Verfassungsmäßigkeit der präventiven Telefonüberwachung gem. § 33 Abs. 1 Nr. 2 und Nr. 3 Nds.SOG, Anmerkungen zum Urteil des Bundesverfassungsgerichts vom 27.7.2005 – Az. 1 BvR 668/04 –, VBlBW 2005, 410-413.

Von Stetten, Annette: Die elektronische Akte in Strafsachen, Segen oder Fluch?, ZRP 2015, 138-141.

Stubenrauch, Julia: Gemeinsame Verbunddateien von Polizei und Nachrichtendiensten, Eine verfassungsrechtliche Untersuchung am Beispiel der Antiterrordatei, Baden-Baden 2009.

Stuckenberg, Carl-Friedrich: Untersuchungen zur Unschuldsvermutung, Berlin 1998.

Stuckenberg, Carl-Friedrich: Die normative Aussage der Unschuldsvermutung, ZStW 111 (1999), 422-460.

Stuckenberg, Carl-Friedrich: Speicherung personenbezogener Daten zur ‚vorbeugenden Straftatenbekämpfung' trotz Freispruchs?, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Rieß, Peter; Zöller, Mark Alexander (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg 2003, 25-55 (zitiert: *Stuckenberg*, in: FG Hilger).

Stümper, Alfred: Prävention und Repression als überholte Unterscheidung?, Kriminalistik 1975, 49-53.

Stümper, Alfred: Die Wandlung der Polizei in Begriff und Aufgaben, Kriminalistik 1980, 242-245.

Sydow, Fritz: Verbrechensbekämpfung nach neuem Recht, Kritik am Musterentwurf eines einheitlichen Polizeigesetzes, ZRP 1977, 119-125.

Sydow, Gernot: Informationsgesetzbuch häppchenweise, NVwZ 2008, 481-485.

Sydow, Gernot; *Marsch*, Nikolaus: DS-GVO BDSG, Handkommentar, 3. Aufl., Baden-Baden 2022.

Systematischer Kommentar zur Strafprozessordung: herausgegeben von Wolter, Jürgen, 4. Aufl. Köln 2011 ff. (zitiert: *Bearbeiter*, in: SK-StPO).

Systematischer Kommentar zur Strafprozessordung: herausgegeben von Wolter, Jürgen, 5. Aufl. Köln 2016 ff. (zitiert: *Bearbeiter*, in: SK-StPO).

Szuba, Dorothee: Vorratsdatenspeicherung, Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, Baden-Baden 2011.

Tegtmeyer, Henning: Erwiderung auf Schoreit „Gefahrenabwehr durch Datensammlung?", KritV 1989, 213-225.

Thiel, Markus: Auf dem Weg zu einem neuen „Musterpolizeigesetz" – „Blaupause" für die sicherheitsrechtliche Harmonisierung oder aussichtslose Makulatur?, Die Verwaltung 2020, 1-19.

Thiel, Markus: Modernes Polizeirecht, (Vor-)Überlegungen zum normativen Umgang mit sicherheitsrelevanten „Megatrends" und modifizierten Policing-Ansätzen, GSZ 2021, 97-103.

Tischbirek, Alexander; *Wihl*, Tim: Verfassungswidrigkeit des „Racial Profiling", Zugleich ein Beitrag zur Systematik des Art. 3 GG, JZ 2013, 219-224.

Tischbirek, Alexander: Wissen als Diskriminierungsfrage, Kognitive Herausforderungen des Antidiskriminierungsrechts zwischen implizitem Wissen und selbstlernenden Algorithmen, in: Münkler, Laura (Hrsg.), Dimensionen des Wissens im Recht, Tübingen 2019, 67-86.

Tolmein, Oliver: Europol, StV 1999, 108-116.

Töpfer, Eric: Prüm und die Vernetzung nationaler DNA-Datenbanken in Europa, Zur Unberechenbarkeit großtechnischer Systeme der Inneren Sicherheit, vorgänge 2019, 135-146.

Trute, Hans-Heinrich: Die Erosion des klassischen Polizeirechts durch die polizeiliche Informationsvorsorge, in: Erbguth, Wilfried; Müller, Friedrich; Neumann, Volker (Hrsg.), Rechtstheorie und Rechtsdogmatik im Austausch, Gedächtnisschrift für Bernd Jeand'Heur, Berlin 1999, 403-428 (zitiert: *Trute*, in: GS Jeand'Heur).

Trute, Hans-Heinrich: Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, Die Verwaltung 2009, 85-104.

Trute, Hans-Heinrich; *Kuhlmann*, Simone: Predictive Policing als Formen polizeilicher Wissensgenerierung, GSZ 2021, 103-111.

Tzanou, Maria: Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right, International Data Privacy Law 2013, 88-99.

Uhlig, Sigmar: Die Polizei - Herrin des Strafverfahrens? Aktuelle Probleme im Verhältnis der Polizei als Mitwirkende bei der Strafverfolgung zur Strafjustiz, DRiZ 1986, 247-251.

Ule, Carl Hermann: Notwendigkeit einheitlicher Polizeigesetze?, in: Merten, Detlef (Hrsg.), Aktuelle Probleme des Polizeirechts (unter Berücksichtigung des Musterentwurfes eines einheitlichen Polizeigesetzes des Bundes und der Länder), Vorträge und Diskussionsbeiträge des 5. Sonderseminars 1976 der Hochschule für Verwaltungswissenschaften Speyer, Berlin 1977, 27-46.

Unruh, Peter: Zur Dogmatik der grundrechtlichen Schutzpflichten, Berlin 1996.

Vesting, Thomas: Zur Entwicklung einer "Informationsordnung", in: Badura, Peter; Dreier, Horst (Hrsg.), Festschrift 50 Jahre Bundesverfassungsgericht, Zweiter Band, Tübingen 2001, 219-240 (zitiert: *Vesting*, in: FS BVerfG).

Vogelgesang, Klaus: Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987.

Volk, Elisabeth: Gesetz zur Änderung der Strafprozessordnung (DNA-Identitätsfeststellungsgesetz) – Anspruch und Wirklichkeit, NStZ 1999, 165-170.

Volkmann, Uwe: Sicherheit und Risiko als Probleme des Rechtsstaats, JZ 2004, 696-703.

Volkmann, Uwe: Polizeirecht als Sozialtechnologie, NVwZ 2009, 216-222.

Voßkuhle, Andreas: Das Verhältnis von Freiheit und Sicherheit – Hat der 11. September 2001 das deutsche Verfassungsrecht verändert?, in: Heckmann, Dirk; Schenke, Ralf P.; Sydow, Gernot (Hrsg.), Verfassungsstaatlichkeit im Wandel, Festschrift für Thomas Würtenberger zum 70. Geburtstag, Berlin 2013, 1101-1120 (zitiert: *Voßkuhle*, in: FS Würtenberger).

Wacke, Gerhard: Das Frankfurter Modell eines Polizeigesetzes, Zugleich Bericht über den Polizeigesetz-Entwurf für Nordrhein-Westfalen, DÖV 1953, 388-395.

Waechter, Kay: Die aktuelle Situation des Polizeirechts, JZ 2002, 854-862.

Walter, Bernd: Die Hoffnung stirbt zuletzt – das mühsame Ringen um ein neues Musterpolizeigesetz, Kriminalistik 2019, 243-247.

Wegener, Bernhard W.: Verfassung in ausgewählten Teilrechtsordnungen: Konstitutionalisierung und Gegenbewegungen im Sicherheitsrecht, in: Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer, Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Speyer vom 7. bis zum 10. Oktober 2015, Berlin 2016, 293-331

Weichert, Thilo: Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463-1469.

Wellbrock, Rita: Der Hessische Regelungsentwurf für die polizeiliche Datenverarbeitung, CR 1986, 149-157.

Werckmeister, Georg: Informationsrecht – Grundlagen und Anwendung im Überblick, DVR 1978, 97-114.

Werner, Wolfram: Der Parlamentarische Rat 1948-1949, Akten und Protokolle, Band 3: Ausschuß für Zuständigkeitsabgrenzung, Boppard am Rhein 1986.

Weßlau, Edda: Vorfeldermittlungen, Probleme der Legalisierung „vorbeugender Verbrechensbekämpfung" aus strafprozeßrechtlicher Sicht, Berlin 1989.

Weßlau, Edda: Datenübermittlungen und Datenverarbeitung in den Informationssystemen von Europol, in: Wolter, Jürgen; Schenke, Wolf-Rüdiger; Hilger, Hans; Ruthig, Josef; Zöller, Mark A. (Hrsg.), Alternativentwurf Europol und europäischer Datenschutz, Heidelberg 2008, 318-345 (zitiert: *Weßlau*, in: AE Europol).

Westphal, Dietrich: Leitplanken für die Vorratsdatenspeicherung – Abrücken von „Solange", Das Urteil des BVerfG vom 2. 3. 2010, EuZW 2010, 494-499.

Weyer, Johannes: Techniksoziologie, Genese, Gestaltung und Steuerung sozio-technischer Systeme, Weinheim und München 2008.

Wiesel, Georg: Befriedigend, aber manches fehlt noch, Ausbaustand des Informationssystems INPOL: Noch keine Falldatei für Straftaten von bundesweiter Bedeutung, Kriminalistik 1986, 587-591.

Wiesel, Georg; *Gerster*, Helmut: Das Informationssystem der Polizei INPOL, Konzept und Sachstand, Wiesbaden 1978.

Willke, Helmut: Systemisches Wissensmanagement, Stuttgart 1998.

Winner, Langdon: Do Artifacts Have Politics?, Daedalus 109 (1/1980), 121-136.

Wischmeyer, Thomas: Regulierung intelligenter Systeme, AöR 143 (2018), 1-66.

Wischmeyer, Thomas: Predictive Policing, Nebenfolgen der Automatisierung von Prognosen im Sicherheitsrecht, in: Kulick, Andreas; Goldhammer, Michael (Hrsg.), Der Terrorist als Feind?, Tübingen 2020, 193-213.

Wojtech, Michael: Wann kommt die elektronische Akte im Strafverfahren?, NJW-Spezial 2012, 632-633.

Wolf, Georg: Verbrechensbekämpfung und Rollenverteilung auf die damit befaßten Institutionen, Kriminalistik 1975, 389-394.

Wolf, Rainer: Zur Antiquiertheit des Rechts in der Risikogesellschaft, Leviathan 15 (1987), 357-391.

Wolff, Heinrich Amadeus: Die Grenzverschiebung von polizeilicher und nachrichtendienstlicher Sicherheitsgewährleistung, Das Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt, DÖV 2009, 597-606.

Wolff, Heinrich Amadeus: Der EU-Richtlinienentwurf zum Datenschutz in Polizei und Justiz – Gehalt und Auswirkungen auf das Strafprozess- und Polizeirecht, in: Kugelmann, Dieter; Rackow, Peter (Hrsg.), Prävention und Repression im Raum der Freiheit, der Sicherheit und des Rechts, Belastbarkeit der Konzepte von Strafe und Gefahrenabwehr zwischen Staat und EU, Baden-Baden 2014, 61-93.

Wolff, Heinrich Amadeus: Verfassung in ausgewählten Teilrechtsordnungen: Konstitutionalisierung und Gegenbewegungen – Sicherheitsrecht, DVBl. 2015, 1076-1084.

Wolter, Jürgen: Heimliche und automatisierte Informationseingriffe wider Datengrundrechtschutz, Gesamtanpassung vor Gesamtreform von Strafprozeß- und Polizeirecht, Teil 1, GA 1988, 49-90.

Wolter, Jürgen: Freiheitlicher Strafprozeß, vorbeugende Straftatenbekämpfung und Verfassungsschutz, zugleich Besprechung des Entwurfs eines StVÄG 1988, StV 1989, 358-371.

Wolter, Jürgen: Formen des Vorermittlungsverfahrens und Reform des Ermittlungsverfahrens, Zugleich: Grundlagen der Alternativentwürfe AE-ZVR und AE-EV, in: Kreuzer, Arthur; Jäger, Herbert; Otto, Harro; Quensel, Stephan; Rolinski, Klaus (Hrsg.), Fühlende und denkende Kriminalwissenschaften, Ehrengabe für Anne-Eva Brauneck, Mönchengladbach 1999, 501-532 (zitiert: *Wolter*, in: EG Brauneck).

Wolter, Jürgen: Zur Verbindung von Strafprozessrecht und Polizeirecht, in: Kühne, Hans-Heiner; Jung, Heike; Kreuzer, Arthur; Wolter, Jürgen (Hrsg.), Festschrift für Klaus Rolinski, Baden-Baden 2002, 273-285 (zitiert: *Wolter*, in: FS Rolinski).

Würtenberger, Thomas: Modernisierung des Polizeirechts als Paradigma für die Entwicklung des Rechtsstaates, in: Heckmann, Dirk (Hrsg.), Modernisierung von Justiz und Verwaltung, Gedenkschrift für Ferdinand O. Kopp, Stuttgart 2007, 428-442 (zitiert: *Würtenberger*, in: GS Kopp).

Würtenberger, Thomas: Entwicklungslinien eines transnationalen informationellen Polizeirechts, in: Manssen, Gerrit; Jachmann, Monika; Gröpl, Christoph (Hrsg.), Nach geltendem Verfassungsrecht, Festschrift für Udo Steiner zum 70. Geburtstag, Stuttgart 2009, 948-965 (zitiert: *Würtenberger*, in: FS Steiner).

Würtenberger, Thomas; *Tanneberger*, Steffen: Sicherheitsarchitektur als interdisziplinäres Forschungsfeld, in: Riescher, Gisela (Hrsg.), Sicherheit und Freiheit statt Terror und Angst, Perspektiven einer demokratischen Sicherheit, Baden-Baden 2010, 97-125.

Zedner, Lucia: Pre-crime and post-criminology?, Theoretical Criminology 11 (2007), 261-281.

Ziercke, Jörg: Polizeiföderalismus oder Bundeskriminalpolizei – Welche Organisationsstruktur verlangt die künftige polizeiliche Arbeit?, in: Pitschas, Rainer; Stolzlechner, Harald (Hrsg.), Auf dem Weg in einen „neuen Rechtsstaat", Zur künftigen Architektur der inneren Sicherheit in Deutschland und Österreich, Berlin 2004, 63-77.

Ziercke, Jörg: Internationale Erscheinungsformen von Kriminalität und Gewalt, Internationale Kooperationsformen und die Rolle des BKA, Kriminalistik 2005, 700-707.

Zirpins, Walter: Die Entwicklung der polizeilichen Verbrechensbekämpfung in Deutschland, Hamburg 1955.

Zöller, Mark A.: Vorsorge für die künftige Strafverfolgung – Zugleich ein Beitrag zum Entwurf eines Strafverfahrensänderungsgesetzes 1996, RDV 1997, 163-171.

Zöller, Mark A.: Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz, Heidelberg 2002.

Zöller, Mark A.: Der Rechtsrahmen der Nachrichtendienste bei der "Bekämpfung" des internationalen Terrorismus, JZ 2007, 763-771.

Zöller, Mark A.: Der Austausch von Strafverfolgungsdaten zwischen den Mitgliedstaaten der Europäischen Union, ZIS 2011, 64-69.

Zöller, Mark A.: Der Beurteilungsspielraum des Gesetzgebers im Recht der Inneren Sicherheit, in: Herzog, Felix; Schlothauer, Reinhold; Wohlers, Wolfgang; Wolter, Jürgen (Hrsg.), Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächtnisschrift für Edda Weßlau, Berlin 2016, 551-566 (zitiert: *Zöller*, in: GS Weßlau).

Zöller, Mark A.: Die zweckändernde Nutzung von personenbezogenen Daten im Strafverfahren – Gegenwart und Zukunft von § 161 StPO, StV 2019, 419-427.

Zöllner, Wolfgang: Informationsordnung und Recht, Berlin 1990.

digital | recht

Staat und digitale Gesellschaft

Sebastian Golla

Die kriminalbehördliche Informationsordnung

Polizei und Staatsanwaltschaften speichern heute in einem kaum überschaubaren Umfang Daten. Diese Arbeit untersucht die kriminalbehördliche Informationsordnung aus juristischer und kriminologischer Sicht. Sie betrachtet die praktischen Anforderungen an Dateien und Informationssysteme, die hierfür geltenden rechtlichen Rahmenbedingungen sowie die Perspektiven dieses Feldes, das für die Sicherheitsproduktion immer bedeutsamer wird, aber auch Risiken für Bürgerinnen und Bürger mit sich bringt.